ENTERPRISE RISK MANAGEMENT BEST PRACTICES
From Assessment to Ongoing Compliance

ANNE M. MARCHETTI
Enterprise
Risk Management
Best Practices
FOUND IN 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Asia, and Australia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers’ professional and personal knowledge and understanding.

The Wiley Corporate F&A series provides information, tools, and insights to corporate professionals responsible for issues affecting the profitability of their company, from accounting and finance to internal controls and performance management.
To my parents, Jim and Barbara Marchetti,
to whom I owe all my love and gratitude.
## Contents

**Preface**  xi

**Chapter 1: Overview of Enterprise Risk Management**  1

- ERM Introduction 1
- Guidance: History and Relationship 3
- Organization View 5
- ERM Today 7
- Increased Pressure to Manage Risk 9
- Additional Evidence 10
- Perceived Barriers to Risk Management 11
- Building the Business Case for ERM: Value and Benefits 11
- Keys to Success 13
- Summary 15
- Notes 16

**Chapter 2: Corporate Governance and Roles and Responsibilities**  17

- Board Behavior 18
- Corporate Culture 19
- Roles and Responsibilities 20
- Summary 23

**Chapter 3: ERM Defined**  25

- Definitions and Concepts 28
- Risk Categories 30
- Internal Environment 31
- Summary 34
- Note 34
# Contents

## Chapter 4: The ERM Process: Step by Step 35
- Step 1: Strategy and Objective Definition 36
- Step 2: Event Identification 38
- Step 3: Risk Assessment 40
- Step 4: Risk Response 41
- Step 5: Communication 45
- Step 6: Monitoring 46
- Oversight 47
- Summary 47
- Notes 48

## Chapter 5: COSO Framework and Financial Controls 49
- Focus on Financial Controls 49
- Control Environment 52
- Integrity and Ethical Values 53
- Board of Directors 55
- Management’s Philosophy and Operating Style 57
- Organizational Structure 57
- Financial Reporting Competencies 58
- Authority and Responsibility 59
- Human Resources 60
- Summary 61
- Notes 62

## Appendix 5A: Excerpt from a Code of Ethics Policy 63
- Our Guiding Principles and Values 64
- Conflicts of Interest 64
- Confidential Information; Intellectual Property 65

## Appendix 5B: Whistleblower Program 67
- Reports Regarding Accounting Matters 67
- Investigation of Suspected Violations 68
- Discipline for Violations 68

## Appendix 5C: Approval Policy and Procedures 69
- Policy 69
- Purpose 69
- Scope 69
- Approvals/Documentation 70
Chapter 6: Financial Controls and Risk Assessment 74

- Risk Assessment 74
- Financial Reporting Objectives 75
- Financial Reporting Risks 76
- Fraud Risk 77
- Entity-Level Controls 83
- Example: Risk Assessment and Financial Controls 84
- Evaluating Deficiencies 86
- Summary 87
- Notes 87

Appendix 6A: Entity-Level Control Assessment 88

- Control Assessment Overview 88
- Control Environment 90
- Overall Evaluation of Control Environment 95
- Risk Assessment 96
- Overall Evaluation of Risk Assessment 98
- Control Activities 99
- Overall Evaluation of Control Activities 100
- