Stepping Through the IS Audit

Jennifer Bayuk, CISA | Reviewed by Bob Darlington, CISA, CIA

The first time that many auditees are aware of an impending audit is when they receive a memo, e-mail or telephone call from the lead auditor attempting to schedule the opening meeting for the engagement. This introduction to the audit leaves auditees wondering "Why me?" or "What did I do wrong?" These questions are often followed by an overwhelming feeling of confusion with regards to how they should prepare. To the outsider, the audit process appears to be an extremely confusing one, especially for those who have not been exposed in the past. This causes the value of the audit to be questioned and the potential benefits to be ignored.

Stepping Through the IS Audit has been written with the first time auditee in mind. It provides understanding and guidance with respect to the audit process. This helps the auditee approach the audit with confidence and understanding to effectively participate in the process.

In the first part of the book the author explains that IS audits are meant to address management concerns and that these concerns are based on risk. This risk could be addressed by IS management personally supervising all risk-inherent activities. This, however, is not reasonable or possible because of the sheer number of activities or projects that takes place in the IS area simultaneously. The only alternative is to define processes, determine how to tell if they are effective, then set them in motion and evaluate the results. Auditors help with the evaluation by providing an independent review of the process and controls in place, to ensure that they are working as intended by management.

To facilitate understanding, the author discusses some of the history of IS auditing along with key legislation such as the Foreign Corrupt Practices Act of 1977 and regulatory body requirements. These have made it critical that senior corporate management ensure that all business processing be appropriately controlled.

The author, as part of the introduction to audit, discusses the risk identification process that takes place between senior audit and IS management in order to understand the activities and risks within the IS department. The author does this by taking the reader through a sample information gathering session which results in the identification of a number of risk areas suitable for audit. It is demonstrated through this discussion that the identification of risk involves input from both the client and the auditor.

In the second half of the book the author steps the reader through the actual audit process which addresses the areas of:

- identification of the control objectives
- preparation of the audit program
- preliminary data gathering
- performance of the actual audit field work
- preparation of the audit report

For each area, the author provides the reader with an overview and discussion of what should take place at each stage in the audit process. She also demonstrates how the auditee can assist so he or she can get the most out of the audit. This may include clarification of the auditor's understanding of the audit area or identification of additional concerns for the auditors to review.

The author has included in every chapter a section with recommendations to the auditee. The purpose of these are to encourage participation from the auditee to ensure that the audit report will provide a correct representation of the area and the concerns which need to be brought to the attention of senior management.

The book provides an excellent example of the use of COBIT for the preparation of the audit program as well as its summarization for status reporting. The author reinforces the information that is presented in the various sections of the book through the use of a case study which walks through some of the discussions that may take place during the course of an actual audit. This case also helps to demonstrate some of the issues, such as user availability and access requirements, that may be faced by auditees and auditors during the performance of the audit.

The book is easy to read and provides an excellent explanation of the audit process for people about to experience their first audit as well as being excellent for new auditors. The author deals with the topic in sufficient detail to provide an understanding of the background and processes of audit without overwhelming the reader. I would suggest passing on a copy of this book to any new auditors or auditees about to undergo their first audit.

Bob Darlington, CIA, CISA
is a senior audit specialist with Canadian Pacific Railway. He is currently the chairman of the Education Board for ISACA International and is vice-president of the Toronto Chapter. He has contributed to the 1999 and 2000 CISA Technical Information Manual, and participated in the CISA Job Analysis Study. He is also a member of the program committees for the 2000 CACS and 2000 International conferences.

Ordering information for this book can be found in the Bookstore.