ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Definitive Guide to Cybersecurity Certifications for In-house Counsel

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by metamorworks / *Shutterstock.com*

Cheat Sheet

- **Benefits all around.** Whether to increase your professional brand or to help your organization, cybersecurity certifications can help.
- **Entry-level or advanced.** Depending on your goals, there is a cybersecurity certification that can get you there.
- **It’s not either/or.** Multiple or overlapping certifications may make sense depending on one’s responsibilities or interests.
- **Perform a cost/benefit analysis.** Before starting, consider: (1) money needed to acquire training materials; (2) time spent preparing for exams; and (3) ongoing demands.

Having started my first in-house cybersecurity role in 2009 at Southern California Edison (and later working for Meta Platforms), I'm often asked by colleagues new to the field for career advice.

Managers, even up to the chief legal officer level, want to know where to invest their training dollars.

Over the years, I've compiled my advice into the following Q&A:

1. Who is this guide for?

The number of security-related certifications is voluminous, and even the most esoteric one might be helpful to some attorney or company (*see* Security Certification Roadmap).

In-house lawyers

The certifications here are those I think would be most useful for a "typical" in-house cybersecurity counsel – a role I define as one whose duties includes:

- Building out an organization's Governance, Risk Management and Compliance (GRC) function, and
- Incident response/business continuity.

(Related - want to know how your peers build out their cyber legal practices? Review the following: (1)"What is a Cybersecurity Legal Practice?***; (2) So What Does General Counsel Have to Do With Cybersecurity, Anyway?)***

Managers (even if not in-house lawyers themselves)

Managers — this article is also for you. Some companies may be in a position to provide educational support for employees pursuing a certification. As stewards of company resources, managers must be thoughtful in their investments. My goal is to help you understand what that investment might look like, and to help you build a business case for it.

Finally, a growing number of law enforcement and regulatory agency lawyers seek operational knowledge to help them fairly and effectively regulate entities under their jurisdiction. This article is for you, too.

