

# Auditor's Risk Management Guide— Integrating Auditing and ERM

By Paul J. Sobel, CPA, CIA  
Reviewed by: Emani Sarathy, CISA



The recent growing list of bankruptcies, frauds and accounting irregularities is not only sending shockwaves through the equity and capital markets but also lessening the confidence in accountants and auditors. While legislation, boards, audit committees and auditing have been in place for a long time, there is an opportunity for auditing to evolve alongside leading-edge management practices and help restore confidence in the value addition that auditors can provide.

This book focuses on adjusting the audit approach to dwell largely on the risk management practices. It is a practical guide designed for the audit practitioner and is organized in two parts.

Part 1, Risk Management-based Auditing, provides:

- A broad understanding of corporate governance, ERM principles and different auditing approaches
- An outline of the approach for understanding the strategy and risks inherent in the business
- Step-by-step instructions on how to execute the risk management-based audit methodology

Part 2, Case Studies, provides nine detailed case studies illustrating the risk management-based audit methodology and tools in different audit scenarios.

Finally, a CD-ROM is included, which provides an electronic version of various work programs, checklists and other tools.

The book provides excellent assistance to audit practitioners in:

- Embedding strategy and objectives in the audit planning
- Including management's tolerance for risk in audit judgments, along with auditor's tolerance
- Increasing focus on how management measures and monitors performances
- Evaluating the organization's abilities to manage risks on an ongoing basis

The corporate management reader will attain deep insight into the role of ERM in corporate governance. The senior management reader will understand his/her own role while delegating authority to risk owners, keeping in mind the business risks and their tolerances.

Risk owners will be able to use this as a handbook in designing, implementing, measuring and monitoring risk management activities.

Using his vast experience, the author, currently the vice president of risk management at Aquilla Inc., Kansas City,

Missouri, USA, with more than 20 years of auditing experience, includes the following topics within this book:

- An overview of ERM, starting from basic meanings of risk and corporate governance through the ERM funnel
- The evolution of auditing approaches, including control-based, process-based, risk-based and risk management-based
- The integration of strategy into risk management-based auditing
- Aspects of risk assessment in detail at the business level along with quantification techniques
- Discussions on how to perform risk management-based audit through phases including objectives risk assessment, process design, testing, risk management infrastructure and action planning
- A number of real-life applications, case studies and illustrations to support the theory
- Exhibits at the end of every chapter that serve as checklists and quantitative analysis

The book is outstanding in the way it is organized and the extent of details it covers. It starts off with concepts related to ERM, then explains several audit approaches and finally builds the auditor's angle of auditing risk management activities. A funneling approach is used throughout, wherein the reader is guided from generalities to specifics. Sufficient diagrams, matrix, exhibits and best practices are included. A CD-ROM, which has electronic versions of all the work programs, checklists and other tools, is also supplied.

## Editor's Note:

*Auditor's Risk Management Guide—Integrating Auditing and ERM* is available now from the ISACA Bookstore. For information see the ISACA Bookstore Supplement in this *Journal*, visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore), e-mail [bookstore@isaca.org](mailto:bookstore@isaca.org) or telephone +1.847.253.1545, ext. 401.

## Emani Sarathy, CISA

is an independent consultant in software process, quality and audit. With an engineering degree in electronics and telecommunications and a post-graduate degree in industrial engineering, he has been serving the software industry for the last 20 years. Currently, he is working on an off-campus Ph.D. with the Birla Institute of Technology and Science, India, in the area of integrated software internal auditing.

*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.

© Copyright 2003 by *Information Systems Audit and Control Association* Inc., formerly the *EDP Auditors Association*. All rights reserved. ISCA™ *Information Systems Control Association*™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the *Information Systems Audit and Control Association* Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

[www.isaca.org](http://www.isaca.org)