How to Ace the CISM® Examination in Ten Steps

George Pajari, CISSP®, CISM®, CSSK™

© 2014 George Pajari. Available under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

Introduction

So you want to be Certified in Information Security Management™. Here is what I did to pass the exam -- steps that helped me score the highest mark in the world (of those writing the Sept. 2013 sitting).

1. Know Thyself; Know How to Study

It's probably been a few years since you had to study for an exam. Spend a little time studying about how to study.

Different people learn in different ways. Some prefer to study alone by reading reference material. Some thrive in a classroom setting. While cognitive psychologists still debate the validity of learning preferences, the theory is attractive. Read up on learning styles¹ and figure out what works best for you. There's a lot to cover and doing so in a manner compatible with your personality can only help. Also read about current research in effective learning² to learn some techniques to make your study time as effective as possible.

Finally, ask yourself, are you ready? Not just the obvious matter of having the requisite experience to qualify for the CISM if you pass the exam, but have you had sufficient practical experience to be able to master the material required to do well on the exam?

2. View it as a Waypoint, Not an Endpoint

Passing the CISM exam should not be viewed as the end-goal but as a waypoint, albeit an important waypoint, on your career path. This is important for two reasons: first, the field of information security is moving too quickly for any professional to rest on his laurels. Secondly, if you try to study just for the CISM exam you are less likely to pass. View your studies as part of your wider professional self-development. If you do that you are more likely to pursue tangents and explore related material while studying for the CISM. Not only will this make you a better infosec professional, but also it will help you on the CISM exam.

3. Reach Out for Help

Don't try to do it yourself alone. Join your local ISACA chapter. Not only do some offer exam-prep seminars (free or for a modest fee), many certificate holders are happy to act as mentors if asked politely and if you show you are serious and willing to do the heavy lifting (don't ask questions you can easily answer through your own research; don't abuse the relationship). ISACA themselves provide many useful resources from the COBIT documents (significantly discounted for members) as well as articles from past issues of the ISACA Journal.

¹ For example, Learning Styles from the University of Western Ontario: http://www.sdc.uwo.ca/learning/?styles
4. Use the ISACA Review Manual as a Point of Departure

The ISACA CISM Review Manual is an essential resource for preparing for the exam, but it is not a Body of Knowledge (BoK). It provides a detailed outline of the material you are responsible for knowing but does not provide sufficient explanation of that material to prepare you for the exam. Reading only the Review Manual is unlikely to enable you to pass the exam.

5. Build your Own Glossary; Follow Threads

My recommended approach for reading the Review Manual is whenever you come across a concept that you are not completely familiar with and is not fully explained in the Manual, add it to your personal glossary and then Google for information and documents. Read them and write your own explanation in your glossary. As you read that material you will come across other new concepts. Add those to your glossary. Research them. Rinse and repeat.

This is one of the two real secrets to preparing for the CISM exam. It accomplishes two critically important things:

- It gives you the information and background you need to do well on the exam. As mentioned earlier, the Review Manual is not sufficiently comprehensive to provide you with the information you need.

- Switching between reading the Review Manual, searching the Internet for related information, and distilling that information by writing your own glossary helps you remember the material (see the New York Times article on learning, referenced above).

To put this into perspective, I estimate for every hour I spent reading the Review Manual, I spent at least four hours reading related documents (found on the Internet) and adding to my glossary.

6. Use the Sample Questions

Attempting the ISACA sample exam questions is essential. This is the other secret to acing the actual exam. There are three reasons for this:

1. It provides invaluable feedback to guide you in your studies.

2. It reinforces your learning (see the NYT article referred to above).

3. It points out material not covered (or only touched upon) in the Review Manual. I was surprised at the number of questions that referenced material not found in the Manual.

After completing your study of a CISM domain, try answering questions on that domain. Once you have finished studying all the domains, try answering questions on all domains. Then try the sample exams. This is critical. There is no way I could have scored as well as I did without making heavy use of the sample questions. When you attempt the sample questions, add any unfamiliar terms to your glossary and research them after your mini-self-test (see #5 above). When you score yourself, examine every question you got wrong and determine why you got it wrong. If you did not understand a concept, add it to your glossary (see #5 above). If you misunderstood the question, make sure you comprehend why the question was asked the way it was and how you can avoid misunderstanding similar questions in the future. You will learn more from the questions you get wrong than those you get right. Do not waste
this opportunity by simply shrugging your shoulders at having gotten some wrong and moving on without careful retrospection.

Finally, do not, repeat, DO NOT, use non-ISACA sample questions (free or purchased). This has nothing to do with protecting ISACA's commercial interests. The issue is that the quality of non-ISACA questions is highly variable and if you get a bad batch, not only will you be misled as to the type and nature of the questions you will face on the actual exam, you run the risk of learning incorrect information.

7. Develop a Plan and Stick to It

There is a lot of material to cover, especially if you do it properly (i.e. by following steps #5 and #6). If you don't plan carefully you risk realising that you are two weeks away from the exam date with hundreds of pages of material still to read. Not only will last-minute cramming be unlikely to succeed, you risk being a nervous wreck walking into the exam hall, another sure-fire way to fail spectacularly.

Start your studies by taking the first few sections of the Review Manual. Keep track of the time you spend. Read the sections carefully. Add to your glossary and follow any threads and unfamiliar concepts as recommended in step #5. After you have progressed through a couple of dozen pages of the Review Manual, do the math. Figure out how many pages per hour you covered. Count the pages in the Manual and estimate the number of hours in total you will need. Add ten or twenty hours for the practice questions, and more importantly, studying the questions you got wrong. Then divide by the number of days before your exam date. You now know how many hours per day you must devote to preparation if you are to succeed. Keep a diary and measure your progress against the calendar. And after each domain, re-check your figures to see if your pages-per-hour rate estimate is still accurate or if you need to increase the time you spend studying every day.

