CISSP exam tips

From students and instructors

INFOSEC™

Pass your CISSP exam with tips from those in the trenches

The CISSP is one of the most challenging certifications to earn, and its exam has been described as an inch deep and a mile wide due to the sheer amount of material CISSP holders are required to understand. That's why earning a CISSP is the "gold standard" for many security professionals.

As of January 2021, there are more than 92,000 CISSP holders in the U.S. and more than 147,000 worldwide — many of which have been Infosec instructors, students and community members. Collected here are some of the most common tips and strategies gathered from more than 17 years of IT and security instruction and thousands of individuals who have taken and passed the CISSP exam.

Study hard, and good luck!

Tips from CISSP instructors

Tips from CISSP students

Tips from the Infosec community

Understanding the new CAT exam format

In December 2017, the English-language CISSP exam switched from a traditional computer based testing (CBT) format to a computer adaptive testing (CAT) format, meaning:

- » The exam is now tailored to your ability — the difficulty and number of questions change based on your previous answers
- » Initial test questions are easier and establish a baseline; later questions are designed to have a 50% chance of you answering correctly
- » Your grade is based on the difficulty of the questions you answered, not the total number of questions answered correctly

CISSP exam changes:

CBT vs. CAT

- » Same content, different format
- » Exam time reduced from 6 hours to 3 hours
- » Questions reduced from 250 to between 100-150
- » 25 of the questions remain unscored and used to evaluate future tests

From (ISC)²:

Why change the exam?

- » A more precise and efficient evaluation of a candidate’s competency
- » More opportunities for examination administration
- » Shorter test administration sessions
- » Enhanced exam security

Every question is the first question

Perhaps the biggest change with the new CAT exam is that you can no longer review previous questions or change previous answers. Since each question is used to create a baseline for your CISSP knowledge — and to provide a question you have a 50% chance of answering next — there is no going back. As Infosec instructors like to say, it's as though every question is the first question.

The CAT format can be particularly difficult for test takers who are used to marking questions for review and returning to them later with ideas or thoughts that were sparked by other questions.

Advice from the trenches

> "The new CAT format is designed to hone in on your weaknesses. A single question can touch on multiple domains, so a broad level of understanding is important."

Gil Owens
Infosec alum

> "Unlike the PMP and CBAP exams, the CISSP exam didn't give an option to bookmark and go back to previously answered or skipped questions. Surprisingly, I found this to be a good thing. It ensured that I gave due respect to each question."

Infosec community member

> "I preferred the CAT format over the long format. It's intimidating, but suffering for three hours max seems a heck of a lot better than six."

Infosec community member

Calm your nerves and start strong

The first few questions of your exam will help to establish your baseline, so it's important to start strong. As (ISC)² states, the first question you get should be "well below the passing standard." If you get answers correct, the subsequent questions will become more challenging. With the new format "each item presented will feel challenging," (ISC)² warns.

Many test takers have commented on the awkward wording of certain questions, but that may be intentional. One Infosec community member said the questions mimicked the real-world situation of someone relaying information in a panic — and it was up to the test taker to choose the least bad out of four bad options. Test takers also frequently reported settling into a groove after the first 15-30 minutes as they got a feel for the exam's wording and logic.

Advice from the trenches

"You must read the questions entirely and then read them again to understand what is being asked."

Infosec community member

"Stay calm. You will be nervous the first few questions, and you may never feel comfortable. I sure didn't. Read the question, re-read the question — if you have to, break down the sentences to smaller sentences. Then, start weeding out bad answers."

Infosec community member

"You can expect to miss about half of the questions on the exam. If you pass, that means you missed really hard questions."

Joe Wauson
Infosec alum

Have a strategy for approaching each question

Understanding the eight CISSP domains is the most fundamental aspect of passing the CISSP exam, but don't underestimate the importance of smart test taking skills. One Infosec professor has a system for examining each question:

- Break the question down into important parts
- Look for any keywords, such as MOST, BEST, NOT or LEAST, and then read the question again to determine exactly what is being asked
- Review each answer for errors and inconsistencies rather than correctness
- Identify and remove the worst answers, then begin looking for the right answer

Advice from the trenches

> "There were almost always two answers I could immediately rule out. I would literally draw four circles on my laminated sheet and check off those I knew were incorrect. This helped me out a lot since you can't exactly do that on the computer screen."

Infosec community member

> "The questions I encountered on the test jumped around a lot between domains and very few were just straight definitions. Be prepared to put on your critical thinking hat and work through the problems."

