Book Review

Reviewed by A. Krista Kivisild, CISA, CA, CPA, who has had a diverse career in audit while working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/regulatory auditing, value-for-money auditing and operational auditing. She has served as a volunteer instructor, training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; and has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter.

IT Auditing and Application Controls for Small and Mid-sized Enterprises:
Revenue, Expenditure, Inventory, Payroll, and More

Former US President John F. Kennedy said, "The Chinese use two brush strokes to write the word 'crisis.' One brush stroke stands for danger; the other for opportunity. In a crisis, be aware of the danger, but recognize the opportunity." Businesses recognize that they need to take advantage of opportunities to keep growing. And while risk is inevitable, some risk is too great a danger when compared to its associated opportunity, especially for small and midsized enterprises (SMEs) that need to take a more pragmatic approach to ensure they stay afloat in today's business environment. The risk associated with the IT environment and applications is particularly difficult to communicate to the business as many of the related concepts are not well understood by those outside of the technology realm. How can security professionals evaluate the magnitude of risk and communicate it appropriately to businesses so that they can factor this into their decision making?

IT Auditing and Application Controls for Small and Mid-sized Enterprises: Revenue, Expenditure, Inventory, Payroll, and More offers a practical approach to identify the risk associated with the SME IT environment and the likely applications and controls deployed in an SME. The book is written to help financial statement auditors understand this risk, which can also help IT auditors understand the appropriate language to use to communicate risk appropriately to the business so that it is understood.

The book is thorough and covers specific operational and financial statement risk to different cycles (e.g., revenue, expenditure, inventory, payroll) to help explain cycle risk, controls and the related application-level controls. It also covers the IT audit and controls that emerged from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Public Company Accounting Oversight Board

By Jason Wood, William Brown and Harry Howe

(PCAOB), and it overlays COSO with COBIT®. This is critical for those auditing IT or adhering to the US Sarbanes-Oxley Act of 2002 (SOX) to understand and be able to use. There is a section to discuss, evaluate and present IT audit deficiencies in language and terms that will facilitate a more useful discussion with management and financial statement auditors.

The book addresses spreadsheet and desktop tools, their risk and top exposures. Any auditor who has been working to ensure their company complies with SOX or similar legislation in other jurisdictions will have a significant interest in helping management understand risk and ensure the protection and reliability of sensitive spreadsheet information. The book concludes with a section to discuss key reports, report writing tools, and the related risk and exposures.

This book provides a practical approach to understanding the basics of IT audit and application controls. By using the language of businesses, it helps to bridge the communication gap between IT and management. This book is recommended to any professional new to IT audit or it can also be used as a reference book that covers the key basics required for SOX legislation compliance for anyone who is involved in conducting, reviewing or evaluating IT audit work. Only once enterprises understand risk and controls can they begin to evaluate opportunities and help businesses make better decisions.

EDITOR'S NOTE

IT Auditing and Application Controls for Small and Mid-sized Enterprises: Revenue, Expenditure, Inventory, Payroll, and More is available from the ISACA® Bookstore. For information, visit w*ww.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.
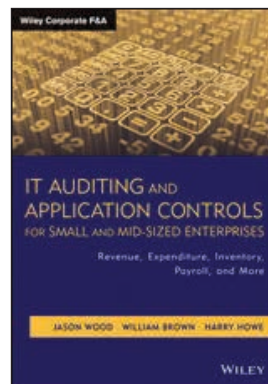
Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article: