SYNGRESS

CISSP Study Guide

2E

Eric Conrad • Seth Misenar • Joshua Feldman

- Pass the exam the first time
- Filled with exercises, real-world examples, questions, and answers

CISSP® Study Guide

Second Edition

Eric Conrad
Seth Misenar
Joshua Feldman

Technical Editor

Kevin Riggins

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS.

Table of Contents

Copyright

Acquiring Editor: Chris Katsaropoulos

Development Editor: Heather Scherer

Project Manager: Paul Gottehrer

Designer: Joanne Blank

Syngress is an imprint of Elsevier

225 Wyman Street, Waltham, MA 02451, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Application submitted

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

For information on all Syngress publications visit our website at http://store.elsevier.com

ISBN: 978-1-59749-961-3

Printed in the United States of America

12 13 14 15 16 10 9 8 7 6 5 4 3 2 1

Acknowledgments

Eric Conrad: I need to first thank my wife, Melissa, and my children, Eric and Emma, f their love and patience while I wrote this book. Thank you to the contributing authors ar my friends Joshua Feldman and Seth Misenar.

Thank you to my teachers and mentors: Thank you, Miss Gilmore, for sending me on m way. Thank you, Dave Curado and Beef Mazzola, for showing me the right way to do i Thank you, Stephen Northcutt, Alan Paller, Deb Jorgensen, Scott Weil, Eric Cole, Ed Skoudi Johannes Ullrich, Mike Poor, Ted Demopoulos, Jason Fossen, Kevin Johnson, John Stran Jonathan Ham, and many others from the SANS Institute, for showing me how to take it the next level.

I would like to thank the supergroup of information security professionals who answere my last-minute call and collectively wrote the 500 questions comprising the two sets online practice exams: Rodney Caudle, David Crafts, Bruce Diamond, Jason Fowler, Phil Keibler, Warren Mack, Eric Mattingly, Ron Reidy, Mike Saurbaugh, and Gary Whitsett.

Seth Misenar: I would like to thank my wife, Rachel, the love of my life, who showe continued patience, support, and strength while entertaining two young children through this writing process. I am grateful to my children, Jude and Hazel, who, at 3 and 0, we amazingly gracious when Daddy had to write. And I count myself lucky to have suc wonderful parents, Bob and Jeanine, who, as always, provided much of their time to ensu that my family was taken care of during this writing period."

About the authors

Lead Author

Eric Conrad (CISSP®, GIAC GSE, GPEN, GCIH, GCIA, GCFA, GAWN, GSEC, CompTIA CAS and Security +) is a SANS Certified Instructor and president of Backshore Communication which provides information warfare, penetration testing, incident handling, and intrusio detection consulting services. Eric started his professional career in 1991 as a UNIX® systen administrator for a small oceanographic communications company. He gained informatio security experience in a variety of industries, including research, education, power, Interne and health care, in roles ranging from systems programmer to security engineer to HIPA security officer and ISSO. He has taught thousands of students in courses including SAN Management 414: CISSP®; Security 560: Network Penetration Testing and Ethical Hackin and Security 504: Hacker Techniques, Exploits, and Incident Handling. Eric is a graduate the SANS Technology Institute with a Master of Science degree in Information Securit Engineering. His earned his Bachelor of Arts in English from Bridgewater State College. Er lives in Peaks Island, Maine, with his family, Melissa, Eric, and Emma. His website http://ericconrad.com.

Contributing Authors

Seth Misenar (CISSP®, GIAC GSE, GPEN, GCIH, GCIA, GCFA, GWAPT, GCWN, GSE MCSE, MCDBA, and CompTIA CASP) is a Certified Instructor with the SANS Institute and als serves as lead consultant for Jackson, Mississippi-based Context Security. Seth's backgroun includes security research, network and Web application penetration testing, vulnerabilit assessment, regulatory compliance efforts, security architecture design, and general securit consulting. He has previously served as a physical and network security consultant fo Fortune 100 companies as well as the HIPAA and information security officer for a sta government agency. Seth teaches a variety of courses for the SANS Institute, includin Security Essentials, Web Application Penetration Testing, Hacker Techniques, and the CISSP course. Seth is pursuing a Master of Science degree in Information Security Engineering fro the SANS Technology Institute and holds a Bachelor of Science degree from Millsaps Colleg Seth resides in Jackson, Mississippi, with his family, Rachel, Jude, and Hazel.

