THE INTERNAL AUDITOR’S GUIDE TO
RISK ASSESSMENT

2nd Edition

RICK A. WRIGHT JR., CIA

INTERNAL AUDIT FOUNDATION
To Lynn... ILYTM.
Contents

Acknowledgments ......................................................... xiii
About the Author .......................................................... xv
Introduction ................................................................. 1

Section 1: Understanding the Nature of Risk

Chapter 1: Defining Risk .................................................. 9
Chapter 2: Risk Categories ............................................... 13
Chapter 3: Risk Characteristics ......................................... 23
Chapter 4: The Influence of Change on Risk ....................... 29

Section 2: Choosing the Best Risk Assessment Approach for Your Organization

Chapter 5: IIA Standards for Risk ....................................... 37
Chapter 6: Risk Assessment Best Practices and Emerging Ideas 39
Chapter 7: Adapting Your Risk Assessment Approach to Your Organization .... 45

Section 3: Techniques for Conducting Your Organization’s Risk Assessment

Chapter 8: Creating and Validating the Audit Universe .......... 51
Chapter 9: Understanding Organizational Objectives ............ 59
Chapter 10: Identifying Risks, Part 1—Using Risk Factors ....... 65
Chapter 11: Identifying Risks, Part 2—Using Specific Risks ............................... 73
Chapter 12: Common Mistakes to Avoid When Identifying Risks ..................... 81
Chapter 13: Risk Measurement, Part 1—Impact and Likelihood ......................... 85
Chapter 14: Risk Measurement, Part 2—Risk Factors versus Specific Risks .... 97
Chapter 15: Risk Prioritization ................................................................. 105
Chapter 16: Risk Assessment Frequency ................................................... 111
Chapter 17: Engagement Risk Assessment .................................................. 115

Section 4: Identifying Risk Appetite and Solving Common Challenges
Chapter 18: Defining Risk Appetite ............................................................ 123
Chapter 19: Integrating Organizational Risk Philosophy with Risk Assessment .... 127
Chapter 20: Solutions to Implementation Challenges ..................................... 133
Chapter 21: Summary and Conclusion ....................................................... 139

The Risk Assessment Toolkit—An Overview ............................................. 143
Notes ........................................................................................................ 147
Glossary ..................................................................................................... 149

Internal Audit Foundation Sponsor Recognition ......................................... 153
Internal Audit Foundation Board of Trustees .............................................. 155
Internal Audit Foundation Committee of Research and Education Advisors .... 157
<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>Too-Negative Risk Mindset</td>
<td>10</td>
</tr>
<tr>
<td>Figure 1.2</td>
<td>Too-Positive Risk Mindset</td>
<td>10</td>
</tr>
<tr>
<td>Figure 1.3</td>
<td>Balanced Risk Mindset</td>
<td>11</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Inherent Risk versus Residual Risk</td>
<td>24</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>Interrelationships of Internal and External Risk Drivers</td>
<td>26</td>
</tr>
<tr>
<td>Figure 5.1</td>
<td>IIA Standard 2010 – Planning</td>
<td>38</td>
</tr>
<tr>
<td>Figure 9.1</td>
<td>The Risk Assessment Process</td>
<td>59</td>
</tr>
<tr>
<td>Figure 10.1</td>
<td>Example of a Defined Risk Factor</td>
<td>69</td>
</tr>
<tr>
<td>Figure 12.1</td>
<td>The Risk Assessment Process</td>
<td>83</td>
</tr>
<tr>
<td>Figure 13.1</td>
<td>Risk Heat Map</td>
<td>88</td>
</tr>
<tr>
<td>Figure 13.2</td>
<td>Risk Heat Map Scoring Matrix (Numeric Scale)</td>
<td>89</td>
</tr>
<tr>
<td>Figure 13.3</td>
<td>Risk Heat Map with Classifications (High, Moderate, Low)</td>
<td>90</td>
</tr>
<tr>
<td>Figure 14.1</td>
<td>Assigning Risk Scores to Specific Risks (Numeric Scale)</td>
<td>100</td>
</tr>
<tr>
<td>Figure 14.2</td>
<td>Assigning Risk Scores to Specific Risks (High-Moderate-Low)</td>
<td>101</td>
</tr>
<tr>
<td>Figure 14.3</td>
<td>Assigning Risk Scores to Specific Risks (Average Impact/Likelihood)</td>
<td>102</td>
</tr>
<tr>
<td>Figure 19.1</td>
<td>Including Risk Philosophy as a Risk Factor in the Audit Universe</td>
<td>129</td>
</tr>
<tr>
<td>Figure 19.2</td>
<td>Rating Scale for Management’s Awareness of Risk Philosophy</td>
<td>129</td>
</tr>
<tr>
<td>Figure 19.3</td>
<td>Using Risk-Taking Maturity as a Weighted Component of an Organization’s Risk Score</td>
<td>130</td>
</tr>
<tr>
<td>Figure 19.4</td>
<td>Rating Scale for an Organization’s Risk-Taking Maturity</td>
<td>131</td>
</tr>
<tr>
<td>Figure 19.5</td>
<td>Using Risk Philosophy as an Audit Objective in Risk Engagements</td>
<td>132</td>
</tr>
</tbody>
</table>
Tables

