A reader recently wrote to me as follows: "Just today I accepted a job offer. This organization has no information technology (IT) audit presence currently and it will be a challenge for me." He then posed a series of interesting questions.

> How do you go into an IT department and formulate policies, procedures and/or standards (or whatever comes before the other). <

Asking about formulating policies, standards and procedures strikes me as unusual for an IT auditor. Auditors do not normally promulgate policy; they normally verify compliance with policy. That said, I think an essential phase in any such work is to avoid walking into the IT department like a gunslinger ready to tell everyone what to do. Anyone thinking about creating or modifying policies needs upper-management support before trying to do anything else at the policy level.

Next, my practice is to investigate the current situation carefully and respectfully. Talk to key managers and employees about the current state of controls. Listen more than you talk; take detailed notes as people are speaking. Because I type quickly, I prefer to display what I am writing using a projector in real time; participants can see exactly what I'm noting and can make corrections and additions at once to keep me on track. In addition, give or send your interlocutors a copy of what you have written before you leave them or as soon as possible. You want to be sure that the effort is seen as a collaboration, not as a punitive raid.

Be sure to include non-IT departments. In addition to production departments, you must consult the human resources, records management, legal, public relations and facilities departments. All of these experts have unique and important contributions to the developing picture of how information is managed and protected in your institution.

In addition to speaking with individuals, you can also use focus groups and surveys to gather information about how information and IT resources are currently managed. Be sure to solicit areas of concern and to provide for anonymity if necessary.

Using the initial findings, you can apply techniques such as Computer-Aided Thematic Analysis (TM) (see my paper listed at <http://www.mekabay.com/methodology/index.htm>) to sort through and organize the masses of information you have collected. Present a preliminary report to the members of the IT department and ask for comments and suggestions. Present your findings in one-on-one meetings, not by convening a group and slamming them with a book full of perhaps critical findings. Indeed, whenever possible, you should avoid presenting new information and proposals to any group of people all at once -- the interpersonal conflicts and positional rivalries among committee members often obscure the value of your work and lead people to object to proposals for political reasons rather than substance.

As for how to promulgate information protection policies, I always recommend that clients use
existing templates as a starting point to save a lot of time. Two particularly helpful documents are


> How does one provide assurance that network and other significant systems are operating as intended by management? <

> How does one provide assurance that system controls are in place and are effectively and efficiently protecting corporate assets? <

> How does one assure that regulatory requirements relevant to related to systems operations are being complied with? <

> How does one provide assurance that corporate policies on information systems promoting the well being of the company are clear and concise and are enforced?" <

Answering these questions in significant detail is impossible in the format of this column. I will take an easy way out by pointing to the newly-published *Computer Security Handbook, 4th Edition* from Wiley (ordering information is at the end of this article). Sy Bosworth and I worked for two years as editors of this new edition, and we're proud of the work of our contributors. Chapter 28 covers security policy guidelines; chapters 31 through 33 cover employment practices and policies, operations security and production controls, and e-mail and Internet usage policies. Chapter 35 summarizes material on social psychology and information security policy implementation that readers may have seen in this series of columns over a year ago. Chapter 36 specifically addresses the computer systems security audit process. Chapter 37 reviews vulnerability assessment and intrusion detection; chapter 38 covers monitoring and control systems; and chapter 39 looks at application controls. Chapter 45 is a summary of management roles and responsibility in information protection and chapter 46 looks at practical guidelines for developing security policies. Finally, with regards to your questions, chapters 2, 27, and 52 address questions of law and standards that must be considered in promulgating and implementing effective information assurance plans.

More about the _Handbook_ in another column later.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor of Information Assurance in the Department of
Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 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.