DUMPSBOSS.

# Certified Secure Software Lifecycle Professional

## ISC2 CSSLP

### Version Demo

**Total Demo Questions: 15**

**Total Premium Questions: 349**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

## QUESTION NO: 1

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

## ANSWER: D

**Explanation:**

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 NO: 2

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

**A.** Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

**B.** Single Loss Expectancy (SLE)/ Exposure Factor (EF)

**C.** Asset Value X Exposure Factor (EF)

**D.** Exposure Factor (EF)/Single Loss Expectancy (SLE)

## ANSWER: A

**Explanation:**

The Annualized Loss Expectancy (ALE) that occurs due to a threat can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO). Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO) Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Single Loss Expectancy (SLE) is the value

in dollars that is assigned to a single event. SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate Single Loss Expectancy (SLE).

## QUESTION NO: 3

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards? Each correct answer represents a complete solution. Choose all that apply.

**A.** AU audit and accountability

**B.** Human resources security

**C.** Organization of information security

**D.** Risk assessment and treatment

## ANSWER: A B C

**Explanation:**

Following are the various international information security standards:

**Answer: Risk assessment and treatment: Analysis of the organization's information security risks Security policy: Management direction Organization of information security: Governance of information security Asset management: Inventory and classification of information assets Human resources security: Security aspects for employees joining, moving, and leaving an organization Physical and environmental security: Protection of the computer facilities Communications and operations management: Management of technical security controls in systems and networks Access control: Restriction of access rights to networks, systems, applications, functions, and data Information systems acquisition, development and maintenance: Building security into applications Information security incident management: Anticipating and responding appropriately to information security breaches Business continuity management: Protecting, maintaining, and recovering business-critical processes and systems Compliance: Ensuring conformance with information security policies, standards, laws, and regulations A is incorrect. AU audit and accountability is a U.S. Federal Government information security standard.**

## QUESTION NO: 4

You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAP/NIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system?

**A.** Validation

**B.** Definition

**C.** Verification

**D.** Post Accreditation

**ANSWER: B**

**Explanation:**

The definition phase of the DITSCAP/NIACAP model takes place at the beginning of the project, or at the initial C&A effort of a legacy system. C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows: 1.Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A). 2.Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing. 3.Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows the requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process. 4.Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

**QUESTION NO: 5**

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

**A.** Performing data restoration from the backups when necessary

**B.** Running regular backups and routinely testing the validity of the backup data

**C.** Determining what level of classification the information requires

**D.** Controlling access, adding and removing privileges for individual users

**ANSWER: C D**

**Explanation:**

**Answer: The owner of information delegates the responsibility of protecting that information to a custodian. The following are the responsibilities of a custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users C is incorrect. Determining what level of classification the information requires is the responsibility of the owner.**

**QUESTION NO: 6 - (SIMULATION)**

SIMULATION

Fill in the blank with the appropriate security mechanism. is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.

**ANSWER: Exception handling**

**Explanation:**

Exception handling is a computer hardware mechanism or programming language construct that handles the occurrence of events. These events occur during the software execution process and interrupt the instruction flow. Exception handling performs the specific activities for managing the exceptional events.

## QUESTION NO: 7

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

**A.** VI Vulnerability and Incident Management

**B.** Information systems acquisition, development, and maintenance

**C.** DC Security Design & Configuration

**D.** EC Enclave and Computing Environment

**ANSWER: A B C D**

**Explanation:**

**Answer: According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Following are the various U.S. Department of Defense information security standards: DC Security Design & Configuration IA Identification and Authentication EC Enclave and Computing Environment EB Enclave Boundary Defense PE Physical and Environmental PR Personnel CO Continuity VI Vulnerability and Incident Management B is incorrect. Business continuity management is an International information security standard.**

## QUESTION NO: 8

You are responsible for network and information security at a large hospital. It is a significant concern that any change to any patient record can be easily traced back to the person who made that change. What is this called?

