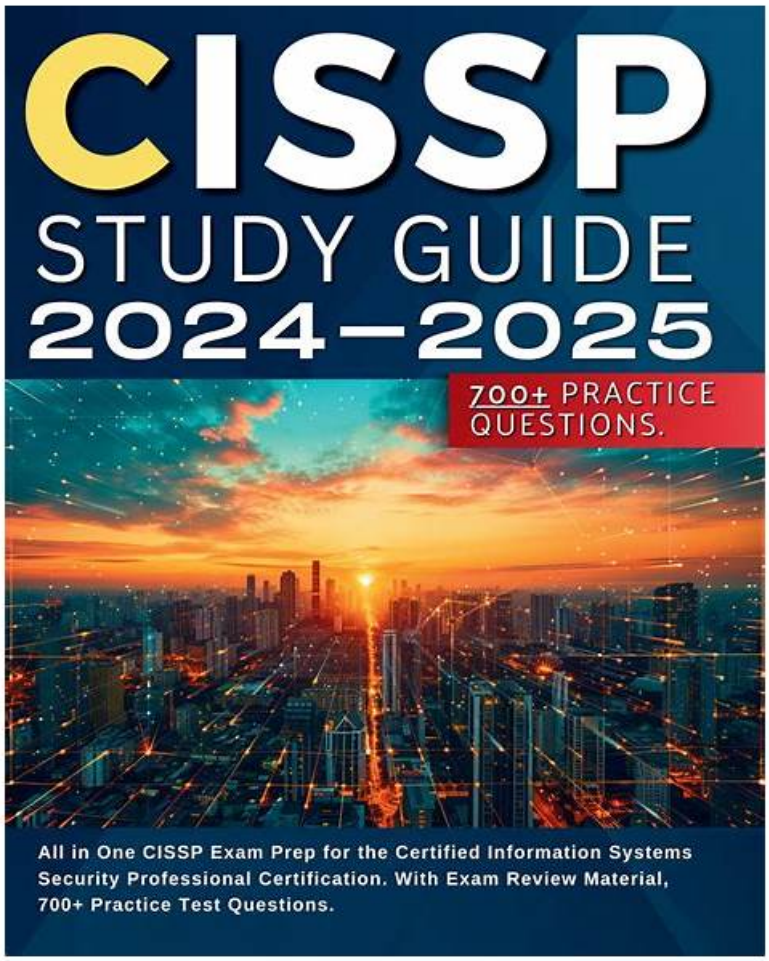
CISSP Valid Exam Pass4sure | CISSP Valid Exam Book



P.S. Free 2026 ISC CISSP dumps are available on Google Drive shared by ActualCollection: https://drive.google.com/open?id=18Z363KzVh7EYr7Xn67xgz0dM4d3PBmvI

Our company has the highly authoritative and experienced team. In order to let customers enjoy the best service, all CISSP exam prep of our company were designed by hundreds of experienced experts. Our CISSP test questions will help customers learn the important knowledge about exam. If you buy our products, it will be very easy for you to have the mastery of a core set of knowledge in the shortest time, at the same time, our CISSP Test Torrent can help you avoid falling into rote learning habits. You just need to spend 20 to 30 hours on study, and then you can take your exam. In addition, the authoritative production team of our CISSP exam prep will update the study system every day in order to make our customers enjoy the newest information.

Introduction of CISSP Exam

The CISSP certification is a globally recognized certification that utilizes a unique CBK (Credential Body of Knowledge) methodology. The CISSP credential is defined as conforming to the requirements of NCEES, the American Society for Testing and Materials (ASTM), and the International Information Systems Security Certification Consortium (ISC). The test will not earn a CISSP valid certification. The new CISSP Exam aims to deliver what the professionals need most the ability to demonstrate that they can apply their knowledge and skills effectively on the jobsite. This exam includes questions from five of the ten domains of knowledge: Access Controls, Application Development Security, Business Continuity and Disaster Recovery Planning, Cryptography, and Risk Management which are also covered in our **CISSP Dumps**. The CISSP certification exam was updated in May 2012. This guide provides an overview of the CISSP (ISC)2 domains and their respective weighting within the examination to further assist candidates with their studies. The guide also provides guidance on how to prepare for the exam, including how to use the ISC2 CBK (Credential Body of Knowledge) to help develop an individualized study plan. The guide also lists sample questions that can be used as part of a final review prior to taking the exam.

