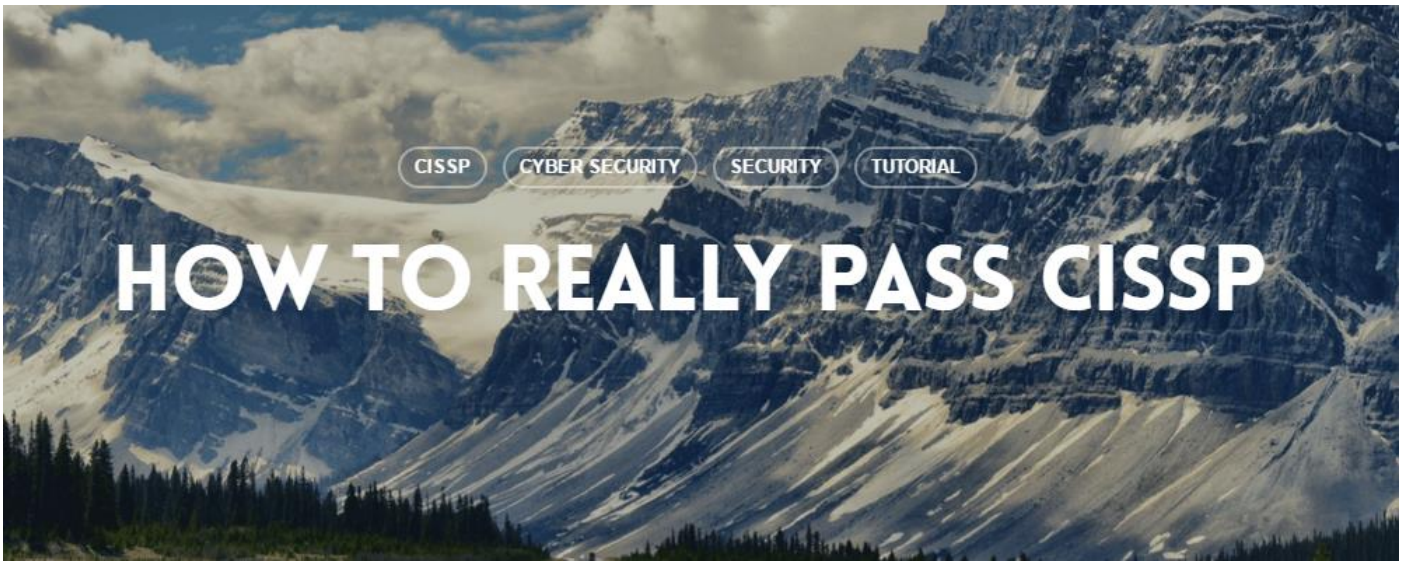



***In this post you find out – How to Really Pass CISSP, First Try in Five Steps.***

**Your all-in-one guide to passing the CISSP exam.**

**How to Really Pass CISSP**

By now, you have probably done your research on what it is you need to do in order to become CISSP and that passing the exam is not as straight-forward as other IT Security certifications. This blog aims to provide you with clear instructions and a solid strategy for passing the exam.

Embarking on the path of CISSP certification in 2014, I knew few qualified CISSPs and was dependent on publicly available (and unverified) information in the forums and the web.

**What I Learnt…**
A lack of information on how to really pass the CISSP exam…
There was no concise guide to passing the exam. Each forum post, website, CISSP exam experience was different to the next. Determining what I actually needed to do for the exam was unclear. The more I researched CISSP study and exam requirements, the less clear it became… I had to figure it out the hard way and this is what I learnt.

Developing a well formed strategy is crucial to passing CISSP. Combined with long study hours, perseverance and the right guidance as shown in these five steps.

**Five Steps to Pass CISSP:**
- ✓ Step One: Know what CISSP is
- ✓ Step Two: Know the Exam
- ✓ Step Three: CISSP Study Materials
- ✓ Step Four: Winning Strategy
- ✓ Step Five: Exam Strategy

CISSP® | Certified Information Systems Security Professional

**Step One: Know what CISSP is**

CISSP is a managerial exam, aimed at measuring competency in **IT Security** decision-making.

