Chapter 1

(ISC)^2 and the CISSP Certification

In This Chapter

- Finding out about (ISC)^2 and the CISSP certification
- Understanding CISSP certification minimum requirements
- Registering for the exam
- Developing a study plan
- Taking the CISSP exam and waiting for results

Some say that the Certified Information Systems Security Professional (CISSP) candidate requires a breadth of knowledge 50 miles across and 2 inches deep. To embellish on this statement, we believe that the CISSP candidate is more like the Great Wall of China, with a knowledge base extending over 3,500 miles, with a few holes here and there, stronger in some areas than others, but nonetheless one of the Seven Wonders of the Modern World.

The problem with many currently available CISSP preparation materials is in defining how high the Great Wall actually is: Some material overwhelms and intimidates CISSP candidates, leading them to believe that the wall is as high as it is long. Other study materials are perilously brief and shallow, giving the unsuspecting candidate a false sense of confidence as he or she merely attempts to step over the Great Wall, careful not to stub a toe. *CISSP For Dummies* answers the question, “What level of knowledge must a CISSP candidate possess to succeed on the CISSP exam?”

About (ISC)^2 and the CISSP Certification

The International Information Systems Security CertificationsConsortium, or (ISC)^2, established the Certified Information Systems Security Professional (CISSP) certification program in 1989. The (ISC)^2 is a nonprofit, tax-exempt corporation chartered for the explicit purpose of developing and administering the certification and education programs associated with the CISSP (as well as several CISSP concentrations, and the Systems Security Certified Practitioner, or SSCP, and the Certification and Accreditation Professional, (or CAP) certification. The CISSP certification is based on a Common Body of Knowledge (CBK) identified by the (ISC)^2 and defined through ten distinct domains:

- Access Control
- Telecommunications and Network Security
- Information Security and Risk Management
- Application Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Compliance, and Investigations
- Physical (Environmental) Security

You Must Be This Tall to Ride (And Other Minimum Requirements)

The CISSP candidate must have a minimum of four years of professional work experience in one or more of the domains listed in the preceding section. After being notified of a passing score on the CISSP examination, the candidate must submit a qualified third-party endorsement (from another CISSP; the candidate's employer; or any licensed, certified, or commissioned professional, such as a banker, attorney, or certified public accountant) to validate the candidate's work experience. This endorsement must be submitted within 90 days of the date of the exam results notification letter or the application and exam results are voided. A percentage of submitted applications will be randomly audited, requiring additional documentation (normally a resume and confirmation from employers of work history) and review by (ISC)^2. Final notification of certification upon receipt of the endorsement letter will normally be sent by (ISC)^2 via e-mail within one business day (seven business days if audited).

The candidate must also subscribe to the (ISC)^2 Code of Ethics and renew certification every three years. The CISSP certification can be renewed by accumulating 120 Continuing Professional Education (CPE) credits or by re-taking the CISSP examination. You earn CPE credits for various activities, including taking educational courses or attending seminars and security conferences, membership in association chapters and meeting attendance, vendor presentations, university or college course completion, providing security training, publishing security articles or books, serving on industry boards, self-study, and volunteer work. You must submit evidence of any such activities to (ISC)^2 for determining and documenting CPE credits. In most cases, this can be done online in the secure area of the (ISC)^2 Web site. There is also an $85 (U.S.) annual maintenance fee payable to (ISC)^2. Maintenance fees are billed in arrears for the preceding year and may be paid online, also in the secure area of the (ISC)^2 Web site.

The minimum requirement for CISSP certification is four years of professional work experience in one or more of the ten domains of the CISSP CBK. However, you can be credited for one year of experience if you have either a four-year college degree or a master's degree in Information Security from a National Center of Excellence (but you cannot combine both the four-year degree and the master's degree to get two years of credit).

See Chapter 3 for more information on earning CPE credits and maintaining your CISSP certification.

Registering for the Exam

You can register for the CISSP exam online, via mail, or via fax.

