# A Guide to Information Security Certifications

Many people are confused by the massive number of information security certifications available today. Some people already have one or more and are looking to expand, while others are just getting started with certification and need a place to start. This guide aims to help with both scenarios.

I'm going to highlight a few of the certification options and offer a couple of recommended paths for professionals in various stages of their careers. I'll be rating each credential based on the criteria below:

**Difficulty** - How hard the test itself is, i.e. study-time needed, difficulty of material, etc.
**Who** - Who should be considering the certification.
**Respect** - Respect rating within the technical infosec-geek community.
**Renown** - How well-know the certification is throughout the industry.
**Requirements** - What's needed to get the cert, e.g. prerequisites, exams, practicals, labs, etc.
**Cost** - What it'll cost you (or your company) to get the credential.
**Pros** - Positive comments about the certification.
**Cons** - Downsides to the certification.
**Comments** - My own input on the credential.

** Note: Numbers are on a scale from 1-10, with 10 being the highest

## Security+

**Sponsor:** CompTIA
**Difficulty:** 2
**Respectability:** 2
**Renown:** 4
**Requirements:** Single Exam, +-100 Questions
**Cost:** $225 USD (discounts available online)
**Who:** This certification is for people just getting into the field. If you don't have any other certifications, and your experience/skills are still developing, this is the certification for you.
**Pros:** It's a fairly easy cert to get and I understand it's getting a decent amount of recognition within federal organizations. It's also a fair, solid test

that asks decent questions rather than a bunch of vendor-specific garbage.
**Cons:** It's entry-level and thus not strong as a standalone bargaining chip.
**Comments:** I enjoyed taking this test due to its honesty and legitimacy. The study material was good material to be going over, and the test actually covered the material. The questions weren't particularly tricky; you either knew the content or you didn't, which I respect.

**SSCP** (Systems Security Certified Practitioner)
**Sponsor:** ISC$^2$
**Difficulty:** 4
**Respectability:** 3
**Renown:** 2
**Requirements:** Single Exam, 125 Questions, 3 hours; 1 Year Experience
**Cost:** $350 USD
**Who:** The SSCP is for serious, dedicated information security professionals who are not quite ready to take the CISSP exam. Only one (1) year of experience is required for this exam vs. 3-4 (depending on if you have your bachelors) for the CISSP.
**Pros:** The SSCP is administered in a very professional fashion, just like the CISSP, and it thus carries some degree of the respect that goes along with that credential. It's also from ISC$^2$ just like the CISSP, so that helps it as well. It shows that you're serious about your career.
**Cons:** Unfortunately, the certification that hurts the SSCP the most is in fact its older sibling -- the CISSP. If you check the job boards, precious few jobs ask for the SSCP. The reasoning there is that the experience requirement for the CISSP is much of what makes it so respectable. To take that away and ask half the number of questions diminishes the value of the SSCP significantly.
**Comments:** If you can't show the 3-4 years experience required for the CISSP, or you don't feel you can pass the CISSP exam, *and* someone else is paying, I'd say go for the SSCP. If nothing else, it will help prepare you for the CISSP that will surely be in your future. Also consider that you can take the CISSP exam even if you don't have the experience to get the credential. Once you get the experience you'll then be awarded the certification. That being said, if you want to get a truly valuable credential that doesn't require the experience (and you're technical enough), go for the GSEC (covered below) instead .

**CISSP** (Certified Information Systems Security Professional)
**Sponsor:** ISC$^2$
**Difficulty:** 5
**Respectability:** 4
**Renown:** 10
**Requirements:** Single Exam, 250 Questions, 6 hours; 4 Years Experience
**Cost:** $500 USD
**Who:** The CISSP is for serious, dedicated information security professionals who intend to stay in the field and grow. It says to employers that you are serious about your career and are familiar with the core basics of 10 separate areas within the field. In today's market, managers and career professionals are expected to have this credential.
**Pros:** The CISSP is the undisputed king of infosec certifications. It's the first infosec cert to receive ISO recognition -- a great achievement not only for the certification itself, but also for the field as a whole. It commands a great deal of respect in many IT circles (and HR circles), and this can be clearly seen via job search results. It can help your chances greatly of getting high-paying jobs, and is an *excellent* addition to any resume. If you are only going to get **one** infosec certification, it should be the CISSP.
**Cons:** While the CISSP is the king of information security certifications, it suffers from being thought of as something it isn't. Many still mistakingly view it as proof that someone is an expert in the field, and that couldn't be farther from the truth. ISC$^2$ has explicitly stated in the past that the test is designed to test a broad base of general knowledge, not to certify someone as a master of their field. Also, despite the rumors of impossibility, the exam also supports over a 70% first-time pass rate.
**Comments:** The CISSP is a great exam because it is not easy to take (experience in the field is required ), and once you are able to take it, it's administered in a professional, controlled environment. What people fail to realize is that it's geared for high-level security professionals such as managers. Obviously, anyone can go for it, but it's not designed to test technical skills or the ability to actually *perform* in the trenches of an infosec environment. **It's a test designed to ensure that you are familiar with some basic concepts; it's when people lose sight of this that the confusion starts.** As for the difficulty factor, I started studying for mine on a Monday (a "bootcamp") and passed the exam on that Saturday -- and that's with **zero** previous exposure to the CISSP study material. A buddy of mine just got his as well, and his study consisted of around 2 weeks of