Joshua Feldman (CISSP®, NSA IAM) supports the Department of Defense Informatio Systems Agency (DISA), Field Security Operations (FSO), as a contractor working for SAI Inc. Since 2002, he has been a subject matter expert and training developer for DISA's cybe security mission. During his tenure, he contributed to the DoD 8500 series, specifical conducting research and authoring sections of the DoD 8570.01-M, also known as the DoD I Workforce Improvement Program. He has taught well over 1000 DoD students through h "DoD IA Boot Camp" course. He has contributed to many of the DISA-sponsored cybe security training programs, ranging from computer network defense to the basic cybe security awareness course taken by users throughout the DoD. He is a regular presenter an panel member at the Information Assurance Symposium hosted by both DISA and NSA Before joining the support team at DoD/DISA, Joshua spent time as an IT security engineer the Department of State, Diplomatic Security. There, he traveled to embassies worldwide t conduct Tiger Team assessments of the security of each embassy. Joshua got his start in th IT security field when he left his position teaching science for Montgomery County Publ Schools in Maryland and went to work for NFR Security Software. At the time, NFR was on of the leading companies producing network intrusion detection systems.

About the Technical Editor

Kevin Riggins (CISSP®) has over 22 years of experience in information technology and ha focused on information security since 1999. He has been a Certified Information System Security Professional since 2004 and currently works for a Fortune 500 financial servic company, where he leads a team of information security analysts responsible for intern consulting, risk assessments, and vendor security reviews. He writes about variou information security topics on his blog, Infosec Rambling (http://www.infosecramblings.com), his articles have been published in *(IN)Secure* magazin and he is a frequent speaker at conference and industry association meetings.

Chapter 1

Introduction

Exam objectives in this chapter

- How to Prepare for the Exam
- How to Take the Exam
- Good Luck!

This book is born out of real-world information security industry experience. The authors o this book have held the titles of systems administrator, systems programmer, networ engineer/security engineer, security director, HIPAA security officer, ISSO, securit consultant, instructor, and others.

This book is also born out of real-world instruction. We have logged countless road mil teaching information security classes to professionals around the world. We have taug thousands of students in hundreds of classes, both physically on most of the continents a well as online. Classes include CISSP®, of course, but also penetration testing, securit essentials, hacker techniques, and information assurance boot camps, among others.

Good instructors know that students have spent time and money to be with them, and tim can be the most precious. We respect our students and their time; we do not waste it. W teach our students what they need to know, and we do so as efficiently as possible.

This book is also a reaction to other books on the same subject. As the years have passe the page counts of other books have grown, often exceeding 1000 pages. As Larry Wall on said, “There is more than one way to do it.”[1] Our experience tells us that there is anoth way. If we can teach someone with the proper experience how to pass the CISSP exam in a day boot camp, is a 1000-page CISSP book really necessary?

We asked ourselves: What can we do that has not been done before? What can we d better or differently? Can we write a shorter book that gets to the point, respects ou students’ time, and allows them to pass the exam?

We believe the answer is yes, and you are reading the result. We know what is importan and we will not waste your time. We have taken William Strunk’s advice to “omit needle words”[2] to heart. It is our mantra.

This book teaches you what you need to know and does so as concisely as possible.

How to Prepare for the Exam

Read this book, and understand it: all of it. If we cover a subject in this book, we are doing s because it is testable (unless noted otherwise). The exam is designed to test you understanding of the Common Body of Knowledge (CBK), which may be thought of as th universal language of information security professionals. It is said to be "a mile wide and tw inches deep." Formal terminology is critical: Pay attention to it.

The Common Body of Knowledge is updated occasionally, most recently in January 201 This book has been updated to fully reflect the 2012 CBK. The (ISC)$^{2®}$ Candidate Informatio Bulletin (CIB) describes the current version of the exam; downloading and reading the CIB a great exam preparation step. You may download it fro https://www.isc2.org/cib/Default.aspx.

Learn the acronyms in this book and the words they represent, backward and forwar Both the glossary and index of this book are highly detailed and map from acronym to nam We did this because it is logical for a technical book and also to get you into the habit understanding acronyms forward and backward.

Much of the exam question language can appear unclear at times. Formal terms from th Common Body of Knowledge can act as beacons to lead you through the more difficu questions, highlighting the words in the questions that really matter.

The CISSP exam is a management exam

Never forget that the CISSP exam is a management exam. Answer all questions as a information security manager would. Many questions are fuzzy and provide limite background; when asked for the best answer, you may think, "It depends."

