Stepping Through the IS Audit, 2nd Edition

By J. L. Bayuk, CISA, CISM

Reviewed by C. Warren Axelrod, Ph.D., CISM, CISSP

At first blush, one gets the impression that this concise, well-organized book is targeted to those looking to become information systems (IS) auditors or those who are just beginning their careers in IS auditing. However, upon reading further, it is clear that the author is trying to reach another audience—namely the auditee who is subject to IS audits. In fact, it is the latter, who far outnumber the auditors themselves, who are most in need of a book such as this. There is a reasonably large body of literature on how to conduct audits, but far fewer books on how those being audited should handle an audit. Because of this, many audits are conducted in an adversarial atmosphere and do not reap the full benefits to the organization whose processes and controls are being reviewed.

So the question is, how well does the book achieve its dual goals of informing new and prospective IS auditors and advising auditees?

The book provides a very informative introduction to the history of the profession from its beginning as electronic data processing (EDP). For younger readers, the term EDP is prehistoric—in line with the typewriter, carbon paper, rotary telephone and the like. The background gives the reader a useful perspective as to how the IS audit profession arrived at where it is today.

"Auditors can start the audit relationship on a friendlier note by giving auditees copies of this book."

The next two chapters, on the audit planning and execution processes, are the guts of the text. The carefully constructed chapters explain how audits are all about risk exposure and how to minimize its impact by invoking mitigating controls. The reader is led through the audit planning process of identifying risks, assessing them, specifying which areas audits should cover and establishing an audit program.

The chapter on audit execution describes preliminary data gathering, ensuing field work and testing, and the audit report, which lists audit points and recommendations, along with the executive summary. The author then addresses the all-important remediation and tracking phases without which an audit becomes just one more piece of "shelfware."

The next chapter treats the reader to a hypothetical case study, which is written in a light, easy-to-read format incorporating dialog and humor.

Appendix A is noteworthy as it provides a detailed survey template for an audit program, listing control objectives and control activities to implement the objectives and explaining how the controls can be tested. This is useful for the established IS auditor to verify that his/her survey is complete, and it can be a savior for the auditee who will be subject to such an examination.

A book such as this is meant to lower the fence that is often raised between auditor and auditee. It rightly advocates a cooperative, as opposed to adversarial, relationship between the many cases. Too often, an overenthusiasticauditor will want to demonstrate that he/she is smarter and more knowledgeable than the object of the audit, and an intimidated auditee might fail to respond adequately and accurately or could well respond out of scope with distressing results. The book's author has worked on both sides of the fence, having been an auditor and now an auditee. This range of experience brings the balance and reason that is expressed so well in the book. Too often, auditors, who are not responsible for implementing their own recommendations, propose technically infeasible and economically unjustifiable solutions to what may not even be the important issues. It takes the experience of the author, as expressed in the book, to moderate such excesses and guide the auditor and auditee along a path that is win-win for the participants and benefits the audited organization as a whole.

From appearances, one might assume that the book is a guide for the novice IS auditor. But, in reality, the book has two valuable strengths—one is to educate auditees as to what to expect in an IS audit and how to deal with the process and the issues, and the other is to help auditors understand auditees' concerns and questions. Few books or articles offer this. The challenge is to get this message across by making the book available to a broader audience. Perhaps auditors can start the audit relationship on a friendlier note by giving auditees copies of this book. Many auditees would have a much more positive view of any auditor who wanted to share this information with them.

C. Warren Axelrod, Ph.D., CISM, CISSP
is director, global information security, for Pershing LLC, a BNY Securities Group company. He develops and enforces corporate security policies, standards and architectures. He is involved in the financial services industry and at national levels with security and critical infrastructure protection issues. He was honored with a *ComputerWorld* Premier 100 IT Leader Award in 2003. He is the author of *Outsourcing Information Security* (Artech House, 2004). He also chairs the GAISP Information Security Policy Principles Working Group.

Editor's Note

Stepping Through the IS Audit, 2nd Edition, is now available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.253.1545, ext. 401.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal. Information Systems Control Journal* does not attest to the originality of authors' content.

www.isaca.org