Common Body of Knowledge Review Guide

This guide is designed to help you prepare for the CISSP Exam. It gives you some background, points the way to study material, provides some study strategy, and imparts some Exam-taking tips. This Guide is for we mortals with too little time to study and too many other things with which to occupy our minds, like work and family. It gives the reader the benefit of our corporate experience with the Exam. Unfortunately, we are ethically bound not to talk about the Exam's specific content. There's one last thing here. The CISSP designation is unique in that it requires more than the demonstrable knowledge of a body of information. It indicates that the holder is able to integrate cyber security knowledge into the greater worlds of IT and the overall organization.

Background:

First off, you need to know about the International Information Systems Security Certifications Consortium, Inc. (ISC² or ISC^2). They're a global, not-for-profit organization dedicated to maintaining a Common Body of Knowledge (CBK) for Information Security (IS), certifying industry professionals and practitioners in an international IS standard, administering training and certification examinations, and ensuring credentials are maintained, primarily through continuing education. Their homepage is http://www.isc2.org/.

When you go there, you will learn that you must to be able to demonstrate at least five years experience in at least one of the ten information security "Domains" that constitute what ISC^2 refers to as the CBK. You must also ascribe, by signature, to the ISC^2 Code of Ethical Behavior.

Once you have all that out of the way, all that is left is to pass the Exam! The process is mapped out for you when you decide to begin the process.

- The Exam is 250 well-researched multiple-choice questions.
- Each question is required to be founded on at least two references from the body of recognized literature. (We'll get into the references later.)
- No acronyms are used in the Exam without being spelled out.
- All ten Domains are represented in the Exam, but the questions are not distributed evenly across the Domains. The questions go through a rigorous process before being placed in the Exam.
- here is no extra penalty for wrong answers. (Wrong answers are not subtracted from the right answers.) You need to get 700 "points" out of a possible 1000 to pass. ISC^2 applies some statistical sorcery to the scores to ensure Exam batch-to-batch equivalence. That's right, it's a "curve". They say the questions themselves are not weighted. In the end, it's a distinction without a difference.
- The folks on either side of you will be taking the same test, but the order of their questions will be different. You will have six hours to complete the Exam. The Exam questions force you to read them carefully and consider context.

- There are 25 new questions on the Exam that are being researched for inclusion on the test but are not graded. You won't know which ones, though.
- You should understand that while the CBK is a learnable stack-o'-facts, the Exam tests your in-depth knowledge and your ability to integrate knowledge and experience, not your ability to memorize those facts.
- Experience pays off. So does a calm approach on Exam day.

Study Strategy:

- There is a lot to know and you should use the "Eating an Elephant" technique…one bite at a time with time to digest between bites. Note again the emphasis on time. Give yourself plenty of it.

- Regiment yourself. Announce the date you're taking the test to your friends, family, and colleagues. This will intensify the pressure and help you keep on track.

- Begin by reviewing ISC^2's CBK Study Guide. This gives you an unambiguous list of the stack-o'-facts you need to know. Unfortunately, there is no "meat" on those bones! Not a scrap. You have to go forth and find the "meat". Read on.

- Next have a look at ISC^2's reference list. After looking this list over, you have two choices, 1) curl up in a fetal position and cry or 2) start focusing in on those references you realistically have time to absorb. Here is where the materials cited below will help you narrow the field. Speaking of which, consider carefully those materials cited in the Materials and References section. These are the items that your colleagues found to be helpful.

- Attack the Domains one at a time, remembering that you will want to review the material. Remember to make time for review.

- Assemble the material reflecting each Domain in turn.

- Read, review, and repeat. Repetition and review are good.

- You know how you best learn new material (e.g., auditory, visual, kinetic). Use those techniques that help you learn. For example, if you are an auditory learner, get into a CISSP prep class. If you are visual, read. If you are kinetic, write everything down.

- Did we mention that review is good?

- Identify those non-security areas in which you need deeper knowledge and get up to speed on them. We can't tell you what to study here, but you'll see your technical knowledge gaps as you study.

- Identify those security areas where you need additional help. Focus on them.

- Don't get yourself wound around the axle of thinking you need to know everything about everything, like *elliptic curves* or *derivation of the factors of the product of large prime numbers*. Just learn the words and be able to associate them with concepts, like (in this case) keystream generation. As you look over the "test" Exam questions, you'll see what we're getting at.

