

Cover image: © iStock.com/kentoh
Cover design: Wiley

Copyright © 2015 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
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, or online at www.wiley.com/go/permissions.

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 for 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 publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Graham, Lynford.

Internal control audit and compliance : documentation and testing under the new COSO framework / Lynford Graham.

1 online resource. -- (Wiley corporate F&A series)

Includes index.

Description based on print version record and CIP data provided by publisher; resource not viewed.

ISBN 978-1-118-99621-8 (cloth); ISBN 978-1-118-99647-8 (ebk);

ISBN 978-1-118-99630-0 (ebk) 1. Auditing, Internal. I. Title.

HF5668.25

657'.458—dc 3

2014035947

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Preface xi

Acknowledgments xv

Chapter 1: What We All Share	1
Need for Control Criteria	1
Overview of the COSO Internal Control Integrated Framework	2
Holistic, Integrated View	3
Revised COSO Internal Controls Framework	6
What We Must Do	8
Basic Scoping and Strategies for Maintenance	11
Where We Depart	12
Triangle of Efficiency	13
Controls versus Processes	14
The Debate Continues	18
Organization of This Book	18
Appendix 1A: COSO 17 Principles	20
Chapter 2: Setting the Scope of Your Documentation Project: Identifying the Core	21
Start with Business Objectives	21
After the Initial Year	24
Mapping the Entity to the Financial Statements: Ins and Outs	25
Consider Risks, Not Just Quantitative Measures	27
Inherent and Control Risk	28
Overstatement and Understatement	28
Does "In Scope" Imply Extensive Testing?	37
A Consolation	39
Be Careful Out There!	40
Appendix 2A: Summary of Scoping Inquiries	42

Chapter 3: The Risk Assessment Component	45		
Risk Assessment Principles in COSO	46		
Cost Control	46		
Basics	47		
Likelihood, Magnitude, Velocity, and Persistence	48		
Separate Assessments of Inherent and Control Risks	50		
Role of Assertions	51		
Assertions	52		
Principles 6 and 7: Specify Suitable Objectives; Identify and Analyze Risk	56		
Identifying Risks	59		
External Sources of Risk Information	60		
Internal and External Reporting Risks	61		
Compliance Risks	61		
Disclosed Material Weaknesses in Risk Assessment	62		
Principle 8: Assess Fraud Risk	62		
Auditor Responsibility to Detect Fraud	65		
Antifraud Controls for Management to Consider	66		
Ties to Other Principles and Components	66		
Principle 9: Identify and Assess Significant Change	66		
Gathering Information to Support the Risk Assessment and Consider Change	68		
Appendix 3A: SAS No. 99 Exhibit: Management Antifraud Programs and Controls	72		
Attachment 1: AICPA "CPA's Handbook of Fraud and Commercial Crime Prevention" Code of Conduct	87		
Attachment 2: Financial Executives International Code of Ethics Statement	91		
Appendix 3B: Understanding Fraud Risk Assessment	93		
Chapter 4: Control Environment	99		
Principle 1: Commitment to Integrity and Ethical Values	100		
Principle 2: Board of Directors (Governance) Demonstrates Independence from Management and Exercises Oversight of the Development and Performance of Internal Control	104		
Principle 3: Management Establishes, with Board Oversight, Structures, Reporting Lines, and Appropriate Authorities and Responsibilities in the Pursuit of Objectives	109		
		Principle 4: Commitment to Attract, Develop, and Retain Competent Individuals in Alignment with Objectives	110
		Principle 5: The Organization Holds Individuals Accountable for Their Internal Control Responsibilities in the Pursuit of Objectives	113
		Appendix 4A: Understanding and Awareness of Control Responsibilities	117
		Chapter 5: Control Activities	120
		Principle 10: Selects and Develops Control Activities to Mitigate Risk and Achieve Objectives	120
		Principle 11: Selects and Develops General Controls over Technology	132
		Principle 12: Deploys through Policies and Procedures	141
		Summing Up	143
		Appendix 5A: Linking Common Control Activities and Assertions	146
		Appendix 5B: Linkage of Principles to Controls, Policies, and Procedures	158
		Chapter 6: Information and Communication	165
		Principle 13: Generates Relevant Information	166
		Principle 14: Communicates Internally	168
		Principle 15: Communicates Externally	170
		Chapter 7: Monitoring	173
		Principle 16: Select, Develop, and Perform Ongoing and/or Separate Evaluations	174
		Principle 17: Evaluate and Communicate Deficiencies as Appropriate	176
		Chapter 8: Evidence and Testing	179
		Sufficient Evidence	179
		Gathering Information	187
		Testing and Sampling	194
		Nonsampling Situations	202
		Confusion of Sample Size Guidance in Practice Today	203
		Information Technology General Controls	204
		Testing Security and Access	205
		Appendix 8A: Sample Size Tutorial	211

Chapter 9: Developing Questionnaires and Conducting Interviews	217	Chapter 13: Illustrative Forms and Templates	337
Surveys of Employees	219	Historical Perspective	338
Conducting Interviews	224	2013 Framework Examples	340
Management Inquiries: Sample Questions	234	Appendix 13A: Information-Gathering Form—Principle Focused	348
Appendix 9A: Sample Practice Aids	239	Appendix 13B: Information Gathering Form—Revenue	350
Chapter 10: Assessing the Severity of Identified Controls Deficiencies	248	Appendix 13C: Walk-through Documentation Form	353
It's Inevitable	248	Appendix 13D: Information Technology General Controls Assessment Form	355
Alignment of Public and Private Company Standards for Assessing Deficiency Severity	251	Appendix 13E: Documentation of Financial Reporting Software and Spreadsheets	364
Control Deficiencies and Definitions	252	Appendix 13F: Sampling Form for Tests of Controls	368
Key Factors When Assessing the Severity of a Deficiency	263	Appendix 13G: Summary of Internal Control Deficiencies	371
Conditions Indicating Control Deficiencies	270	Appendix 13H: Control Environment Component Evaluation Summary	372
Examples of Evaluating the Severity of Deficiencies	277	Chapter 14: Summing Up	373
Overall Assessment	281	 	
Appendix 10A: A Framework for Evaluating Control Exceptions and Deficiencies	283	About the Author	375
Appendix 10B: Assessing the Potential Magnitude of a Control Deficiency	299	Index	377
Chapter 11: Reporting Requirements	302		
Nonpublic Entity Reporting	302		
Public Company Annual and Quarterly Reporting Requirements	304		
Reporting on Management's Responsibilities for Internal Control	309		
Required Company and Auditor Communications	312		
Reporting the Remediation of Weaknesses	314		
Coordinating with the Independent Auditors and Legal Counsel	315		
Appendix 11A: Illustrative AICPA Report on Internal Controls	316		
Chapter 12: Project Management and Tools Assessment Design	318		
Project Management	318		
Structuring the Project Team	319		
Tools Assessment Design	325		
Features of a Good Tools Solution	326		
Value of a Pilot Project	331		
Coordinating with the Independent Auditors	334		