

IN THIS CHAPTER

- » Learning about ISC2 and the CISSP certification
- » Understanding CISSP certification requirements
- » Developing a study plan
- » Registering for the exam
- » Taking the CISSP exam
- » Getting your exam results

Chapter 1

ISC2 and the CISSP Certification

In this chapter, you get to know the ISC2 and learn about the CISSP certification, including professional requirements, how to study for the exam, how to get registered, what to expect during the exam, and (of course) what to expect after you pass the CISSP exam!

The International Information System Security Certification Consortium, or ISC2, (www.isc2.org) was established in 1989 as a not-for-profit, 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 accredited by the American National Standards Institute (ANSI) to the ISO/IEC 17024 standard. This international standard helps 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 diminished the popularity of many vendor certifications over the years).



The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 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 ISC2 and defined through eight distinct domains:

- » Security and Risk Management
- » Asset Security
- » Security Architecture and Engineering
- » Communication and Network Security
- » Identity and Access Management (IAM)
- » Security Assessment and Testing
- » Security Operations
- » Software Development Security

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

The CISSP candidate must have a minimum of the equivalent of five cumulative years of professional (paid), *full-time*, direct work experience in two or more of the domains listed in the preceding section. Full-time experience is accrued monthly and requires full-time employment for a minimum of 35 hours per week and 4 weeks per month to get credit for 1 month of full-time work experience. Part-time experience can also be credited if you are employed fewer than 35 hours per week but at least 20 hours per week; 1,040 hours of part-time experience would be the equivalent of 6 months of full-time experience. Credit for work experience can also be earned for paid or unpaid internships. You'll need documentation from the organization confirming your experience or from the registrar if you're interning at a school.

The work experience requirement is a hands-on one; you can't satisfy the requirement just by having "information security" listed as one of your job responsibilities. You need to have *specific* knowledge of information security and to perform work that requires you to apply that knowledge regularly. Some examples of full-time information security roles that might satisfy the work experience requirement include (but aren't limited to)

- » Security analyst
- » Security architect
- » Security auditor
- » Security consultant
- » Security engineer
- » Security manager
- » Risk manager

Examples of information technology roles for which you can gain partial credit for security work experience include (but aren't limited to)

- » Systems administrator or systems engineer
- » Network administrator or network engineer
- » Database administrator
- » Software developer

For any of these preceding job titles, your particular work experience might result in your spending some of your time (say, 25 percent) doing security-related tasks, which is legitimate for security work experience. Five years as a systems administrator, for example, spending a quarter of your time doing security-related tasks, earns you 1.25 years of security experience.

Furthermore, you can get a waiver for a maximum of one year of the 5-year professional experience requirement if you have one of the following:

- » A 4-year college degree (or regional equivalent)
- » An advanced degree in information security from one of the National Centers of Academic Excellence in Cyber Defense (CAE-CD)
- » A credential that appears on the ISC2-approved list, which includes more than 45 technical and professional certifications, such as various SANS GIAC certifications, Cisco and Microsoft certifications, and CompTIA Security+

(For the complete list, go to www.isc2.org/Certifications/CISSP/Prerequisite-Pathway.)

See Chapter 2 to learn more about relevant certifications on the ISC2-approved list for an experience waiver.



TIP

In the United States, CAE-CD programs are jointly sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). For more information, go to www.nsa.gov/Academics/Centers-of-Academic-Excellence.

If you lack the minimum required experience to become a CISSP, you can still take the CISSP certification exam and become an Associate of ISC2. Then you'll have 6 years to meet the minimum experience requirement and become a fully certified CISSP.

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 online training environment, ISC2 and other organizations offer CISSP training 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 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 to 6 hours a day — and more on the weekends. But stick to the 60-day plan. If you need 360 hours of study, you may be tempted to spread this study 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 on your family and friends) than 2 months. In the end, you'll likely find yourself studying only as much as you would have in a 60-day period anyway.

Studying on your own

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

Begin by downloading *The Ultimate Guide to the CISSP* from the ISC2 website at www.isc2.org/Certifications/CISSP. This guide provides a good overview of the CISSP certification and the exam, as well as links to several helpful CISSP study resources.

Next, read this ISC2-approved book, and review the online practice at www.dummies.com. (See the introduction for more information.) *CISSP For Dummies* is written to provide a thorough and essential review of all the topics covered on the CISSP exam. Then read any additional study resources to further your knowledge and reinforce your understanding of the exam topics. You can find several excellent study resources in the official *CISSP Certification Exam Outline*. Finally, rinse and repeat: Do another quick read of *CISSP For Dummies* as a final review before you take the actual CISSP exam.



