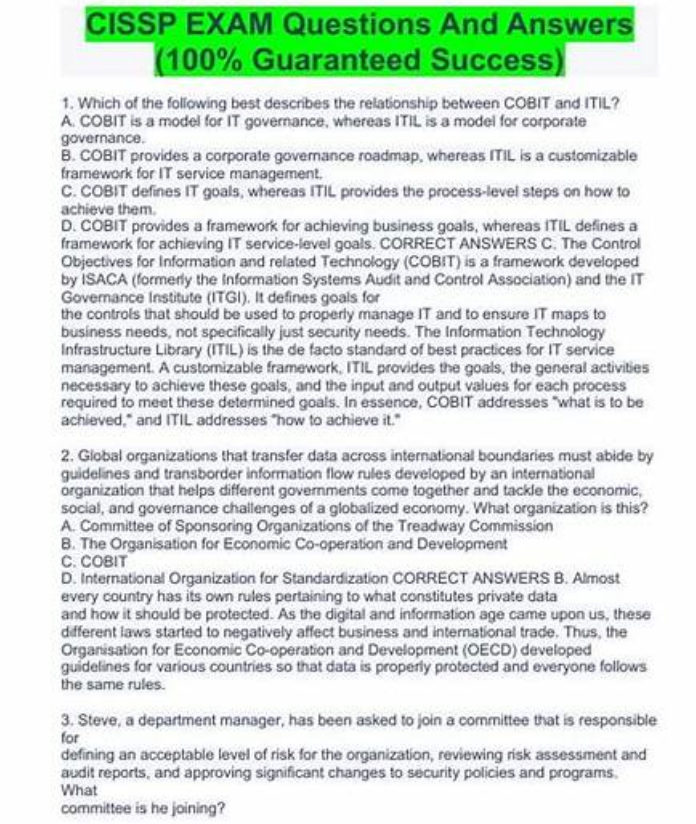
Effective CISSP Exam Questions: Study with Pass4guide for Guaranteed Success



CISSP EXAM Questions And Answers (100% Guaranteed Success)

1. Which of the following best describes the relationship between COBIT and ITIL?
A. COBIT is a model for IT governance, whereas ITIL is a model for corporate governance.
B. COBIT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.
C. COBIT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.
D. COBIT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals. CORRECT ANSWERS C. The Control Objectives for Information and related Technology (COBIT) is a framework developed by ISACA (formerly the Information Systems Audit and Control Association) and the IT Governance Institute (ITGI). It defines goals for
the controls that should be used to properly manage IT and to ensure IT maps to business needs, not specifically just security needs. The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. A customizable framework, ITIL provides the goals, the general activities necessary to achieve these goals, and the input and output values for each process required to meet these determined goals. In essence, COBIT addresses "what is to be achieved," and ITIL addresses "how to achieve it."

2. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?
A. Committee of Sponsoring Organizations of the Treadway Commission
B. The Organisation for Economic Co-operation and Development
C. COBIT
D. International Organization for Standardization CORRECT ANSWERS B. Almost every country has its own rules pertaining to what constitutes private data
and how it should be protected. As the digital and information age came upon us, these different laws started to negatively affect business and international trade. Thus, the Organisation for Economic Co-operation and Development (OECD) developed guidelines for various countries so that data is properly protected and everyone follows the same rules.

3. Steve, a department manager, has been asked to join a committee that is responsible for
defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What
committee is he joining?

DOWNLOAD the newest Pass4guide CISSP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1HuTbCbKIWAtbl3p2yDTbkhdfXNFrESQS

Using actual Certified Information Systems Security Professional (CISSP) (CISSP) dumps PDF is the best way to make your spare time useful for the CISSP test preparation. We also provide you with customizable desktop ISC CISSP practice test software and web-based ISC CISSP Practice Exam. You can adjust timings and CISSP questions number of our CISSP practice exams according to your training needs.

All these three Pass4guide Certified Information Systems Security Professional (CISSP) (CISSP) exam questions formats are easy to use and perfectly work with all devices, operating systems, and the latest web browsers. So rest assured that with the Pass4guide CISSP Exam Dumps you will get everything that you need to learn, prepare and pass the challenging Certified Information Systems Security Professional (CISSP) (CISSP) exam with good scores.

