

## ***Introduction***

---

# **Preparing for the CISSP Exam**

---

There is really nothing magical about preparing for the CISSP exam, just organization and perseverance. Many people have successfully completed the exam and over time have shared many tips, tricks, and strategies that they used to master the exam. To help you get organized for the task ahead, and to lessen your anxiety about the exam, this section documents some of the suggestions of CISSPs who have gone before you. The section covers key points you need to know to properly prepare yourself to take the examination, from the twinkling in your eye to the receipt of the certificate designating you as a Certified Information Systems Security Professional.

### ***Find Out What You Need to Know***

Once you have decided to investigate the CISSP certification and think that certification might be right for you at this stage of your career, then you need to find out what it is that you are expected to know in order to become certified. To be a CISSP you must demonstrate a mastery of the Common Body of Knowledge (CBK) by successfully completing a 250 question examination administered by the (ISC)<sup>2</sup>. You can quickly determine what subjects are contained in the CBK by reviewing the *CISSP Study Guide* that (ISC)<sup>2</sup> offers via its Web site. This reference guide provides an outline of the subjects, topics, and sub-topics contained within each domain in the CBK, and with it you can readily identify terms and concepts that you need to know for the exam.

### ***Find Out if You Meet Certification Requirements***

There is no need to proceed further on your path to certification if you are not qualified to take the exam or to be a CISSP. Because of the stipulations placed on the certification by (ISC)<sup>2</sup>, you need not peruse the CISSP reading

list, attend CISSP preparation classes, or create a study plan unless you can meet the qualifications for applying for the examination. Go to the (ISC)<sup>2</sup> Web site (<http://www.isc2.org>) and review the examination application form to ensure that you are aware of and can comply with the requirements for taking the exam. These include:

- **Experience.** First, you must have three years of direct experience in at least one of the ten CBK domains. This experience must be through performance of duties as a practitioner, auditor, consultant, vendor, investigator, or instructor, and extends only to actual time worked. Required experience is cumulative. That is, if 50 percent of your job performance was directly related to a particular CBK domain, and you had worked in that capacity for four years, then you would have accumulated two years of direct work experience for the purpose of certification. You should also be aware that experience is a better teacher than study, and those with broad working experience in the CBK will have a much easier time passing the exam than those who do not.
- **Code of Ethics.** Also, to apply for the examination, you have to agree to read the (ISC)<sup>2</sup> Code of Ethics, to confirm that you have not in the past violated any of its provisions, and to confirm that you will adhere to the (ISC)<sup>2</sup> Code of Ethics in the future. Read the Code of Ethics; and if you find you cannot abide by them, then stop here and go back; the CISSP certification is not for you.
- **Background.** Finally, upon application, you must provide background information that could result in the rejection of your application. You must report to the (ISC)<sup>2</sup> if you have been convicted of a felony or if you currently have such a charge pending against you; you may be disqualified. Or if you have every been involved or publicly identified with hackers or hacking, you must explain this on your application, and it could lead to your application being rejected if your background with hackers/hacking does not comport with the Code of Ethics. Your application must also stipulate whether or not you have ever had a professional license, certification, membership, or registration revoked, or if you have been censured or disciplined by a professional organization or government agency. Reporting information of this nature will not automatically result in the rejection of your application, but it must be reviewed by the (ISC)<sup>2</sup> to determine if your conduct is consistent with the Code of Ethics.

### ***Find Out What You Know and Do Not Know***

When you have determined that you can meet the requirements for applying for the examination, and have a good idea of the kind of knowledge that you are expected to know to be certified, then you need to get a rough idea of what you know now, so that you can pinpoint your strengths and weaknesses

by domain. By taking a practice examination such as the one provided in this book, you can identify which domains you need to improve your knowledge, and which ones you do not need to worry about (or at least not have to spend too much time studying for). Because you only need to score 70 percent to pass the exam, that percentage is a good benchmark to apply to your expertise in each domain. If you can score 70 percent or above in a given domain on a practice exam, that is a good indicator that you are in fairly good shape to take the exam. Likewise, in domains where you fail to score 70 percent, then you should have a pretty strong indication that you need to do some work. Knowing where you need to concentrate your study efforts is the most important element in developing a plan for mastering the CISSP examination.