ISC CISSP Certification is a prestigious credential that demonstrates an individual's commitment to the field of information security. It is a challenging certification to obtain, but the benefits are well worth the effort. With the demand for cybersecurity professionals

on the rise, obtaining a CISSP certification can open up many rewarding career opportunities.

ISC CISSP Exam is considered one of the most challenging and prestigious information security certifications available today. It is administered by the International Information Systems Security Certification Consortium (ISC) and is recognized in over 160 countries around the world. CISSP exam consists of 250 multiple-choice questions and takes up to six hours to complete. Candidates must score at least 700 out of 1,000 points to pass the exam.

>> CISSP Valid Exam Pass4sure <<

Free PDF Quiz ISC - CISSP –Valid Valid Exam Pass4sure

Our technology and our staff are the most professional. What are the CISSP practice materials worthy of your choice, I hope you spend a little time to find out. First of all, after you make a decision, you can start using our CISSP Exam Questions soon. We will send you an email within five to ten minutes after your payment is successful. You can choose any version of CISSP study guide, as long as you find it appropriate.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q706-Q711):

NEW QUESTION # 706
Annualized Loss Expectancy (ALE) value is derived from an algorithm of the product of annual rate of occurrence and

- A. Previous year's actual loss.
- B. Single loss expectancy.
- C. Cost of all losses expected.
- D. Average of previous losses.

Answer: B

Explanation:
Single Loss Expectancy (SLE) x Annualized Rate of Occurance (ARO) = ALE pg. 18 Krutz: The CISSP Prep Guide

NEW QUESTION # 707
In what way can violation clipping levels assist in violation tracking and analysis?

- A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.
- B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.
- C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.
- D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Answer: A

Explanation:
Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.
The following are incorrect answers:
Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant. This is not the best answer, you would not record ONLY security relevant violations, all violations would be recorded as well as all actions performed by authorized users which may not trigger a violation. This could allow you to indentify abnormal activities or fraud after the fact.
Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status. It could record all security violations whether the user is a normal user or a privileged user.
Clipping levels enable a security administrator to view all reductions in security levels which have
been made to user accounts which have incurred violations. The keyword "ALL" makes this

question wrong. It may detect SOME but not all of violations. For example, application level attacks may not be detected.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1239). McGraw-Hill. Kindle Edition.
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION # 708
At which of the basic phases of the System Development Life Cycle are security requirements formalized?

- A. Disposal
- B. System Design Specifications
- C. Development and Implementation
- D. Functional Requirements Definition

Answer: D

Explanation:
During the Functional Requirements Definition the project management and systems development teams will conduct a comprehensive analysis of current and possible future functional requirements to ensure that the new system will meet end-user needs.
The teams also review the documents from the project initiation phase and make any revisions or updates as needed. For smaller projects, this phase is often subsumed in the project initiation phase. At this point security requirements should be formalized.
The Development Life Cycle is a project management tool that can be used to plan, execute, and control a software development project usually called the Systems
Development Life Cycle (SDLC).
The SDLC is a process that includes systems analysts, software engineers, programmers, and end users in the project design and development. Because there is no industry-wide
SDLC, an organization can use any one, or a combination of SDLC methods.
The SDLC simply provides a framework for the phases of a software development project from defining the functional requirements to implementation. Regardless of the method used, the SDLC outlines the essential phases, which can be shown together or as separate elements. The model chosen should be based on the project.
For example, some models work better with long-term, complex projects, while others are more suited for short-term projects. The key element is that a formalized SDLC is utilized.
The number of phases can range from three basic phases (concept, design, and implement) on up.
The basic phases of SDLC are:
Project initiation and planning
Functional requirements definition
System design specifications
Development and implementation
Documentation and common program controls
Testing and evaluation control, (certification and accreditation)
Transition to production (implementation)
The system life cycle (SLC) extends beyond the SDLC to include two additional phases:
Operations and maintenance support (post-installation)
Revisions and system replacement
System Design Specifications
This phase includes all activities related to designing the system and software. In this phase, the system architecture, system outputs, and system interfaces are designed. Data input, data flow, and output requirements are established and security features are designed, generally based on the overall security architecture for the company.
Development and Implementation
During this phase, the source code is generated, test scenarios and test cases are developed, unit and integration testing is conducted, and the program and system are documented for maintenance and for turnover to acceptance testing and production. As well as general care for software quality, reliability, and consistency of operation, particular care should be taken to ensure that the code is analyzed to eliminate common vulnerabilities that might lead to security exploits and other risks.
Documentation and Common Program Controls
These are controls used when editing the data within the program, the types of logging the program should be doing, and how the program versions should be stored. A large number of such controls may be needed, see the reference below for a full list of controls.