8. Prepare Physically and Mentally for Exam Day

Writing the exam is gruelling, mentally and physically. Too much stress will severely reduce your chances of success.

Being prepared is the best way to reduce your stress.

Stop studying two days before the exam. If you do not know the material by then, two more days is not going to make a difference and the additional stress will negate any possible benefit from last-minute cramming.

Get plenty of sleep for several nights before the exam.

Eat regularly in the days before the exam. Have a healthy moderately-sized breakfast on the morning of the exam. Avoid consuming more caffeine that you would normally any other morning.

9. Write the Exam in Four Logical Passes

The ISACA CISM exam is a paper-based exam with a separate question booklet and answer sheet. You have 240 minutes to answer 200 questions.

---

3 For this observation I am indebted to my mentor Rob Slade who warned me about this, and about which my personal research has confirmed in spades.

4 See, for example, How Stress Affects Your Test Scores, http://collegepuzzle.stanford.edu/?p=2242
Pass 1
Go through and answer every tenth question (take care when marking the answer sheet — this is to reduce the possibility of “off by one” errors in transcribing your results to the answer sheet). Mark the questions you have answered in the exam booklet. Maximum one minute per question.

Pass 2
Answer all remaining questions, one minute at most. Mark in the exam booklet any questions for which you have doubts about your answer; leave unanswered any questions you are completely unsure about. But in any case, never spend more than one minute on any one question.

I’m guessing at this point you should have fewer than 30 questions unanswered and fewer than 50 marked to revisit.

At this point you ought to have used less than three hours.

Pass 3
Go through and answer all questions you skipped in the first two passes. Spend no more than two minutes on each unanswered question. Use the “invert the question” technique if it applies (see below). If nothing within two minutes, guess. Answer every question.

Pass 4
Spend whatever time is left reviewing questions you were not sure about. I was still thinking about a question when time was called. I was one of two people left in the exam hall at the end of the four hours.

10. Attack each question methodically
At the risk of stating the obvious, let me repeat the basic approach for all exam questions:

- read the question very very carefully
- then read all the answers very very carefully
- then read the question again
- then read all the answers again
- then eliminate the obviously wrong answers
- then carefully consider the remaining possible answers in light of the question

Remember the following:

- Every question has been very carefully written. Every word is there for a reason (but that reason could be to mislead or distract). Equally, words that are not there are not there for a reason. Do not read in words that are not there. Be careful about making assumptions.
- Frequently all the possible answers will be correct. The best, most generally applicable answer is the correct one.
• Sometimes all the possible answers will be poor choices. The least bad answer is the correct one.

• There are answers that look very close to the right answer but have a slightly incorrect word or phrasing. Do not assume this is a quirky or idiomatic expression, it could be a distractor.

• While the question has been very very carefully written, that does not mean every word or fact is necessary, some questions have extraneous or distracting facts.

• Answer the questions from a management perspective, selecting the answer with the broadest applicability.

Many questions do not provide enough information to definitively select the best answer. You will have to make some assumptions. This is where things get very dangerous very quickly. You must be conscious of the assumptions you are making and check them to ensure they are:

• reasonable

• general/global (i.e. not specific to your particular current circumstances)

In most cases the best approach is to first eliminate the obviously wrong answers. Then, when left with two or more possible correct answers, is one a subset of the other, if so, discard the specific and select the more general (i.e. the superset) BUT ONLY IF the superset applies in all cases.

A technique that can be helpful is to invert the question. Consider the following question:

The PRIMARY objective for information security program development should be:

A. establishing strategic alignment with the business.
B. establishing incident response programs.
C. identifying and implementing the best security solutions.
D. reducing the impact of the risk in the business.

All are objectives so we need to determine the primary. Turn the question upside down.

Could you have an information security program if:

A. it was not aligned with the business (yes, but not optimal)
B. it did not have an incident response program (yes, but not optimal)
C. it did not identify and implement the best security solutions (yes, but not optimal)
D. it does not reduce the impact of the risk in the business (of course not -- for why else do we have information security)

Hence D is the best answer.

If you absolutely cannot make a final decision on a question, even after considering everything above, go with the very first answer that you thought of. After all, you probably did find the answer in the material that you read. Accept that your subconscious might be smarter than you are.

---

5 ISACA CISM Review Questions, Answers & Explanations Manual 2013, page 37, question S1-123.
Summary

Making the commitment to become a Certified Information Security Manager (CISM) is a worthy and laudatory undertaking. Studying for a professional certification is a good thing in general for many reasons:

- Forces you to study the known unknowns. As with most professionals in any field, we typically use 20% - 40% of the body of knowledge that is our specialty. Preparing for an exam provides some motivation to review those areas you are less familiar with.

- Helps you discover your unknown unknowns. Working through a comprehensive knowledge outline such as the CISM Review Manual uncovers those corners of the field you were unaware of.

- Brings discipline and completeness to your work. Even in the areas you are comfortably familiar with, reviewing the literature may show you best practices and more structured and mature (in the Capability Maturity Model sense) approaches.

- Adds credibility. Passing the CISM exam not only certifies your understanding of the material, the dedication to successfully prepare for the exam demonstrates a degree of professionalism and commitment that reflects well on your professionalism. When you are proposing a certain approach to your colleagues and management it helps to have the credibility that certification brings.

So take your game to the next level by preparing for, and successfully obtaining a certification that attests to your ability, knowledge, and commitment to information security management.

The current version of this article as well as a much shorter version may be found on my blog at:

http://orangehazmat.wordpress.com/2014/04/28/writing-the-isaca-cism-exam/