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.pass4itsure.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 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.

QUESTION 2

The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

A. Service-oriented discovery and analysis modeling

B. Service-oriented business integration modeling

C. Service-oriented logical architecture modeling

D. Service-oriented logical design modeling

Correct Answer: C

The service-oriented logical architecture modeling integrates SOA software assets and establishes SOA logical environment dependencies. It also offers foster service reuse, loose coupling and consolidation. Answer: A is incorrect. The service-oriented discovery and analysis modeling discovers and analyzes services for granularity, reusability, interoperability, loose- coupling, and identifies consolidation opportunities. Answer: B is incorrect. The service-oriented business integration modeling identifies service integration and alignment opportunities with business domains\\' processes. Answer: D is incorrect. The service-oriented logical design modeling establishes service relationships and message exchange paths.

QUESTION 3

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 4

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

Correct Answer: B

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 5

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

A. Identifying the risk

B. Assessing the impact of potential threats

C. Identifying the accused

D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Correct Answer: ABD

There are three goals of risk management as follows: Identifying the risk Assessing the impact of potential threats Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer: C is incorrect. Identifying the accused does not come under the scope of risk management.