Think and answer like a manager. Suppose the exam states that you are concerned wi network exploitation. If you are a professional penetration tester, you may wonder wheth you are trying to launch an exploit or mitigate one. What does "concerned" mean? Your CS is probably trying to mitigate network exploitation, and that is how you should answer on th exam.

The notes card approach

As you are studying, keep a "notes card" file for highly specific information that does n lend itself to immediate retention. A notes card is simply a text file (you can create it with simple editor such as WordPad) that contains a condensed list of detailed information.

Populate your notes card file with any detailed information (which you do not alread

know from previous experience) that is important for the exam, such as the five levels of th Software Capability Maturity Model (CMM; covered in Chapter 5, Domain 4: Softwa Development Security), or the ITSEC and Common Criteria levels (covered in Chapter Domain 6: Security Architecture and Design).

The goal of the notes card file is to avoid getting lost in the "weeds," drowning in specif information that is difficult to retain on first sight. Keep your studies focused on co concepts, and copy specific details to the notes card file. When you are done, print the file. A your exam date nears, study your notes card file more closely. In the days before your exa really focus on those details.

Practice tests

Quizzing can be the best way to gauge your understanding of this material and your readine to take the exam. A wrong answer on a test question acts as a laser beam showing you wh you know and, more importantly, what you do not know. Each chapter in this book has 1 practice test questions at the end, ranging from easy to medium to hard. The Self Te Appendix includes explanations for all correct and incorrect answers; these explanations a designed to help you understand why the answers you chose were marked correct incorrect. This book's companion website is located http://booksite.syngress.com/companion/Conrad. It contains 500 questions writte specifically for this book—two full practice exams. Use them. The companion site als contains 10 podcasts, each providing an overview of one of the ten domains of knowledge.

You should aim for at least 80% correct answers on any practice test. The real exa requires 700 out of 1000 points, but achieving over 80% correct on practice tests will giv you some margin for error. Take these quizzes closed book, just as you will take the re exam. Pay careful attention to any wrong answers, and be sure to reread the relevant sectio of this book. Identify any weaker domains (we all have them)—those domains where yo consistently get more wrong answers than in others—and then focus your studies on thos weak areas.

Time yourself while taking any practice exam. Aim to answer at a rate of at least on question per minute. You need to move faster than true exam pace because the actual exa questions may be more difficult and therefore take more time. If you are taking longer tha that, practice more to improve your speed. Time management is critical on the exam, an running out of time usually equals failure.

Read the glossary

As you wrap up your studies, quickly read through the glossary toward the back of this boo It has over 1000 entries and is highly detailed by design. The glossary definitions should a be familiar concepts to you at this point.

If you see a glossary definition that is not clear or obvious to you, go back to the chapter is based on and reread that material. Ask yourself, "Do I understand this concept enough answer a question about it?"

Readiness checklist

These steps will serve as a readiness checklist as you near the exam day. If you remember think like a manager, are consistently scoring over 80% on practice tests, are answerin practice questions quickly, understand all glossary terms, and perform a final thorough rea through of your notes card, you are ready to go.

Taking the Exam

The CISSP exam was traditionally taken via paper-based testing: old-school paper and penc This has now changed to computer-based testing (CBT), which we will discuss shortly.

The exam has 250 questions and a 6-hour time limit. Six hours sounds like a long tim until you do the math: 250 questions in 360 minutes leaves less than a minute and a half answer each question. The exam is long and can be grueling; it is also a race against tim Preparation is the key to success.

Steps to becoming a CISSP

Becoming a CISSP requires four steps:

1. Proper professional information security experience
2. Agreeing to the $(ISC)^2$ code of ethics
3. Passing the CISSP exam
4. Endorsement by another CISSP

Additional details are available on the examination registration form available www.isc2.org.

The exam currently requires 5 years of professional experience in 2 or more of the 1 domains of knowledge. Those domains are covered in Chapters 2 to 11 of this book. You ma waive 1 year with a college degree or approved certification; see the examination registratio form for more information.

You may pass the exam before you have enough professional experience and become a Associate of (ISC)^2. Once you meet the experience requirement, you can then complete th process and become a CISSP.

The (ISC)^2 code of ethics is discussed in Chapter 10, Domain 9: Legal, Regulation Investigations, and Compliance.

Passing the exam is discussed in the "How to Take the Exam" section below, and we discu endorsement in the "After the Exam" section, also below.

