Chapter 6

An expert's tips for cracking tough CISSP exam

Rahul Kokcha, an experienced instructor for CISSP explains how to prepare for the CISSP exam, what are important topics, and what you do not need to focus.

WHAT YOU WILL LEARN...

- History of CISSP certification
- Importance of CISSP certification
- The CISSP exam pattern
- What material you should use to prepare for exam
- What are important topics for the exam
- What is never asked in the exam
- My personal experience
- Some sample questions

WHAT YOU SHOULD KNOW...

- This article is intended to prepare readers to crack the CISSP exam. Readers are expected to know the syllabus for the exam.

The History of CISSP Certification

The Certified Information Systems Security Professional (CISSP) is an independent vendor neutral qualification governed and granted by International Information Systems Security Certifications Consortium (ISC)2 . A group founded in 1988 by a few industry associations. The goal was to standardize the knowledge and skills required in information security industry. The group after a series of brainstorming meetings finalized the curriculum popularly known as Common Body of Knowledge (CBK) and then in 1994 the CISSP certification was launched. Since its inception the CISSP certification has gained much deserved respect of people and industry and it is evidenced by the fact that the CISSP became the first certification in the industry to receive ANSI accreditation for ISO 17024 international standard.

Importance of CISSP Certification

After ANSI accreditation, the CISSP certification gained more reputation and recognition in the industry and many organizations started to make CISSP a requirement for certain job positions. Currently there are more than 75,000 certified professionals most holding good positions in industry. CISSP is not just another security certification, it is considered a gold standard of information

security. CISSP is also formally approved by the U.S. Department of Defense in both their information assurance technical (IAT) and information assurance managerial (IAM) categories for their DoD directive 8570. According to my experience, once you obtain your CISSP you stand out from the crowd and people do not ask much to test you during your interview. They are more confident in their selection of hiring you.

The CISSP Exam Pattern

The CISSP exam tests your knowledge on concepts, standards and best practices. The exam is very generic and is not focused on a particular country, industry or an organization.

The exam does not test your language skills. Sometimes the english speaking people find it a little difficult to adjust themselves with the way the questions are written. English is a very flexible language, the British english is quite different from American and the same exam is written for all, so don't go deep into the meaning of words and grammar used in questions. Some of the questions are quite tricky, the correct answer to a question may be a wrong answer to some other question. You need to read the entire question and all options carefully, do not just guess the right answer, but evaluate each option why it is not correct. With some questions you will be able to eliminate three wrong options, so the remaining is right even if you do not know the answer otherwise. With some questions you will end up with some confusion over two possible choices. Here you need to be careful. Remember the exam is not written for your organization so how you actually work in your organization may not be the best practice. Also all true statements are not right answers to a question. This is a management level exam, think at a higher level. Many questions use FIRST, LAST, EXCEPT and NOT words so be careful while answering such questions.

Remember the CISSP exam is:

- Truly international, not specific to any country
- Vendor Neutral, does not cover any product knowledge
- Not specific to any particular industry
- Not specific to your organization or any other organization
- Not specific to your way of thinking or your style of working

What material you should use to prepare for exam

In my opinion the best book is Official (ISC)2 Guide to the CISSP CBK. While studying for exam I followed this book and was able to crack the exam in my first attempt. Most of my students also (as I recommend them) study only this book and are able to clear the exam.

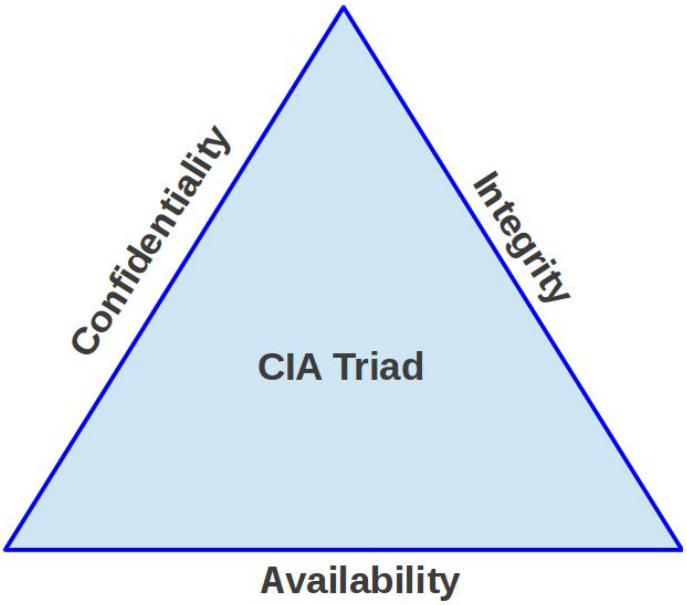
To evaluate your preparation go for The (ISC)2 Self-Assessment Tool (StudiScope). The questions here are as per exam standard. No other question bank I tried so far, available on internet whether free or paid, are even close to the exam standard. Believe me I have tried many.