WARNING

Don't rely on *CISSP For Dummies* (as awesome and comprehensive as it is!) or any other book — no matter how thick it is — as your *sole* resource to prepare for the CISSP exam.

Joining a study group can help you stay focused and provide a wealth of information from other security professionals' broad perspectives and experiences. It's also an excellent networking opportunity (the talking-to-real-people type of network, not the TCP/IP type of network)! Study groups or forums can be hosted online or at a local venue. Find a group that you're comfortable with and that is flexible enough to accommodate your schedule and study needs. Or create your own study group!

Finally, answer *lots* of practice exam questions. Many resources are available for CISSP practice exam 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 you need to know to successfully answer questions on the CISSP exam. For this reason, we recommend taking as many practice exams as possible. Start with the online practice at www.dummies.com/go/getaccess. (See the introduction for more information.)



WARNING

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 the ISC2 nondisclosure agreement, which could result in your losing your CISSP certification permanently.

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.

If you're weak in networking or applications development, for example, talk to the networking group or developers in your company. They may be able to show you a few things that can help you make sense of the volumes of information 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 and due diligence as they relate to information security. Review your company's plans for business continuity and disaster recovery, for example. Those plans don't exist? Perhaps you can lead this initiative to help both yourself and your company.

Getting official ISC2 CISSP training

Classroom-based CISSP training is available as a 5-day, 8-hours-a-day seminar led by ISC2-authorized instructors at ISC2 facilities and ISC2 Official Training Providers worldwide. Private onsite training is also available, led by ISC2-authorized instructors and taught in your office space or a local venue. This option is convenient and cost-effective if your company sponsors your CISSP certification and has ten or more employees taking the CISSP exam. If you generally learn better in a classroom environment or find that you have knowledge or experience in only two or three of the domains, you might seriously consider classroom-based training or private onsite training.

If it's inconvenient or impractical for you to travel to a seminar, you can enroll in online training seminars that provide the benefits of learning from an ISC2-authorized instructor at your computer. Online training seminars include real-time, instructor-led seminars offered on a variety of schedules, with weekday, weekend, and evening options to meet your needs, as well as access to recorded course sessions for 60 days. Self-paced training is another convenient online option that provides virtual lessons taught by authorized instructors with modular training and interactive study materials. Self-paced online training can be accessed from any web-enabled device for 120 days and is available anytime and as often as you need.

You can find information, schedules, and registration forms for official ISC2 training at www.isc2.org/Certifications/CISSP.



TIP

The American Council on Education's College Credit Recommendation Service has evaluated and recommended three college credit hours for completing an Official ISC2 CISSP Training Seminar. Check with your college or university to find out whether these credits can be applied to your degree requirements.

Attending other training courses or study groups

Other reputable organizations offer high-quality training in both classroom and self-study formats. Before signing up and spending your money, we suggest 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 they are 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.

Taking practice exams

Taking practice exams is a helpful way to get familiar with the types of questions and topics you need to be familiar with for the CISSP exam. Be sure to take advantage of the online practice exam questions that are included with this book. (See the introduction for more information.) Although the practice exams don't simulate the adaptive testing experience, you can simulate a worst-case scenario by configuring the test engine to administer 150 questions (the maximum number you might see on the CISSP exam) with a time limit of 3 hours (the maximum amount of time you have to complete the CISSP exam). Learn more about computer-adaptive testing for the CISSP exam in the "About the CISSP Examination" section, later in this chapter, and on the ISC2 website at <https://isc2.org/Certifications/CISSP/CISSP-CAT>.



REMEMBER

To study for the CISSP exam successfully, you need to know your most effective learning styles. Boot camps are best for some people, for example, whereas others learn better over longer periods. Furthermore, some people gain more value from group discussions, whereas reading alone works better for others. Know thyself, and use what works best for you.

Are you ready for the exam?

Are you ready for the big day? We can't answer this question for you. You must decide, based on your learning factors, study habits, and professional experience, when you're ready for the exam. Unfortunately, there is no magic formula for determining your chances of success or failure on the CISSP examination.

In general, we recommend a minimum of two months of focused study. Read this book, and continue taking the practice exam on the Dummies.com website until you consistently score 80 percent or better in all areas. *CISSP For Dummies* covers *all* the information you need to know 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 eight domains. Continue by reviewing other study materials (particularly in your weak areas), actively participating in an online or local study group, and taking as many practice exams from as many sources as possible.

Then, when you feel like you're ready for the big day, find a romantic spot, take a knee, and — wait, wrong big day! Find a secure Wi-Fi hotspot (or another Internet connection), take a seat, and register for the exam!