### ***Build a Study Plan***

Now that you know and have confirmed the domains on which you need to focus the majority of your time, you can build a study plan that permits you enough time to prepare for the exam. How much time is enough? Because even the best-laid plans go awry, you should expect to spend one month for every domain in which you fail to score 70 percent on a practice exam. Because of the need to anticipate distracters such as work, vacation, and family obligations, one month per domain is a good rule of thumb. Once you have calculated how much time you need to prepare, you can go to the (ISC)<sup>2</sup> Web site once again and identify an examination date and location that is consistent with this schedule. You should plan on applying for the exam at least six months prior to the exam date to ensure that you reserve a seat. Spaces go particularly fast for examinations offered in larger cities.

### ***Reference Materials***

Unlike several other certifications, there is no single reference work that you can purchase and cover the entire CBK to the depth necessary to pass the examination. Therefore, you need to build time into your study plan to locate, obtain, purchase, and use reference materials. The bibliography in this book is a good starting place for identifying by domain references that might be helpful to you. The (ISC)<sup>2</sup> Web site also provides an up-to-date reading list that you should consider in preparing for the examination. Many of the references can be readily purchased over the Internet and, in the case of many U.S. Government publications, can be downloaded cost-free. If you are fortunate, your organization or co-workers may already have many of the references that you need, or your company may be willing to purchase them if they are judged to be of long-term value.

### ***Study Courses***

If you are particularly weak (a score of 40 percent or lower) in several domains, your plan should include time for a formal CISSP preparation course. The

(ISC)<sup>2</sup> offers an intensive eight-day course over two weeks that provides comprehensive training in all ten domains. The Computer Security Institute and other firms offer shorter versions of the CISSP preparation instruction, focusing on students who desire refresher training in all ten domains. Also, the (ISC)<sup>2</sup> offers a one-day overview to familiarize potential CISSPs with the CBK. If you have the need, and can afford the time and expense, these courses can significantly improve your chances for passing the examination. The security professionals who teach such classes are CISSPs themselves and can help you learn how to understand the intent of the questions and how to best answer them. These courses cover a lot of important material that you need to know for the exam. However, because they cover so much, it is virtually impossible to retain it all for a long period of time. Therefore, if you take one of these courses, schedule yourself for an exam two to six weeks following the course.

### ***Group Study***

Your plan should also build in opportunities for collective study. If you can find someone to study with in your company or organization, in your local chapter of a professional security organization, or in your neighborhood, then you can prepare for the examination together. Dividing study tasks and responsibilities among two or more students is an effective means of expanding knowledge of the CBK, in reducing the amount of time required to prepare, and in providing a sounding board to discuss difficult concepts and ideas. Do not overlook online study groups either. They can provide you with an outlet for asking those peculiar but important questions that you cannot find the answer for in your reference materials. Typically, CISSPs belong to these study groups and can help you based on their actual experience.

### ***What to Study***

You will find it most productive if you concentrate on procedures rather than on the specifics of particular security technologies. The examination is designed to assess your grasp of terms and concepts at a high level across a broad collection of subjects. The proper perspective for approaching the examination is that of a corporate- or department-level information security officer who is required to perform various tasks that require having broad knowledge across the entire spectrum of the CBK. This would include knowledge of industry-standard procedures and standards, as well as a working knowledge of security technologies and the problems they are designed to counter. Knowledge of platform-specific vulnerabilities and controls is not required.

