[Sep 29, 2024 Fully Updated ISC Certification (CSSLP) Certification Sample Questions [Q18-Q33

[Sep 29, 2024] Fully Updated ISC Certification (CSSLP) Certification Sample Questions
Latest ISC CSSLP Real Exam Dumps PDF

Who should take the exam

if you have the following prerequisite and required skills then you should take this exam for getting Certified Secure Software Lifecycle Professional (CSSLP) certificate.

- 3 years of cumulative paid full-time SDLC professional work experience in 1 or more of the 8 domains of the CSSLP CBK- 4-year degree leading to a Baccalaureate, or regional equivalent in Computer Science, Information Technology (IT) or related fields.- Minimum of 4 years of cumulative paid full-time Software Development Lifecycle (SDLC) professional work experience in 1 or more of the 8 domains of the (ISC)2 CSSLP CBK **QUESTION 18**

Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.

* Programmers should use multiple small and simple functions rather than a single complex function.
* Software should avoid ambiguities and hidden assumptions, recursions, and GoTo statements.
* Programmers should implement high-consequence functions in minimum required lines of code and follow proper coding standards.

* Processes should have multiple entry and exit points.

Explanation/Reference:

Explanation: The various coding practices that are helpful in simplifying the code are as follows:

Programmers should implement high-consequence functions in minimum required lines of code and follow the proper coding standards. Software should implement the functions that are defined in the software specification. Software should avoid ambiguities and hidden assumptions, recursion, and GoTo statements. Programmers should use multiple small and simple functions rather than a complex function.

The processes should have only one entry point and minimum exit points. Interdependencies should be minimum so that a process module or component can be disabled when it is not needed, or replaced when it is found insecure or a better alternative is available, without disturbing the software operations.

Programmers should use object-oriented techniques to keep the code simple and small. Some of the object-oriented techniques are object inheritance, encapsulation, and polymorphism. Answer: D is incorrect. Processes should have only one entry point and the minimum number of exit points.

QUESTION 19

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

* Phase 2
* Phase 4
* Phase 3
* Phase 1

Security Test and Evaluation (ST&E) occurs in Phase 3 of the DITSCAP C&A process. Answer D is incorrect. The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation Answer A is incorrect. The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer B is incorrect. The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase

3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation

QUESTION 20

The Data and Analysis Center for Software (DACS) specifies three general principles for software assurance which work as a framework in order to categorize various secure design principles. Which of the following principles and practices does the General Principle 1 include? Each correct answer represents a complete solution. Choose two.

* Principle of separation of privileges, duties, and roles
* Assume environment data is not trustworthy
* Simplify the design
* Principle of least privilege

General Principle 1- Minimize the number of high-consequence targets includes the following principles and practices: Principle of

least privilege Principle of separation of privileges, duties, and roles Principle of separation of domains Answer B is incorrect. Assume environment data is not trustworthy principle is included in the General Principle 2. Answer C is incorrect. Simplify the design principle is included in the General Principle 3.

QUESTION 21

Which of the following is an example of penetration testing?
* Implementing NIDS on a network
* Implementing HIDS on a computer
* Simulating an actual attack on a network
* Configuring firewall to block unauthorized traffic
Explanation/Reference:

Explanation: Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/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 testing 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. AnswerA, B, and D are incorrect. Implementing NIDS and HIDS and configuring firewall to block unauthorized traffic are not examples of penetration testing.

QUESTION 22

Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?
* RTO
* RTA
* RPO
* RCO
The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance. The RTO attaches to the business process and not the resources required to support the process. Answer B is incorrect. The Recovery Time Actual (RTA) is established during an exercise, actual event, or predetermined based on recovery methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered infrastructure to the business. Answer D is incorrect. The Recovery Consistency Objective (RCO) is used in Business Continuity Planning in addition to Recovery Point Objective (RPO) and Recovery Time Objective (RTO). It applies data consistency objectives to Continuous Data Protection services. Answer C is incorrect. The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an “acceptable loss” in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster.

QUESTION 23

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?
* Copyright
* Utility model
* Trade secret
* Cookie
* Explanation:

A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information.
is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer B is incorrect. A utility model is an intellectual property right to protect inventions. Answer D is incorrect. A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. A Web server cannot access cookies created by other Web servers.