Table 2.1: Components and Outcomes of Operational Activity ......................... 17
Table 9.1: Specific Risk Identification Template (with business objective examples) .................................................. 63
Table 10.1: Examples of Risk Factors Placed in Risk Categories ....................... 68
Table 10.2: Audit Universe Risk Identification Using Risk Factors .................... 70
Table 11.1: Specific Risk Identification Template (with business objective and risk examples) ................................................. 76
Table 12.1: Example of the Difference Between Risk and Consequence .............. 82
Table 12.2: Example of Poor Risk Identification (focusing on controls instead of business objectives) ........................................ 82
Table 13.1: Heat Map Scoring Weighted Toward Impact .................................. 89
Table 13.2: Example of Criteria for Measuring Impact .................................... 92
Table 13.3: Example of Criteria for Measuring Likelihood ............................... 94
Table 14.1: Using Risk Factors to Measure Impact and Likelihood ................... 98
Table 15.1: Absolute Ranking ........................................................................ 106
Table 15.2: Relative Ranking ......................................................................... 107
Table 15.3: Prioritization Risk Factors (Embedded) ....................................... 109
Table 15.4: Prioritization Risk Factors (Isolated) ........................................... 110
Table 17.1: Risk Rating Using High, Moderate, Low ....................................... 117
Table 17.2: Risk Rating on a Scale of 1 to 3 .................................................. 117
Table 17.3: Risk Rating on a Scale of 1 to 5 .................................................. 118
Table 17.4: Risk and Control Matrix Example .............................................. 118
Table 18.1: Risk Appetite Defined as a Maximum Amount ............................... 124
Table 18.2: Risk Appetite Defined as Willingness to Take Risks ........................ 125
Acknowledgments

Many individuals contributed to the original writing and subsequent update of this book. I must first thank my wife, Lynn, for her many hours of parenting our four sons—alone—and providing an environment where I could focus on writing. She is an angel, and I am greatly blessed to have her as my life partner. I love you, Sweetheart!

Other people whom I consider mentors and friends helped with various tasks, including reviewing draft manuscripts and providing tools for the online toolkit that accompanies the book. I am indebted to the following individuals:

- Karen Begelfer, Chief Audit Executive, Sprint
- Steve Brown, Chief Audit Executive, PRGX Global
- Allen Engel, Senior Audit Manager, Farmers Insurance
- Lynn Fountain, Business/Risk Consultant, Trainer, and Author
- Nancy Frazee, Principal, nVision Risk
- Pamela Stroebel Powers, Owner/Managing Member, Powers CPA
- Kellie Schull, Engagement Manager, Comcast
- Doug Von Feldt, Innovation and Continuous Improvement Leader, Crimson Corporation

I would be remiss if I didn’t also thank staff at The IIA and the Internal Audit Foundation. Two individuals, Deborah Pouallion and Candace Sacher, were especially instrumental in bringing this book to fruition. Deborah was the lead content editor for the original writing of this book and a tremendous mentor to me. She helped guide me through the nuances of the editing process and taught me many new lessons about writing and publishing. Candace was the project manager for the second edition update and kept me on task while coordinating with reviewers and other editing staff. Finally, members of the Foundation’s Committee of Research and Education Advisors (CREA) also provided great support by offering candid feedback that has greatly enhanced the value of the final product.
About the Author