### ***Confirmation Letter***

Once you have applied for the examination, you will receive a confirmation letter from the (ISC)<sup>2</sup> stating the time, date, and location of the examination,

as well as other information you will need to take the exam. Be sure to bring this letter with you to the examination, along with a photo ID card to verify your identity. Without them you will not be allowed access to the exam site.

### ***The Night Before***

The night before the examination you should concentrate on getting a good night's rest, not in cramming for the examination. This is not the kind of exam that you can or should pull an "all-nighter" for. You should anticipate the need to memorize some material well before the exam. The CBK contains lists of information that you need to have at your fingertips — the OSI Model for example. Set aside time in your plan for memory drills to ensure you have this information down rote on the day of the examination. Consider using note cards, acrostics, or whatever it takes to help you remember information such as this. The evening prior to the exam you should not spend more than two or three hours making your final preparations. Use the remainder of the evening to relax and prepare for a good night's sleep.

### ***The Morning Of***

Make sure that you know how to get to the examination site so that you can get there in leisurely fashion, keeping your stress level as low as possible. Build in enough time to eat breakfast. It will help you get through a long examination. At least have a cup of coffee and read the newspaper to help you relax. Do whatever is necessary for you to remain calm going into the exam. You should plan on getting to the exam site at least 30 minutes prior to the time you are advised to arrive, just in case something goes wrong. It is advisable to take a bio break before going into the examination room because stringent procedures for leaving the room will be in effect once the exam starts.

### ***At the Exam Site***

You can anticipate producing your photo ID and confirmation letter to gain access to the examination site. The proctors are all security professionals and will check you in by the numbers. You will be required to take a seat at a standard writing table. You can expect to have sufficient space to work comfortably. Once the head proctor begins, you will be given verbal instructions, which will take about 30 minutes. During that time, the proctor will describe procedures in effect for the exam (restroom breaks, refreshments, scratch paper, asking questions, etc.). Each examinee will be provided a sealed examination booklet and an answer sheet, along with a pencil.

Multiple versions of the examination will be issued so that students sitting side-by-side will each have a different version. You will not be allowed to talk, and may be disqualified if you do. Upon the proctors' direction, all examinees will break the seal of their test booklets at the same time, and the

exam will begin. Once the exam starts, the head proctor will function as the official timekeeper and will periodically inform you of the time remaining, either verbally or by posting it in writing.

### ***What to Bring Along/Leave Behind***

It might be a good idea to bring along bottles of water or other refreshments, and also some snacks. However, be considerate of others taking the exam and do not bring anything that might cause noise when opening or unwrapping it. When you check in, show the proctor what you have brought along so that he or she can see that your bag only contains refreshments. You should also attempt to find out what the rules are on getting to your bag once the examination has started. Avoid bringing phones, pagers, calculators, PDAs, and other electronics with you to the exam. If you do, you will not be allowed to use them or even to have them within arm's length. You will be required to turn them off and stow them in the back of the room. If you have alarms on any of these devices (or on your watch), be sure to deactivate them to avoid distracting others.

### ***Your Objective***

The test will consist of 250 multiple-choice questions, each having four possible answers. Your task is to select the best answer from the four answers provided. The questions are arrayed in no particular order, and it is not obvious how many questions there are for each domain. You will only be graded on your answers to 225 of the examination questions. The remaining 25 questions are included in the examination as part of the vetting process for new questions. You will have no way of knowing which questions will be graded and which ones will not. Remember, you must attain a score of 70 percent to pass the examination. That should be your goal. You get no bonus points if you score above 70 percent. In fact, if you pass, you will never know your passing score. Hence, from your point of view, a score of 71 is the same as a score of 98.

### ***About the Questions***

There are a few generalizations that can be made about examination questions without revealing their content. Negative questions — those that ask you to identify an answer that is an exception — are avoided on the exam as much as possible. Also, the examination avoids the use of acronyms. The CISSP exam is international in scope and attempts to minimize U.S.-specific questions. The examination is given in English only. However, if English is not your first language and you need to use a dictionary to translate from your native language to English and vice versa, then bring one with you and ask the proctor if you might be permitted to use it.