passively glancing at the material while leveling his WoW character. Again, that's not to say it's not an excellent certification to have, it's just that the difficulty (or value) should not be overestimated.

**CISA** (Certified Information Systems Auditor)
**Sponsor:** ISACA
**Difficulty:** 6
**Respectability:** 5
**Renown:** 8
**Requirements:** Single 200 Question Exam, 4 Hours; 5 Years Experience
**Cost:** $475 USD
**Who:** The CISA credential is ideal for anyone already doing, or looking at getting into information security auditing. If you're not familiar with auditing, think of accounting. It's basically ensuring that proper processes are in place and that people (and technologies) are doing what they're supposed to be doing.
**Pros:** The credential is highly recognized and sports even more hits than the CISSP via Monster.com and other job searches. It's highly sought after due to the myriad of regulations hitting the infosec industry. Considered a "professional" certification, it seems to borrow some respect from the CPA/Accountant arena.
**Cons:** Again, many jobs that request CISA also will take a CISSP. Certain jobs ask for CISA specifically, but most are just looking for this "class" of cert, and will accept a CISSP in its place.
**Comments:** Information security auditing, as a field, is becoming more and more needed. Due to the continued release of new legislation, along with the requirement to enforce what already exists, this will do nothing but accelerate. Adding a CISA to your resume is definitely a good move, and should probably be your second or third certification, right after your CISSP (unless you go for your GSEC first).

**CISM** (Certified Information Systems Manager)
**Sponsor:** ISACA
**Difficulty:** 6
**Respectability:** 5
**Renown:** 7
**Requirements:** Single 200 Question Exam, 4 Hours; 5 Years Experience; 3 Years Security Management Experience.

**Cost:** $475 USD
**Who:** The CISM credential is for information security managers. It's for those who wish to show that they can manage an enterprise information security program.
**Pros:** The credential comes from ISACA, which is a respected organization, and the position of information security manager is so important to companies that any credentials that speak to one's competence will be helpful.
**Cons:** Once again the CISSP is still the leader in this area, and while the certification can definitely help, anyone hiring for an ISM position is going to be looking at a lot more than certifications.
**Comments:** Anyone wanting to get into an ISM position needs to be looking at this credential, but it doesn't have the power of CISSP in my view. I think that out of the two big ISACA certs, the CISA offers more of a punch, albeit not necessarily for managers.

**GSEC** (GIAC Security Essentials Certification)
**Sponsor:** GIAC (SANS)
**Difficulty:** 7
**Respectability:** 7
**Renown:** 7
**Requirements:** Two 100-Question, Open-book, Open-Google Online Exams
**Cost:** $800 USD (Cost of exam without training)
**Who:** The GSEC is for highly-technical, serious information security professionals who actively work with the technical side of infosec on a daily basis. Those who are looking to show considerable technical knowledge over a large number of infosec subjects would be well-served by attaining this credential.
**Pros:** The SANS organization is universally recognized as a top-notch infosec training and certification organization. Any certification from them commands a decent degree of respect, both with engineers and increasingly with human resources as well.
**Cons:** The CISSP still owns the majority of the spotlight in this arena. Relatively few employers are aware of the GSEC, and even of those who do recognize it, most view the CISSP as just as (or more) valuable.
**Comments:** The GSEC does not show expertise in any particular infosec area; it shows that the cert-holder is technically-oriented and has a wide base of infosec knowledge, as well as the ability to find answers under

pressure. No certs at this level demonstrate true mastery. One particular thing to note with this exam vs. the CISSP is that the actual exam portions are taken from home and are open-book, meaning you can use anything you want during the exams. Critics claim this makes the exam less respectable than the CISSP since the CISSP is taken under supervision and no study materials may be used. I argue that precisely the opposite is true. Infosec professionals are not databases. We don't pride ourselves in not having to consult external resources when solving problems; in fact, we do it constantly. To imply that an exam that tests your ability to solve problems in precisely this fashion is somehow less respectable is, in my view, a grave mistake. The GSEC exam structure represents the real world -- you're faced with a difficult problem, you find the answer and solve it. You don't see consultants losing contracts because they had to Google for solutions that saved their clients money. Ultimately this debate comes down to an old argument: hands-on vs. academic. The GSEC tests one's ability to get the answer to semi-difficult questions in a pinch, and for this reason I think it's a very valuable credential. I expect that the business world's acceptance of it as a legitimate, respectable certification will only continue to grow.