Infosec community member

> "Often there are several right answers, but you need to pick the answer that is most correct. It requires a deeper level of understanding — not just memorization."

Gil Owens
Infosec alum

Think like a manager, not a technician

Many CISSP exam questions don't have a "right" answer. Instead, your goal is to choose the "best" answer from a managerial point-of-view.

One Infosec instructor often poses a question to his students to help drive home this concept: what is the best way to prevent data loss? Technical students may focus on a solution such as encryption; however, the best is answer is much more straightforward — simply do not collect any data at all.

Advice from the trenches

"I feel what really held me back was not being able to think like a manager. I kept trying to fix the problem as a technical analyst, which was where a lot of my experience was at the time."

Infosec community member

"If in doubt, pick the answer that is most concerned with management principles. Think about how frameworks relate to standards, how policies relate to programs, how infosec programs relate to business."

Infosec community member

"The CISSP exam isn't about all the technical definitions you know. It proves you understand security concepts, theories and how to apply them in business scenarios to achieve a common goal."

Julian Tang
Infosec alum

Fail one domain, fail all

You must score above the proficiency level in all eight CISSP domains in order to pass the CISSP exam, according to (ISC)². The eight domains and their weights, which will be updated in May 2021, include:

1. Security and Risk Management — 15%
2. Asset Security — 10%
3. Security Architecture and Engineering — 13%
4. Communication and Network Security — 13%
5. Identity and Access Management (IAM) — 13%
6. Security Assessment and Testing — 12%
7. Security Operations — 13%
8. Software Development Security — 11%

Don't make the mistake of thinking your strongest domains will carry you to a passing grade. Instead, focus on improving your weak areas.

Advice from the trenches

"Comments to the CISSP exam being an 'inch deep, mile wide' are very true."

Infosec community member

"The identity and access management domain is one of the top causes of failure from what I hear anecdotally."

Ken Magee
Infosec Instructor

"I think the common theme from people who don't pass the CISSP is they tested before they were ready. They knew they were weak in some domains, and then got a bunch of questions on those domains they weren't prepared to answer."

Gil Owens
Infosec alum

Build your three pillars

Although there are a lot of helpful tips and suggestions from those who have taken the exam, nothing is more valuable than your own knowledge, experience and preparation. If one of those three fundamental support legs is missing, your chances of failing increases dramatically.

Every CISSP hopeful has their favorite method of learning — including live instruction, recorded videos, practice exams, books, group study sessions and more — but we've found that those that take advantage of the wide variety of resources available to them and have a solid foundation of knowledge, experience and preparation are much more likely to pass their CISSP exams on the first attempt.

Advice from the trenches

"Explain the concepts to someone, or if no one is around just speak out loud as if you are teaching a class. If you can't explain it, you don't know it."

Infosec community member

"In addition to attending class, I used the Sybex book provided as part of my course and reviewed the video material in the Infosec Flex Center. Before attending your boot camp, I recommend going through all the videos in the Flex Center and getting familiar with the material. If you have the time, also take a few of the practice tests."

Julian Tang
Infosec alum

"I spent quite a bit of time replaying recordings from the boot camp. This was one of the things that drew me to Infosec — the ability to replay recordings of class after the course ended. I found this extremely helpful and cannot emphasize this enough."

Gil Owens
Infosec alum

Prepare for every possibility

No matter how knowledgeable, experienced and prepared you are, there's always a chance you may not pass your CISSP exam on the first try — maybe it's due to stress, having an off day or a number of other reasons.

That's why Infosec CISSP Boot Camps come with an Exam Pass Guarantee. If you don't pass your exam on your first try, you'll get a second attempt for free — along with the ability to re-sit your boot camp for up to one year.

After your boot camp, you'll get extended access to 100s of other on-demand courses, so you can start earning CPEs, building new skills or working towards your ISSEP, ISSAP or ISSMP specialization.