Computer-based testing (CBT)

(ISC)^2 has partnered with Pearson VUE (http:// http://www.pearsonvue.com/) to provic computer-based testing (CBT). Pearson VUE has testing centers located in over 160 countri around the world; go to their website to schedule your exam. The transition to compute based testing began on June 1, 2012. Paper exams will have only limited availability: "Aft September 1, 2012, exams will be offered via CBT only, except for candidates located areas outside of a 75-mile radius from an approved testing center and on a case-by-ca basis."[3]

According to (ISC)^2, "Most candidates will receive their results immediately after they hav completed the exam. In some cases, candidates may have to wait longer to receive offici results."[4] (ISC)^2 reports that, with regard to CBT, "It usually takes less time to comple the test; however, candidates are given exactly the same amount of time to complete th exam via CBT or paper and pencil."[5] See https://www.isc2.org/cbt-faqs.aspx for mo information about (ISC)^2 CBT. Note that information regarding CBT is subject to change, s please check the (ISC)^2 website for any updates to the exam, including the CBT process.

Pearson VUE's (ISC)^2 website is http://www.pearsonvue.com/isc2/. It includes usef resources, including the "Pearson VUE Testing Tutorial and Practice Exam" a Microsoft Windows® application that allows candidates to try out a demo exam, explore functionalit test the "Flag for Review" function, etc. This can help reduce exam-day jitters, and familiari with the software can also increase your test-taking speed.

How to take the exam

The exam has 250 multiple-choice questions with four possible answers: A, B, C, or D. Eac question has one correct answer. A blank answer is a wrong answer, so guessing does not hu you. At the end of your exam, all 250 questions should have one answer chosen.

The questions will be mixed from the ten domains, but the questions do not (overtly) sta the domain on which they are based. There are 25 research questions (10% of the exam) th

do not count toward your final score. These questions are not marked; you must answer a 250 questions as if they count.

Scan all questions for the key words, including formal Common Body of Knowledge term Acronyms are your friend: You can identify them quickly, and they are often important (they are formal terms). Many words may be "junk" words, placed there to potentiall confuse you. Ignore them. Pay careful attention to small words that may be important, suc as "not."

The two-pass method

There are two successful methods for taking the exam: the two-pass method and the thre pass method. Both begin the same way.

Pass one

Answer all questions that you can answer quickly (e.g., in less than 2 minutes). You do n need to watch the clock; your mind's internal clock will tell you roughly when you have bee stuck on a question longer than that. If you are close to determining an answer, stick with i If not, skip the question (or provide a quick answer), and flag the question for later reviev This helps manage time. You do not want to run out of time (e.g., missing the last 1 questions because you spent 20 minutes stuck on question 77).

Pass two

Ideally, you will have time left after pass one. Go back over any flagged questions an answer them all. When you complete pass two, all 250 questions will be answered.

Pass two provides a number of benefits, beyond time management. Anyone who has bee stuck on a crossword puzzle, put it down for 20 minutes, and picked it up to have answe suddenly appear obvious understands the power of the human mind's background processe Our minds seem to chew on information, even as we are not consciously aware of th happening. Use this to your advantage.

A second benefit is the occasional "covert channel" that may exist between questions on th exam. Question 132 asks you what port a Secure Shell (SSH) daemon listens on, for exampl and you do not know the answer, but then question 204 describes a scenario that mentio SSH runs on TCP port 22. Question 132 is now answered. This signaling of information w not necessarily be that obvious, but you can often infer information about one answer base on a different question; use this to your advantage.

The three-pass method

During the optional (and controversial) third pass, recheck all your answers, ensuring yo understood and answered the question properly. This is to catch mistakes such as missing keyword. Suppose, for example, that when you read the question "Which of the followi physical devices is not a recommended preventive control?" you missed the word "not." Yo answered the question on the wrong premise, and gave a recommended device (like a lock when you should have done the opposite and recommended a detective device such as close circuit television (CCTV).

The third pass is designed to catch those mistakes. This method is controversial becaus people often second-guess themselves and change answers to questions they proper understood. Your first instinct is usually your best: If you use the third-pass method, avo changing these kinds of answers.

