CSSLP$^{Q\&As}$

Certified Secure Software Lifecycle Professional Practice Test

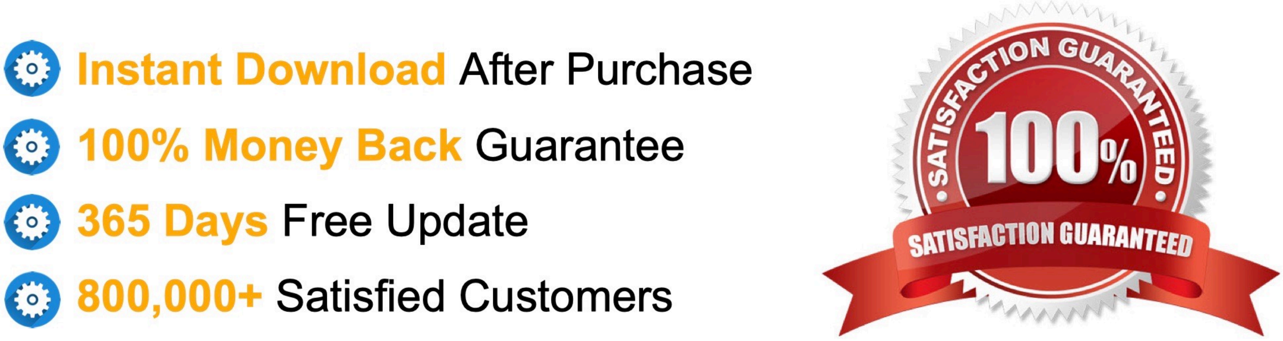
Pass ISC CSSLP Exam with 100% Guarantee

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



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

QUESTION 1

Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

A. ISO 27006

B. ISO 27005

C. ISO 27003

D. ISO 27004

Correct Answer: A

ISO 27006 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 Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS. The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A. Defining the scope of process Annex B. Asset valuation and impact assessment Annex C. Examples of typical threats Annex D. Vulnerabilities and vulnerability assessment methods Annex E. Information security risk assessment (ISRA) approaches Answer: C is incorrect. The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). Answer: D is incorrect. 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. Answer: B is incorrect. The ISO 27005 standard provides guidelines for information security risk management.

QUESTION 2

Which of the following phases of NIST SP 800-37 CandA methodology examines the residual risk for acceptability, and prepares the final security accreditation package?

A. Security Accreditation

B. Initiation

C. Continuous Monitoring

D. Security Certification

Correct Answer: A

The various phases of NIST SP 800-37 CandA are as follows: Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

QUESTION 3

Which of the following are the types of intellectual property? Each correct answer represents a complete solution. Choose all that apply.

A. Patent

B. Copyright

C. Standard

D. Trademark

Correct Answer: AB

Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. 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. A trademark is a distinctive sign used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer: C is incorrect. It is not a type of intellectual property.

QUESTION 4

Copyright holders, content providers, and manufacturers use digital rights management (DRM) in order to limit usage of digital media and devices. Which of the following security challenges does DRM include? Each correct answer represents a complete solution. Choose all that apply.

A. OTA provisioning

B. Access control

C. Key hiding

D. Device fingerprinting

Correct Answer: ACD

The security challenges for DRM are as follows: Key hiding: It prevents tampering attacks that target the secret keys. In the key hiding process, secret keys are used for authentication, encryption, and node-locking. Device fingerprinting: It prevents fraud and provides secure authentication. Device fingerprinting includes the summary of hardware and software characteristics in order to uniquely identify a device. OTA provisioning: It provides end-to-end encryption or other secure ways for delivery of copyrighted software to mobile devices. Answer: B is incorrect. Access control is not a security challenge for DRM.

QUESTION 5

Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. File-based

B. Network-based

C. Anomaly-based

D. Signature-based

Correct Answer: C

The anomaly-based intrusion detection system (IDS) monitors network traffic and compares it against an established baseline. This type of IDS monitors traffic and system activity for unusual behavior based on statistics. In order to identify a malicious activity, it learns normal behavior from the baseline. The anomaly-based intrusion detection is also known as behavior- based or statistical-based intrusion detection. Answer: D is incorrect. Signature-based IDS uses a database with signatures to identify possible attacks and malicious activity. Answer: B is incorrect. A network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. It monitors all traffic in a network or traffic coming through an entry-point such as an Internet connection. Answer: A is incorrect. There is no such intrusion detection system (IDS) that is file-based.

CSSLP Practice Test CSSLP Exam Questions CSSLP Braindumps