2. What's my goal in getting a certification (or for paying for a team member to get one)?

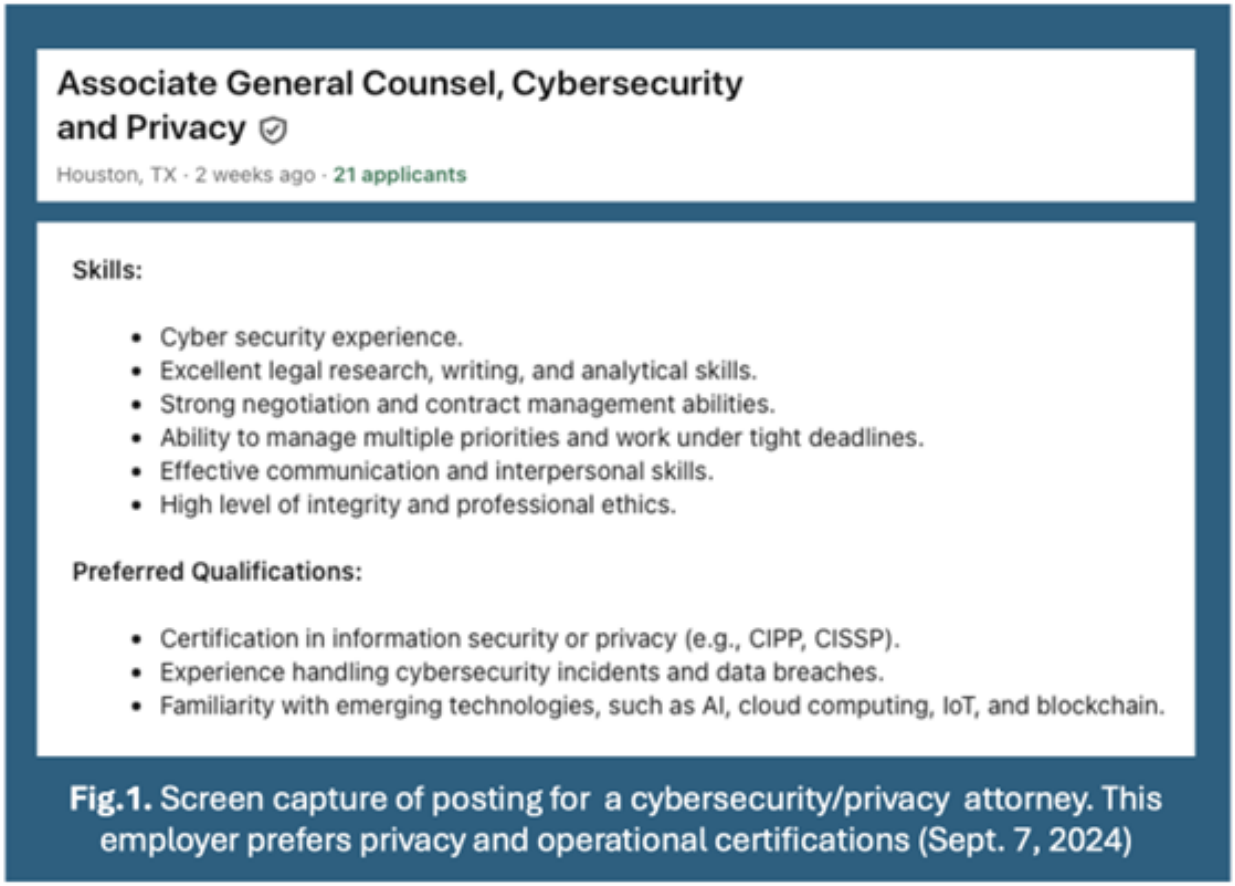

Fig.1. Screen capture of posting for a cybersecurity/privacy attorney. This employer prefers privacy and operational certifications (Sept. 7, 2024)

Most of us have two goals in pursuing a certification:

1. To strengthen our professional brand, and
2. To gain substantive knowledge that benefits the employers we serve.

Earning a certification can meet both goals. Employers use them as a tool to screen new hires (see figure 1). And knowledge gained while training will help us better understand industry practices; acquire specialized knowledge; and hopefully engage more effectively with our technical and operational peers in keeping their organizations and customer base safe.

3. What if I only want the education?

Some of us only want to increase our knowledge. If that's the goal, there may be more cost-effective options than pursuing a certification. For example, courses designed to help students pass an exam are literally designed to "teach to the test." Also, cybersecurity certifications are geared towards operational professionals, not legal ones. This means those tests cover content that goes beyond the needs of most attorneys. For example, one of the certifications referenced below, the CISSP, requires applicants to learn the five different types of firefighting agents used in data center fire suppression systems. Most attorneys will likely never need that level of knowledge.

For practitioners in this boat, consider looking to free resources; university programs; and consultants who can offer more cost-effective group training courses that are tailored toward your team's specific needs. Look also to ACC, which launched its Cybersecurity Toolkit for In-house Lawyers. Similarly, the ACC Foundation will be offering a new cybersecurity 101 track for its 2025 Cybersecurity Summit.

4. Is there a cybersecurity certification specifically for attorneys?

Yes, but other certifications may offer a greater return on investment. GIAC (Global Information

Assurance Certification) and the SANS Institute offer a certification geared towards attorneys called GLEG. However, it isn't well known in legal circles, and may not bolster one's brand. Besides, attorneys are already familiar with many subjects covered by GLEG, such as eDiscovery and contract management. Brushing up on the cyber-specific permutations can be done more cost-effectively through Continuing Legal Education credits.

The certifications referenced here are more well-known than GLEG, and they provide operational and technical training most lawyers don't encounter. Therefore, they provide more bang for the buck.

5. In that case, what certification should I pursue?

With an abundance of certification options, I suggest starting with entry-level options to build up your foundational skills. Pursue more advanced certifications as your skills advance.

Entry-level certifications

For newly minted cyber counsel, I suggest:

- The Certified in Cybersecurity certification by ISC2 and
- Privacy certifications offered by the IAPP.

Training to these certifications will take you a long way to becoming even more effective members of the cyber legal community.

The Certified in Cybersecurity (CC) by the International Information System Security Certification Consortium (ISC2)

The CC is geared towards newcomers to the field of cyber and covers the following educational domains:

- Security principles;
- Business continuity/incident response;
- Access control; and
- Security operations.

As an entry-level certification, it should be within the capability of most new cybersecurity counsel to absorb.

Thinking of pursuing a CC? Take the official introductory quiz.

Costs of Pursuing a CC:

There's the "usual" costs involved in pursuing any certification:

- Paying for training materials (books, courses);
- Paying for an exam;
- Investing time and money to study. Information about purchasing official prep materials can be found here. But, typically, pursuing an entry-level certification will cost less than pursuing an elite one.