Acceptance
In the acceptance phase, preferably an independent group develops test data and tests the code to ensure that it will function within the organization's environment and that it meets all the functional and security requirements. It is essential that an independent group test the code during all applicable stages of development to prevent a separation of duties issue. The goal of security testing is to ensure that the application meets its security requirements and specifications. The security testing should uncover all design and implementation flaws that would allow a user to violate the software security policy and requirements. To ensure test validity, the application should be tested in an environment that simulates the production environment. This should include a security certification package and any user documentation.
Certification and Accreditation (Security Authorization)
Certification is the process of evaluating the security stance of the software or system against a predetermined set of security standards or policies. Certification also examines how well the system performs its intended functional requirements. The certification or evaluation document should contain an analysis of the technical and nontechnical security features and countermeasures and the extent to which the software or system meets the security requirements for its mission and operational environment.
Transition to Production (Implementation)
During this phase, the new system is transitioned from the acceptance phase into the live production environment. Activities during this phase include obtaining security accreditation; training the new users according to the implementation and training schedules; implementing the system, including installation and data conversions; and, if necessary, conducting any parallel operations.
Revisions and System Replacement
As systems are in production mode, the hardware and software baselines should be subject to periodic evaluations and audits. In some instances, problems with the application may not be defects or flaws, but rather additional functions not currently developed in the application. Any changes to the application must follow the same SDLC and be recorded in a change management system. Revision reviews should include security planning and procedures to avoid future problems. Periodic application audits should be conducted and include documenting security incidents when problems occur. Documenting system failures is a valuable resource for justifying future system enhancements.
Below you have the phases used by NIST in it's 800-63 Revision 2 document
As noted above, the phases will vary from one document to another one. For the purpose of the exam use the list provided in the official ISC2 Study book which is presented in short form above. Refer to the book for a more detailed description of activities at each of the phases of the SDLC.
However, all references have very similar steps being used. As mentioned in the official book, it could be as simple as three phases in it's most basic version (concept, design, and implement) or a lot more in more detailed versions of the SDLC.
The key thing is to make use of an SDLC.
SDLC phases
Reference(s) used for this question:
NIST SP 800-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Software Development Security ((ISC)2 Press) (Kindle Locations 134-157). Auerbach Publications. Kindle Edition.

NEW QUESTION # 709
What does electronic vaulting accomplish?

- A. It automates the Disaster Recovery Process (DRP)
- B. It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems
- C. It protects critical files.
- D. It stripes all database records

Answer: C

NEW QUESTION # 710
Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?

- A. Preventive/Administrative Pairing
- B. Preventive/Physical Pairing
- C. Preventive/Technical Pairing
- D. Detective/Technical Pairing

Answer: C

Explanation:
Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34

NEW QUESTION # 711
.....

Living in such a world where competitiveness is a necessity that can distinguish you from others, every one of us is trying our best to improve ourselves in every way. It has been widely recognized that the CISSP Exam can better equip us with a newly gained personal skill, which is crucial to individual self-improvement in today's computer era. With the certified advantage admitted by the test ISC certification, you will have the competitive edge to get a favorable job in the global market.