



Security Certifications

by Ray Bernard, PSP

Designations tell you who you're working with and who you're hiring, and they're the next step in your own security education.

Certifications

For most people, and especially for security practitioners, the events of September 11th elevated the importance of security. Many security professional associations assessed themselves in a new light, and new organizations sprung up dedicated to addressing one function or another related to security.

Now, four years later, it is worth looking at the current roster of security association certifications. CSOs and others with responsibility for both physical and IT security will need to know a little about the certifications in both disciplines.

Perspective

There are several perspectives from which to view a professional security association and its certifications:

- How you, yourself, would benefit directly from the educational programs and certification training
- The consideration given by employers or clients for your demonstration of advanced knowledge through certification
- The expanded knowledge and contacts pool available to you through your colleagues in certification
- Certifications that you should require of your employees
- Certifications that you should require of service providers who form a part of or support your security programs and projects

Certification reflects a set of professional standards that have to be met, which include the demonstration of a certain level of expertise or competence. Thus security certifications commonly involve both an experience and an educational component, although a forensic examiner, for example, may need to be certified before beginning work in that field. Some certifications require sponsorship or endorsement of the applicant by one or more association members. Certifications usually require periodic renewal involving continuing education, and so it is prudent to check an association's current membership list to verify that an asserted certification standing is current.

Security Education

Safety and security go hand in hand, and so certifications related to Fire and Life Safety issues are included in this article's review. Academic degrees, certifications by private

Security Certifications

companies and law enforcement related certifications are not included in this review. Certifications that do not include a validated educational component (for example, those that are based upon years of experience only) are also not included.

Higher Education

Security related academic educational opportunities are significant, and should be considered in addition to the professional association certifications presented in this article. For a listing of universities offering degrees and classes in security, see the document links on the Academic Resources page of the *ASIS International* website: <http://www.asisonline.org/education/academicresources.xml>. This page also contains downloadable documents chronicling ASIS's in-depth research in support of security academic education by the *ASIS International Academic/Practitioner Symposiums*. Also see the *National Academic Consortium for Homeland Security* (NACHS) at <http://homelandsecurity.osu.edu/NACHS/members.html> for a list of more than 290 consortium member universities.

Technology and Certifications

Some security certifications are very technology focused, while others are more general or pertain to security management issues rather than technology. Security is a business function, and the business security requirements are primary drivers for the deployment of security technology. This means that practitioners in security management positions must have some understanding of the uses and limitations of technology. Conversely, those who specify, design, provide, operate and maintain security systems must have some understanding of the role the technology plays in the overall security scheme, in support of management's security strategies, policies and procedures. There are significant bodies of knowledge at each level (managerial and technological).

Being a Professional

There are many definitions and descriptions for the term "professional". The most common attributes ascribed to professionals are advanced or specialized knowledge; practical skills; adherence to standards or to a code of professional conduct; training or education culminating in a degree or professional certification; and a high level of competency. The road to professional competency is not an accidental journey, or even a finite journey. It begins with the decision and the desire to achieve professional standards in one's work, followed by a path of career-long learning.

The single most commonly heard comment from practitioners who attend certification preparation classes or embark on a personal course of study is this expression of personal realization, "I should have done this a long time ago."

It has also been said that a professional knows what he knows, and also knows what he doesn't know. Achieving the latter is the greater challenge, but it can be answered by obtaining a good understanding of the spectrum of knowledge that exists in one's profession; that's something that security management and high level certifications provide. The advantage of having such knowledge is that one is never at a loss, but

Security Certifications

instead knows that “someone else knows” and can reach out for the required knowledge when needed.

Most certification programs provide a list of books and reference materials, and offer study guides. Some associations offer certification test preparation classes, and some private organizations offer comprehensive training for certifications in the IT (information technology) domain. Professional education is often an evolutionary process, beginning with specialization in a limited area and progressing to a more general command of the field, enabling one to assume larger and more complex responsibilities. Thus a common and workable path is to become certified first in the area closest to one’s current or intended area of specialization, and then to proceed on with additional education as best fits one’s job requirements or personal interests.

Security Certification Subjects

Table 1 provides a chart of professional security certifications for corporate, physical and IT security. Rather than reflect the specific knowledge elements of each certification, the chart is designed to minimize the number of knowledge categories to provide an overview that’s comprehensible and doesn’t require page-turning to view. Because the full breadth and depth of each certification isn’t depicted in the chart, a list of certification descriptions is provided to furnish a little more information about each certification.

In recent years national legislation such as HIPAA, Sarbanes-Oxley, as well as state legislation like California Senate Bill 1836, have impacted the risk management picture. As a result, privacy certifications are also being developed, such as the *Certified in Healthcare Privacy (CHP)* designation jointly developed by the Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA), who also developed the *Certified in Healthcare Security (CHS)* certification. Fullfilling both requirements achieves the *Certified in Healthcare Privacy & Security (CHPS)* designation. The International Association of Privacy Professionals has developed the *Certified Information Privacy Professional (CIPP)*.