On study time: ISC2 notes that it typically takes 14 hours to complete its online training course. Some amount of post-training study would be advisable. But, as an entry-level certification, I think most counsel willing to put in some elbow grease can get certified.

The IAPP Certifications by The International Association of Privacy Professionals (IAPP)

Most of us have heard of IAPP, which operates the largest privacy certification program in the world. IAPP certification comes in various flavors. The CIPP/US (Certified Information Privacy Professional / United States) is a popular option. Others include certification as a privacy manager; as a privacy technologist; or as a privacy practitioner focusing on various global regions such as Asia, Europe and more. There is even a new certification for AI called the AIGP (AI Governance Professional).

Thinking of pursuing an IAPP certification? IAPP offers introductory quizzes like this one: AIGP (AI Governance Professional).

Why include a privacy certification in a guide for cybersecurity counsel? First, because the overlap between privacy and cybersecurity often requires joint work. For example, many companies are also hiring lawyers to fulfill a joint cyber/privacy role (see fig. 1). If privacy attorneys are reading my article, I encourage you to pursue a cybersecurity certification for the same reason.

Next, obtaining a CIPP certification, and IAPP membership, mark practitioners as members of the privacy/security club. An effective cyber attorney builds out networks of technical, legal, and government contacts who can assist in a crisis. Being part of IAPP makes such networking easier. Emphasizing the overlap between privacy and cybersecurity, IAPP launched a Cybersecurity Law Center in 2024. IAPP is not yet planning to introduce a cybersecurity certification.

Costs of an IAPP certification

Costs are similar to those for obtaining a CC certification – paying for study materials and time to prepare for the test. IAPP offers training courses; training manuals; and practice exams (start here).

How difficult are IAPP certifications to obtain? These are entry-level certifications, and I feel that most attorneys pursuing them will be successful. IAPP recommends devoting at least 30 hours of study

before taking their exams.

Advanced certifications

Most counsel will never need to go beyond the CC and IAPP certifications. For those wanting more, however, consider pursuing an advanced one, such as the "Certified Information Security Manager" (CISM) or the "Certified Information System Security Professional (CISSP). Both options represent the gold standard in leadership-oriented cybersecurity certifications.

The "Certified Information Security Manager" (CISM) **by the Information Systems Audit & Control Association (ISACA)**

The CISM affirms one's "ability to assess risks, implement effective governance, and proactively respond to incidents." In particular, the CISM trains practitioners to build and operate programs that are conscious of factors such as budget and headcount, and which are aligned to their organization's overall business goals. Technical training is included, but the CISM's main goal is building up managers. In my opinion, the skills developed in obtaining a CISM could be transferred to meeting the needs of any enterprise GRC function.

CISMs must demonstrate proficiency in the following domains:

- Information security governance;
- Information risk management;
- Information security program development and management; and
- Information security incident management.

Thinking of pursuing the CISM? Take the official introductory quiz.

Costs of a CISM

With all these benefits, what are the costs? First are the "usual" ones referenced earlier, such as acquiring study materials and studying for the test (start here). The sample tests, training manual, and courses, will be more expensive than an entry level option.

Study time represents the biggest variable. For example, one practitioner shared his study plan for pursuing the CISM, which included 90 hours of study. Although factors such as experience, education and more can alter that estimate, it may be a useful starting point for counsel, and their managers, in planning out a study schedule.

Next, as an advanced certification, the CISM imposes a greater number of requirements beyond passing the exam. First, an attorney seeking it must gain experience across the full spectrum of domains listed above. If your practice is narrower, consider asking your manager for opportunities to expand your repertoire before pursuing the CISM.

Further, at least three years must be in leadership positions. ISACA gives successful test-takers five years to accrue this experience. But due to the still-limited number of cyber managerial roles, the CISM may be out of reach to even highly experienced cyber counsel.

The “Certified Information Security System Professional (CISSP) **by ISC2**

A premier certification, the curriculum for the CISSP contains management training, technical education, and more. There is seeming similarity to CISM training, but the proportions are different. Where the CISM concentrates on managerial skills, the CISSP’s curriculum focuses on developing technical acumen.

To acquire the CISSP, a practitioner must demonstrate knowledge in the following domains:

- Security and risk management;
- Asset security;
- Security architecture and engineering;
- Communication and network security;
- Identity and access management;
- Security assessment and testing;
- Security operations; and
- Software development security.

Thinking of pursuing the CISSP? Take the official introductory quiz.

