ConversationalGeek®

Conversational Guide to CISSP Certification

By Derek A. Smith (CCISO, CISSP)

In this book, you will learn:

- Everything you need to know about becoming CISSP certified
- How to effectively prepare and study for the CISSP exam
- The best ways to support your study

Sponsored by

getCISSPcertified.com

getCISSPcertified.com is the brainchild of cybersecurity veteran Derek A. Smith. With over 30 years of security and law enforcement experience as both a Federal agent and information security professional, Derek built getCISSPcertified.com to connect with those seeking to achieve CISSP, aiding in their journey with training that uses real-world experience and application to help ensure success in certification.

For more information, visit
www.getCISSPcertified.com

Conversational Guide to CISSP Certification

Derek A. Smith

ConversationalGeek®

Conversational CISSP Study Guide

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Derek A. Smith
Project Editor:	Pete Roythorne
Copy Editor:	Pete Roythorne
Content Reviewer:	Nick Cavalancia

Note from the Author

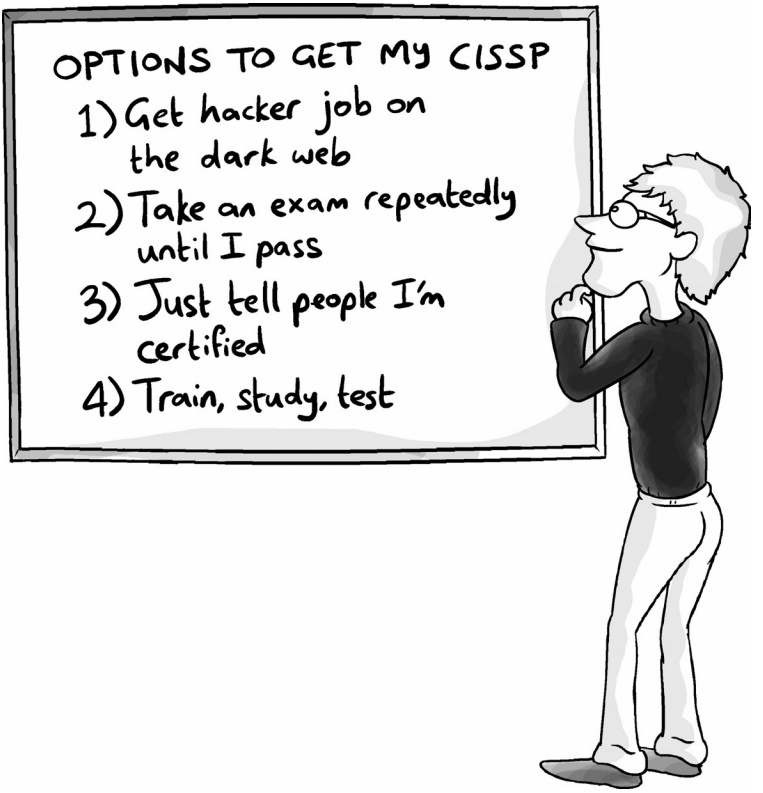
Before we start, I want to congratulate you on beginning your journey to becoming a Certified Information System Security Professional (CISSP). The International Information Security Systems Certification Consortium – or (ISC)² – has gone to great length to produce and maintain a world-class and world-renowned exam, recognized as the gold standard of Information Security certifications.

Preparing for an exam of this magnitude is no easy endeavor, even for the most experienced InfoSec professional, so if you are looking for tips on what the CISSP certification is all about and how best to prepare for it, then you have come to the right place.

Keep reading this guide.

Derek A. Smith, CCISO, CISSP
Cyber Security Expert, Author, Speaker, and Trainer

Everything you need to know about becoming a CISSP



The CISSP is an information security certification for experienced security analysts. It was created by the International Information Systems Security Certification Consortium $(ISC)^2$ to ensure professionals in computer security have a standardized body of knowledge for the IT security industry. It covers eight different areas, or domains, which are thought to be the critical areas security professionals need to understand to be successful in their role.