Registering for the Exam

The CISSP exam is administered via computer-adaptive testing at local Pearson VUE testing centers worldwide. To register for the exam, go to the ISC2 website (www.isc2.org/Register-For-Exam) and click the Register link, or go directly to the Pearson VUE website (www.pearsonvue.com/isc2).



WARNING

Pearson VUE is the only authorized testing center for the CISSP exam. Fraudulent proxy test services sometimes attempt to contact security professionals and CISSP candidates. Do not fall for these scams. ISC2 encourages candidates (and ISC2 members) to report exam fraud (or cheating) at <https://my.isc2.org/s/report-fraud>.

On the Pearson VUE website, you first need to create an account for yourself; 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 you should definitely do if you've never taken a computer-based test), and then download and read the ISC2 nondisclosure agreement (NDA).



TIP

Download and read the ISC2 NDA when you register for the exam. Sure, the text is legalese, but it isn't unusual for CISSPs to be called upon to read contracts, license agreements, and other “boring legalese” as part of their information security responsibilities, so get used to reading it (and also get used to not signing legal documents without actually reading them!). You're given 5 minutes to read and accept the agreement at the start of your exam, but why not read the NDA in advance to avoid the pressure and distraction on exam day and simply accept the

agreement? If you don't accept the NDA in the allotted 5 minutes, your exam ends and you forfeit your exam fees!

When you register, you're required to quantify your relevant work experience, answer a few questions regarding any criminal history and other potentially disqualifying background information, and agree to abide by the ISC2 Code of Ethics.

The current exam fee in the United States is \$749. You can cancel or reschedule your exam by contacting Pearson VUE by telephone at least 24 hours in advance of your scheduled exam or online at least 48 hours in advance. The fee to reschedule is \$50. The fee to cancel your exam appointment is \$100.



WARNING

If you fail to show up for your exam or you're more than 15 minutes late for your exam appointment, you forfeit your entire exam fee!



TIP

Great news! If you're a US military veteran and you're eligible for Montgomery GI Bill or Post-9/11 GI Bill benefits, the Veterans Administration will reimburse you for the full cost of the exam, whether you pass or fail. In some cases, ISC2 Official Training Providers also accept the GI Bill for in-person certification training.

About the CISSP Examination

The CISSP examination is a grueling 3-hour, 100- to 150-question marathon. To put that into perspective, in 3 hours, you could almost/maybe run an actual half-marathon, watch *Braveheart* or *The Lord of the Rings: The Two Towers*, or cook a 12-pound turkey. Each of these feats, respectively, closely approximates the physical, mental, and emotional toll of the CISSP examination.

The CISSP exam is an *adaptive* exam, which means that the test changes based on how you're doing. The exam starts out relatively easy and grows progressively harder as you answer questions correctly. That's right — the better you do on the exam, the harder it gets. But that's not a bad thing! Think of it as being like skipping a grade in school because you're smarter than the average bear. The CISSP exam assumes that if you can answer harder questions about a given topic, logically, you can answer easier questions about that same topic, so why waste your time?

You have to answer a minimum of 100 questions. After you've answered the minimum number of questions, the testing engine either concludes the exam (if it determines with 95 percent confidence that you're statistically likely to pass or fail the exam) or continues asking up to a maximum of 150 questions until it reaches 95 percent confidence in either result. If you answer all 150 questions, the

testing engine determines whether you passed or failed based on your answers. If you run out of time (exceed the 3-hour time limit) but have answered the minimum number of questions (100), the testing engine determines whether you passed or failed based on your answers to the questions you completed.

The CISSP exam contains up to 25 pre-test items. They are included for research purposes only. (Taking the test is kind of like being a test dummy — for dummies.) The exam doesn't identify which questions are real and which are trial questions, however, so you have to answer all questions truthfully and honestly and to the best of your ability!

Three types of questions appear on the CISSP exam:

» **Multiple choice:** Select the *best* answer from four choices, as in this example:

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

The FTP control channel is port 21, but is it TCP, UDP, or IP?

» **Drag and drop:** Drag and drop the correct answer (or answers) from a list of possible answers on the left side of the screen to a box on the right side. Here's an example:

Which of the following are message authentication algorithms? Drag and drop the correct answers from left to right.

