



Nonprofit  
Risk Management  
Center

Find the answer here | [nonprofitrisk.org](http://nonprofitrisk.org)

# **World-Class Risk Management**

*for Nonprofits*

---

*By Norman Marks & Melanie Lockwood Herman*



# Nonprofit Risk Management Center

Find the answer here | [nonprofitrisk.org](http://nonprofitrisk.org)

The mission of the Nonprofit Risk Management Center is to inspire effective risk management and risk champions across the nonprofit sector. As a trusted advisor on a wide spectrum of risk topics, NRMC partners with mission-focused, high-performing nonprofit organizations to make risk management accessible and impactful. NRMC also develops and advocates innovative approaches to loss control and risk leadership. In addition to consulting services, NRMC develops innovative Web applications, provides in-person and virtual training, and publishes articles and books covering a spectrum of risk issues facing mission-driven organizations. These resources are offered to inspire the confidence needed to take the risks that bring nonprofit missions to life.

## **Nonprofit Risk Management Center**

204 South King Street  
Leesburg, VA 20175  
703.777.3504

## **Staff**

Erin Gloeckner, *Director of Consulting Services*  
Eric Henkel, *Project Manager*  
Melanie Lockwood Herman, *Executive Director*  
Kay Nakamura, *Director of Client Solutions*

ISBN-10: 1-893210-33-2

ISBN-13: 978-1-893210-33-2

Copyright © 2017 Nonprofit Risk Management Center. All rights reserved.

No part of this publication may be reproduced without permission from the Nonprofit Risk Management Center. To request permission to reproduce or share any content in this publication, write to: [info@nonprofitrisk.org](mailto:info@nonprofitrisk.org).

The content of this book expresses the views and opinions of the authors and the Nonprofit Risk Management Center. Nothing contained herein should be interpreted as legal advice, and readers are encouraged to seek legal counsel for answers to questions about specific legal matters and exposures. This book is offered as an educational and informational resource.

## About the Authors

**Norman Marks**, CPA, CRMA is a semi-retired chief audit executive and chief risk officer. He is a globally-recognized thought leader in the professions of risk management and internal auditing and remains an evangelist for “better run business,” focusing on corporate governance, risk management, internal audit, enterprise performance, and the value of information. He is also a mentor to individuals and organizations around the world.

Norman has been honored as a Fellow of the Open Compliance and Ethics Group and an Honorary Fellow of the Institute of Risk Management for his contributions to risk management.

He is the author of four earlier books:

- Auditing that Matters
- World-Class Internal Audit: Tales from My Journey
- Management’s Guide to Sarbanes-Oxley Section 404: Maximize Value Within Your Organization (described as “the best Sarbanes-Oxley 404 guide out there for management”), and
- How Good is your GRC? Twelve Questions to Guide Executives, Boards, and Practitioners.

Norman’s blogs can be found at [www.normanmarks.wordpress.com](http://www.normanmarks.wordpress.com) and <https://iaonline.theiia.org/blogs/marks>.

**Melanie Lockwood Herman**, Esq. is Executive Director of the Nonprofit Risk Management Center. She has held leadership positions in the nonprofit sector throughout her career. Melanie is the principal author of more than 20 books on various risk management topics and is the architect of NRMC’s popular web applications: *My Risk Management Plan*, *My Risk Management Policies* and *My Risk Assessment*. Melanie’s essays and articles on risk topics are published by NRMC in the *RISK eNews*, available at [www.nonprofitrisk.org/resources/e-news/](http://www.nonprofitrisk.org/resources/e-news/) and also in *Risk Management Essentials*, at [www.nonprofitrisk.org/resources/risk-management-essentials/](http://www.nonprofitrisk.org/resources/risk-management-essentials/).