It's interesting to hear different people's perspectives. Risk managers, compliance officers and managers will tell you it's a very technical exam. While engineers, architects and other techies will tell you it's not very technical.

CISSP Expert, Eric Conrad, author of CISSP Study Guide (2015) settles this debate by confirming that CISSP is a managerial exam.

This is important to know when preparing for the exam as questions are not formatted logically as you would see in other IT Security exams.

CISSP is a significant investment in time and money so you need to weigh this up with your circumstances

to determine how best to meet these investments. Cost of sitting CISSP exam can be found at: https://www.isc2.org/uploadedfiles/certification_programs/exam_pricing.pdf

**Step Two – Know the Exam**

- ✓ 250 questions
- ✓ 25 questions are experimental and not graded. Which questions these are is unknown.
- ✓ Pass mark is 700 out of 1000 – weighted.
- ✓ 6 hours to complete the exam.
- ✓ Breaks are permitted but restricted (you may be escorted for any bathroom visits).
- ✓ Exam is not open book.
- ✓ Computer based testing is the most common standard.
- ✓ PearsonVue is one of the most popular training centres offering test centre where candidates can sit the CISSP exam. Plan in advance by visiting the training centre site in order to locate your closest centre and book your exam in advance.
- ✓ Know the exam structure inside out. A free outline is available here at (ISC)2 website.

**Know the Content**

CISSP content is broad but not very deep. In other words, you need to know the principles of each of domains and sub-topics but you don't need to be an expert in all of them.

The CISSP exam contains a total of 8 domains, consisting of:

- ✓ Security and Risk Management
- ✓ Asset Security
- ✓ Security Engineering
- ✓ Communication and Network Security
- ✓ Identity and Access Management
- ✓ Security Assessment and Testing
- ✓ Security Operations
- ✓ Software Development Security

Prior to 2015, there were 10 domains with similar content. The differences between the old version of CISSP and the current version will be discussed in a separate post, as part of The CISSP Manifesto series.

**Code of Ethics**

On top of the 8 high-level domains described above, CISSP candidates also need to know (and practice!) the Code of Ethics.

Know this inside out as this will be included in the CISSP exam.

You can access (ISC)2 Code of Ethics at: https://www.isc2.org/ethics/default.aspx

**Step Three – CISSP Study Materials**

One book is not enough.

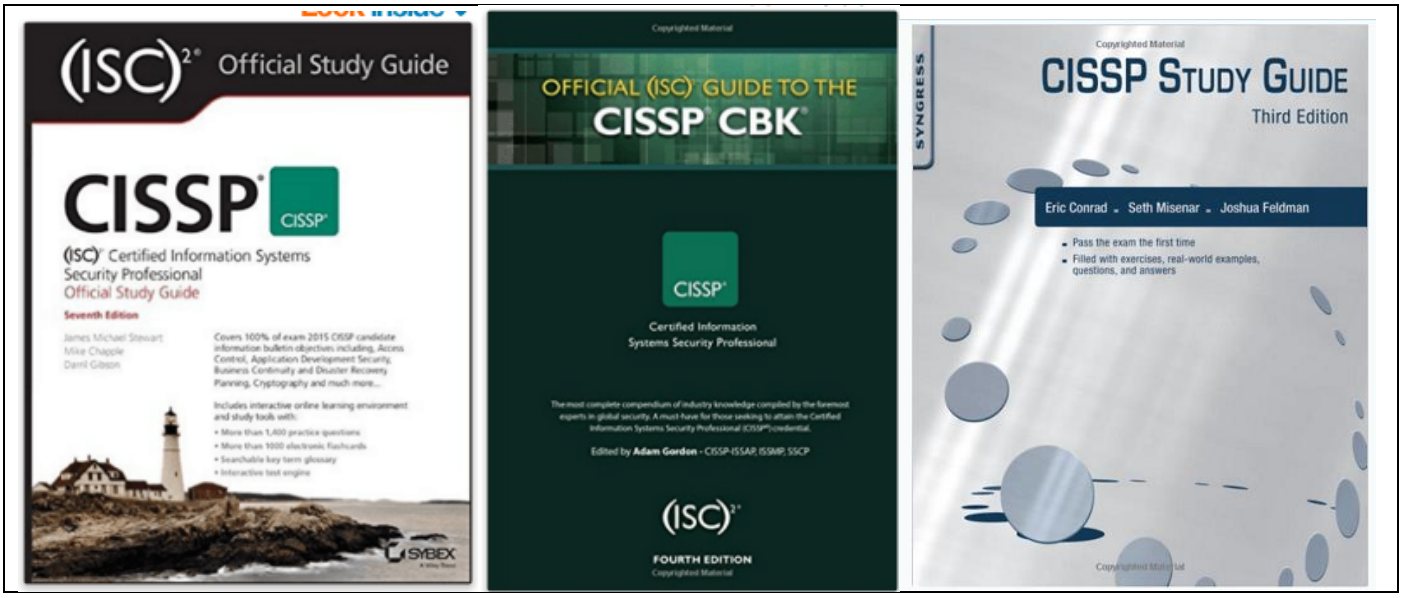
An array of resources is required. It is important to ensure that you use the most up to date books and resources to prepare.