Why train with Infosec

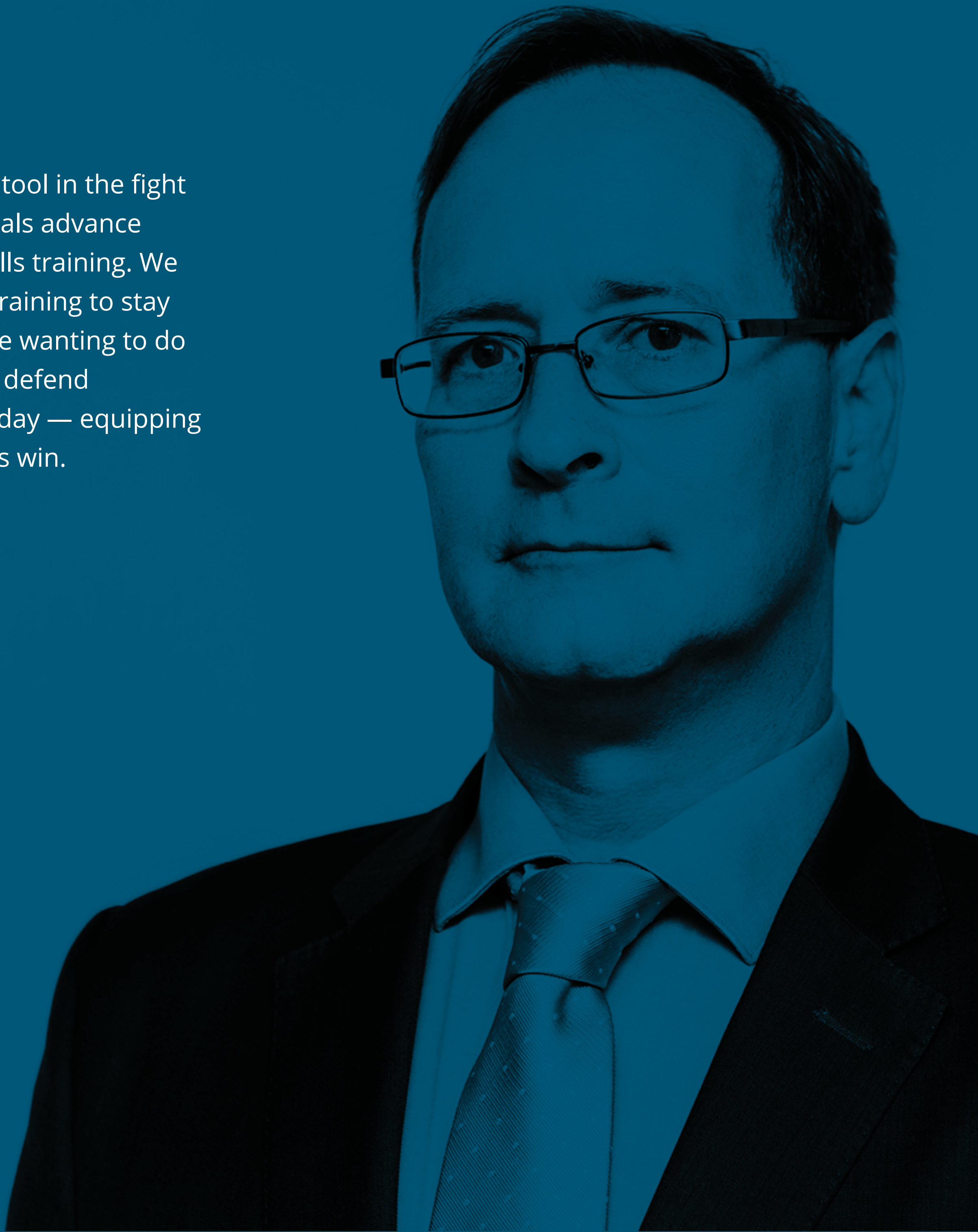
- ✓ Immediate access to Infosec Skills — including a bonus boot camp prep course — from the minute you enroll to 90 days after your boot camp
- ✓ Six days of expert, live CISSP training, plus a day to take the exam
- ✓ 90-day extended access to all boot camp video replays and materials
- ✓ Unlimited CISSP practice exam attempts
- ✓ CISSP exam voucher
- ✓ Learn by doing with hundreds of additional hands-on courses and labs
- ✓ 100% Satisfaction Guarantee
- ✓ Exam Pass Guarantee (online students)

Learn More About CISSP Training

About Infosec

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We help IT and security professionals advance their careers with a full regimen of certification and skills training. We also empower all employees with security awareness training to stay cybersecure at work and home. Driven by smart people wanting to do good, Infosec educates entire organizations on how to defend themselves from cybercrime. That’s what we do every day — equipping everyone with the latest security skills so the good guys win.

Learn more at infosecinstitute.com.



Sources

- CISSP computerized adaptive testing, (ISC)²
- The ultimate guide to the CISSP certification
- CISSP Training Boot Camp