Melanie earned a Bachelor of Arts in Urban Affairs from the American University (Washington, DC), and a Juris Doctor from George Mason University School of Law (Arlington, VA). She is a member of the District of Columbia Bar Association. Melanie currently serves on four national nonprofit boards (American Foundation for the Blind, Camp Fire, the National Human Services Assembly, and United Methodist Insurance). Melanie has been honored nine times as a member of *The NonProfit Times* “Power and Influence Top 50.” In the 2017 NPT list, Melanie was described as “One of the most prolific writers and lecturers on the topic of nonprofit risk.”

# Table of Contents

<b>FOREWORD BY GRANT PURDY</b> . . . . .	ix
<b>INTRODUCTION</b> . . . . .	xiii
What is World-Class Risk Management? . . . . .	xiii
The Language of Risk . . . . .	xix
Reflection Questions: World-Class Risk Management and the Language of Risk . . . . .	xx
<b>CHAPTER 1: WHY IS RISK MANAGEMENT IMPORTANT?</b> . . . . .	1
Defining Risk . . . . .	6
Reflection Questions: The Importance of Risk Management . . . . .	12
Suggested Individual or Team Activity . . . . .	12
<b>CHAPTER 2: EFFECTIVE RISK MANAGEMENT</b> . . . . .	13
The ISO 31000 Risk Management Principles . . . . .	14
Risk Management Principles Revisited . . . . .	24
Defining Risk Management: A New Approach . . . . .	27
Reflection Questions: Risk Management Principles . . . . .	31
Suggested Individual or Team Activity . . . . .	31
<b>CHAPTER 3: RISK MANAGEMENT MATURITY</b> . . . . .	33
Maturity Models . . . . .	33
Using the NRMC Model to Evaluate Risk Maturity . . . . .	44
Reflection Questions: Risk Management Maturity . . . . .	48
<b>CHAPTER 4: RISK MANAGEMENT IN THE NONPROFIT SECTOR</b> . . . . .	49
Inspiration for Effective Risk Management . . . . .	54
Reflection Questions: Inspiration for Our Focus on Risk Management . . . . .	59
<b>CHAPTER 5: RISK REPORTING</b> . . . . .	61
Heat Maps . . . . .	62
Risks to Objectives . . . . .	66
Integrating Risk and Performance . . . . .	67
World-Class Risk Reporting . . . . .	70
Reflection Questions: Risk Reporting . . . . .	74
Suggested Individual or Team Activity . . . . .	75

<b>CHAPTER 6: EMBEDDING RISK MANAGEMENT IN STRATEGY-SETTING</b> . . . . .	77
Understand the Assumptions Behind Strategies. . . . .	80
The Strategy-Setting Process . . . . .	81
Reflection Questions: Risk Management in Strategy Setting . . . . .	83
<b>CHAPTER 7: BAKING RISK MANAGEMENT INTO DECISION-MAKING PROCESSES</b> . . . . .	85
Decision-Making . . . . .	88
The Risk Management Process as a Decision-Making Tool . . . . .	91
Risk Beyond the Organization . . . . .	94
Suggested Individual or Team Activity . . . . .	95
<b>CHAPTER 8: RISK LEADERSHIP</b> . . . . .	97
Reflection Questions: Risk Leadership . . . . .	105
Suggested Individual or Team Activity . . . . .	106
<b>CHAPTER 9: RISK OVERSIGHT BY THE BOARD</b> . . . . .	107
What is Risk Oversight?. . . . .	108
The Board's Risk Agenda . . . . .	115
Board Risk Competence. . . . .	117
Board Risk Information . . . . .	118
Board Approval of Risk Levels. . . . .	120
Reflection Questions: Risk Oversight. . . . .	122
<b>CHAPTER 10: RISK-AWARE CULTURE</b> . . . . .	123
What is Risk Culture? . . . . .	124
Risk Management Framework. . . . .	132
Reflection Questions: Risk Culture . . . . .	134
<b>CHAPTER 11: RISK IDENTIFICATION AND MONITORING</b> . . . . .	135
Top-Down or Bottom-Up. . . . .	137
IT Risk. . . . .	138
Facilitated Workshops. . . . .	140
What Needs to Go Right?. . . . .	142
Continuous Risk Identification. . . . .	143
Reflection Questions: Risk Identification and Monitoring . . . . .	146
<b>CHAPTER 12: RISK ANALYSIS</b> . . . . .	147
The Risk Bow Tie Exercise: A First Step into Risk Analysis. . . . .	150
The Level of Risk. . . . .	154
Risk Models. . . . .	158
Multiple Potential Effects . . . . .	160
Reflection Questions: Risk Analysis. . . . .	163
Suggested Individual or Team Activity . . . . .	163

