

Preparing for the CISSP Exam:

Everything You Wanted to Know About the CISSP but were Afraid to Ask

By **Debbie Christofferson, CISSP, CISM**
DebbieChristofferson@earthlink.net

Preparing for the CISSP Exam

Are you planning to add the CISSP to your array of credentials, or to those of your staff? The CISSP opens doors to pay and positions that might be otherwise closed, and guarantees employers a demonstrated level of security knowledge.

As the recognized industry credential for security professionals, the CISSP defines a baseline for hiring and career growth. Individuals demonstrate a commitment to the field and a minimum level of knowledge and experience by holding the CISSP. For a more detailed report, send an email request to DebbieChristofferson@earthlink.net or call 480-988-4194.

Employers who hire the CISSP set a higher standard for security in their organizations. Supporting the CISSP helps raise employee satisfaction for security professionals. It also increases competitive advantage in a connected economy where security dominates.

So what does it take to qualify for and receive the coveted CISSP credential, and what are the best ways to study and pass the exam?

- ▲ Possess four years of direct security experience.
- ▲ Exchange a bachelor or master's college degree or equivalent life experience for one year of experience.
- ▲ Meet and subscribe to the ISC(2) Code of Ethics.
- ▲ Answer a handful of questions satisfactorily and honestly regarding criminal history and background.
- ▲ Pay the exam fee (about \$500 USD) and pass a 250-question multiple choice test within a single 6-hour sitting at a 70% or higher pass rate.

The exam itself is rigorous and oriented to business and technology, based on risk. Ten domains cover a common body of knowledge. You must pass them all at once:

- ▲ Access Control
- ▲ Applications & Systems Development
- ▲ Business Continuity Planning
- ▲ Cryptography
- ▲ Law, Investigation & Ethics
- ▲ Operations Security
- ▲ Physical Security
- ▲ Security Architecture
- ▲ Security Management Practices
- ▲ Telecommunications, Network & Internet Security

The International Information Systems Security Certification Consortium, or ISC(2) administers the CISSP at www.isc2.org, who revalidated the content in 2002.

CISSP Exam Preparation

Taking an independent practice test without any advance work is the single most effective way to define a study course for your CISSP exam preparation. Answering questions with a paper document works best for me. It allows you to carry it with you and complete questions in pieces during breaks over time or days. Your results will clearly show the areas where you need to increase your knowledge. Calculate your score individually by domain.

Spend your time on the areas where you fell below 80% (okay, 85% for you Engineers!). Do not spend time revisiting or studying domains where you already exhibit strength.

Test question phrasing is the most important thing to comprehend, and the reason practice test study guides work so well. Breaking practice down by domains, and then focusing extra study on those where you score lowest (below 80%) best leverages your time and study. Taking the exam cold turkey is not a good alternative if you really expect to pass.

CISSP Exam Preparation

In Certification Magazine, Tim Sosbe lists preferred materials and alternatives used to prepare for the CISSP exam. He showed self-study books and practice exams as our top choices of preparation, and I agree with his results. It is inexpensive and allows us to study independently. Vendor boot camps and virtual labs rated low. In general, I do not find study groups to be a good use of time, or the use of multiple study or reference books on security. These offer easy alternatives to increase your knowledge base.

If you can afford the investment, a review course offers a good alternative. It increases your odds of passing the exam and demonstrates exam verbiage and content. Some industry conferences offer these in condensed format at lower rates compared to full-fledged training. Each of us differs in our needs and learning styles. Choose preparation methods that work best for your own situation.

Taking the exam:

Arrive on time and bring your admission letter and a valid picture ID (only a driver's license, government-issued ID card, or a passport is accepted). Read carefully and then choose the most correct answer. Underscore pivotal words in each question if pre-testing showed any tendency to misunderstand wording. Take breaks as you need them. Break time counts within the 6-hour window for the exam, but you will work better if you are refreshed. Bring a snack to re-energize during the last hour when mental tiredness and hunger may set in.

People vary on how long they take to complete the exam, and some of us do take advantage of the entire 6-hour slot.

