

AUDITING THE RISK MANAGEMENT PROCESS

K.H. SPENCER PICKETT



WILEY

John Wiley & Sons, Inc.

AUDITING THE RISK MANAGEMENT PROCESS

AUDITING THE RISK MANAGEMENT PROCESS

K.H. SPENCER PICKETT



WILEY

John Wiley & Sons, Inc.

This publication includes extracts from AS/NZS 4360:2004 *Risk management*; HB 436-2004 *Risk management guidelines* and HB 158-2002 *A guide to the use of AS/NZS 4360 Risk management within the internal audit process*, all published by SAI Global Ltd, Sydney, Australia. www.riskinbusiness.com. Reprinted with permission.

Extracts from Committee of Sponsoring Organizations, *Enterprise Risk Management*, Summary and Framework, Spetember 2004, reprinted with permission from AICPA; Copyright © 2004 by The Committee of Sponsoring Organizations of the Treadway Commission.

This book is printed on acid-free paper. ∞

Copyright © 2005 by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights reserved.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, 201-748-6011, fax 201-748-6008.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Pickett, K.H. Spencer.

Auditing the risk management process / K.H. Spencer Pickett.

p. cm.

Includes index.

ISBN 0-471-69053-8 (cloth)

1. Auditing, Internal. 2. Risk management—Auditing. I. Title.

HF5668.25.P529 2005

658.15'11—dc22

2005000043

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ABOUT THE INSTITUTE OF INTERNAL AUDITORS

The Institute of Internal Auditors (IIA) is the primary international professional association, organized on a worldwide basis, dedicated to the promotion and development of the practice of internal auditing. The IIA is the recognized authority, chief educator, and acknowledged leader in standards, education, certification, and research for the profession worldwide. The Institute provides professional and executive development training, educational products, research studies, and guidance to more than 80,000 members in more than 100 countries. For additional information, visit the Web site at *www.theiia.org*.

*This book is dedicated
to the memory of Jenny Topham*

CONTENTS

<i>Preface</i>		xiii
<i>List of Abbreviations</i>		xv
Chapter 1	Why Risk Management?	1
	Introduction	1
	Risk Management Framework Model: Phase One	5
	Risk Management Framework Model: Phase Two	10
	Risk Management Framework Model: Phase Three	14
	Risk Management Framework Model: Phase Four	20
	Risk Management Framework Model: Final	25
	Summary	30
	Notes	30
Chapter 2	Determining Risk Management Maturity	33
	Introduction	33
	Risk Management Maturity Model: Phase One	35
	Risk Management Maturity Model: Phase Two	38
	Risk Management Maturity Model: Phase Three	45
	Risk Management Maturity Model: Phase Four	50
	Risk Management Maturity Model: Final	57
	Summary	64
	Notes	65
Chapter 3	Enterprise-Wide Risk Management	69
	Introduction	69
	Enterprise Risk Management Model: Phase One	70
	Enterprise Risk Management Model: Phase Two	73
	Enterprise Risk Management Model: Phase Three	79
	Enterprise Risk Management Model: Phase Four	80
	Enterprise Risk Management Model: Final	88