Recommended CISSP Exam Material:

- ✓ CISSP ® Certified Information Systems Security Professional Study Guide 7th Ed – By James Stewart, Mike Chapple, Darril Gibson
- ✓ CISSP Study Guide Paperback by Eric Conrad
- ✓ Official (ISC)2 Guide to the CISSP CBK,
- ✓ Fourth Edition (ISC2 Press) Hardcover by Adam Gordon

A plethora of FREE resources available on the web Practice Exams (discussed further below).

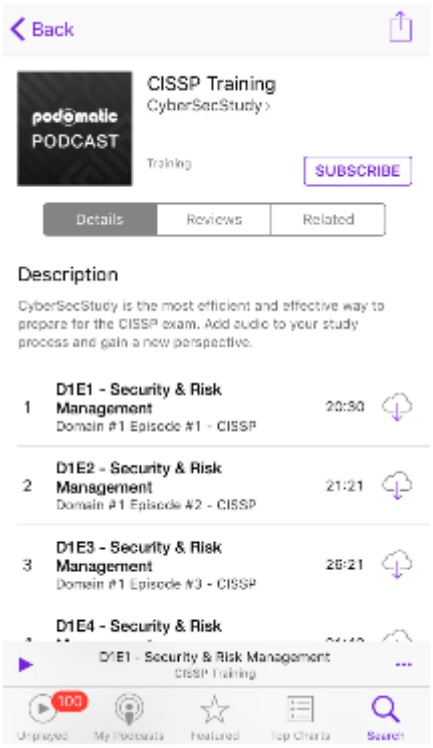
Older materials such as Shon Harris CISSP All-in-One 6th edition is still useful however post-2015 materials (although limited) are recommended.




**Other CISSP Resources**

**Podcasts**
When studying for CISSP I would listen to CyberSecStudy's CISSP Training Podcast as I ran daily errands. I found this a great way to maintain CISSP study consistency.

CISSP Podcast:




The content is pre-2015 CISSP exam however was useful with reinforcing concepts such as Security Models – still used in today's exam.

**Amazon Kindle**
Investing in a Kindle is a great way to take your CISSP materials with you wherever you might go, without having to lug around heavier cumbersome paperback versions. The study materials recommended below all come in Kindle format.

Keeping one hard-copy version of your main CISSP materials is useful for a central point of reference.

**Step Four – Winning Strategy**

**How to Study**
Go through and study each chapter's domain individually until you get 80 – 90% on the practice exams before you move on to the next domain.

This will enable you to test your comprehension level of the material you have covered.

Any areas which you are weak in you can then revise/retest before moving on to the next domain.

The order, in which you study the domains, comes down to the individual's strengths and weaknesses in each of the CISSP domains.

It is recommended to start with first domain – Security Governance through Principles and Policies. That way you will solidify the overarching principles (AIC!) and can then work through the remaining domains at your own discretion.