While privacy certifications are outside the intended scope of this article, they are mentioned here because Chief Security Officer responsibilities will generally encompass privacy where a separate Chief Privacy Officer position does not exist. So although privacy certifications are not examined here, they are worthy of this brief mention.

Additionally, Table 1 identifies whether a security certification is can be considered to be primarily in the realm of corporate security management, physical security or information security or IT security. Note that information security is a category that overlaps with IT security, which deals not only with electronic information systems and networks, but with telecommunications and messaging systems as well.

Finally it should be noted that certifications originating from outside the U.S. are not included here due to space considerations.

Security Certifications

Table 1. Professional Security Certifications Overview

Security Subject	ASIS <i>CPP</i> (1)	ASIS <i>PSP</i> (2)	ASIS <i>PCI</i> (3)	ACFEI <i>CFE</i> (4)	NCMS <i>ISP</i> (5)	IAHSSP <i>CHPA</i> (6)	HIMMS/ AHIMA <i>CHS</i> (7)	AH&LA <i>CLSS</i> (8)	AH&LA <i>CLSD</i> (9)	ISSA/ (ISC) ² <i>CISSP</i> (10)	(ISC) ² <i>SSCP</i> (11)	ISACA <i>CISA</i> (12)	ISACA <i>CISM</i> (13)	SANS <i>GIAC</i> (14)	IISFA <i>CIFI</i> (15)	CII <i>CCISP</i> (16)	SIA <i>CSPM</i> (17)
Industry Specific	—		—	—	—	Healthcare	Healthcare	Hospitality	Hospitality	—		—	—	—	—	—	—
Security Management (M), Physical (P), Information (I) or IT Security (IT)	M, P, I	P	M, P, I	M	M, P, I, IT	P, I	I, IT	M, P, I	M, P, I	IT	IT	IT	IT	IT	IT	I, IT	P
Security Management, Planning and Principles	●			●	●	●	●	●	●	●			●	●			
Security Risk Assessment	●	●			●	●	●		●	●	●		●	●			
Risk Management	●	●			●	●	●		●	●			●				
Physical Security	●	●			●	●	●	●	●	●							●
Information Security	●				●	●	●			●		●	●	●		●	
Intellectual Property	●				●	●											
Personnel Security	●	●	●			●	●	●	●								
Facility Security Design	●	●			●												●
Safety	●	●						●	●								
Corporate Investigations	●		●	●	●	●	●	●	●	●							
Accounting and Financial Controls	●			●			●										
Forensics Investigations	●			●		●	●								●		
Information Systems Security			●			●	●				●	●	●		●	●	
Network Security					●		●			●	●		●	●	●	●	
Business Continuity Planning/Disaster Recovery	●									●	●				●		
Incident Response	●					●	●	●	●	●	●	●		●	●	●	
Computer Forensics (Cybercrime)						●	●							●	●	●	
Legal Aspects	●		●	●			●	●	●	●					●		
Security Education	●				●		●			●							

Security Certifications

Audits, Self Assessment, Compliance Monitoring				●	●						●	●			●		
COMSEC/TEMPTEST ¹					●												
Counter Intelligence ²					●												

1. COMSEC stands for military communications security. TEMPTEST is an acronym for *Transient Electromagnetic Pulse Emanation Surveillance Technology*. A system developed by the US Government to protect against an attacker to analyzing the electromagnetic radiation emitted from the computer hardware to obtain information. It was created in response to the fact that information can be read from computer radiation (for example, from a CRT or LCD display) easily at quite a distance.
2. Counter intelligence in this sense means the use of, or the detection and/or nullification of electronic surveillance equipment, commonly referred to as “bugging”.

Security Certifications

Security Certifications

The following certification descriptions are numbered to match the column number in Table 1.

- 1. Certified Protection Professional (CPP)** – This preeminent security certification from ASIS International covers five major security management subject areas in depth: Security Principles & Practices, Business Principles & Practices, Personnel Security, Physical Security and Information Security. The development of the PSP designation has allowed the CPP certification to adjust its focus slightly, incorporating more elements of enterprise risk security management. This certification is ideal for CSOs, corporate security directors and senior security managers. (www.asisonline.org)
- 2. Physical Security Professional (PSP)** – The ASIS International certification for security professionals whose primary responsibility is to conduct threat surveys; design integrated security systems that include equipment, procedures, and people; or install, operate, and maintain those systems. It covers the subject areas of Physical Security Assessment, Selection of Integrated Physical Security Measures and Implementation of Physical Security Measures. (www.asisonline.org)
- 3. Professional Certified Investigator (PCI)** – The ASIS International certification for security professionals whose primary responsibility is conducting investigations. It covers the subject areas of case management, evidence collection, and case presentation. (www.asisonline.org)
- 4. Certified Fraud Examiner (CFE)** – offered by the Association of Certified Fraud Examiners. This certification covers these four areas of knowledge: Criminology & Ethics, Financial Transactions, Fraud Investigation, and the Legal Elements of Fraud. (www.cfenet.com)
- 5. Industrial Security Professional (ISP)** – offered by the National Classification Management Society, whose purpose is to advance the practice of classification management in the disciplines of industrial security, information security, government designated unclassified information, and intellectual property. This certification is primarily for those working in government or private industry projects that involved the management and protection of classified government information. (www.classmgmt.com)
- 6. Certified Healthcare Protection Administrator (CHPA)** – offered by the International Association of Healthcare Security and Safety Professionals (IAHSSP). This certification covers these four areas of knowledge as they specifically apply to Healthcare organization security: management, security, safety, and risk management. (www.iahss.org)
- 7. Certified in Healthcare Security (CHS)** – sponsored by the Healthcare Information and Management Systems Society and administered by American Health Information Management Association, this certification denotes advanced