Why Should You Want the CISSP Certification?

Obtaining your CISSP is essential if you want to be successful in your career. Many employers value the CISSP as a standard of professionalism for security professionals. While the investments in time and money are substantial, the career rewards can be valuable as professionals with the CISSP designation are in high demand.

Burning Glass Technologies, a career site, reported that nearly a quarter of cybersecurity job postings requested the CISSP. And according to the $(ISC)^2$, "certified information security professionals earn a worldwide average of 25% more than their non-certified counterparts."

Possessing the CISSP certification and the knowledge needed to obtain it can help you to enter and advance in the community of cybersecurity leaders. If nothing else, having your CISSP demonstrates to employers that you are a professional who knows how to design, engineer, implement, and run an information security program.

It's worth noting that the CISSP is the first information security credential that could meet the strict conditions of ISO/IEC Standard 17024.

How Do You Become CISSP Certified?

To become a CISSP you must fulfill the following requirements:

1. Prove your experience – you must have five years of paid full-time security work experience in at least two of the eight CISSP Common Body of Knowledge domains (Security & Risk Management, Asset Security, Security Engineering, Communications & Network Security, Identity & Access Management, Security Assessment & Testing, Security Operations, and Software Development Security).

If you don't meet the five-year threshold, don't panic… you do have two alternative options:

- You can obtain a one-year waiver if you: hold a four-year college degree, or have an advanced degree in information security from a U.S. National Center of Academic Excellence in Information Security, or hold a credential from the $(ISC)^2$-approved list (www.isc2.org/Certifications/CISSP/Prerequisite-Pathway#).
- If you don't have these, you can still enroll and pass the CISSP exam and become an Associate of $(ISC)^2$. This gives you up to six years to obtain the required work experience for your CISSP certification.

2. **Pass the exam** – You must complete the CISSP exam with a minimum score of 700 out of 1,000. The exam includes a mix of multiple-choice and advanced innovative questions.

The (ISC)^2 CISSP webpage (**www.isc2.org/Certifications/CISSP**) offers a download of the exam outline as well as a link to a Study App (available through the App Store and Google Play). You can also obtain the official textbook and test your knowledge with CISSP Flash Cards. If you need more than self-study materials, (ISC)^2 and a lot of third parties offer CISSP in-class and online training.

3. **Get endorsed** – Once you complete the CISSP exam, you'll have to subscribe to the (ISC)^2 Code of Ethics (**www.isc2.org/Ethics**) and complete an endorsement form (**www.isc2.org/Endorsement**) to become a CISSP. The endorsement form must be signed by another (ISC)^2 certified professional who can verify your professional work experience. You must submit the completed form within nine months of passing your exam to become fully certified, because passing the exam doesn't automatically grant you certification status.

4. **Prepare for an Audit** – It is crucial that you don't fudge or cut any corners in your CISSP application process because the (ISC)^2 randomly selects certified individuals for auditing. If you are found to have falsified any of your application data, your CISSP will be revoked.

Keeping Your CISSP

After you become fully certified, you'll have to maintain your credential. The CISSP certification lasts for three years. During this period, you must make time for at least 120 continuing professional education (CPE) credits within each three-year interval. Of these 120 credits, at least 80 must be Type A, or directly relating to the information security profession. The remaining 40 credits can be either Type A or Type B; Type B credits constitute other forms of professional skills development. Also, CISSPs are required to pay an $85 maintenance fee during the three-year cycle ($255 total). The $(ISC)^2$ will provide you with full information on CPEs once you are certified, but for more details on maintaining your certification status, visit isc2.org.

The CISSP Exam Format

The CISSP exam recently went through a change. This does not happen very often.

$(ISC)^2$ has introduced Computerized Adaptive Testing (CAT) for all English CISSP exams worldwide. Based on the same exam content outline as the linear, fixed-form exam, $(ISC)^2$ claims the CAT version is a more precise and efficient evaluation of your competency. It enables you to prove your knowledge by answering fewer items and completing the exam in half the time.