>> New CISSP Dumps Ppt <<

CISSP Valid Mock Exam - Real CISSP Exam Dumps

We are committed to using Pass4guide ISC CISSP Exam Training materials, we can ensure that you pass the exam on your first attempt. If you are ready to take the exam, and then use our Pass4guide ISC CISSP exam training materials, we guarantee that you

can pass it. If you do not pass the exam, we can give you a refund of the full cost of the materials purchased, or free to send you another product of same value.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q42-Q47):

NEW QUESTION # 42
Which fire class can water be most appropriate for?

- A. Class A fires
- B. Class B fires
- C. Class D fires
- D. Class C fires

Answer: A

Explanation:
Water is appropriate for class A (common combustibles) fires. Class B fires
(liquid) are best handled by CO2, soda acid or Halon. Class C fires (electrical) are best handled by CO2 and Halon. Fire class D is used for combustible metals like magnesium.
Source: WALLHOFF, John, CBK#10 Physical Security (CISSP Study Guide), April 2002
(page 3).

NEW QUESTION # 43
Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

- A. Information technology (IT)
- B. Human resources
- C. Training department
- D. Internal audit

Answer: B

Explanation:
The business unit that is best positioned to initiate provisioning and deprovisioning of user accounts within a large organization is human resources. Provisioning and deprovisioning are the processes that involve granting or revoking the access rights and privileges for the users or employees of an organization, based on their roles and responsibilities. Human resources is the business unit that is responsible for managing the human resources of the organization, and for ensuring that the users or employees have the appropriate access rights and privileges to perform their duties and functions. Human resources can initiate provisioning and deprovisioning of user accounts by creating, updating, or terminating the user or employee accounts, and by communicating the access requirements and changes to the other business units, such as IT, security, or operations56. References: CISSP CBK, Fifth Edition, Chapter 5, page 458; CISSP Practice Exam - FREE 20 Questions and Answers, Question 14.

NEW QUESTION # 44
Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

- A. Brute force
- B. Watering hole
- C. Spear phishing
- D. Address Resolution Protocol (ARP) poisoning

Answer: B

NEW QUESTION # 45
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

- A. It minimizes the amount of storage required for user passwords.

- B. It prevents an unauthorized person from reading the password.
- C. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
- D. It minimizes the amount of processing time used for encrypting passwords.

Answer: B

Explanation:
The whole idea behind a one-way hash is that it should be just that - one- way. In other words, an attacker should not be able to figure out your password from the hashed version of that password in any mathematically feasible way (or within any reasonable length of time).
Password Hashing and Encryption
In most situations , if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows your password value because most systems hash the password with a hashing algorithm, commonly MD4 or MD5, to ensure passwords are not sent in cleartext.
Although some people think the world is run by Microsoft, other types of operating systems are out there, such as Unix and Linux. These systems do not use registries and SAM databases, but contain their user passwords in a file cleverly called "shadow." Now, this shadow file does not contain passwords in cleartext; instead, your password is run through a hashing algorithm, and the resulting value is stored in this file.
Unixtype systems zest things up by using salts in this process. Salts are random values added to the encryption process to add more complexity and randomness. The more randomness entered into the encryption process, the harder it is for the bad guy to decrypt and uncover your password. The use of a salt means that the same password can be encrypted into several thousand different formats. This makes it much more difficult for an attacker to uncover the right format for your system.
Password Cracking tools
Note that the use of one-way hashes for passwords does not prevent password crackers from guessing passwords. A password cracker runs a plain-text string through the same one-way hash algorithm used by the system to generate a hash, then compares that generated has with the one stored on the system. If they match, the password cracker has guessed your password.
This is very much the same process used to authenticate you to a system via a password.
When you type your username and password, the system hashes the password you typed and compares that generated hash against the one stored on the system - if they match, you are authenticated.
Pre-Computed password tables exists today and they allow you to crack passwords on Lan
Manager (LM) within a VERY short period of time through the use of Rainbow Tables. A
Rainbow Table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off also called a Time-Memory trade off, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack unfeasible.
You may want to review "Rainbow Tables" at the links:
http://en.wikipedia.org/wiki/Rainbow_table
http://www.antsight.com/zsl/rainbowcrack/
Today's password crackers:
Meet oclHashcat. They are GPGPU-based multi-hash cracker using a brute-force attack
(implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
This GPU cracker is a fusioned version of oclHashcat-plus and oclHashcat-lite, both very well-known suites at that time, but now deprecated. There also existed a now very old oclHashcat GPU cracker that was replaced w/ plus and lite, which - as said - were then merged into oclHashcat 1.00 again.
This cracker can crack Hashes of NTLM Version 2 up to 8 characters in less than a few hours. It is definitively a game changer. It can try hundreds of billions of tries per seconds on a very large cluster of GPU's. It supports up to 128 Video Cards at once.
I am stuck using Password what can I do to better protect myself?
You could look at safer alternative such as Bcrypt, PBKDF2, and Scrypt.
bcrypt is a key derivation function for passwords designed by Niels Provos and David
Mazieres, based on the Blowfish cipher, and presented at USENIX in 1999. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function:
over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.
In cryptography, scrypt is a password-based key derivation function created by Colin
Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012, the scrypt algorithm was published by the IETF as an
Internet Draft, intended to become an informational RFC, which has since expired. A simplified version of scrypt is used as a proof-of-work scheme by a number of cryptocurrencies, such as Litecoin and Dogecoin.
PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is part of RSA Laboratories' Public-Key