First, you need to find a suitable exam date and location. It's given throughout the year at various locations (typically at colleges, community centers, or convention centers) worldwide. You can find exam schedules on the (ISC)^2 Web site at `www.isc2.org`.

Unlike many other certification exams, the CISSP examination isn't conveniently available at Thomson Prometric or Pearson VUE testing centers.

Some travel may be necessary, which requires planning in advance for travel arrangements . . . possibly including airline, rental car, and hotel reservations. If you're traveling to another country for your CISSP examination, visa requirements may apply.

After you find a suitable exam date and location on the (ISC)^2 Web site, complete the online registration form or download a copy of the form so that you can mail or fax it back to (ISC)^2. If you're registering online or via fax, you need to use a MasterCard or Visa for payment. If registering by mail, you can pay for the exam via MasterCard, Visa, personal check, or money order. The current fee to take the test is $499 if you register more than 16 days in advance. The mailing address for registrations is:

(ISC)^2 Services
2494 Bayshore Boulevard, Suite 201,
Dunedin, FL 34698 U.S.A.

The number for fax registration is 727-738-8522.

When you register, you'll be required to quantify your work experience in information security. You're not required to have experience in *all* the ten domains, but the cumulative total of your work experience must be at least four years.

We recommend that you register early, for several reasons:

- The total charge of $499 for early registration and the $100 rescheduling fee is exactly the same as the fee for normal registration: $599.
- By committing to a specific testing date, you're more likely to stay focused and avoid procrastination.
- Registering early allows you to better plan your travel arrangements and possibly save some money by booking reservations well in advance.
- Space is limited at all test centers. Reservations are accepted on a first-come, first-served basis; in the case of registrations by mail, the date of the postmark is used. If the test date fills up before you register (and this is a hot certification), you may be hard-pressed to find another test date and location that suits you this year.

Great news! If you're a U.S. military veteran and are eligible for Montgomery GI Bill benefits, the Veteran's Administration will reimburse you for the full cost of the exam, pass or fail (the VA doesn't cover exam preparation costs).

Developing a Study Plan

Many resources are available to help the CISSP candidate prepare for the exam. Self-study is a major part of any study plan. Work experience is also critical to success and can be incorporated into your study plan. For those who learn best in a classroom or training environment, (ISC)^2 offers CISSP review seminars.

We recommend that you commit to an intense 60-day study plan leading up to the CISSP exam. How intense? That depends on your own personal experience and learning ability, but plan on a minimum of 2 hours a day for 60 days. If you're a slow learner or reader, or perhaps find yourself weak in many areas, plan on 4–6 hours a day and more on the weekends. But stick to the 60-day plan. If you feel you need 360 hours of study, you may be tempted to spread this out over a 6-month period for 2 hours a day. Consider, however, that committing to 6 months of intense study is much harder (on you, as well as your family and friends) than 2 months. In the end, you will find yourself studying only as much as you would have in a 60-day period.

Self-study

Self-study can include books and study references, a study group, and practice exams.

Begin by requesting an official *CISSP Candidate Information Bulletin (CIB)* from the (ISC)^2 Web site (`www.isc2.org`). It's free and will be e-mailed to you as a password-protected Adobe Acrobat PDF document. This booklet provides a good outline of the subjects on which you'll be tested.

Next, read this book, take the practice exam and review the materials on the accompanying CD-ROM. *CISSP For Dummies* is written to provide the CISSP candidate an excellent overview of all the broad topics covered on the CISSP exam.

Also, focus on weak areas that you've identified. Read additional references; we list several great ones on the CD-ROM. As a minimum, we highly recommend *The CISSP Prep Guide: Gold Edition* by Ronald L. Krutz and Russell Dean Vines (John Wiley & Sons, Inc.).

You can also find several study guides at `www.cissps.com`, `www.cccure.org`, and `www.cramsession.com`.

Joining or creating your own study group will help you stay focused and also provide a wealth of information from the broad perspectives and experiences of other security professionals.