**A.** Availability

**B.** Confidentiality

**C.** Non repudiation

**D.** Data Protection

**ANSWER: C**

**Explanation:**

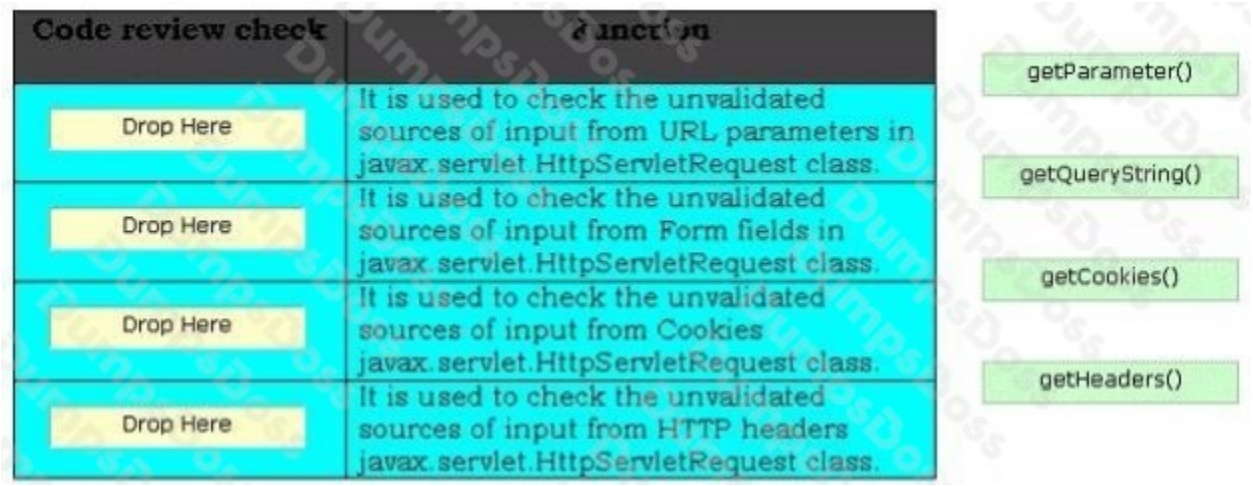
Non repudiation refers to mechanisms that prevent a party from falsely denying involvement in some data transaction.

