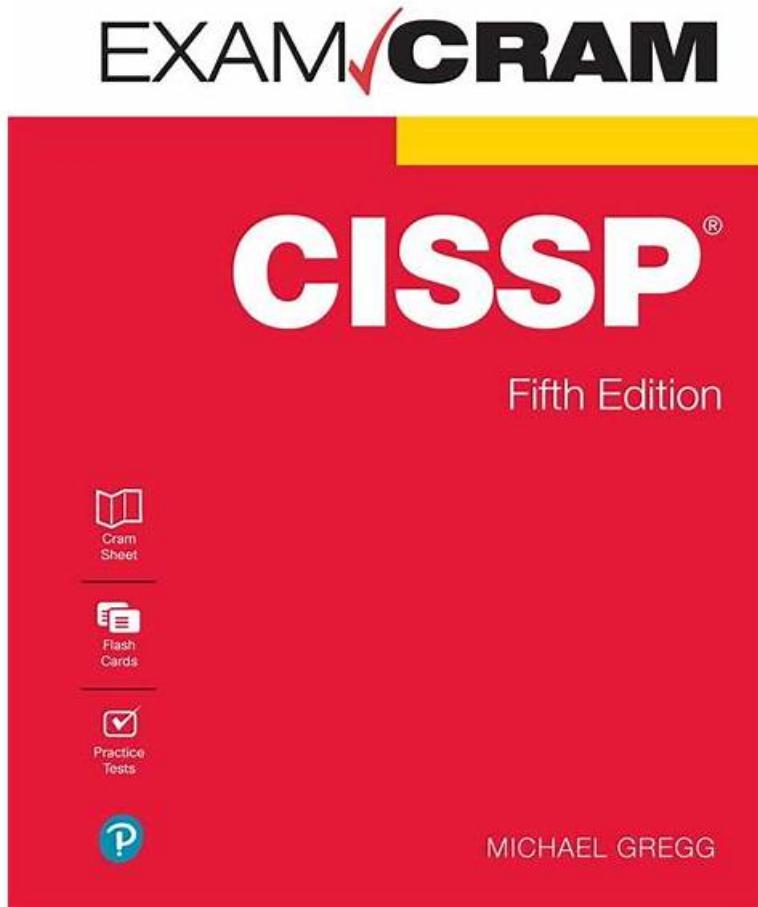


New CISSP Exam Cram - Valid Exam CISSP Book



What's more, part of that Exam4Free CISSP dumps now are free: https://drive.google.com/open?id=1ygf0_aTKpJkYVGaXYig3QQ83XKhPWr0H

As is known to all, practice makes perfect. This proverb also can be replied into the exam. We have the CISSP Study Materials with good reputation in the market. The CISSP exam dumps not only contains the quality, but also have the quantity, therefore it will meet your needs. Just think that you just need to practice it for some time, a certificate will be obtained by your own efforts, it will be a quite delightful thing. So act now, you will be very happy to see it come true.

What is ISC CISSP Certification Exam

The ISC CISSP certification is an international standard for information security professionals. It is the only certified CISSP-ISSMP credential that is recognized by the U.S. Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT), and the National Institute of Standards and Technology (NIST).

The CISSP certification was developed by the International Information Systems Security Certification Consortium (ISC) and is widely considered one of the most difficult certifications to attain. The CISSP exam tests for knowledge of concepts such as network security, software security, cryptography, physical security, and general security principles. Candidates must pass a rigorous 8-hour long exam and demonstrate proficiency in at least 10 out of 12 knowledge areas. By passing the CISSP certification exam with the help of **CISSP Dumps**, professionals can prove that they have the knowledge and skills related to information security that are essential for enterprise security leaders. The CISSP certification is defined as conforming to the requirements of the National Council of Examiners for Engineering and Surveying (NCEES), the American Society for Testing and Materials (ASTM), and the International Information Systems Security Certification Consortium (ISC).

The advantages of obtaining the ISC CISSP Certification

ISC CISSP Certification Benefits ISC recognizes the importance of professional development for current CISSPs. The ISC CISSP CBK Review Program was introduced to provide CISSPs with the opportunity to earn continuing professional education (CPE) credits or retain their certification status. ISC also offers the CPE library, which contains informative, educational content on various information security topics. Certified CISSPs receive additional opportunities to network with peers, get involved with industry events, learn new skills, and continue to acquire knowledge in the field of information security.

ISC's CISSP Certification holds many advantages for those who obtain it. First, it is beneficial for companies because they are able to hire more secure employees. Secondly, obtaining the certification will make you eligible to receive incentives offered by Microsoft, Google, and other IT firms. Thirdly, individuals who obtain the certification are able to work in more advanced positions. Fourth, the credential is accepted worldwide and your compensation level will increase as a result of this recognition. Finally, ISC offers continuing professional education credits that give you an opportunity to earn credits or maintain your credentials with the program also offering informative CPE library content on various information security topics which can be accessed by certified professionals.

CISSP stands for Certified Information Systems Security Professional. It is a certification that shows that an individual possesses comprehensive, technical knowledge of the information security field. The CISSP preparation material preparation is available in numerous varieties online. You can use this CISSP exam material like **CISSP Dumps**, to pass your CISSP examination with great ease. The main purpose of the CISSP certification is to confirm professional competence in information security management and to enhance it continuously by learning new skills and techniques of cybersecurity.