After the exam

If you pass, you will not know your score; if you fail, you will receive your score, as well a a rating of domains from strongest to weakest. If you do fail, use that list to hone you studies, focusing on your weak domains, then retake the exam. Do not let a setback like th prevent you from reaching your goal. We all suffer adversity in our lives. How we respond what is really important. The current retake policy of the exam is as follows: "From the da of the candidate's first exam attempt, candidates must wait 30 days to retake the exam. Fro the date of the second attempt, candidates must wait 90 days to retake the exam. From th date of the third attempt, candidates must wait 180 days from the date of the third attem to retake the exam."[6]

Once you pass the exam, you will need to be endorsed by another CISSP before earning th title CISSP; $(ISC)^2$ will explain this process to you in the email they send with your passi results.

Good Luck!

We live in an increasingly certified world, and information security is growing into a fu profession. Becoming a CISSP can provide tremendous career benefits, as it has for th authors' team.

The exam is not easy, but worthwhile things rarely are. Investing in an appreciating asset always a good idea, as you are investing in yourself. Good luck; we look forward welcoming you to the club!

REFERENCES

1. Well L. *Perl, the First Postmodern Computer Language*. presented at Linux World *http://www.wall.org/~larry/pm.html*; 1999; March 3.

2. Strunk W. *Elements of Style*. private printing. Ithaca, NY 1918.

3. (ISC)2. *Frequently Asked Questions about Computer-Based Testing: A Faster, More Efficient Way to Get Certified*. Vienna, VA *https://www.isc2.org/cbt-faqs.aspx*; 2012.

4. Ibid.

5. Ibid.

6. Ibid.

Chapter 2

Domain 1

Access Control

Exam objectives in this chapter

- Cornerstone Information Security Concepts
- Access Control Models
- Procedural Issues for Access Control
- Access Control Defensive Categories and Types
- Authentication Methods
- Access Control Technologies
- Types of Attackers
- Assessing Access Control

Unique Terms and Definitions

- *Subject*—An active entity on an information system.
- *Object*—A passive data file.
- *Discretionary Access Control (DAC)*—Gives subjects full control of objects they have bee given access to, including sharing the objects with other subjects.
- *Mandatory Access Control (MAC)*—System-enforced access control based on subject clearances and object's labels.
- *Role-Based Access Control (RBAC)*—Subjects are grouped into roles, and each defined ro has access permissions based upon the role, not the individual.

Introduction

Access control is the basis for all security disciplines, not just IT security. The purpose access control is to allow authorized users access to appropriate data and deny access unauthorized users. Seems simple, right? It would be easy to completely lock a system dow to allow just predefined actions with no room for leeway. In fact, many organization including the U.S. military, are doing just that—restricting the access users have to systems a very small functional capability. However, with increasing dependence on the Internet perform work, systems must be flexible enough to be able to run a wide variety of softwa

that is not centrally controlled.

Another concern that impacts access control is the dependence on antiquated (also know as *legacy*) software applications. Large IT infrastructures (such as the U.S. military) may ru mission-dependent applications that are over 10 years old! The cost of replacing these legac applications is often too large for the organization to complete in one funding cycle. I professionals must often manage security while running insecure legacy applications th introduce access control risks.

One thing is certain: With the dependence on IT as a means of doing business, and acce control as one of the first lines of defense, understanding how to properly implement acce controls has become vital in the quest for secure communications.

Exam Warning

As we will discuss in Chapter 4, Domain 3: Information Security Governance and Risk Management, the mission an purpose of access control is to protect the confidentiality, integrity, and availability of data.

Access controls protect against threats such as unauthorized access, inappropria modification of data, and loss of confidentiality. Access control is performed by implementi strong technical, physical, and administrative measures. This chapter focuses on the technic and administrative aspects of access control; physical security is addressed in Chapter 1 Domain 10: Physical (Environmental) Security. Remember that physical security is implicit most other security controls, including access control.

Note

In 2006, thieves broke into a well-known U.S. military contracting company's accounting department office building. Th thieves did not steal valuable items such as computer flatscreen monitors, small electronic devices (MP3 players, phones etc.), or laptop computers from the office. Instead, they targeted and stole just one thing: the hard drives from the employe benefits database. At the time, this database held not only the employees' personally identifiable information (PII), such a Social Security numbers, home addresses, birthdays, etc., but also their stock portfolio vesting shares in the company retirement plan and employee stock ownership program. Access control to the data was now compromised, not through sophisticated online spear phishing attack but by a group of thieves. This is a classic example of how physical securit impacts data access controls.

Cornerstone Information Security Concepts

Before we can explain access control we must define cornerstone information securi concepts. These concepts provide the foundation upon which the ten domains of the Commo