- Talk to people! Every organization has an expert or so in any security subject area you could imagine. Join the listed focus groups. (Somebody out there can tell you how a *discrete logarithm in a finite field* relates to cryptographic keystreams or the price of tea in China.)

Study Materials and Resources:

First, go to the ISC^2 homepage and order a Study Guide. It's free, but they want you to order one on-line and they don't want you sharing it. This is your road map for the security CBK.

Arm yourself with some of the more helpful texts. The authors of this document found these books to be helpful:

- The CISSP Prep Guide, Wiley Press, R.L. Krutz and R.D. Vines. After looking over the ISC^2 Study Guide, consider reading through one of these prep guidebooks. This one is concise and gives you the first layer of "meat". It also shows you where you need additional material.

- CISSP Exam Cram, Coriolis Press, Mandy Andress. This, too, could serve as your second-level study guide after the ISC^2 Study Guide. This book covers the same material as the Prep Guide, but there's not quite as much "meat". Again, it shows you where you're weak.

- The classic text is Information Security Management Handbook (Fourth Edition) edited by Micki Krause and Harold F. Tipton and from the CRC Press/Auerbach Publications. This is a loose compilation of essays and such. Although lots of the CBK seems to stem from this book, not everyone agrees that it's all that great in the completeness realm.

- If you can get hold of a copy, look at CISSP Examination Textbooks (Two Volumes) by S. R. Vallabhaneni at SRV Professional Publications. Folks have had lots of different opinions about these, too.

The reader is fortunate that there are now lots of books hitting the CISSP marketplace. Just go to a bookseller of your choice (e.g., Amazon) and search on "CISSP".

The Web is a fantastic source for material. Unfortunately, there's also lots of junk, so focus on the good stuff. A search with the "CISSP" key word will cough up lots of material. In addition, a search on the Domain titles will uncover lots of material, too. Just remember that not everything out there applies to your particular task of passing the Exam. Here are some of the better Web sources:

- CCECURE is a great resource. They are now compiling a series of Open Study Guides (OSG), one for each Domain. The good news is that their Access Control, Telecommunications and Network, and Applications and Systems Development Domain texts are said to be among the best sources in the business. The bad news is that the remaining seven Domains are very much works in progress. In addition to their OSG Guides, they have lots of other security study material. The price is right, too.

- Of course ISC^2 is at http://www.isc2.org/ and is a "gotta-have". There is no study material there, but there are references to lots of it. They also host a series of preparation courses.

- Although it caters to those already CISSPed, http://www.cissps.com/, provides pointers to some learning material.

- There is an Internet CISSP Study Group hosted by SecurityFocus. You can post questions there or just lurk and listen.

Exam-Taking Tips:

- Enter the Exam room as rested and relaxed as possible. Forget about last minute cramming. Passing the CISSP Exam depends on in-depth understanding. Cramming the night before won't help you. Rest will.

- Pay attention to the Exam Proctors. ISC^2 is serious about the security of the Exam and the testing environment, so expect a great deal of regimentation and scrutiny. If you break their rules, you're out of there, so listen carefully.

- Study the questions carefully. No word is wasted. Every word is important. Remember that the "easy" questions might have a nuance you are not expecting. Remember also, these questions are highly researched. Every word in the question is there for a reason. On the flip side, try not to read into a question a meaning or context that is not literally in the question. Us "Old-Timers" do this sometimes.

- Look closely for key words, especially NOT, NEVER, ALWAYS, FIRST, and BEST.

- Think the "big picture". Look for the most universal or general choice in a list of all right answers. (Yeah, they do that to you!)

- Answer the questions on the answer sheet with a light mark so you can easily erase it if you change your mind. After you finish making all your choices, go back and darken them in. Don't forget that last bit!

- Answer all the easy questions in order as you go down the list.

- Go back and attack the "hard" questions. Try to eliminate the obviously wrong choices. Every choice you eliminate works in your favor. If you just don't know, guess. Your chance of getting it right is 25% (there are always four choices), even better if you can throw out any obviously wrong choices.

- Stop and stretch occasionally. Have a snack. Take a bio-break.

Parting Words:

There are several reactions folks have when they get up from taking the Exam. The universal response is exhaustion. Some folks have no feeling about how they did until "The Letter" arrives. Some folks wonder if they took the right test! Stay loose, relax, and good luck.

NOTE: Thanks to the Veteran Administration's Office of Cyber Security