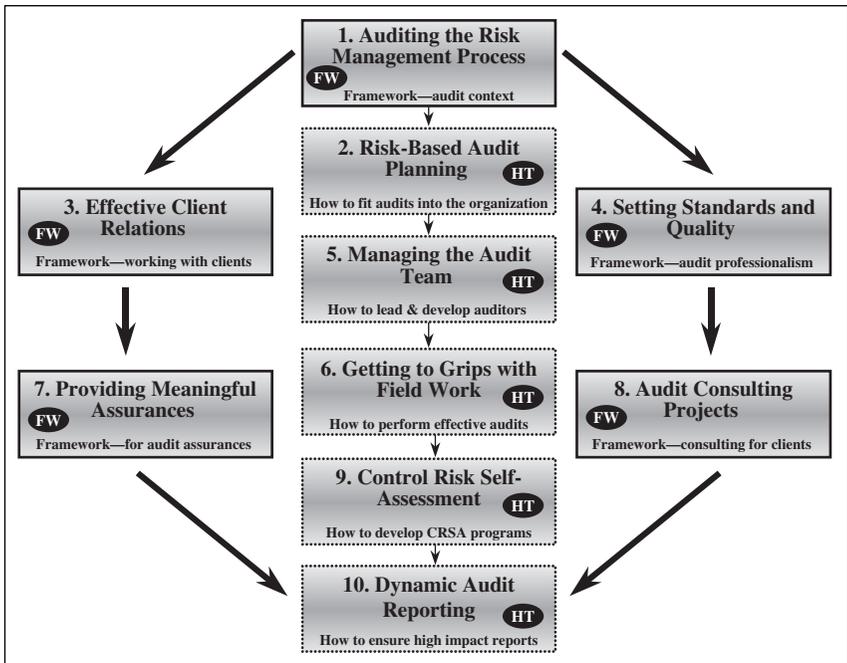
	Summary	95	
	Notes	95	
Chapter 4	Risk Appetite		97
	Introduction	97	
	Risk Appetite Model: Phase One	98	
	Risk Appetite Model: Phase Two	102	
	Risk Appetite Model: Phase Three	105	
	Risk Appetite Model: Phase Four	108	
	Risk Appetite Model: Final	110	
	Summary	114	
	Notes	115	
Chapter 5	Control Risk Self-Assessment		117
	Introduction	117	
	Control Risk Self-Assessment Model: Phase One	118	
	Control Risk Self-Assessment Model: Phase Two	122	
	Control Risk Self-Assessment Model: Phase Three	125	
	Control Risk Self-Assessment Model: Phase Four	129	
	Control Risk Self-Assessment Model: Final	136	
	Summary	139	
	Notes	140	
Chapter 6	Developing an Audit Approach		141
	Introduction	141	
	Audit Approach Model: Phase One	144	
	Audit Approach Model: Phase Two	150	
	Audit Approach Model: Phase Three	153	
	Audit Approach Model: Phase Four	162	
	Audit Approach Model: Final	165	
	Summary	172	
	Notes	173	
Chapter 7	The Illusion of Perfection		177
	Introduction	177	
	Poor Practice Model: Phase One	178	
	Poor Practice Model: Phase Two	184	

	Poor Practice Model: Phase Three	189
	Poor Practice Model: Phase Four	193
	Poor Practice Model: Final	196
	Summary	200
	Notes	200
Chapter 8	A Holistic ERM Concept	203
	Introduction	203
	ERM Program Model: Phase One	203
	ERM Program Model: Phase Two	207
	ERM Program Model: Phase Three	210
	ERM Program Model: Phase Four	215
	ERM Program Model: Final	219
	Summary	223
	Notes	223
<i>Appendix A</i>	<i>Applying an ERM Diagnostic Tool</i>	<i>225</i>
<i>Index</i>		<i>265</i>

PREFACE

Auditing New Horizons is a new series of short books aimed primarily at internal auditors, but which will also be useful to external auditors, compliance teams, financial controllers, consultants, and others involved in reviewing governance, risk, and control systems. Likewise, the books should be relevant to executives, managers, and staff as they are increasingly being asked to review their systems of internal control and ensure that there is a robust risk management process in place in all types of organizations. Each book provides a short account of important issues and concepts relevant to the audit and review community. The series will grow over the years and

Figure P.1 The Auditing New Horizon Book Series



John Wiley & Sons, Inc., is working alongside the Institute of Internal Auditors, Inc., to ensure that each new title reflects both current and emerging developments. The framework for Auditing New Horizons is illustrated in Figure P.1.

FrameWork (FW) books set out various models, supported by reference material that can be employed to ensure best practice pointers can be assessed for their impact on current practice. HowTo (HT) books use similar models but focus more on checklists and worked examples that can be employed to implementing aspects of relevant underlying frameworks. Each book is immersed in the Institute of Internal Auditor's Professional Practices Framework in terms of their published standards, advisories, and assorted guidance. Because the books are fairly succinct, reference to other sources will need to be limited. There are no detailed case studies taken from well-known companies in this book series because of the fast-changing pace of business, where current material quickly falls out of date. The books do, however, refer to many short examples of what happens in different organizations as a way of illustrating important points. The dynamic nature of the governance, risk, and control context means that some new book titles for the Auditing New Horizons series may change over the coming years. We hope that readers find the series both interesting and stimulating and that this series will provide a reference source that adds value to internal auditing, external auditing, and other review functions.