QUESTION 24

You work as a Security Manager for Tech Perfect Inc. You want to save all the data from the SQL injection attack, which can read sensitive data from the database and modify database data using some commands, such as Insert, Update, and Delete. Which of the following tasks will you perform? Each correct answer represents a complete solution. Choose three.
* Apply maximum number of database permissions.
* Use an encapsulated library for accessing databases.
* Create parameterized stored procedures.
* Create parameterized queries by using bound and typed parameters.
The methods of mitigating SQL injection attacks are as follows: 1.Create parameterized queries by using bound and typed parameters. 2.Create parameterized stored procedures. 3.Use a encapsulated library in order to access databases. 4.Minimize database permissions. Answer A is incorrect. In order to save all the data from the SQL injection attack, you should minimize database permissions.

QUESTION 25

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?
* Deployment
* Requirements Gathering
* Maintenance
* Design
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 26

Harry is the project manager of the MMQ Construction Project. In this project, Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project’s deadline. Management asked Harry to find a supplier who can fulfill the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?
* Transference
* Avoidance
* Mitigation
* Acceptance

Explanation/Reference:

Explanation: This is an example of mitigation. By changing to a more reliable supplier, Harry is reducing the probability the supplier will be late. It’s still possible that the vendor may not be able to deliver the stained glass windows, but the more reputable supplier reduces the probability of the lateness. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions.

AnswerA is incorrect. Transference is when the risk is transferred to a third party, usually for a fee. While

this question does include a contractual relationship, the risk is the lateness of the windows. Transference focuses on transferring the risk to a third party to manage the risk event. In this instance, the management of the risk is owned by a third party; the third party actually creates the risk event because of the possibility of the lateness of the windows. AnswerB is incorrect. Avoidance changes the project plan to avoid the risk. If the project manager and management changed the window-type to a standard window in the project requirements, then this would be avoidance. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. AnswerD is incorrect. Acceptance accepts the risk that the windows could be late and offers no response.

QUESTION 27

The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.
* The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.
* The level of risk tolerance.
* The techniques and methodologies an organization plans to employ, to evaluate information system- related security risks.
* The RMF primarily operates at Tier 1.

Explanation/Reference:

Explanation: The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the

following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system.

The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out.Answer: D is incorrect. The RMF primarily operates at Tier 3.

QUESTION 28

Which of the following documents were developed by NIST for conducting Certification & Accreditation (C&A)? Each correct answer represents a complete solution. Choose all that apply.
* NIST Special Publication 800-60
* NIST Special Publication 800-53
* NIST Special Publication 800-37A
* NIST Special Publication 800-59
* NIST Special Publication 800-37
* NIST Special Publication 800-53A

Explanation/Reference:

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. AnswerC is incorrect. There is no such type of NIST document.

QUESTION 29

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.
* Security operations
* Maintenance of the SSAA
* Compliance validation
* Change management
* System operations
* Continue to review and refine the SSAA

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation Answer F is incorrect. It is a Phase 3 activity.

QUESTION 30

Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.
* File and object access
* Data downloading from the Internet
* Printer access
* Network logons and logoffs
Explanation/Reference:

Explanation: The following types of activities can be audited: Network logons and logoffs File access Printer access Remote access service Application usage Network services 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 security auditing, the type of event to be audited should be specified in the audit policy. Auditing is an essential component to maintain the security of deployed systems. Security auditing depends on the criticality of the environment and on the company’s security policy. The security system should be reviewed periodically. Answer: B is incorrect. Data downloading from the Internet cannot be audited.

QUESTION 31

Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.
* Integrity
* Authenticity
* Confidentiality
* Availability
Explanation/Reference:

Explanation: The elements of security are as follows: 1.Confidentiality: It is the concealment of information or resources. 2.Authenticity: It is the identification and assurance of the origin of information. 3.Integrity: It refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes. 4.Availability: It refers to the ability to use the information or resources as desired.

QUESTION 32

Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.
* Biba model
* Clark-Biba model
* Clark-Wilson model
* Bell-LaPadula model
Explanation/Reference:

Explanation: The Biba and Clark-Wilson access control models are used in the commercial sector. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. The Clark-Wilson security model provides a foundation for specifying and analyzing an integrity policy for a computing system. Answer: D is incorrect. The Bell-LaPadula access control model is mainly used in military systems. Answer: B is incorrect. There is no such access control model as Clark-Biba.

QUESTION 33

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

* Computer Misuse Act
* Lanham Act
* Computer Fraud and Abuse Act
* FISMA

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a ‘risk-based policy for cost-effective security’. FISMA requires agency program officials, chief information officers, and Inspectors Generals (IGs) to conduct annual reviews of the agency’s information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act. Answer A is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement: Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine “not exceeding level 5 on the standard scale” (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences. Answer C is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

ISC CSSLP Dumps - Secret To Pass in First Attempt: https://www.dumpsmaterials.com/CSSLP-real-torrent.html]