Rick A. Wright Jr., CIA, is director of internal audit and enterprise risk management for YRC Worldwide. He has more than 20 years of experience in internal audit practice and training. His career has included roles with various organizations, including The Institute of Internal Auditors (IIA), Kansas City Southern Railway, H&R Block, and Resources Global Professionals. He has been an adjunct professor teaching accounting, finance, fraud, and strategic management courses. He is also founder of Resonate Training and Assurance Services, LLC, where he continues to pursue his passion for adult learning as an author, speaker, and training facilitator.

Wright is an active member of The IIA’s Kansas City Chapter. He holds a bachelor of science in accounting from Missouri State University and an MBA from DeVry University’s Keller Graduate School of Management.
Section 1: Understanding the Nature of Risk
Defining Risk

What do you think of when you hear the word risk? Perhaps you immediately associate negative connotations with the word. Or perhaps you have dabbled in the investment world and reward comes to mind. Do you think something bad is about to happen? Or do you see an opportunity to achieve something better than the current state? Maybe you have a different take on the word risk altogether. Regardless, your perception toward risk and your understanding of its meaning will dictate consciously or subconsciously certain aspects of your approach to risk assessment.

Creating a Balanced Risk Mindset

It is important that your mindset toward risk is properly calibrated. If it is too heavily weighted toward the negative consequences, the results will likely overestimate the impact and likelihood of risk factors and position you as narrow minded and lacking in vision in the minds of your stakeholders (see figure 1.1). If you lean too far in the other direction and are too tolerant of risk, your perception of risk will not align with the organization and you may fail to identify potentially significant negative consequences (see figure 1.2). Either way, you are likely to be seen as either incompetent or lacking in credibility to some degree if your risk mindset is not balanced in regard to positive opportunities and negative threats (see figure 1.3). Both will constrain your ability to create value for your organization.

Everyone intuitively knows that risk itself is neither good nor bad. It presents both opportunities and consequences or threats, but people often tend to focus first on the negative aspects. Organizations must take some risk to grow and stay healthy—sometimes even to survive. As auditors, we must have an appropriate view of the nature of risk, know what it means to an organization, and recognize that it rightfully exists. This is essential to effective risk assessment. It could be stated that the primary role of management is to invest assets (put them at risk) to achieve objectives. Risk is useful to an organization; therefore, the goal should be to optimize risk, not eliminate it.
Figure 1.1. Too-Negative Risk Mindset
*Source:* Author’s creation.

Figure 1.2. Too-Positive Risk Mindset
*Source:* Author’s creation.
Risk Definitions

Risk has many interpretations that are influenced by the lens in which it is examined. The IIA defines risk as “the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.” Another similar definition of risk comes from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO’s *Enterprise Risk Management - Integrating with Strategy and Performance* defines risk as “the possibility that events will occur and affect the achievement of strategy and business objectives.”

There are a couple of points I want to make about the definition of risk that internal auditors choose. First, the definitions listed above present risk in the context of uncertainty and consequences, but they do not depict it in terms of negative outcomes. Second, any relevant definition of risk must address the relationship between risk and organizational objectives. The identification and prioritization of risk—two key components of the risk assessment process—are inextricably linked with organizational objectives. I prefer a slightly modified version of The IIA’s definition of risk:

**Risk**—The possibility of an event or condition occurring that will have an impact on the ability of an organization to achieve its objectives.

This definition is simple and free of internal audit lingo, making it a business-friendly definition useful for dialogue with any audit client. In addition, it highlights the uncertain nature of risk, which is essential to recognize. Finally, this definition differentiates between “events”...
(e.g., natural disasters), which may be one-time, finite occurrences, and “conditions” (e.g., a dangerous work environment such as a mining operation), which may be ongoing and inherent to certain organizations.

Now that the definition of risk is established, let’s look at risk categories as a framework for identifying and analyzing different types of risks in your organization.