In my opinion the CISSP exam is not difficult at all, people find it difficult because they were not prepared when they appeared. And the key is the right material, if you use right material to prepare yourself for the exam, nothing can go wrong. There are thousands of CISSP certified professionals, if they passed you can also.

What are important topics for the exam

Confidentiality, integrity and availability are considered core principles of information security. It is popularly known as the CIA triad (see figure 2). It is essential to understand how a particular topic fits into this CIA triad.

I would like to list the important topics domain-wise. Important to note the exam is not limited to the topics I mention here and you cannot afford to limit yourself on these topics. But yes these are most important, don't even think of skipping any of them.



Domain 1: Access Control Access control principles Information classification benefits access control categories User identification guidelines Authentication methods Biometric accuracy Identity management Single sign-on Kerberos SESAME Discretionary access control Mandatory access control Role based access control Intrusion detection and intrusion prevention system Threats

Domain 2: Software Development Security Compiled language vs Interpreted language Buffer overflow Covert channel Mobile code TOC/TOU SDLC Various tests like unit test, integration test, etc. Java security Polymorphism Polyinstantiation Object oriented security Security Kernel Processor privilege states Memory protection Change management Configuration management Malware protection Relational database management model Metadata Database vulnerabilities and threats Knowledge discovery in database

Domain 3: Business Continuity and Disaster Recovery Planning Project initiation and management steps Prudent man rule Business impact analysis Recovery time objective Recovery point objective Maximum tolerable downtime Recovery strategy Hot, warm and cold site Test exercises

Domain 4: Cryptography Link vs End-to-end encryption Stream vs block cipher One time pad Advantages and disadvantages of symmetric encryption Advantages and disadvantages of asymmetric encryption Confidential message Open messaage Confidential message with proof of origin RSA vs ECC MAC vs Digital signature M of N principle PKI concepts IPSEC SSL

Domain 5: Information Security Governance and Risk Management Policies, Standards, Procedures, Baselines and Guidelines Security policy best practices Policy types Best practices Role of security officer, data owner and data custodian Risk management Qualitative vs Quantitative risk assessment Risk management principles

Domain 6: Legal, Regulations, Investigations, and Compliance Intellectual property law Privacy Monitoring Incident response Digital investigation

Domain 7: Operations Security Redundancy and fault tolerance Problem management Change management Configuration management Patch management Object reuse

Domain 8: Physical (Environmental) Security CPTED Perimeter intrusion detection Key control Types of glass Glass break sensors Interior intrusion detection Fire detection Fire classes Fire suppression

Domain 9: Security Architecture and Design Types of security models Examples of security models Evaluation criteria System access control mechanisms Secure memory management Processor states Layering Process isolation

Domain 10: Telecommunications and Network Security OSI reference model TCP/IP model All threats and vulnerabilities like DoS, sniffing, etc Common services like IPSEC, wireless, DNS, etc Emerging technologies like MPLS, SEM/SEIM, etc What is never asked in the exam The following things are not targeted in CISSP exam: Any law specific to a country In-depth knowledge of any product Any regulation specific to an industry In-depth knowledge on how a technology works (beyond concepts)