One question often arises: should I pursue the CISM or the CISSP? It’s a “great taste, less filling” type of question. Both certifications offer tremendous value for-in house cybersecurity counsel. I suggest applicants ask themselves:

- Do you want a certification aimed at developing management and strategic planning skills or technical expertise?
- Do you meet either certification’s experience requirements?

Some examples of the similarities and differences between the two may be helpful. Both the CISM and CISSP teach the need for stakeholder buy-in in building out security programs. The CISM provides more training in seeking such input than the CISSP. Both certifications also require managers to recognize the need to build in fire suppression systems in data centers. The CISM stops there. By contrast the CISSP further requires applicants to know the five different types of firefighting agents used in those systems.

For more guidance, I suggest reading this "CISM v. CISSP" article, authored by a member of the software development community.

Notably, the CISSP offers one distinct advantage over the CISM, in terms of meeting experience prerequisites. Although the CISSP, too, requires applicants to accrue five years of varied cybersecurity experience before being fully certified, there is no need for managerial experience. Also, someone who passes the test can be provisionally certified as an "Associate of ISC2," which gives them six years to accumulate the required work experience before retaking the test.

Costs of a CISSP

Again, factor in costs for study materials; for the exam; and time to study (start here). As with the CISM, the biggest variable is study time. Practitioners report devoting between 50 hours to 200 hours , depending on their experience and existing acumen.

6. Should I get multiple certifications? What are the ongoing maintenance costs?

I encourage people who ask that question to consider the following:

Is it worth my time and money to pursue multiple certifications?

Each counsel must ask that question for themselves. For comparison, I estimate investing in about 100 hours of study time to gain three certifications. There were also the financial costs of purchasing study materials and exam fees, which cost over US$6,000 over the three certifications. Unless your employer foots the bill, these costs add up.

Am I prepared to cover ongoing membership costs and continuing education requirements?

All certifications charge annual membership fees. Many employers may pay for one membership, but few will pay for all of them. ISACA charges US$135 to US$145 for membership. ISC2 charges US$50 to US$135, and IAPP charges between US$50 to US$295.

There are also ongoing continuing education requirements. Maintaining a CC requires 45 credits every three years (a "credit" is typically between 50 minutes to an hour). Maintaining a CISM or CISSP requires 120 credits every three years. Finally maintaining IAPP certifications require 20 credits, per certification, every two years.

That said, if the reader wants to pursue multiple certifications, taking some prudent steps can minimize the load:

First providers often charge one membership fee for all certifications issued under its banner. For example, I have the CIPP/US and AIGP certifications, and they are all covered under my IAPP membership. Next, many IAPP continuing education courses cover multiple subjects. For example, taking a continuing education course on AI privacy could meet the training requirements for my AIGP and CIPP/US certifications.

Next, some of these organizations allow tasks, such as authoring articles or books, to count towards

continuing education requirements. For example, my authorship of this article may meet the continuing education requirements for my certifications.

Finally, all three organizations permit some degree of reciprocity, so that courses approved by one issuing body may meet continuing education requirements of the others. All non-organization credits are subject to audit. Still, this reciprocity goes a long way into making the pursuit of multiple certifications feasible.