Before the exam, take one to two weeks out to go through all of the domains inside out before you sit the exam.

Remember:
- ✓ 50% of your time should be spent studying CISSP materials
- ✓ 50% of your time should be spent practising exam samples.

**Plan**
Setup a study schedule. This will depend on how quickly you decide to the CISSP exam.

Anywhere from 2 months to 1 year of preparation depending on how quickly you would like to sit the exam and previous familiarity with the content.

**Consistency is Key**
Daily practice if possible, even an hour during week days and up to 10 hours on the weekend, whatever you can spare.

This is a tough stretch for most busy Information Security Professionals!

However there are a few techniques to assist with this.

**How Do You Learn?**
Know what learning style suits you. Visual, auditory, kinesthetic or a combination?

How you learn will determine whether you select to attend training, self-study etc.

I have spoken to many CISSPs who have attended boot-camps and training courses with mixed reviews on the effectiveness. It really depends on how best you learn.

CISSP Boot Camp usually runs for 5 days straight and can cost anywhere between £1489 and £2499, not cheap! This requires an investment in time and money.

A cost-effective alternative is to enrol in an online course. eForensics Magazine (eforensicsmag.com) is a great organisation and offer online CISSP course – 2015 CBK for a fraction of the cost of in class trainers.

For more information see: https://eforensicsmag.com/course/the-ultimate-cissp-study-guide-w22/

Another good strategy may be to see how far you can get with studying CISSP on your own before deciding whether you need to invest in additional training.

**Join a Study Group**
Look for any CISSP Study groups in your area. Meetup.com is a good place to locate study groups in your area.

If there is not one in your city – start your own.

It will make the marathon to becoming CISSP more enjoyable, keep you on track and you can network with other professionals in your area.

Join our London CISSP Study Chapter at: http://www.meetup.com/London-CISSP-Study-Meetup/

**Other Study Tips**
- ✓ Don't Cram
- ✓ Don't Memorise
- ✓ Do-Know the Concepts. For ex. AIC (Availability, Integrity and Confidentiality).
- ✓ Mnemonics are a great tool for remembering acronyms.

Cramming a couple of weeks before sitting CISSP is not a suggested strategy as the material you have studied needs to be committed to long-term memory.

Memorising material is also not recommended as you need to understand CISSP CBK concepts fully to pass! The exam questions are designed in such a way to test your comprehension so that memorising information is ineffective.

**Know the Concepts – Availability, Integrity and Confidentiality (AIC)**

Understanding AIC will give you a solid understanding of the principles of Information Security as you move through CISSPs CBK; you can then apply these concepts to the technology.

For example – You may be asked what the difference between a Message Digest and a digital signature. Recalling AIC principles, you will know that a message digest is used for Integrity and a digital signatures are used for authentication.

Mnemonics are useful for remembering acronyms you need to know as part of the exam. An example familiar to many antipodeans is – Never Eat Soggy Weetabix or NESW. A way for schools to teach: North, East, South and West.

More mnemonic techniques can be found at: https://www.mindtools.com/memory.html

**Practice Exams (Plenty!)**

The exam will test you on CISSP's Common Body of Knowledge (CBK). Practice exams are your way measuring **your ability to Pass.**

As mentioned. Practice exams are just as important as the study materials.

You should also anticipate using a variety of different exams. I have seen some candidates state they practiced 5000 questions before sitting CISSP exam. I would estimate I completed 2000 practice questions as part of my preparation.