My personal experience

Initially when I planned to write the CISSP exam I bought the *Official (ISC)2 Guide to the CISSP CBK* and started reading from chapter 1. After a few pages I found I started to lose my interest as it was all theory and so far I used to learn the things by experimenting. You won't believe it took me nearly two months to finish just the first chapter. Then I gave a second thought whether I should do this exam or not as I was thinking it is going to take more than a year that way. But I was very keen to obtain this gold standard certification. When re-evaluated I realized I was going too slow because I didn't have the target date to prepare myself for the exam. In my opinion the task with no defined end date just becomes never ending when one has to do hard work to complete it [in short man is a lazy animal :-)]. So I quickly re-energized myself and booked the exam scheduled after nearly 4 months. And I think I made the right decision. This accelerated my learning and I was able to finish the whole book in less than 3 months with spending just 3-5 hours per day after I came back from office. I made a quick review of the book in about a week and started finding some good question banks on internet. And that was a big mistake I feel. I had totally lost my confidence that I can pass as those questions were expecting me to remember everything from the book from security architectures to various laws and ethics statements. I was about to re-schedule my exam before I tried the The (ISC)2 Self-Assessment Tool (StudiScope). My exam as well as all study tools were sponsored by my company and I quickly got approval to purchase the official assessment tool. I attempted the assessment test 2 days after and I scored 88% in my first attempt. I was much relaxed. I spent rest of the time in just reviewing the book and attempted these assessments.

Exam Day Experience: I was quite nervous but at the other side, the assessment tool had helped me gain confidence for the exam. Finally the exam clock started and I swiftly started marking my response for questions one by one. I found whenever I get a questions I was not sure about I tend to get more nervous. Soon I started skipping such question and marked them for later review. The rest of the exam with this strategy just went perfect. After finishing all questions I came to marked ones and in the second time I was able to answer few of them just straight away. Rest I just guessed.

When finished six hours were almost passed. I think I was lucky I didn't spent too much time on questions I was not sure about, doing this I would have left some questions unanswered. The same happened with the middle-east guy who was sitting next to me. He could not answer approx 40 questions because of time.

I guide my students to monitor the time they spend on each question while doing assessment tests. Going too slow will leave less time and more questions in the end. Going too fast means you are not spending the required time to understand the question and evaluate each answer. Avoid both as much as you can.

Some sample questions

1. Which of the following ensures that the application's hardware remain highly available?
    a. Disk Mirroring
    b. Clustering
    c. RAI
    d. RAIT
2. What is the advantage of digital signatures over message authentication codes?
    a. Digital signature provides integrity verification while message authentication code can not
    b. Digital signature provides confidentiality while message authentication code can not
    c. Digital signature provides authenticity while message authentication code can not
    d. Digital signature works faster than message authentication codes
3. What is not secured in end-to-end encryption?
    a. Packet payload
    b. Public key
    c. Packet header
    d. Private key
4. When due diligence and due care is observed it is said to be:

a. Prudent person rule
b. Proactive approach
c. Negligence
d. Reactive approach

5. Which of the following algorithms can be used for Kerberos encryption

a. DSA
b. RSA
c. DES
d. ECC

6. Which of the following provide isolation between subjects and objects?

a. Reference monitor kernel
b. Security monitor kernel
c. Trusted computing base
d. Security kernel

7. What is the purpose of using Secure Hash Algorithm in virtual private networks?

a. Authentication
b. Key validation
c. Integrity
d. Encryption

8. Which of the following documents has optional statements?

a. Policy
b. Regulation
c. Baseline
d. Guideline

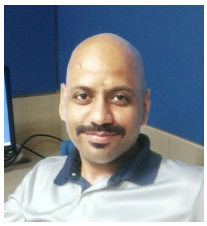
9. Which of the following glass type you will use for windows opening at street level

a. Tempered glass
b. Wired glass
c. Laminated glass
d. Bullet resistant glass

10. If an IDS runs a script on firewall to block an attacking address, what type of control it is?

a. Corrective
b. Preventive
c. Detective
d. Compensating

About the author



Rahul Kokcha (Technical Manager - Information Security at Koenig Solutions Limited) is an experienced instructor of CISSP. He has trained professionals from over 35 countries. He has earned various international titles to his name like CISSP, Chartered IT Professional (CITP), MBCS and MIET, apart from various IT certifications. Having more than a decade of experience in consulting and training, Rahul specializes in InfoSec domain with his wide range of experience.