LIST OF ABBREVIATIONS

BASEL:	Committee on Banking Supervision
CAE:	Chief Audit Executive
CEO:	Chief Executive Officer
CFO:	Chief Finance Officer
COSO:	Committee of Sponsoring Organizations
CRO:	Chief Risk Officer
CRSA:	Control Risk Self-Assessment
CSA:	Control Self-Assessment
ERM:	Enterprise Risk Management
H&S:	Health and Safety
IIA:	Institute of Internal Auditors
IS:	Information Systems
IT:	Information Technology
KPI:	Key Performance Indicators
OECD:	Organization of Economic Cooperation and Development
PPF:	Professional Practices Framework
PR:	Public Relations
RA:	Risk Assessment
RI:	Risk Identification
RM:	Risk Management
RO:	Risk Owner
SEC:	Securities and Exchange Commission
SIC:	Statement on Internal Control

WHY RISK MANAGEMENT?

The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.

IIA Standard 2110

INTRODUCTION

Internal auditing has grown tremendously over the years to reflect its new high-profile position in most larger organizations. It has shifted from back-office checking teams to become an important corporate resource. The focus on professionalism and objectivity has driven the new-look auditor toward high-impact work that can really make a difference. The key development that has underpinned this change relates to the shift from enforcing controls on employees to using an assessment of risk to empower management and their staff to establish meaningful controls over their business. This move from must-do to want-to control cultures has allowed employees more scope to innovate and experiment.

Unfortunately, in the past, robust risk management processes have not always been in place. The rapid change programs of the 1980s and '90s meant that many organizations were likened to speeding trains that would leave behind anyone who was not bold enough to jump on board and hang on for dear life. Investors expected quick returns, while competition was about being the first to bring new or improved products to the marketplace—or at least give that impression. The resultant crashes and scandals that rebounded throughout the last decade underpinned the lack of clear direction or ethical values that could be described as the much-needed rail signals and brakes—to continue our train analogy.

Reckless trading against the backdrop of the cutthroat competition of the 1990s continued into 2000 and beyond, before the regulators started to get tough. The old governance models of a select board of high achievers

gathered around a powerful CEO, whose only accountability was to publish financial accounts that had been reviewed by a friendly auditor, could not cope with the new business dynamic. In this type of environment, regulations were seen as obstacles to be sidestepped. Corporate lawyers were often used to design roadmaps to allow the executive teams to weave a path through legal provisions and industry-specific regulations. Societal concerns came to a head in 2002, with the publication of the Sarbanes-Oxley Act, to enshrine personal responsibility at the top of each company to adhere to the rules and demonstrate that this is the case. The link between risk management and corporate governance has been explored by the Institute of Internal Auditors (IIA):

Risk management is a fundamental element of corporate governance. Management is responsible for establishing and operating the risk management framework on behalf of the board.¹

In the past, control frameworks have helped in setting standards, but they often acted as basic benchmarks to be checked off against and often ended up as just checks in the Compliance Box, something that is done and then filed away—until the same time next year. Nowadays, the new focus is firmly on risk—to the business, executives, and stakeholders. Several societal concerns appear at the forefront of this idea of risk, including the risks that:

- Published accounts are misleading.
- Performance information is fudged.
- Regulatory disclosures are not supported by sound evidence.
- Senior executives are making uninformed assertions about the adequacy of controls over financial reporting and compliance procedures.
- The corporate asset base is not properly protected from waste, loss, attack, or natural disaster.
- The corporate reputation militates against customer loyalty.
- Operations and processes are inefficient and inflexible.
- The wrong people are being promoted and recruited.
- The organization is failing to meet the changing expectations of customers, the marketplace, and stakeholders generally.

Attempts to address these issues have led organizations in the direction of Enterprise Risk Management (ERM). That is a wholesale approach to identifying and managing risk across all aspects of the business—from a strategic standpoint. As each risk changes in impact and urgency, so