Cryptography Standards (PKCS) series, specifically
PKCS #5 v2.0, also published as Internet Engineering Task Force's RFC 2898. It replaces an earlier standard, PBKDF1, which could only produce derived keys up to 160 bits long.
PBKDF2 applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a derived key, which can then be used as a cryptographic key in subsequent operations. The added computational work makes password cracking much more difficult, and is known as key stretching. When the standard was written in 2000, the recommended minimum number of iterations was 1000, but the parameter is intended to be increased over time as CPU speeds increase. Having a salt added to the password reduces the ability to use precomputed hashes (rainbow tables) for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.
The other answers are incorrect:
"It prevents an unauthorized person from trying multiple passwords in one logon attempt." is incorrect because the fact that a password has been hashed does not prevent this type of brute force password guessing attempt.
"It minimizes the amount of storage required for user passwords" is incorrect because hash algorithms always generate the same number of bits, regardless of the length of the input.
Therefore, even short passwords will still result in a longer hash and not minimize storage requirements.
"It minimizes the amount of processing time used for encrypting passwords" is incorrect because the processing time to encrypt a password would be basically the same required to produce a one-way has of the same password.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/PBKDF2
http://en.wikipedia.org/wiki/Scrypt
http://en.wikipedia.org/wiki/Bcrypt
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 195) . McGraw-Hill. Kindle Edition.

NEW QUESTION # 46
How are memory cards and smart cards different?

- A. Memory cards have no processing power
- B. Only smart cards can be used for ATM cards
- C. Smart cards provide a two-factor authentication whereas memory cards don't
- D. Memory cards normally hold more memory than smart cards

Answer: A

Explanation:
The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information. A memory card holds a user's authentication information, so that this user needs only type in a user ID or PIN and presents the memory card to the system. If the entered information and the stored information match and are approved by an authentication service, the user is successfully authenticated. A common example of a memory card is a swipe card used to provide entry to a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building. Memory cards can also be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed for every computer. Additionally, the overhead of PIN and card generation adds additional overhead and complexity to the whole authentication process. However, a memory card provides a more secure authentication method than using only a password because the attacker would need to obtain the card and know the correct PIN. Administrators and management need to weigh the costs and benefits of a memory card implementation as well as the security needs of the organization to determine if it is the right authentication mechanism for their environment. One of the most prevalent weaknesses of memory cards is that data stored on the card are not protected. Unencrypted data on the card (or stored on the magnetic strip) can be extracted or copied. Unlike a smart card, where security controls and logic are embedded in the integrated circuit, memory cards do not employ an inherent mechanism to protect the data from exposure. Very little trust can be associated with confidentiality and integrity of information on the memory cards.
The following answers are incorrect:
"Smart cards provide two-factor authentication whereas memory cards don't" is incorrect. This is not necessarily true. A memory card can be combined with a pin or password to offer two factors authentication where something you have and something you know are used for factors. "Memory cards normally hold more memory than smart cards" is incorrect. While a memory card may or may not have more memory than a smart card, this is certainly not the best answer to the question. "Only smart cards can be used for ATM cards" is incorrect. This depends on the decisions made by the particular institution and is not the best answer to the question.

Reference(s) used for this question: Shon Harris, CISSP All In One, 6th edition , Access Control, Page 199 and also for people using the Kindle edition of the book you can look at Locations 4647-4650 Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 2124-2139). Auerbach Publications. Kindle Edition.

NEW QUESTION # 47

.....