## QUESTION NO: 9 - (DRAG DROP)

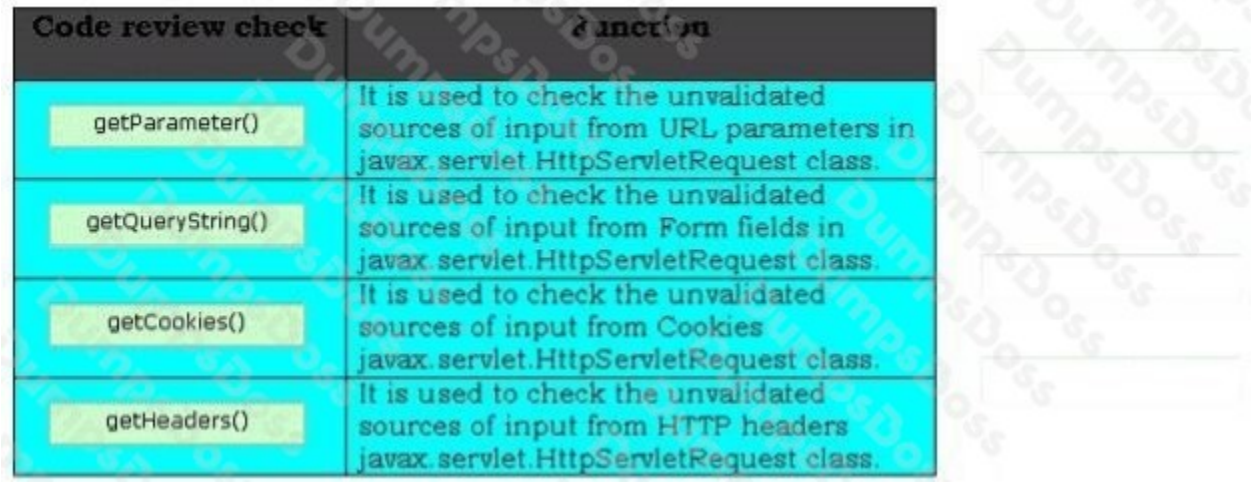
DRAG DROP

Security code review identifies the unvalidated input calls made by an attacker and avoids those calls to be processed by the server. It performs various review checks on the stained calls of servlet for identifying unvalidated input from the attacker. Choose the appropriate review checks and drop them in front of their respective functions.

**Select and Place:**




**ANSWER:**




**Explanation:**

The various security code review checks performed on the stained calls of servlet are as follows: getParameter(): It is used to check the unvalidated sources of input from URL parameters in javax.servlet.HttpServletRequest class.

getQueryString(): It is used to check the unvalidated sources of input from Form fields in javax.servlet.HttpServletRequest class. getCookies(): It is used to check the unvalidated sources of input from Cookies javax.servlet.HttpServletRequest class. getHeaders(): It is used to check the unvalidated sources of input from HTTP headers javax.servlet.HttpServletRequest class.

## QUESTION NO: 10

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

**A.** Level 2

**B.** Level 3

**C.** Level 5

**D.** Level 1

**E.** Level 4

## ANSWER: B

**Explanation:**

The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

## QUESTION NO: 11

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

**A.** DoD 8910.1

**B.** DoD 7950.1-M

**C.** DoDD 8000.1

**D.** DoD 5200.22-M

**E.** DoD 5200.1-R

## ANSWER: B

**Explanation:**

The various DoD directives are as follows:

DoD 5200.1-R: This DoD directive refers to the 'Information Security Program Regulation'. DoD 5200.22-M: This DoD directive refers the 'National Industrial Security Program Operating Manual'. DoD 7950.1-M: This DoD directive refers to the

'Defense Automation Resources Management Manual'. DoDD 8000.1: This DoD directive refers to the 'Defense Information Management (IM) Program'. DoD 8910.1: This DoD directive refers to the 'Management and Control of Information Requirements'.

## QUESTION NO: 12

An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

**A.** Service Level Agreement

**B.** Release Policy

**C.** Service Level Requirements

**D.** Underpinning Contract

## ANSWER: A B C D

**Explanation:**

You will most probably find this information in the Service Level Agreement document. Amongst other information, SLA contains information about the agreed Service Hours and maintenance slots for any particular Service. Service Level

Agreement (frequently abbreviated as SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract'. Contracts between the Service Provider and other third parties are often (incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no 'agreement' between third parties (these agreements are simply a 'contract'). Operating Level Agreements or OLA(s) however, may be used by internal groups to support SLA (s).

**Answer: B is incorrect. Release Policy is a set of rules for deploying releases into the live operational environment, defining different approaches for releases depending on their urgency and impact. C is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. D is incorrect. Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level targets in an SLA.**

## QUESTION NO: 13

Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

**A.**

**B.** Reviewing the classification assignments at regular time intervals and making changes as the business needs chang

**C.** Running regular backups and routinely testing the validity of the backup data.

**D.** Delegating the responsibility of the data protection duties to a custodian.

**E.** Determining what level of classification the information requires.

**ANSWER: A B C E**

**Explanation:**

**Answer: The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to a custodian. An information owner can be an executive or a manager of an organization. He will be responsible for the asset of information that must be protected. B is incorrect. Running regular backups and routinely testing the validity of the backup data is the responsibility of a custodian.**

## QUESTION NO: 14

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: 15

Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

**A.**

**B.** It provides for entry and storage of individual system dat

**C.** It performs vulnerability/threat analysis assessment.

**D.** It provides data needed to accurately assess IA readiness.

**E.** It identifies and generates IA requirements.

**ANSWER: A B E**

**Explanation:**

**Answer: The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. A is incorrect. It is a function performed by the ASSET system.**