



# CSSLP<sup>Q&As</sup>

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.lead4pass.com/CSSLP.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Which of the following is a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event?

- A. Corrective controls
- B. Audit trail
- C. Security audit
- D. Detective controls

Correct Answer: B

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts, or other entities. The process that creates audit trail should always run in a privileged mode, so it could access and supervise all actions from all users, and normal user could not stop/change it. Furthermore, for the same reason, trail file or database table with a trail should not be accessible to normal users. Answer: C is incorrect. A computer security audit is a manual or systematic measurable technical assessment of a system or application. Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems. Automated assessments, or CAAT's, include system generated audit reports or using software to monitor and report changes to files and settings on a system. Systems can include personal computers, servers, mainframes, network routers, and switches. Answer: D is incorrect. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer: A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control.

---

### QUESTION 2

Which of the following refers to a process that is used for implementing information security?

- A. Classic information security model
- B. Five Pillars model
- C. Certification and Accreditation (CandA)
- D. Information Assurance (IA)

Correct Answer: C

Certification and Accreditation (CandA or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The CandA process is used extensively in the U.S. Federal Government. Some CandA processes include FISMA, NIACAP,



DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer: D is incorrect. Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security. Answer: A is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad, addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance. Answer: B is incorrect. The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

---

### QUESTION 3

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

Correct Answer: B

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 4



Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

- A. NSA-IAM
- B. NIACAP
- C. ASSET
- D. DITSCAP

Correct Answer: B

NIACAP is a process, which provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that maintain the information assurance and the security posture of a system or site. Answer: D is incorrect. DITSCAP is a process, which establishes a standard process, a set of activities, general task descriptions, and a management structure to certify and accredit the IT systems that will maintain the required security posture. Answer: A is incorrect. The NSA-IAM evaluates information systems at a high level and uses a subset of the SSE-CMM process areas to measure the implementation of information security on these systems. Answer: C is incorrect. ASSET is a tool developed by NIST to automate the process of self-assessment through the use of the questionnaire in NIST.

#### QUESTION 5

Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

- A. Federal Information Security Management Act of 2002 (FISMA)
- B. The Electronic Communications Privacy Act of 1986 (ECPA)
- C. The Equal Credit Opportunity Act (ECOA)
- D. The Fair Credit Reporting Act (FCRA)

Correct Answer: A

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). 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 general (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: C is incorrect. The Equal Credit Opportunity Act (ECOA) is a United States law (codified at 15 U.S.C. 1691 et seq.), enacted in 1974, that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex, marital status, or age; to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The law applies to any person who, in the ordinary course of business, regularly participates in a credit decision, including banks, retailers, bankcard companies, finance companies, and credit unions. Answer: B is incorrect. The Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. 2510) was



enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act, 18 U.S.C. 2701-2712. Answer: D is incorrect. The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA), it forms the base of consumer credit rights in the United States. It was originally passed in 1970, and is enforced by the US Federal Trade Commission.

---

#### QUESTION 6

Which of the following policies can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations?

- A. Informative
- B. Advisory
- C. Selective
- D. Regulatory

Correct Answer: A

An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. The informative policy can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer: D is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer: B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information. Answer: C is incorrect. It is not a valid type of policy.

---

#### QUESTION 7

Which of the following is the most secure method of authentication?

- A. Biometrics
- B. Username and password
- C. Anonymous
- D. Smart card

Correct Answer: A

Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment. It is the most secure method of



authentication. Answer: B is incorrect. Username and password is the least secure method of authentication in comparison of smart card and biometrics authentication. Username and password can be intercepted. Answer: D is incorrect. Smart card authentication is not as reliable as biometrics authentication. Answer: C is incorrect. Anonymous authentication does not provide security as a user can log on to the system anonymously and he is not prompted for credentials.

---

#### QUESTION 8

What NIACAP certification levels are recommended by the certifier? Each correct answer represents a complete solution. Choose all that apply.

- A. Comprehensive Analysis
- B. Maximum Analysis
- C. Detailed Analysis
- D. Minimum Analysis
- E. Basic Security Review
- F. Basic System Review

Correct Answer: ACDE

NIACAP has four levels of certification. These levels ensure that the appropriate CandA are performed for varying schedule and budget limitations. The certifier must analyze the system's business functions. The certifier determines the degree of confidentiality, integrity, availability, and accountability, and then recommends one of the following NIACAP certification levels: Level 1 - Basic Security Review Level 2 - Minimum Analysis Level 3 - Detailed Analysis Level 4 Comprehensive Analysis Answer: B and F are incorrect. No such types of levels exist.