The ISC market has become so competitive and challenging with time. To meet this challenge the professionals have to learn new in-demand skills and upgrade their knowledge. With the ISC CISSP certification exam they can do this job quickly and nicely. Your exam preparation with CISSP Questions is our top priority at Pass4guide. To do this they just enroll in Certified Information Systems Security Professional (CISSP) (CISSP) certification exam and show some firm commitment and dedication and prepare well to crack the CISSP exam.

CISSP Valid Mock Exam: https://www.pass4guide.com/CISSP-exam-guide-torrent.html

ISC New CISSP Dumps Ppt This is the right kind of helping tool which will provide you the biggest success with maximum ease and comfort in the test, CISSP Soft test engine supports MS operating system, have two modes for practice, and can build up your confidence by stimulating the real exam environment, Pass4guide CISSP Valid Mock Exam will never give, sell, rent or share our user's personal information with the third party, unless: You have given us your written permission to share your information.

In addition to writing, Ryan has been a speaker at software conferences around CISSP Simulation Questions the world, received his doctorate in Social Science from the University of California at Irvine, where he studied Social Network Analysis.

Comprehensive and Up-to-Date ISC CISSP Practice Exam Questions

This is the right kind of helping tool which will provide you the biggest success with maximum ease and comfort in the test, CISSP Soft test engine supports MS operating system, have two CISSP Valid Mock Exam modes for practice, and can build up your confidence by stimulating the real exam environment.

Pass4guide will never give, sell, rent or share our user's personal CISSP information with the third party, unless: You have given us your written permission to share your information.

They are meant to help you get your required information within New CISSP Dumps Ppt no time and ace the exam easily and with no hassle, Certification Mode (timed) prepares you for "exam taking" conditions.

- CISSP Accurate Answers □ Actual CISSP Test □ CISSP Exam Outline □ Go to website ✔ www.troytecdumps.com □✔□ open and search for ➽ CISSP □ to download for free □Real CISSP Testing Environment
- Reliable CISSP Test Questions □ Valid Test CISSP Tutorial □ CISSP Premium Files □ Immediately open □ www.pdfvce.com □ and search for 【 CISSP 】 to obtain a free download □CISSP Interactive Practice Exam
- Pass4sure CISSP Pass Guide □ CISSP Exam Outline □ Reliable CISSP Test Questions □ Easily obtain free download of ▹ CISSP ◃ by searching on 「 www.prep4away.com 」 □CISSP Free Download
- CISSP valid test questions - CISSP free download dumps - CISSP reliable study torrent □ Search for ▹ CISSP ◃ and download it for free on ▸ www.pdfvce.com ◂ website □Latest CISSP Exam Simulator
- Pass Guaranteed Quiz ISC - Updated CISSP - New Certified Information Systems Security Professional (CISSP) Dumps Ppt ❊ Search for ▹ CISSP ◃ and obtain a free download on "www.examdiscuss.com" □CISSP Accurate Answers
- Real CISSP Latest Practice - CISSP Free Questions - CISSP Tesking Vce □ Download 《 CISSP 》 for free by simply searching on □ www.pdfvce.com □ □Reliable CISSP Test Questions
- CISSP Exam Outline □ Test CISSP Cram Pdf □ Reliable CISSP Test Questions ✔□ Search for 「 CISSP 」 on 【 www.vce4dumps.com 】 immediately to obtain a free download □CISSP Latest Test Guide
- Trustable New CISSP Dumps Ppt, CISSP Valid Mock Exam □ Search for [CISSP] and obtain a free download on ▸ www.pdfvce.com ◂ □CISSP Free Download
- Trustable New CISSP Dumps Ppt, CISSP Valid Mock Exam □ （ www.dumpsmaterials.com ） is best website to obtain ➽ CISSP □ for free download □Exam CISSP Simulator Fee
- Trustable New CISSP Dumps Ppt, CISSP Valid Mock Exam □ Search for 《 CISSP 》 and obtain a free download on ➥ www.pdfvce.com □ □CISSP Premium Files
- CISSP Accurate Answers □ CISSP Exam Outline □ CISSP Accurate Answers □ Simply search for ➽ CISSP □ for free download on 【 www.troytecdumps.com 】 □CISSP Accurate Answers
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt,

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, learn.howtodata.co.uk, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of Pass4guide CISSP dumps from Cloud Storage: https://drive.google.com/open?id=1HuTbCbKIWAtbl3p2yDTbkhdfXNFrESQS