If you already prepared for the existing format, don’t worry. While the exam has been reduced from six hours to three, and questions to be answered has decreased from 250 to 100-150, the other parameters remain the same.

The new question format includes multiple-choice and advanced innovative questions, and the passing score is 700 out of 1000 points.

Here is a list of the key domains and their weight within the exam:

- Security and Risk Management – 15%
- Asset Security – 10%
- Security Engineering – 13%
- Communications and Network Security – 14%
- Identity and Access Management – 13%
- Security Assessment and Testing – 12%
- Security Operations – 13%
- Software Development Security – 10%

How to Prepare for the CISSP Exam in Eight Weeks

To pass the exam, you have to approach the questions from a management perspective instead of the technical perspective of most IT certification exams. You should be able to explain issues such as architecture and access control for protecting information system assets to clients and other stakeholders. To do this, you have to understand how to assess the business or organization's current operational policies for incident response and make recommendations to those concerned for improvements to business or organization security.

You need to know how to compare and contrast different cryptographic protocols and make recommendations based on this analysis of security needs. Creating systems of policies, standards, procedures, and guidelines with clients and stakeholders in mind should be the end goal of a CISSP.

Being able to explain the importance of disaster recovery policies and demonstrate multiple and effective strategies to stakeholders is a key skill tested in the CISSP.

In terms of technical knowledge, you must demonstrate proficiency in several areas. Proficiency in network architecture and design, being able to implement network architecture to anticipate threats and best use given sometimes limited resources. This includes demonstrating a clear understanding of software security applications lifecycle effectiveness. You also should have the ability to collect digital forensic evidence while maintaining the integrity of the evidence gathered. Finally, you

must demonstrate knowledge of physical security systems and how they add value to network security systems.

How to Pass the First Time

Even the most complicated tasks can be tackled using the simplest of solutions, and the CISSP is no exception. Your most significant help in passing the CISSP exam is absolutely going to be your experience. With five years under your belt, you really should be strong in at least two of the eight domains.

That being said, that leaves around six domains that you might not have much experience in at all. However, you are not alone if you feel overwhelmed by this, almost every CISSP I know, and every student I taught to pass the exam felt the same way. Very few CISSPs have experience in all eight domains before passing the exam, and I would be surprised to find many that regularly focus on all eight once they have qualified. It's really not common in the industry.

Accepting you have weaknesses is essential, and you can use it to help guide where you spend your study time. First of all, keep things simple. You can break your approach down into two stages which should take around two months to get you ready for the exam: *preparation*, which should take 1 week at the most, and *studying*, which should take approximately 7 weeks.

Stage 1: Preparation

Here I am talking about preparing for how you will study, what you will study, and when! This should really only take a day to sit down and work out, but if you decide to order any supplies or study material, it could take you a full week.

Nobody ever picked up the CISSP book and read it from start to finish and got the most benefit they could. You have to be methodical in your approach and know how to get the right

results from your study. Your first steps into CISSP preparation should be:

- Understand your strengths and weaknesses – Highlight which domains you've worked in or studied, where you need minimal study, and which domains you need to focus on the most.

- Find out which learning style is the best for you.

- Map out when you can study – Don't just "plan" on studying, create a schedule, and put time aside, away from distractions when you can really focus.

- Decide where you will study – Studying at home is sometimes hard, particularly with family around, and you can find yourself jumping from room to room to avoid distractions. So, try and find alternatives, like studying in the local library, hanging out at a coffee shop, or somewhere similar.

Once you have a plan that covers all the above points, you should have a good idea of what areas you will be focusing on, as well as knowing where and when you will study.

Here is what I recommend to get the most out of your study sessions over the next seven weeks.

Stage 2: Study

Weeks 1 – 4

- Test yourself before and after – Check your knowledge before you read a new domain using practice tests and repeat afterward to measure the improvement. I use the $(ISC)^2$ official study guide to teach my course. In this

book, there are short quizzes at the end of each chapter. Take the exam before and after each chapter and record your progress. This should typically be around 20 questions.

