In February, I posted an article about Jeff Bardin, CISO of the Hanover Insurance Group, on the MSIA Portal <http://tinyurl.com/evzrw>. Mr Bardin and I spoke later about his work and he pointed me to an article he recently published about communicating with C-level executives that will interest readers <http://www.csoonline.com/read/040106/communicate.html>. I wanted to expand on a couple of interesting points raised by Mr Bardin in his article.

He wrote, “1. Seek out a trusted sponsor—a person who can serve as a conduit to getting your message heard. At one firm, I found the VP of Internal Audit to be a great ally. Internal Audit has been trying for years to get companies to comply with their findings; they follow a code like you. Your efforts will only help their cause. Align your information security pitch with their internal controls–oriented message, adding specifics relevant to the 10 domains of ISO17799 or CISSP Common Body of Knowledge.”

Readers will find useful resources bearing on this point at the following Web sites:

The Committee of Sponsoring Organizations of the Treadway Commission <http://www.coso.org/> or COSO defines internal controls as follows (quoting directly from <http://www.coso.org/key.htm>):

Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

The page continues with “Key Concepts” as follows:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is effected by people. It’s not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity’s management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

To buy the complete ISO17799 2005 standards as a downloadable file or on paper, go to <http://tinyurl.com/c7yqm>.

The (ISC)^2 Common Body of Knowledge (CBK) is described at <http://tinyurl.com/z9bso>. The
ten domains are listed as follows:

- 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
- Telecommunications and Network Security.

Having external validation of the points you want to make with upper management can increase your credibility. Remember, many of our colleagues have little or no knowledge of the professional standards underlying information assurance and may erroneously assume that we are making up rules as we go. Being able to point to industry and international standards can make a real difference in acceptance of our proposals.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 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.