After the Exam

Your exam results will be mailed to you in 2-6 weeks, typically two. Once you pass, complete and submit your CISSP application. It must be endorsed by a qualified third party before credential is awarded: Your employer or a licensed, certified or commissioned professional may endorse your candidacy. Your annual \$85 CISSP maintenance fees are due in advance, and must be included with your application. Up to 3 years advance renewal payments are accepted.

If you passed the exam, a CISSP certificate will be enclosed with your letter and an ID card, each with your unique CISSP #. Optionally, you can then list at ISC(2) in the CISSP directory, to participate in their Speakers' Bureau, service in committees, or participate in annual ISC(2) elections.

Applicants who fail the exam are notified of the area(s) where they fell below the 70% level. You can retake the exam without a waiting period, but must re-apply and pay the fee again.

Re-Certification Every 3 Years

The CISSP is renewed in 3-year increments. An annual maintenance fee is required. To keep your CISSP designation, you must earn and submit 120 hours of continuing education credit within that period or retake the exam. Random audits are performed to validate your credits.

Earning education credit is simple for any security professional and updating the database is easy. Criteria:

- ▲ 80-120 A-Credit hours. Eighty hours must be earned in activities directly related to the profession
- ▲ 40 B-Credit hours. Up to forty CPEs may be earned in other educational activities that enhance the CISSP's overall professional skills, knowledge, and competency.
- ▲ Some carry-over permitted if you earn more than 120 hours in a 3-year period

Ways to earn CISSP educational credits to maintain your certification:

- ▲ Educate others on security
- ▲ Write on security
- ▲ Author CISSP exam questions
- ▲ Participate in security forums
- ▲ Serve on professional security group boards and committees
- ▲ Attend security training
- ▲ Subscribe to and read Information Security Magazine

Other Security Certifications

The SSCP, or Systems Security Certified Practitioner offers a subset of the CISSP and this certification test is administered by the ISC(2). Exam time and questions are reduced by half and there are seven domains: (1) Access Controls, (2) Administration, (3) Audit and Monitoring Risk, (4) Response and Recovery, (5) Cryptography, (6) Data Communications, and (7) Malicious Code/Malware.

At an InfoSec World 2004 presentation, 129 security-related certifications were listed. These vary in merit, value and price, and the certifications are not created equally. One can argue that they represent a thinly disguised vendor opportunity to make money in the market. This may be true, but certifications represent a huge and growing trend.

Undeniably, certifications segment the hiring market; just ask any recruiter. CISSP is listed as a required or desired credential in nearly all

open security positions. In an ITAA Survey on Certifications & Hiring, 73% of responding managers said the CISSP carried the greatest weight.

Study Resources

For security resource books and practice test guides, Amazon.com offers the most cost-effective choices. It matters little which brand or title you particularly buy—many of the offerings work well. You can buy used or borrow also from your fellow CISSP libraries. ISC(2) recently added a specific practice test guide, which is highly rated and can be purchased at www.cissp.com for a discount. If you like online practice, many web sites offer practice drill software for the CISSP.

CISSP Return on Investment


An informal survey of about one hundred Information Security Officers at MISTI's InfoSec World 2004 Conference showed that salaries were not increased when their employees passed the CISSP. However, statistics in Cert Magazine and other sources continuously show CISSPs as earning more money.

An average certification provided a 3.2-to-1 return on investment, according to a December, 2002 Cert Magazine report. For every dollar invested in a certification, the certificate receiver realized a \$3.20 return in the form of a pay raise.

Those who have passed the CISSP exam often are seasoned professionals with many years of experience, so money differences reflect more than just the CISSP. However, the CISSP stacks up strongly against others in the field, and sits proudly at the table as one of the big boys.

A CISSP beefs up your resume and career. For employees, it demonstrates a commitment and specific level of security assurance. CISSP stands up to the challenge for value to employers and professionals alike.

Bottom Line

For passing the exam, use the study method that best meets your needs and experience. For specific exam dates and review courses in your area, visit www.isc2.org. 

Debbie Christofferson, CISSP, CISM, has a Fortune 500 management background based on 20 years of business and international experience across the U.S., Europe and Greater Asia. She's a strategic information security expert with 13 years of related management and consulting experience.