I recently spoke with Ed Zeitler, Executive Director of (ISC)^2 about recent developments at this important certification body for security professionals. In part one of this two-part series, Mr Zeitler discusses the recent changes in the requirements for the Certified Information Systems Security Professional (CISSP) designation and the recent acceptance of the CISSP as an international standard.

* Tell us about the recent changes in CISSP certification requirements.

There are three basic changes. First, experience goes from four years to five years. Second, in the past, you had to show experience in only one domain of the Common Body of Knowledge (CBK); now you need experience in at least two domains. Finally, the endorsement for applicants to the base certifications (i.e., CISSP, SSCP and CAP) must come from another (ISC)^2-certified person who subscribes to the (ISC)^2 Code of Ethics.

* What led to the changes?

We are committed to maintaining the professionalism and integrity of the certification. Our latest global survey of information security professionals (with over 4,000 respondents) who have responsibility for managing and developing security policies showed they have an average of 8.6 years of experience. We regularly revise our CBK and our examinations to keep them rigorous and relevant to the ever-changing threat environment. We do not want to lower the bar to meet increasing demands for certifications; we want the industry to rise up to meet those demands. Management must have confidence in our certifications and we want to ensure that rigor is maintained and recognized. IDC has estimated that there are 1.5 million people in the world doing information security and we currently have around 50,000 certificate holders. So our certified members are an elite group.

* How will the changes help to achieve your goals?

We want to keep pace with the complex demands of information security today. To ensure that our certifications remain the gold standard in the industry, additional measures of experience are necessary to prove that candidates clearly demonstrate a thorough understanding of how to implement an effective information security program and manage information security risks. In changing the endorsement requirement so that only an (ISC)^2-credential holder can endorse a candidate, we are better assured that the candidate will make the same ethical commitment as his
or her endorser. And by vouching for the integrity of the candidate, the endorser is in effect putting his or her own professional reputation on the line.

* How did you respond to the recent announcement from the US federal government that all of its Information System Security Officers (ISSOs) would have to achieve formal security certification<https://www.isc2.org/cgi-bin/content.cgi?page=949>?

We have participated in a number of US federal government programs that are aimed at professionalizing the workforce. Our involvement began before my tenure here at (ISC)² but I am now actively involved. Our long history, the quality of our certifications and the fact they are accredited by the International Organization for Standardization (ISO) <http://www.iso.org/iso/en/aboutiso/introduction/index.html> are important to the government experts.<https://www.isc2.org/cgi-bin/content.cgi?page=1156>

* Tell us more about the ISO link.

The accreditation is managed in the US by ANSI.<http://www.ansi.org/> They put us through a rigorous annual review of all our processes to be sure that we conform to their standards for certification bodies (ANSI/ISO/IEC 17024).< http://publicaa.ansi.org/sites/apdl/Documents/Conformity%20Assessment/Personnel%20Certification%20Accreditation/Documents%20related%20to%20accreditation%20under%20ANSI-ISO-IEC%2017024/Public%20Documents/IAF-GD24-2004.pdf> For example, none of our (ISC)² CBK course instructors is permitted to be involved in exam development. And in fact, we don’t refer to our courses as preparatory because they are not designed to teach to a specific exam. We must maintain a strict firewall between our exam and our education operations.

More in part 2, when Mr Zeitler discusses the new CISSP concentrations.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.