---

#### QUESTION 9

Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, and many more vulnerabilities to enhance the security of the network. It encompasses a wide variety of activities. Place the different auditing activities in front of their descriptions.

Select and Place:





Command	Description	
Place Here	It is the activity of recording information to a log file or database about events or occurrences.	Log Analysis
Place Here	It is the activity of manually or programmatically reviewing logged information.	Intrusion Detection
Place Here	These are the notifications that are sent to an administrator whenever a specific event occurs.	Alarm Triggers
Place Here	It is a process to detect unwanted system access by monitoring both recorded information and real time events.	Monitoring
Place Here	It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.	Logging

Correct Answer:



Command	Description
Logging	It is the activity of recording information to a log file or database about events or occurrences.
Monitoring	It is the activity of manually or programmatically reviewing logged information.
Alarm Triggers	These are the notifications that are sent to an administrator whenever a specific event occurs.
Intrusion Detection	It is a process to detect unwanted system access by monitoring both recorded information and real time events.
Log Analysis	It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.

Explanation/Reference:

Auditing encompasses a wide variety of activities as follows: Logging: It is the activity of recording information to a log file or database about events or occurrences. Log Analysis: It is a systematic form of monitoring where the logged

information is analyzed in detail. It is done to find out the

trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. Intrusion Detection: It is a process to detect unwanted system access by monitoring both recorded information and real time events. Alarm Triggers:

These are the notifications that are sent to an administrator whenever a specific event occurs. Monitoring: It is the activity of manually or programmatically reviewing logged information.

#### QUESTION 10

Which of the following security controls works as the totality of protection mechanisms within a

computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

A. Common data security architecture (CDSA)





- B. Application program interface (API)
- C. Trusted computing base (TCB)
- D. Internet Protocol Security (IPSec)

Correct Answer: C

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. Answer: D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer: A is incorrect. The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework. It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an infrastructure for building cross- platform, interoperable, security-enabled applications for client-server environments. Answer: B is incorrect. An application programming interface (API) is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate

#### QUESTION 11

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

- A. Editor
- B. Custodian
- C. Owner
- D. User
- E. Security auditor

Correct Answer: BCDE

The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor 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 the custodian. The following are the responsibilities of the 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 The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

#### QUESTION 12

Which of the following statements are true about declarative security? Each correct answer represents a complete



solution. Choose all that apply.

- A. It is employed in a layer that relies outside of the software code or uses attributes of the code.
- B. It applies the security policies on the software applications at their runtime.
- C. In this security, authentication decisions are made based on the business logic.
- D. In this security, the security decisions are based on explicit statements.

Correct Answer: ABD

Declarative security applies the security policies on the software applications at their runtime. In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. Answer: C is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

---

### QUESTION 13

Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

- A. technical effort

Correct Answer: A

A technical effort is described as any activity, which has an effect on defining, designing, building, or implementing a task, requirement, or procedure. The technical effort is an element of technical management that is required to progress efficiently and effectively from a business need to the deployment and operation of the system.

[Latest CSSLP Dumps](#)

[CSSLP Practice Test](#)

[CSSLP Exam Questions](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

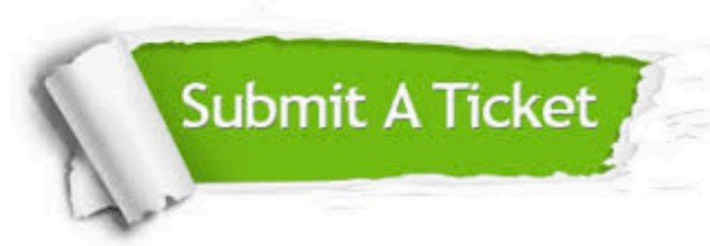
100% Guaranteed Success  
100% Money Back Guarantee  
365 Days Free Update  
Instant Download After Purchase  
24x7 Customer Support  
Average 99.9% Success Rate  
More than 800,000 Satisfied Customers Worldwide  
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.  
To update a previously submitted ticket:



 <p><b>One Year Free Update</b> Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.  
All trademarks are the property of their respective owners.  
Copyright © lead4pass, All Rights Reserved.