Possible Answers

MD5
RADIUS
SHA-2
HMAC
KERBEROS

Correct Answers

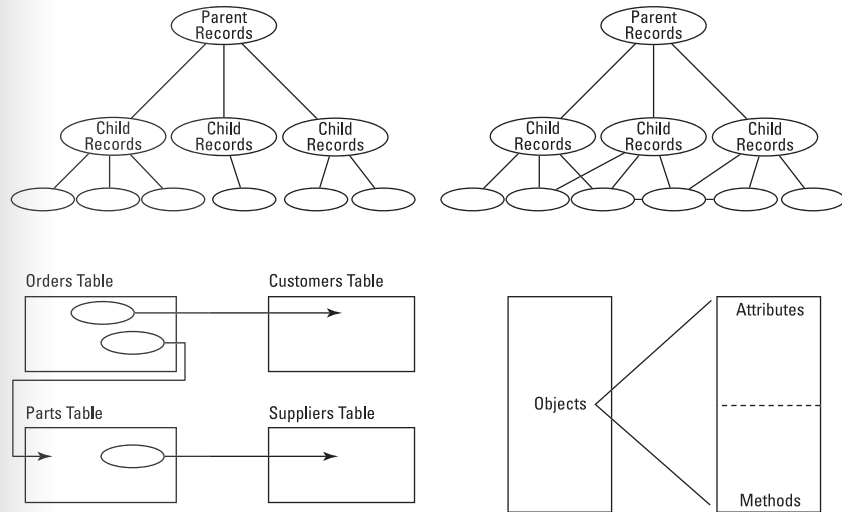
--

© John Wiley & Sons, Inc.

MD5, SHA-2, and HMAC are all correct. You must drag and drop all three answers to the box on the right for the answer to be correct.

» **Hotspot:** Select the object in a diagram that best answers the question, as in this example:

Which of the following diagrams depicts a relational database model?



© John Wiley & Sons, Inc.

Click one of the four panels to select your answer choice.

As described by ISC2, you need a scaled score of 700 (out of 1000) or better to pass the examination. All three question types are weighted equally, but not all questions are weighted equally. Harder questions are weighted more heavily than easier questions, so there's no way to know how many correct answers are required for a passing score. But wait — it gets even better! On the adaptive exam, you no longer receive a score when you complete the CISSP exam; you receive either a pass or fail result. Think of this situation as being like watching a basketball game with no scoreboard or a boxing match with no indication of who's winning until the referee raises the victor's arm.

All questions on the CISSP exam require you to select the *best* answer (or answers) from the choices presented. The correct answer isn't always a straightforward, clear choice. ISC2 goes to great pains to ensure that you *truly* know the material.



TIP

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



WARNING

Wrong choices aren't necessarily obvious on the CISSP examination. You may find a few obviously wrong choices, but they stand out only to someone who has studied thoroughly for the exam.

The Pearson VUE computer-adaptive, 3-hour, 100- to 150-question version of the CISSP examination is now available in English, Chinese, German, Japanese, and Spanish. As of April 15, 2024, ISC2 no longer offers a form-based (linear) exam option in other languages. You're permitted to bring a foreign-language dictionary (nonelectronic *and* nontechnical) to the exam, if you need one. Also, testing options are available for the visually impaired. You need to indicate your preferences when you register for the exam.

After the Examination

In most cases, you receive your unofficial test results at the testing center as soon as you complete the exam, followed by an official email from ISC2.



WARNING

In some rare instances, your unofficial results may not be available immediately. ISC2 analyzes score data during each testing cycle; if there aren't enough test results early in the testing cycle, your results could be delayed up to 8 weeks.

If, for some reason, you don't pass the CISSP examination — you have read only this chapter of *CISSP For Dummies*, for example — you have to wait 30 days to try again. If that happens, we strongly recommend that you read the rest of this book during those 30 days! If you fail a second time, you have to wait 90 days to try again. If *that* happens, we most strongly recommend and highly urge you to read the rest of this book — perhaps a few times — during those 90 days! Finally, if you fail on your third attempt, you have to wait 180 days. You'll have no more excuses; you'll definitely need to read, reread, memorize, comprehend, recite, ingest, and regurgitate this book several times!

After earning your CISSP certification, you must remain an ISC2 member in good standing and renew your certification every 3 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 40 CPE credits during each year of your 3-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 ISC2 website to receive proper credit.

You're also required to pay a \$125 (US) annual maintenance fee to ISC2. Maintenance fees are billed in arrears for the preceding year, and you can pay them in the secure members' area of the ISC2 website.



TIP

If you earn (or already have) multiple ISC2 certifications, you have to pay only a single \$125 annual maintenance fee each year to maintain all your ISC2 certifications.



WARNING

Be truthful on your CPE reporting, and retain evidence of your training. ISC randomly audits some CPE submissions.



TIP

When you receive your certification, register on the ISC2 website and provide your contact information. ISC2 reminds you of your annual maintenance fee, board of directors elections, annual meetings, training opportunities, and events, but *only* if you maintain your contact info — particularly, your email address.