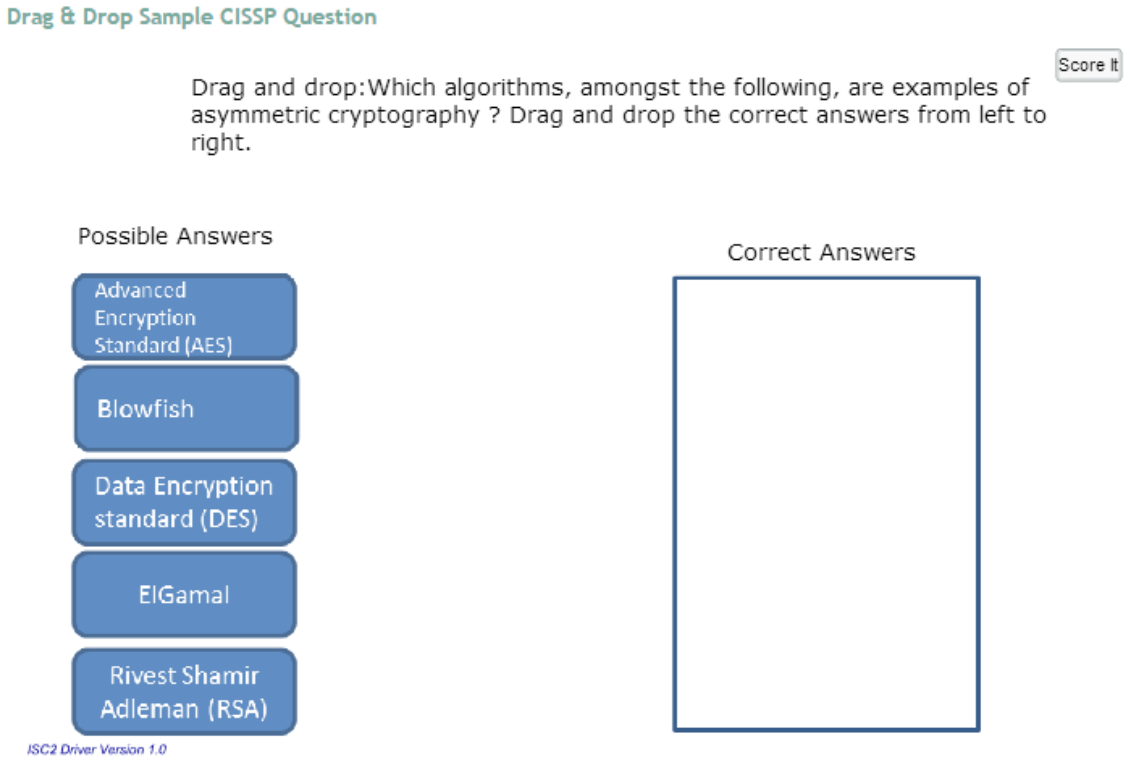
Each CISSP book will contain exam questions at the end of each chapter. You will need more practice than these to be prepared for different styles of questions. Most likely requiring you to purchase 2 or 3 different exam sets. CCCure.com offers CISSP scenario based questions, which I recommend to readers unfamiliar with scenario style questions.

There are also many free versions available and I have provided a list of great free resources at the end of this chapter.

**Exam Questions:**
- ✓ Multiple Choice
- ✓ Scenario
- ✓ Drag/Drop
- ✓ Hotspot

By practising the exams, you will get a better idea of what to expect in the exam. Be prepared for the four different styles of questions mentioned above.

Here is an example of a typical Drag/Drop question you can expect to see in the exam:




For more information go to: https://www.isc2.org/innovative-cissp-questions/default.aspx

**Scenario / Judgement Questions**

Almost half my CISSP exam's questions were scenario / judgement type questions.

In most cases you will see this style of question referred to as a Scenario question.

Based on the exam I sat, these scenarios were designed to test your judgement.

I had not come across this type of questions in any exam before – or in CISSPs practice exams.

I was caught off guard (actually shocked). No practice exam had prepared me for this style of question.
** Exam Tip **
Be prepared to see scenario or judgement based questions containing – such as BEST/MOST/LEAST

You will be presented a scenario and you need to pick the best option out of the multiple choices provided, in some cases all options presented are correct.

This can take you off guard as more than one of the options is correct – at least logically. You will need to think of this from a managerial perspective and select the best option.

Here is an example of judgement style question:

**QUESTION 70**
Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos

**Correct Answer:** A
**Explanation**

**Explanation/Reference:**
SSO can be implemented by using scripts that replay the users multiple log-ins against authentication servers to verify a user's identity and to permit access to system services. Single Sign on was the best answer in this case because it would include Kerberos. When you have two good answers within the 4 choices presented you must select the BEST one. The high level choice is always the best. When one choice would include the other one that would be the best as well.