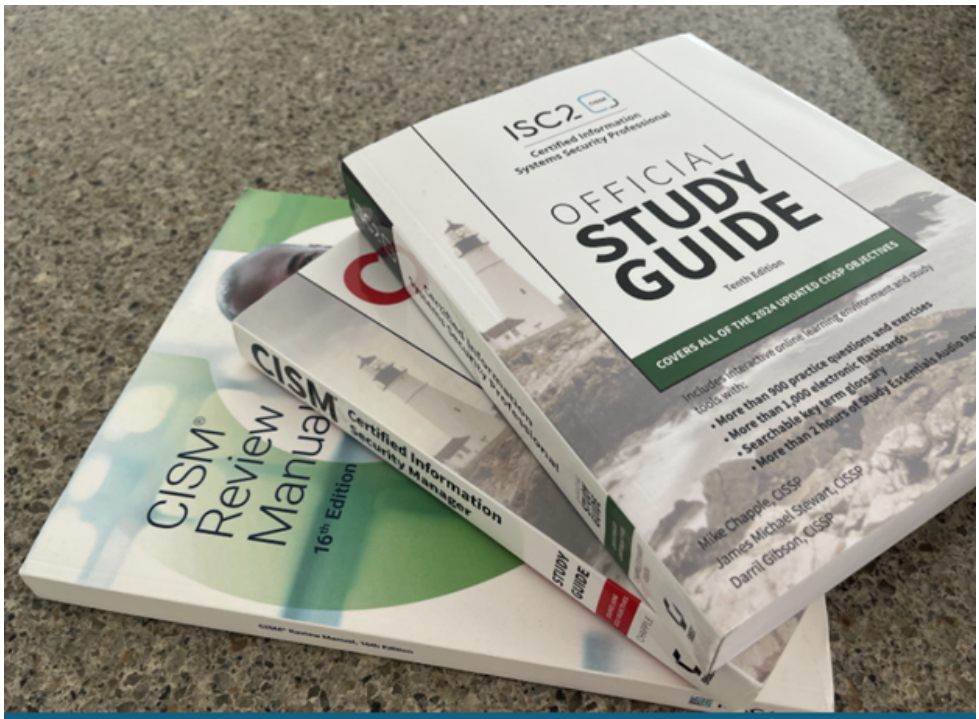

Fig.2. Training manuals for the CISM and CISSP certifications

I encourage readers who are thinking of pursuing multiple certifications to review each organization's continuing education policies before coming to a decision.

- ISACA's Continuing Education Policy
- IC2's Continuing Education Policy
- IAPP's Continuing Education Policy

7. Do you have study tips?

I suggest starting with official training materials offered by, or approved by, the certificate-issuing organizations. Then consider going to third party providers to supplement those official materials.

The following resources are the ones I used in acquiring my three certifications (CISM, CIPP/US, and AIGP), or those that I think may be helpful. Don't take them as endorsements, since everyone's study styles differ. But this information may offer helpful data points for you in charting out your own training regimen.

For the CISM

First, I took an online live training course through Training Camp, an ISACA-approved third party provider. As an approved course, it also provided access to ISACA's training manual and practice exams. My Training Camp point of contact also provided invaluable, personal advice on the application process that helped me acquire the CISM. Note that ISACA offers training, and these other tools, *a la carte* for readers who don't need the entire set. Next, I bought the "CISM Certified Information Security Manager Study Guide" by Mike Chapple. Finally, I bought additional practice exams from Pocket Prep. I found all of these exam prep tools useful.

For the CISSP

If I were to pursue this certification, I would take an ISACA-approved training course such as Training Camp, or one from a reputable third-party provider, such as Udemy (note that Udemy offers courses from multiple CISSP instructors, so you may need to do some research to find one that is right for you). I'd also use Chapple's CISSP guide and Pocket Prep practice exam questions. Finally, one friend who obtained their CISSP also found it helpful to subscribe to this third-party newsletter to receive free CISSP practice questions and exam tips by email.

For the CIPP/US

If money is a factor, I think many attorneys could forego the training course. That said, the course would be useful for students who learn through listening. I also suggest buying IAPP's official practice exams.

For the CC

Did you sign up for the free training? If not, hurry up!

For the AIGP

The most important prep tool is a study manual. IAPP doesn't yet offer a standalone AIGP training manual. Instead, students must currently take one of IAPP's "live" courses (either online or in-person). Thus, my first suggestion: obtaining that manual may be worth paying extra for a live course over a recorded one. IAPP may later release itsAIGP training manual to the public, so check with them before committing to a course. Next, I suggest purchasing IAPP's official practice exam. Finally, for third party materials, I used these flash cards by Quizlet. Finally, for third-party materials, one of my friends who earned the AIGP found this Udemy course useful.

And, generally, I found this article about test preparation very helpful.

Enhance your brand and help your organization

I'm greatly in favor of cyber counsel earning certifications. I believe that training to the right one (or ones) can greatly enhance an individual's professional brand while bringing tremendous value to the organizations they serve.

As with all things, picking the "right" certifications involve balancing multiple factors, including:

- The purpose for seeking it;
- The costs involved in passing exams; and

- The costs involved in maintaining the certification.

Also, I recommend that most counsel start with an entry level certification and then consider pursuing advanced ones as their skills and knowledge mature. I hope this guide provides readers with information for thoughtfully investing your time and money. *Good luck…I'm rooting for you!*

Join ACC

Robert Kang

Professorial Lecturer

George Washington University Law School

Robert Kang is a Professorial Lecturer at the George Washington University Law School, and a consultant. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation’s Cybersecurity Advisory Board.