Chapter 1

(ISC)^2 and the CISSP Certification

In This Chapter

- Finding out about (ISC)^2 and the CISSP certification
- Understanding CISSP certification 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 — maybe 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 while he or she merely attempts to step over the Great Wall, careful not to stub a toe. To help you avoid either misstep, *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 Certification Consortium (ISC)^2 (`www.isc2.org`) was established in 1989 as a nonprofit, tax-exempt corporation chartered for the explicit purpose of developing a standardized security curriculum and administering an information security certification process for security professionals worldwide. In 1994, the Certified Information Systems Security Professional (CISSP) credential was launched.

The CISSP was the first information security credential to be accredited by the American National Standards Institute (ANSI) to the ISO/IEC 17024:2003 standard. This international standard helps to ensure that personnel certification processes define specific competencies and identify required knowledge, skills, and personal attributes. It also requires examinations to be independently administered and designed to properly test a candidate's competence for the certification. This process helps a certification gain industry acceptance and credibility as more than just a marketing tool for certain vendor-specific certifications (a widespread criticism that has caused many vendor certifications to lose relevance over the years).

The ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) are two organizations that work together to prepare and publish international standards for businesses, governments, and societies worldwide.

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 Governance and Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Security Operations
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

You Must Be This Tall to Ride (and Other Requirements)

The CISSP candidate must have a minimum of five cumulative years of professional, full-time, direct work experience in two or more of the domains listed in the preceding section. The work experience requirement is a hands-on one — you can't satisfy the requirement by just having "information security" listed as one of your job responsibilities. You need to have specific knowledge of information security — and perform work that requires you to apply that knowledge regularly.

However, you can get a waiver for a maximum of one year of the five-year professional experience requirement if you have one of the following:

- A four-year college degree
- An advanced degree in information security from a U.S. National Center of Academic Excellence in Information Assurance Education (CAEIAE) or a regional equivalent
- A credential that appears on the (ISC)^2–approved list, which includes more than 30 technical and professional certifications, such as various SANS GIAC certifications, Microsoft certifications, and CompTIA Security+ (For the complete list, go to www.isc2.org/credential_waiver/default.aspx.)

TIP

In the U.S., CAEIAE programs are jointly sponsored by the National Security Agency and the Department of Homeland Security. For more information, go to www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

Registering for the Exam

As of June 1, 2012, the CISSP exam is now being administered via computer-based testing (CBT) at local Pearson VUE testing centers worldwide. To register for the exam, go to the (ISC)^2 website (www.isc2.org), click the Certifications tab, click Computer Based Testing (CBT), and then click the Register Now – Pearson VUE button; alternatively, go directly to the Pearson VUE website (http://pearsonvue.com/isc2/).

On the Pearson VUE website, you have to create a web account first; then you can register for the CISSP exam, schedule your test, and pay your testing fee. You can also locate a nearby test center, take a Pearson VUE testing tutorial, practice taking the exam (which definitely you should do if you've never taken a CBT), and then download the (ISC)^2 non-disclosure agreement (NDA).

TIP

Download and read the (ISC)^2 NDA when you register for the exam. You're given five minutes to read and accept the agreement at the start of your exam. If you don't accept the NDA in the allotted five minutes, your exam will end and you forfeit your exam fees!

When you register, you're required to quantify your work experience in information security, answer a few questions regarding criminal history and related background, and agree to abide by the (ISC)^2 Code of Ethics.

The current exam fee in the U.S. is $599. You can cancel or re-schedule your exam by contacting VUE by telephone at least 24 hours in advance of your scheduled exam or online at least 48 hours in advance. The fee to re-schedule is $20.

WARNING!

If you fail to show up for your exam, you'll forfeit your entire exam fee!

TIP

Great news! If you're a U.S. military veteran and are eligible for Montgomery GI Bill benefits, the Veteran's Administration (VA) will reimburse you for the full cost of the exam, regardless of whether you pass or fail.

Preparing for the Exam

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 you can incorporate it 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 two hours a day for 60 days. If you're a slow learner or reader, or perhaps find yourself weak in many areas, plan on four to six 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 study out over a six-month period for 2 hours a day. Consider, however, that committing to six months of intense study is much harder (on you, as well as your family and friends) than two months. In the end, you'll find yourself studying only as much as you would have in a 60-day period anyway.

Studying on your own

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

Begin by downloading the free official *CISSP Candidate Information Bulletin (CIB)* from the (ISC)^2 website. 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 Dummies website (`www.dummies.com`). *CISSP For Dummies* is written to provide the CISSP candidate an excellent overview of all the broad topics covered on the CISSP exam.

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

Joining or creating your own study group can 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 — using or contributing to brain dumps is unethical and is a violation of your NDA which could result in losing your CISSP certification permanently). However, many resources are available for practice questions. Some practice questions are too hard, others are too easy, and some are just plain irrelevant. Don't despair! The repetition of practice questions helps 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 on the Dummies website (`www.dummies.com`), and try the practice questions at Clément Dupuis and Nathalie Lambert's CCCure website (`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 while you prepare 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 can help make sense of the volumes of information that you're trying to digest.