Security Certifications

competency in designing, implementing, and administering comprehensive security protection programs in all types of healthcare organizations.

8. **Certified Lodging Security Supervisor (CLSS)** – offered by the Educational Institute of the American Hotel and Lodging Association (AH&LA), this certification is perfect for the responsible general manager with security obligations. The subject matter includes Lodging Security Overviews, Legal System, Operational Policies and Procedures, Locks and Keys, Investigating and Reporting, Handling Disturbances, Patrols and Grounds. (www.ahma.com)
9. **Certified Lodging Security Director (CLSD)** – offered by the American Hotel and Lodging Association (AH&LA), the CLSD designation is the premier symbol of professional achievement for lodging security directors and executives. The subject matter includes the material of the CLSS certification plus the additional subjects of Security Planning, Operational Policies and Procedures, Managing Security Department Human Resources & Crisis Management and Emergency Response Procedures. (www.ahma.com)
10. **Certified Information Systems Security Professional (CISSP)** – offered by the International Information Systems Security Certification Consortium (ISC)². The CISSP credential is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers. The CISSP credential demonstrates competence in the following 10 domains of the (ISC)² CISSP Core Body of Knowledge: Access Control Systems and Methodology; Applications and Systems Development Security; Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP); Cryptography; Law, Investigation and Ethics; Operations Security; Physical Security; Security Architecture and Models; Security Management Practices; and Telecommunications and Network Security. (www.isc2.org)
11. **Systems Security Certified Practitioner (SSCP)** – offered by the International Information Systems Security Certification Consortium (ISC)². The SSCP credential is ideal for those working toward or who have already attained positions as Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators. (www.isc2.org)
12. **Certified Information Systems Auditor (CISA)** – offered by the Information Systems Audit and Control Association, is for the experienced computer auditor or computer security professional. The subject areas include Management, Planning and Organization of IS; Technical Infrastructure and Operational Practices; Protection of Information Assets; Disaster Recovery and Business Continuity; Business Application System Development, Acquisition, Implementation and Maintenance; Business Process Evaluation and Risk Management. (www.isaca.org)
13. **Certified Information Security Manager (CISM)** – offered by the Information Systems Auditing and Control Association, was specifically developed for the information security professional who has acquired proven experience working on the “front lines” of information security. Individuals with five years or more of

Security Certifications

- experience managing the information security function of an enterprise. This certification covers Information Security Governance; Risk Management; Information Security Program Management; Information Security Management; Response Management. (www.isaca.org)
- 14. Global Information Assurance Certificate (GIAC)** – offered by SANS Institute is actually a series of certifications for information systems, computer and network security. Each GIAC certification is designed to stand on its own, and represents a certified individual's mastery of a particular set of knowledge and skills. The certifications fall into three categories: Audit, Management and Security Administration. (www.giac.org)
- 15. The Certified Information Forensics Investigator™ (CIFI)** – offered by the International Information Systems Forensics Association is specifically developed for experienced information forensics investigators who have practical experience in performing investigation for law enforcement or as part of a corporate investigations team. The CIFI certification is designed to demonstrate expertise in all aspects of the information investigative process and is dedicated to bringing a level of consistency to the profession than can be recognized outside the field. (www.iisfa.org)
- 16. Certified Critical Infrastructure Security Professional (CCISP) Basic and Advanced** – are two certifications offered by the Critical Infrastructure Institute, and recognized by the Information Systems Security Association (ISSA). the CCISP domain includes knowledge and professional skills required for designing, maintaining, and managing security architectures as well as the extended skills required for critical infrastructure, SCADA, or other high availability environments. (www.ccispcert.com)
- 17. The Certified Security Project Manager (CSPM)** – offered by the Security Industry Association, provides professional accreditation of Project Managers involved in the design and installation of security systems. The program certifies individuals who have demonstrated their proficiency in every aspect of project management as it relates to security systems. The certification program is designed specifically to meet the practical aspects of designing and managing security projects that involve electronic security systems. (www.SecurityLearningNetwork.com)



Ray Bernard is board-certified as a Physical Security Professional (PSP) by ASIS International. Ray is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides high-security consulting services for public and private facilities. Ray is a technical consultant and writer who has provided pivotal direction and technical advice in the security and building automation industries for more than 18 years. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788.