- Do not move on until you are confident you have learned the material – It's easy to read one chapter after another, but unless you can answer at least 90% of the chapter tests correctly, then you still have learning to do. Each chapter only has about 20 questions, so you should be hitting 90%+ easily by your third attempt or sooner.

- Do not waste time on content you already know – Every session counts. Reading a chapter on a subject you know inside out is very likely a waste of time. Instead, focus on your weak areas, and if there is time at the end, use it to check your knowledge on these areas.

- Use multiple study sources – You may learn best by actually doing a task; therefore reading, Computer Based Training (CBT), or live training may be much more challenging for you. However, I suggest you use a variety of resources. You should test your knowledge on a chapter and record your score, then read the chapter, then watch the corresponding CBT video or attend your live training session, and finally test your knowledge again. This won't make your study any easier, but it may help unfamiliar content to sink in after absorbing it in different ways.

Weeks 5 – 7

- Begin using full-length practice tests – In the weeks leading up to the tests, I would recommend moving on to the full practice tests you can get online (or as a CD with a test engine in my course.) Most of the good providers will break down your results into categories so that you can identify which areas you are still weak in. With around two to three weeks left before the exam, you should have covered most of the subjects and now be testing yourself regularly.

- Use the results to figure out where you need to focus and go back to the material to review – Make sure you are testing yourself on a pro/hard level on the test exams. There's no point getting 100% on the easy level only to get overwhelmed on the day of the exam.

Supporting Study Guides

I highly recommend using the official CISSP Common Body of Knowledge (CBK) reference guide. As an $(ISC)^2$ trained instructor, I can tell you that many of the questions logically come from their own material. After all, it *IS* the official study guide. This book is a bit hard to read, and you may find it boring.

Fortunately, there is another, much easier to digest, version of this book: CISSP $(ISC)^2$ Certified Information Systems Security Professional Official Study Guide. Instead of being broken into domains as the CBK is, it is split into chapters breaking the domains into easy to study parts. Make sure you use the sample tests at the end of each chapter to measure your understanding of the material.

While there are other good books on the market, I feel you cannot go wrong using the official guides. There will be no confusion over what was meant or some other author's interpretation of the material.

CBT Videos

You can use CISSP Computer Based Training (CBT) if you wish. I will not recommend any particular one. I will leave that choice up to you. You can watch the videos at work, at home, or while traveling. Combining the study books with CBT content can really help fill any gaps you may have. They can, however, be a little on the pricey side.

Practice Tests

There are many free and fee-based test engines available, and some are pretty good. Be aware that unlike many of the other IT certifications, you are not going to find a test engine with the exact CISSP questions. $(ISC)^2$ is pretty good about maintaining the integrity of the exam.

Get Some Training

Interaction with a real instructor can be quite beneficial. With self-study and CBT training, you are not able to ask questions to increase your understanding. For instance, in my training, I break difficult information down by using real-life scenarios or analogies that are similar but simpler to understand. A live training class will help you prepare for the exam efficiently and will also reduce your preparation stress, as the certified instructor will guide you regarding the certification exam with the help of the training material available.

There are two types of live training classes to choose from:

- CISSP Bootcamp – a boot camp is usually a 40-hour, one-week course. If you are pretty much ready to pass the exam, this method may work for you. I teach boot camps for clients, and I have found that If you are new to the material and have a lot to learn this is not the best method for you as you will be bombarded with a tremendous amount of material that you must digest and absorb in a very short time.

- CISSP learn term course – a long-term course is better in my opinion as you have time to actually read the books and study the other material, such as flashcards, practice questions, etc. I teach my course over six weeks with my students attending live classes with me twice per week.

They have plenty of time for learning, study and review, and their outcome on the exam is much better.

Final Steps

Once you've prepared for your CISSP exam, the time has come for the real evaluation. First, you will need to create your Pearson VUE account. Pearson VUE is one of the chief providers of global, computer-based testing for licensure and certification exams. When you create your account, you will find details regarding the testing locations, policies, accommodations, and more.