REMEMBER

No practice exams exactly duplicate the CISSP exam (and forget about brain dumps). However, many resources are available for practice questions. You'll find that some practice questions are too hard, others are too easy, and some are just plain irrelevant. Don't despair! The repetition of practice questions will help reinforce important information that you need to know in order to successfully answer questions on the CISSP exam. For this reason, we recommend taking as many practice exams as possible. Use the Practice Exam and/or the Flash Cards on the CD-ROM and try the practice questions on the CISSP Open Study Guide (OSG) Web site (`www.cccure.org`).

Getting hands-on experience

Getting hands-on experience may be easier said than done, but keep your eyes and ears open for learning opportunities during your course of study for the CISSP exam.

For example, if you're weak in networking or applications development, talk to the networking group or programmers in your company. They may be able to show you a few things that will help make sense of the volumes of information that you're trying to digest.

Your company should have a security policy that's freely available to its employees, particularly if you have a security function in the organization. Get a copy and review its contents. Are critical elements missing? Do any supporting guidelines, standards, and procedures exist? If your company doesn't have a security policy, perhaps now is a good time for you to educate management about issues of due care, due diligence, and other concepts from the Legal, Regulations, Compliance, and Investigations security domain.

Review your company's Business Continuity and Disaster Recovery plans. They don't exist? Perhaps this is an initiative that you can lead to help both you and your company.

Attending an (ISC)^2 CISSP review seminar

The (ISC)^2 also administers a five-day CISSP CBK Review Seminar to help the CISSP candidate prepare. Schedules and registration forms for the CBK Review Seminar are available on the (ISC)^2 Web site at `www.isc2.org`.

The early rate for the CISSP CBK Review seminar is $2,495 if you register 16 days or more in advance (the standard rate is $2,695). Members of ISSA, IIA, or ISACA also get a $250 discount. (All dollar amounts listed here are U.S. currency, and are subject to change.)

If you generally learn better in a classroom environment or find that you only have knowledge or actual experience in one or two of the domains, you might seriously consider attending a review seminar.

Attending other training courses or study groups

Other reputable organizations such as SANS (`www.sans.org`) offer high-quality training in classroom and self-study formats. Before signing up and spending your money, we suggest that you talk to someone who has completed the course and can tell you about its quality. Usually, the quality of a classroom course depends upon the instructor; for this reason, we think it's valuable to find out from others whether the proposed instructor is as helpful as he or she is reported to be.

Many cities have self-study groups, usually run by CISSP volunteers. For example, one of the authors lives in Seattle, where a CISSP study group has been run by volunteers for many years. There may be such a study group where you live; or, if you know some CISSPs in your area, you might ask them to help to organize a self-study group (and tell him or her you will help!).

TIP

Always confirm the quality of a study course or training seminar before committing your money and time.

See Chapter 3 for more information on starting a CISSP study group.

Are you ready for the exam?

Are you ready for the big day? This is a difficult question for us to answer. You must decide, based on your individual learning factors, study habits, and professional experience when you're ready for the exam. We don't know of any magic formula for determining your chances of success or failure on the CISSP examination. (If you find one, please write to us so that we can include it in the next edition of this book.)

In general, we recommend a minimum of two months of focused study. Read this book and continue taking the practice exam in this book and on the accompanying CD until you can consistently score 80 percent or better in all areas. *CISSP For Dummies* covers *all* the information that you will need to pass the CISSP examination. Read this book (and reread it) until you're comfortable with the information presented and can successfully recall and apply it in each of the ten domains.

Continue by reviewing other materials (particularly in your weak areas) and actively participating in an online or local study group. Take as many practice exams from as many different sources as possible. There are no brain dumps for the CISSP examination, and no practice test will exactly duplicate the actual exam (some are too easy, and others are too difficult), but repetition will help you retain the important knowledge required to succeed on the CISSP exam.