Question taken from IT Cert Pass. Get your free sample CISSP Questions at:
http://www.itcertpass.com/samples.html

Questions can be more vague than this example – so be prepared.

There are not many examples of judgement/scenario style questions available on the web you can expect to see on the CISSP exam. CCCure (www.cccure.org) has scenario styled CISSP questions available on their site to be purchased.

**Ready to Sit the Exam?**
- ✓ You have just finished your one or Two weeks of solid CISSP study prior to sitting the exam.
- ✓ You are consistently scoring 80 – 90% across all of the CISSP Domains.
- ✓ You have covered all of the suggested content (inside out)

If this is the position you have found yourself in – You're ready to take the CISSP exam.

**Step Five – The Exam**

**Timing**
A 6 hour exam schedule is gruelling. Common-sense recommendations such as to being well-rested and wearing appropriate attire, need to be considered.

You are given 6 hours to sit the exam. Sounds like a lot?

When answering 250 questions in 6 hours. That gives you less than 1 and half minutes per question. With this timing, you need a strategy in order to be able to answer questions within this time.

**Exam Strategy**
Given the time constraints, you will need to have a strategy for your exam.

As you need to get the best out of the time you have available. How you choose to tackle answering questions is at the discretion of the individual depending on the style that suits them best.

A few suggestions are provided:

**Click through the entire test to begin with**
You may want to quickly click through the entire exam questions, from start to finish before you start answering any questions. This will give you an overview of what to expect. Possibly even allow you to connect dots amongst questions, enabling you to answer with greater accuracy.

**Read the Questions**
Identify Keywords in questions – Best, least, not, first.

Re-read if unclear

**Answering Questions**

- ✓ Answer what you know to be correct.
- ✓ Flag any questions you're not certain on and go back to these at the end of the exam.
- ✓ Questions you are unsure of the answer to, review these to try to eliminate wrong answers first.
- ✓ Decide what it is that (ISC)2 is looking for.
- ✓ Time Management is important. You have less than 1 and a half minutes per questions. Answer all of the questions – don't leave any blank. Walking out of the exam.

**My Experience**

Walking out of the exam: Underwhelming.

An experience shared by most CISSPs upon completing exam.

For me, I had no idea whether I had passed or failed – due to the nature of judgement style of questions contained in the exam.

Fortunately the Test Centre staff gave the good news – I Passed.

Officially CISSP!

***Certifiably with endorsements, more on that later***

At the end of the day being able to pass CISSP means something, what that is, is debatable.

An Achievement? Professionalism? Competency? An Accomplishment – Absolutely.
I hope this guide has been useful to you. All the best with the CISSP exam.

Here is a summary of the Top Tips and Free Resources.

**Top Tips**

- ✓ Know the concepts
- ✓ Exam Study Strategy – 50% CISSP material and 50%
- ✓ Practice Exams At the end of each of the CISSP domains you cover in the text books, complete the practice exams at the end of each chapter. This will reinforce your learning. Aiming for 80 – 90% before moving to the next domain.
- ✓ Prepare for Judgement/Scenario based questions (BEST/MOST/LEAST).
- ✓ Prepare your own strategy for when you sit the exam and how you will answer questions.

**Free Stuff**

- ✓ A great site where you get a free trial of CISSP Practice questions. This site gives explanations on each of the questions to aid learning. See: www.safaribooksonline.com/library/view/cissp-practice-2250/9781118105948/
- ✓ One hundred page pdf document containing CISSP questions similar to what you will see in the exam: http://www.itcertpass.com/samples.html
- ✓ McGraw-Hill has some good free CISSP questions located at: http://www.mhprofessional.com/sites/CISSPExams/exam.php?id=AccessControl
- ✓ SkillSet.com is a good resource and has trial CISSP questions on offer at: https://www.skillset.com/
- ✓ Another site with good CISSP practice questions: http://searchsecurity.techtarget.com/quiz/Quiz-CISSP-practice-exam-questions-and-answers