>> New CISSP Exam Cram <<

Valid Exam CISSP Book, Latest CISSP Examprep

We try our best to provide the most efficient and intuitive CISSP learning materials to the learners and help them learn efficiently. Our CISSP exam reference provides the instances, simulation and diagrams to the clients so as to they can understand them intuitively. Based on the consideration that there are some hard-to-understand contents we insert the instances to our CISSP Test Guide to concretely demonstrate the knowledge points and the diagrams to let the clients understand the inner relationship and structure of the CISSP knowledge points.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q1347-Q1352):

NEW QUESTION # 1347

Who should perform the design review to uncover security design flaws as part of the Software Development Life Cycle (SDLC)?

- A. A developer subject matter expert (SME)
- **B. security subject matter expert (SME)**
- C. The business owner
- D. The application owner

Answer: B

NEW QUESTION # 1348

A technician is troubleshooting a client's report about poor wireless performance. Using a client monitor, the technician notes the following information:

Which of the following is MOST likely the cause of the issue?

- **A. Channel overlap**
- B. Poor signal
- C. Wrong antenna type
- D. Incorrect power settings

Answer: A

NEW QUESTION # 1349

Which of the following is used to create parity information?

- A. a mirroring code
- B. a clustering code
- C. a striping code
- D. a **hamming** code

Answer: D

Explanation:

Explanation/Reference:

Explanation:

RAID Level 2 consists of bit-interleaved data on multiple disks. The parity information is created using a hamming code that detects errors and establishes which part of which drive is in error. It defines a disk drive system with 39 disks: 32 disks of user storage 66 and seven disks of error recovery coding. This level is not used in practice and was quickly superseded by the more flexible levels of RAID such as RAID 3 and RAID 5.

Incorrect Answers:

B: Clustering code is not used to create parity information.

C: A mirroring code is not used to create parity information. Mirroring is used to describe the method used in RAID level 1.

D: A striping code is not used to create parity information. Striping is the method used to write data across multiple disks in RAID systems.

References:

Krutz, Ronald L. and Russell Dean Vines, *The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams*, 2nd Edition, Wiley Publishing, Indianapolis, 2004, p. 144

NEW QUESTION # 1350

Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:

- A. **physical controls.**
- B. administrative controls.
- C. logical controls.
- D. technical controls.

Answer: A

Explanation:

Explanation/Reference:

Explanation:

Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls. These are all items put into place to protect facility, personnel, and resources.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors:

administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Incorrect Answers:

A: Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls, not administrative controls. Therefore, this answer is incorrect.

B: Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls, not logical controls. Therefore, this answer is incorrect.

C: Guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are examples of physical security controls, not technical controls. Therefore, this answer is incorrect.

References:

NEW QUESTION # 1351

During which phase of an IT system life cycle are security requirements developed?

- A. Functional design analysis and Planning
- B. Initiation
- C. Implementation
- D. Operation

Answer: A

Explanation:

The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.

The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

Conduct the risk assessment and use the results to supplement the baseline security controls;

Analyze security requirements;

Perform functional and security testing;

Prepare initial documents for system certification and accreditation; and

Design security architecture.

Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.

Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:

- Project initiation
- Functional design analysis and planning
- System design specifications
- Software development
- Installation
- Maintenance support
- Revision and replacement

According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase. SDLC POSITIONING FROM NIST 800-64

SDLC Positioning in the enterprise Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64

SDLC Overview from NIST 800-64 Revision 2

NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at: <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

DISCUSSION:

Different sources present slightly different info as far as the phases names are concerned.

People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.

NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.

Within the NIST standard they use different phase, however under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:

The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.

At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.

By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.

NIST says:

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.

I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956

and

NIST S-64 Revision 2 at <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

and

<http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc-system-development>

NEW QUESTION # 1352

.....

It is a truth well-known to all around the world that no pains and no gains. There is another proverb that the more you plough the more you gain. When you pass the CISSP exam which is well recognized wherever you are in any field, then acquire the CISSP certificate, the door of your new career will be open for you and your future is bright and hopeful. Our CISSP Guide Torrent will be your best assistant to help you gain your certificate. We believe that you don't encounter failures anytime you want to learn our CISSP guide torrent.

Valid Exam CISSP Book: <https://www.exam4free.com/CISSP-valid-dumps.html>

- Valid CISSP Test Guide □ CISSP Certification Training ~ CISSP Detail Explanation □ Easily obtain free download of
→ CISSP □□□ by searching on □ www.easy4engine.com □ □Exam CISSP Training
- Exam Dumps CISSP Demo □ Testking CISSP Exam Questions □ Exam CISSP Vce Download ✖ CISSP □✖□
for free by simply entering □ www.pdfvce.com □ website □Testking CISSP Exam Questions
- Free PDF CISSP - High Hit-Rate New Certified Information Systems Security Professional (CISSP) Exam Cram □ Open
► www.troytecdumps.com ▲ and search for ✖ CISSP □✖□ to download exam materials for free □Exam Dumps CISSP
Demo
- Easy Access to ISC CISSP Exam Questions in PDF Format □ Copy URL “www.pdfvce.com” open and search for ✖
CISSP ▲ to download for free □Latest CISSP Exam Discount
- Latest CISSP Exam Fee □ CISSP Reliable Cram Materials □ Latest CISSP Exam Fee □ Search for ⇒ CISSP ⇄ and
download it for free immediately on► www.prepawaypdf.com ▲ □Latest CISSP Braindumps Free

BTW, DOWNLOAD part of Exam4Free CISSP dumps from Cloud Storage: https://drive.google.com/open?id=1ygf0_aTKpJkYVGaXYig3QQ83XKhPWoH