### ***Manage Your Time***

You will have six hours to complete the examination, and will have plenty of time to complete it. You have a total of 360 minutes to complete 250 questions. In other words, you have 1 $\frac{3}{4}$  minutes for each question. That amounts to about 40 questions per hour. An effective strategy that has worked for many is to go through the exam three times. Go through the first time with the objective of answering the questions you know well, or those that you feel 90 percent certain of the answer. Make the second pass looking to answer all the questions that you feel 50 percent certain of the answer. With these, re-read the choices given, try to eliminate incorrect choices, and reconsider the remaining answers. That leaves the third time through to simply guess the answers if necessary. Perhaps by the time you get to this final pass, you will be mainly dealing with the 25 sample questions that will not be graded anyway.

### ***Take Breaks***

Plan to take breaks throughout the examination. Take brief eye/mind/stretch breaks where you are seated every few questions. Perhaps at the 60- or 90-minute mark, stand up and quietly go to the back of the room and take a stretch break, drink something, and eat a snack. Remember that the most common cause of headache is insufficient fluid intake. Try to get your mind off of the exam for a few minutes. This will help maintain your level of alertness. No more than one examinee at a time may go to the restroom, and must be escorted by a proctor while outside the exam room. This, of course, takes time and can lead to delays, so it is best to plan ahead.

### ***Keep Moving***

It is advisable not to spend too much time on any single question. Getting bogged down leads to frustration and loss of confidence. Whereas, looking for questions that you feel certain of the answer provides positive reinforcement and builds confidence. A good rule of thumb is that if you cannot answer a question in two minutes, then move on to the next one. Be sure to read each question carefully in as generic a manner as possible. Do not read into any question specifics that you may be familiar with from your experience. This leads to trouble and confusion. Simply read what the question asks, as well as the answers provided. One effective approach is to mask the answers and carefully read the question before uncovering the answers. You should always be aware of the time remaining so that you can pace yourself accordingly. Be sure to leave yourself enough time at the end to be able to treat the last questions with the level of attention they require. Answer all 250 questions. There is no penalty for guessing. So, if you hear the proctor say that you have five minutes remaining, then you will know that you should go through and guess an answer for each remaining question. You should

also be aware that any question in the exam might provide you with a clue to answering another question somewhere else in the exam. This is another reason why it is important to go completely through the examination at least twice.

### ***Comments Regarding Poor Questions***

You will be provided with an opportunity to comment on specific questions after you have completed the examination. The proctor will provide you with instructions on how to do this before the exam begins. If you have a question that you want to contest or comment on, be sure you can identify the “questionable” question once you have finished. In many cases, those that you will want to comment on will be from the group of 25 sample questions that are not graded. It is important for you to take the time to comment on such questions, not only for yourself but also for others who will take the test after you.

### ***Decompress***

After you have completed the examination, take as much time as you need to decompress, relax, and try to get back to normal after months of eating, breathing, and living CISSP. Enjoy life again. However, do not forget to record some general notes and impressions about those parts of the test that gave you trouble. It may come in handy if you discover that you did not pass. Do not, however, record specific question information — remember the Code of Ethics. Nor should you provide information about specific questions to others, either voluntarily or when asked. You will receive your exam results two to three weeks after you take the exam via normal mail. If you passed the exam, your notification letter will address you as a CISSP and will indicate your CISSP number. Later on, you will receive a CISSP lapel pin and certificate through the mail.

### ***If You're Not Successful***

If you unfortunately do not pass the exam, the letter from the (ISC)<sup>2</sup> containing your exam results will provide your overall score as a percentage, as well as a breakdown of results by domain. This is valuable information that allows you to concentrate on those domains in which you did poorly, and is a great benefit in preparing to take the exam a second time, with hopefully a better result.



---

# PRACTICE STUDY QUESTIONS

---



