

Why Obtain Security Certifications?

By Tim Smit

What certifications are required or desired to continue your ascent up the corporate ladder within the information protection industry?

What certifications are required or desired to continue your ascent up the corporate ladder within the information protection industry?

According to *Certification Magazine*, the top industry certification is the Certified Information Systems Security Professional (CISSP), from the International Information Systems Security Certification Consortium, or (ISC)². The second leading certification is the Certified Information Security Manager (CISM) from the Information Systems Audit and Control Association (ISACA).

The CSO Council, (www.csoonline.com), recommends a combination of both experience and education, depending on the requirements of the role(s) and the requirements of the company.

What do these certifications cover and provide for both you and your organization?

The CISSP Common Body of Knowledge:

- Access Control Systems and Methodology
- Application and Systems Development Security
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)
- Cryptography
- Law, Investigations and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Network Security

The CISM Content Areas:

- Information Security Governance
- Risk Management
- Information Security Program Management
- Information Security Management
- Response Management

“Technological solutions alone cannot protect an organization’s critical information assets. Employers demanding qualified information security staff give their organizations a leading edge by providing the highest standard of security for their customers’, employees’, stakeholders’ and organizational information assets.” ((ISC)², 2006).

The certification(s) “promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services.” (ISACA, 2006).

There are more benefits for obtaining these two certifications.

The CISSP Benefits

- Demonstrates a working knowledge of information security
- Confirms commitment to profession
- Offers a career differentiator, with enhanced credibility and marketability
- Provides access to valuable resources, such as peer networking and idea exchange

Compensation: According to *Certification Magazine*’s 2005 Salary Survey, the CISSP salary ranges from \$105,000 to \$115,000 per year.

Benefits of Certification to the Organization:

- Establishes a standard of best practices
- Allows access to a network of global industry and subject matter/domain experts
- Makes broad-based security information resources readily available
- Adds to credibility with the rigor and regimen of the certification examinations
- Provides a business and technology orientation to risk management

Of course, there are a few potential disadvantages. They are listed below.

Potential Disadvantages of the CISSP

Cost. The study material recommended by the (ISC)², but not limited to, is the Official (ISC)² Guide to the CISSP Exam (Hardcover), \$69.95. Additionally, there are review seminars offered around the globe from multiple vendors. The (ISC)² holds a five-day review session. The cost is \$2695 (\$2245 for ISSA members).

The test expenses consist of a \$599 fee, but if you register 16 days prior to the exam, the cost is then \$499. Once you have passed the exam, the (ISC)² requires an annual fee of \$85 to maintain your certification.

Time. The actual exam is scheduled for six hours, consisting of 250 questions. Additionally, this has not yet accounted for any prep study time prior to the exam.

Maintenance. After you have spent the time and money on obtaining the certification, the presumption is that you will want to maintain that certification for more than a three-year period. The credential holder must earn CPE credits over a three-year period—or retake their certification examinations. CPE credits are earned through activities related to the information security profession including, but not limited to, the following:

- Attending educational courses or seminars
- Attending security conferences
- Being a member of an association chapter and attending meetings
- Listening to vendor presentations
- Completing university/college courses
- Providing security training
- Publishing security articles or books
- Serving on industry boards
- Self-study
- Completing volunteer work, including serving on (ISC)² volunteer committees ((ISC)², 2006)

The CISM Benefits

- Demonstrates a high level of current information security management practice
- Emphasis on management of information security
- Seasoned information security professional

- Offers a new career differentiator (only approximately 5,200 individuals with the CISM designation)

Compensation: According to Certification Magazine's 2005 Salary Survey, a CISM holder's average pay is \$106,000 per year.

Benefits of Certification to the Organization:

- Global recognition and international best practices
- International exposure
- Enables organizations to define core competencies and international standards
- Method of measuring existing staff or comparing prospective new hires

Potential Disadvantages of the CISM

Cost. The study material recommended by ISACA is, but not limited to this, is the Certified Information Security Manager (CISM) Review Manual 2006 English Edition, \$100 for nonmembers and \$75 for members. Also recommended is the CISM Review Questions, Answers & Explanations Manual 2006 English Edition (\$80 for non-members and \$60 for members). Review seminars are also offered. These review seminars are five days for \$350 (non-members) and \$300 (members).

The test expenses consist of a \$510 fee, but, again, if you are a member, the cost is \$390.

Once you have passed the exam, ISACA requires an annual fee of \$65/\$40 to maintain your certification.

Time. The actual exam is scheduled for four hours, consisting of 200 questions.

That does not account for your prep study time prior to the exam.

Maintenance. Maintenance fees and a minimum of 20 contact hours of CPE are required annually. In addition, a minimum of 120 contact hours is required during a fixed three-year period. Upon completing the requirements for initial certification, the CISM will be provided with the CPE policy booklet for detailed criteria to be used in developing a personal CPE program.

Roles and Perceptions

After interviewing a number of individuals who have obtained either one or both of the certifications, the general consensus is that the individuals' roles have changed.

They also noted that the customers who are served by these individuals are extremely sat-

isfied with the knowledge and recommendations that these individuals provide them.

A particular example included a newly certified individual being added to an international security board that had been just created. This professional consults with their international partners on a quarterly basis. The certification enabled them to travel and speak to partners and customers with their information security knowledge and best practices knowledge.

A seasoned certified employee stated, "I talk with the 'C' level board more because I am the only individual who has obtained these certifications within the organization. I basically get to speak my peace with them monthly in regards to security posture and strategies."

Differences

There are many differences between the two certifications, but most notably are the differences in the experience requirements. Only the CISM requires information security management experience, in addition to general information security experience. The CISSP does not require security management experience to obtain the certification.

Summary

Obtaining and combining these two top certifications expands your knowledge and opens more extensive resource options within both the (ISC)² and ISACA with international recognition to you and your organization as leaders within the industry.

Additionally, you have multiple avenues for continuing your education and awareness by maintaining your memberships. These memberships enable you to access current training seminars, online training, conferences, and continuous educational opportunities.

About the Author

Tim Smit, CISSP, CISM, is a Senior Information Protection Network Risk Analyst with Medtronic, Inc.

References

- http://www.certmag.com/articles/templates/cmag_career.asp?articleid=96&zoneid=66
- <http://www.csocouncil.org/>
- <http://www.csoonline.com>
- <http://www.footepartners.com/TCSecurity2005.htm>
- <http://www.isaca.org/cism>
- <https://www.isc2.org/>