<b>CHAPTER 13: RISK EVALUATION, APPETITE, TOLERANCE, AND CRITERIA</b> . . . . .	169
Risk Evaluation . . . . .	169
Risk Appetite and Tolerance. . . . .	170
Risk Criteria. . . . .	179
Financial Stability Board Guidance. . . . .	179
Guidelines and Common Sense . . . . .	183
Risk Levels in a Dynamic World . . . . .	186
Reflection Questions: Risk Evaluation, Tolerance and Criteria . . . . .	187
<b>CHAPTER 14: RISK MONITORING.</b> . . . . .	189
Reflection Questions: Risk Monitoring. . . . .	194
Suggested Individual or Team Activity . . . . .	194
<b>CHAPTER 15: RISK RESPONSE</b> . . . . .	197
Insurance as Risk Response . . . . .	201
Risk Capacity. . . . .	201
Risk Sharing . . . . .	204
Internal Controls . . . . .	205
Reflection Questions: Risk Response . . . . .	206
<b>CHAPTER 16: RISK MANAGEMENT REPORTING</b> . . . . .	207
Technology for Risk Reporting and More . . . . .	210
Regulatory Reporting . . . . .	214
Reflection Questions: Risk Management Reporting. . . . .	215
<b>CHAPTER 17: BUILDING DURABLE RISK MANAGEMENT CAPABILITIES</b> . . . . .	217
Function with a Purpose . . . . .	218
Measure by Measure . . . . .	220
Small Team or Cast of Thousands. . . . .	221
Clarify Roles . . . . .	223
Risk Function Design Samples . . . . .	224
Step by Step . . . . .	227
Review, Learn, and Adapt . . . . .	229
Reflection Questions: Building Durable Risk Management Capabilities . . . . .	231

<b>CHAPTER 18: ASSESSING RISK MANAGEMENT RISK</b> . . . . .	233
Embrace and Embody Risk Management. . . . .	235
Human Bias . . . . .	235
Blindness to Reality . . . . .	238
The Fear of Taking Risk . . . . .	238
Fear of Retribution . . . . .	239
Changes in Risk Levels . . . . .	241
The Business Environment . . . . .	242
The Quality of Information . . . . .	243
Changes in Personnel . . . . .	244
The Ability to Adapt . . . . .	245
Finding the Time . . . . .	245
Decisions Made in Haste . . . . .	246
Deliberate Violations . . . . .	250
Failures of Internal Control . . . . .	250
Errors and Mistakes . . . . .	251
Reflection Questions: Assessing Risk Management Risk . . . . .	252
<b>CHAPTER 19: WORLD-CLASS RISK MANAGEMENT</b> . . . . .	253
Achieving World-Class Risk Management . . . . .	258
<b>EPILOGUE BY ERIN GLOECKNER</b> . . . . .	261
<b>APPENDIX A: EXAMPLE OF A RISK MANAGEMENT POLICY</b> . . . . .	265
<b>APPENDIX B: EXAMPLE OF A RISK MANAGEMENT POLICY – BHP BILLITON</b> . . . . .	267
<b>APPENDIX C: EXAMPLE OF A RISK MANAGEMENT POLICY – CQUNIVERSITY</b> . . . . .	269
<b>APPENDIX D: SAMPLE NONPROFIT AUDIT AND RISK OVERSIGHT COMMITTEE CHARTER</b> . . . . .	275
<b>APPENDIX E: SAMPLE NONPROFIT AUDIT AND RISK OVERSIGHT COMMITTEE CHARTER</b> . . . . .	279