Register to Take Your Exam

Once you complete your Pearson VUE account, you can proceed with the registration, for which you will have to complete the examination agreement. You will have to agree with the truth of your assertions regarding professional experience; you will also have to legally commit to the adherence of the (ISC)² Code of Ethics. Also, you will need to review the candidate background questions. Once completed, just pay the fee for your CISSP exam and you are good to go.

Take the Exam

The ultimate judge of your ability has come; it is the day of your CISSP exam, get to work.

Passed the exam? Great! Now you will have to subscribe to the (ISC)² Code of Ethics to avail your CISSP certification.

Get Yourself Endorsed

The final step is to have your application endorsed within nine months from the date of your exam. To confirm your professional experience, this endorsement form must be finished and signed by an (ISC)² certified professional, who is also

an active member. And in case you are unable to find a certified individual, (ISC)² can endorse you.

Final thoughts on CISSP certification

Keep in mind that the CISSP is about lifelong learning, so passing the exam is just the first step. To retain your CISSP certification, you have to be recertified every three years and get continuous professional education. To earn the Continuing Professional Education (CPE) credits I need to maintain my CISSP certification, I attend and teach cybersecurity courses and webinars, write white papers, books, blogs, speak at and attend events, and so on. Even more valuable, these activities help me continuously improve my knowledge of the information security industry and stay on top of news and trends.

Certifications That Can Help You Reach the CISSP

If you are certain that the CISSP path is right for you, but you have no relevant work experience, look into becoming an Associate of $(ISC)^2$ – as I mentioned earlier in this book. This is ideal for students and career changers and will allow you to take advantage of educational opportunities, forums, and peer networking offered through $(ISC)^2$. Another approach is to get the entry-level A+, Network+ and Security+ certifications from CompTIA. With that foundation, you can apply for a security-related position and get some much-needed hands-on experience in the IT arena.

If you've been working in IT security for a year or two, consider pursuing the $(ISC)^2$ Systems Security Certified Professional (SSCP) credential. Although it's not an official prerequisite, the SSCP is viewed as a precursor to the CISSP, covering many of the same topic domains. In theory, achieving the SSCP can also lead to the kind of security position needed to fulfill the CISSP work experience requirement.

Beyond the CISSP

Once you get your CISSP, you might be interested in specializing in architecture, engineering, or management, perhaps for another boost in pay. The $(ISC)^2$ program offers concentrations in those areas for CISSP credential holders, called ISSAP, ISSEP, and ISSMP, respectively.

And, because cloud computing and virtualization have become extremely important in the IT space over the past few years, there's one more advanced-level $(ISC)^2$ certification to consider: the Certified Cloud Security Professional, or CCSP. This certification, formed in cooperation between $(ISC)^2$ and the Cloud Security Alliance (CSA), is aimed at folks who procure, secure, and manage cloud infrastructures or who purchase cloud services. The CCSP requires five years of relevant on-the-job experience, but you can use the CISSP to substitute for the entire requirement.

Be sure that a CISSP is the route you want to take, and that you can complete the credential, before embarking on this long and expensive journey. However, if you set realistic certification targets and manage your time wisely, you can't help but succeed.

NOTES

The CISSP is the gold-standard of InfoSec certification. Possessing the CISSP certification and the knowledge needed to obtain it can help boost your job prospects in the community of cybersecurity leaders. However, preparing for an exam of this magnitude is no easy endeavor, even for the most experienced InfoSec professional. So, if you're looking for tips on what the CISSP certification is all about and how best to prepare for it, then this book is for you.

About Derek A. Smith

With over 30 years in the security industry, Derek A. Smith is a former government agent, cybersecurity SME, holds a variety of certifications (CISSP, CEH, CCISO, Security+, etc.), eight college degrees, is a published author, conference speaker, cybersecurity analyst for several international and local television news stations, government program manager, and more.