TIP

Your company or organization should have a security policy that's readily available to its employees. 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, Investigations, and Compliance security domain.

Review your company's plans for business continuity and disaster recovery. They don't exist? Perhaps you can lead this initiative to help both you and your company.

Attending an (ISC)^2 CISSP CBK Review or Live OnLine Seminar

The (ISC)^2 also administers five-day CISSP CBK Review Seminars and Live OnLine seminars to help the CISSP candidate prepare. You can find schedules and registration forms for the CBK Review Seminar and Live OnLine on the (ISC)^2 website at `www.isc2.org`.

The early rate for the CISSP CBK Review or Live OnLine seminar in the U.S. is $2,495 if you register 16 days or more in advance (the standard rate is $2,695).

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

If it's not convenient or practical for you to travel to a seminar, Live Online provides the benefit of learning from an (ISC)^2 Authorized Instructor on your computer. Live OnLine provides all the features of classroom based seminars, real-time delivery, access to archived modules, and all official courseware.

Attending other training courses or study groups

Other reputable organizations, such as SANS (`www.sans.org`), offer high-quality training in both 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 on the instructor; for this reason, try 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. You may find a study group where you live; or, if you know some CISSPs in your area, you might ask them to help you organize a self-study group.

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.

Take the testing tutorial and practice exam

If you are not familiar with the operations of computer-based testing, you may want to take a practice exam. Go to the Pearson VUE website and look for the Pearson VUE Tutorial and Practice Exam (at `www.pearsonvue.com/athena`).

The tutorial and practice exam are available for Windows computers only. To use them, you must have at least 512 MB of RAM, 60 MB of available disk space, Windows 2000 or newer (XP, Vista, 7, or 8), and Microsoft Internet Explorer 5 or a newer browser.

Are you ready for the exam?

Are you ready for the big day? We can't answer this question for you. You must decide, on the basis of 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 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 exams — in this book and on the Dummies website — until you can consistently score 80 percent or better in all areas. *CISSP For Dummies* covers *all* the information you need to know if you want 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. You can't find any brain dumps for the CISSP examination, and no practice test can exactly duplicate the actual exam (some practice tests are simply too easy, and others are too difficult), but repetition can help you retain the important knowledge required to succeed on the CISSP exam.

About the CISSP Examination

The CISSP examination itself is a grueling six-hour, 250-question marathon. To put that into perspective, in six hours, you could walk about 20 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, you need a scaled score of 700 or better to pass the examination. Not all the questions are weighted equally, so we can't absolutely state the number of correct questions required for a passing score.

You won't find any multiple-answer, fill-in-the-blank, scenario-based, or simulation questions on the CISSP exam. However, all 250 multiple-choice questions require you to select the *best* answer from four possible choices. So the correct answer isn't always a straightforward, clear choice. In fact, you can count on many questions to appear initially as if 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

Many readers almost instinctively know that FTP's control channel is port 21, but is it TCP, UDP, or IP?

Increasingly, CISSP exam questions are based more on *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 security 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 every exam question still has a *best* answer — perhaps not an ideal answer, but definitely 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.

Wrong choices aren't necessarily obvious on the CISSP examination. You may 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, the exam doesn't identify these questions for the test-taker, so you have to answer all 250 questions as if every one of them is the real thing.

The CISSP examination is currently available in English, Brazilian Portuguese, Chinese, French, German, Japanese, Korean, and Spanish. You're permitted to bring a foreign language dictionary (non-electronic) for the exam, if needed. You need to indicate your language preference when you register for the exam.

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

After the Examination

After passing the CISSP examination, you must submit a qualified third-party endorsement (from another CISSP, your employer, or any licensed, certified, or commissioned professional — such as a banker, attorney, or certified public accountant) to validate your work experience. This endorsement must be submitted within 90 days of your exam; otherwise your application and exam results are voided. (ISC)^2 randomly audits a percentage of submitted applications, requiring additional documentation (normally a résumé and confirmation from employers of work history) and review by (ISC)^2. Within one business day (seven business days, if audited) after it receives the endorsement, (ISC)^2 normally sends final notification of certification via e-mail.

After you earn your CISSP certification, you must remain an (ISC)^2 member in good standing and renew your certification every three years. You can renew the CISSP certification by accumulating 120 Continuing Professional

Education (CPE) credits or by retaking the CISSP examination. You must earn a minimum of 20 CPE credits during each year of your three-year recertification cycle. You earn CPE credits for various activities, including taking educational courses or attending seminars and security conferences, belonging to association chapters and attending meetings, viewing vendor presentations, completing university or college courses, providing security training, publishing security articles or books, serving on relevant industry boards, taking part in self-study, and doing related volunteer work. You must document your annual CPE activities on the secure (ISC)^2 website to receive proper credit. You also have to pay an $85 annual maintenance fee, payable to (ISC)^2. Maintenance fees are billed in arrears for the preceding year, and you can pay them online, also in the secure area of the (ISC)^2 website.

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