About the CISSP Examination

The CISSP examination itself is a grueling 6-hour 250-question marathon. To put that into perspective, in 6 hours you could walk about 25 miles, watch a Kevin Costner movie 1½ times, or sing "My Way" 540 times on a karaoke machine. Each of these feats respectively closely approximates the physical, mental (not intellectual), and emotional toll of the CISSP examination.

As described by the (ISC)^2, a minimum score of "70 percent" is required to pass the examination. Not all the questions are weighted equally, so it's not possible to absolutely state the number of correct questions required for a passing score.

The examination isn't computer based. It is administered the old-fashioned way: exam booklet, answer sheet, and lots of pencils. You may write in the exam booklet, but only answers recorded on the answer sheet are scored.

You won't find any multiple-answer, fill-in-the-blank scenario or simulation questions on the CISSP exam. However, all 250 multiple-choice questions require you to select the *best* answer from 4 possible choices. This means that the correct answer isn't always a straightforward, clear choice. In fact, you can count on many questions to initially appear as though they have more than one correct answer. (ISC)^2 goes to great pains to ensure that you really, *really* know the material. For instance, a sample question might resemble the following:

> Which of the following is the FTP control channel?
>
> **A** TCP port 21
>
> **B** UDP port 21
>
> **C** TCP port 25
>
> **D** IP port 21

Most of you may immediately know that FTP's control channel is port 21, but is it TCP, UDP, or IP?

Increasingly, CISSP exam questions are based more upon *situations* than on simple knowledge of facts. For instance, here's a question you might get:

A system administrator has found that a former employee has successfully logged in to the system. The system administrator should:

A Shut down the system.

B Confirm the breach in the IDS logs.

C Lock or remove the user account.

D Contact law enforcement.

You won't find the answer to this in a book (well, probably not). But there is still a *best* answer to every exam question — perhaps not an ideal answer, but there is a *best* answer.

A common and effective test-taking strategy for multiple-choice questions is to carefully read each question and then eliminate any obviously wrong choices. The CISSP examination is no exception.

WARNING!

Wrong choices aren't so obvious on the CISSP examination. You will find a few obviously wrong choices, but they only stand out to someone who has studied thoroughly for the examination and has a good grasp of all ten of the security domains.

Only 225 questions are actually counted toward your final score. The other 25 are trial questions for future versions of the CISSP examination. However, these questions aren't identified within the exam, so you have to answer all 250 questions as if they're the real thing.

The CISSP examination is currently available in English only. Foreign language dictionaries are permitted. (ISC)^2 also recommends that non-English speaking candidates pass the Test of English as a Foreign Language (TOEFL) exam prior to attempting the CISSP examination.

Chapter 14 covers the details of the exam environment.

Chapter 15 contains suggestions for preparation on the day of the exam.

Waiting for Your Results

Perhaps the most painful part of the CISSP examination is waiting for the results. You can expect to come out of the CISSP examination, at best, with no idea of whether you have passed or failed . . . or worse, with the sinking feeling that you bombed it miserably. Take heart — this is an almost universal reaction, caused by mental fatigue, but it's certainly not the universal result.

(ISC)^2 officially states that you can expect your exam results via first class mail within 4–6 weeks of your examination date. However, (ISC)^2 is getting more efficient and often has results out within 1–2 weeks. No results are given out via telephone. If you don't receive your results within 6 weeks, you should contact (ISC)^2 to inquire about the status.

Your results will be simply *Pass* or *Fail.* No score is given, and your domain strengths/weaknesses aren't identified. You just receive an official letter informing you of your results. When you pass, you receive your CISSP certification number, CISSP certificate, wallet card, lapel pin, and username/temporary password for access to the secure (ISC)^2 Web site.

While waiting for your results, assume the worst and prepare for the retest. Recall specific problem areas from the examination. Write them down and study those areas again. If you fail the examination, this effort will pay huge dividends when you try again. And if you find out that you *did* pass the examination, you'll be a better CISSP!

Chapter 3 reviews what to do after you earn your CISSP certification.