**GCFW, GCFA, GCIA, GCUX, GCIH**
**Sponsor:** GIAC (SANS)
**Difficulty:** 8-9
**Respectability:** 8-9
**Renown:** 5
**Requirements:** Two 100-Question, Open-book, Open-Google, Online Exams
**Cost:** $800 USD (without training)
**Who:** These various certifications represent the "hardcore" SANS offerings. They are more in-depth and difficult than the GSEC, and they focus on one area specifically. GCFW is for firewalls and VPNs, GCIA is for IDS/IPS, GCUX is for Unix security, GCFA is for forensics, and GCIH is for incident handling. These are just a few of those that are offered, and these are geared towards veteran infosec professionals who have already specialized in an area. If this sounds like you, these certs are the way to go.
**Pros:** The GIAC (SANS) organization is universally recognized as a top-notch training and certification organization. *Any* certification from them commands a decent degree of respect, and these specialized certs say to an employer or client that you are truly skilled at what you do.
**Cons:** There are very few holders of these more advanced certifications, and

as such many employers (or clients) may ask questions like, "Is that like a CISSP? Is that the same as a GSEC?"
**Comments:** These certifications *do* show some degree of mastery of a subject. It doesn't mean that *everyone* with one is great, or that those who don't have one aren't great. It does mean, however, that the odds of someone with one of these certifications being qualified for a job in that respective area are fairly high. Think of these as more advanced, more focused GSECs.

**GSE** (GIAC Security Expert)
**Sponsor:** GIAC (SANS)
**Difficulty:** 10
**Respectability:** 10
**Renown:** 4
**Requirements:** Must have three (3) GIAC certifications (GSEC, GCIA and GCIH) with GIAC Gold in at least two; must pass a proctored GSEC exam with average scores of 80 on both tests; 23 hour onsite testing process consists of a mix of open book written exams, research, hands on exams, group work and an oral presentation.
**Who:** The GSE is for those who have literally mastered a number of areas within information security, have superior talent, have a love of difficult-to-attain credentials, and a lot of time on their hands.
**Pros:** If you encounter anyone who knows what all the exam involves, you'll be instantly acknowledged as a world-class information security expert.
**Cons:** You aren't likely to find any of those people. Plus, anyone with these skills doesn't need the certification anyway.
**Comments:** The GSE credential is the final destination for anyone pursuing information security certification. It's a goal in and of itself to me, rather than a means to gain something in the field. In short, nobody with the skills required to get this credential are going to get any additional fame or money because of it. It's a trophy, plain and simple.

If you are just getting into security and you don't have much experience with networking or system administration, you need two things:

1. A serious home network that you can use as a learning environment
2. A job where you can start building experience

Both of these are absolutely critical. Once you have your help desk, sysadmin, or other low-level IT job secured, start studying for and take your Cisco CCNA. Study, practice at home, learn everything you can pertaining to operating systems, networking, programming, and the security philosophy and discipline. Once you feel your security skills are decent, start studying for and take the Security+ and/or SSCP exams.

Once you've been in networking, system administration, programming, and/or security for a while (4 years or so), and you feel your skills are pretty strong, you should be looking at the CISSP. Ignore people who say it's too easy or that it doesn't mean much -- *it doesn't matter*. The fact of the matter is that it's more beneficial to have a CISSP right now than any other information security certification. Remember, you can take and pass the test without having the required experience; you'll get the certificate later once you've satisfied that requirement.

After getting your CISSP, and if you're a technical person, I suggest you look at the GSEC. It's the perfect compliment to the CISSP. The CISSP covers the 10 domains from a manager/birds-eye view, and the GSEC gets down to some technical detail within the same areas.

Another option once you have your CISSP is to go for the CISA instead. If you're more of a manager anyway, and/or looking to head that way, then it may not be necessary to show technical prowess. If that's the case then opt for the CISA instead of the GSEC. The certification is absolutely on fire right now, and the odds are good that with a solid resume and a CISSP/CISA combination you could command around $90K/U.S. fairly easily.

If you have been in infosec for a long time, i.e. 5-10 years or more, and you are a geek at the core, start looking at the more advanced SANS certifications. Pick the one that matches your area of interest within information security and go for it. These credentials represent the top tier of technical certifications, and once you've achieved one of them you're going to be better off growing your career via a method other than certification.

Finally, remember one important thing about all certification:

The value of a certification is exactly the value that others place on it--no more, no less. If you're interested in the actual value of a given cert, check

the job sites, call your recruiter friends, and talk to hiring managers. Just as with currency exchange rates, the only way to determine "true" value is to see how much others are willing to pay for it.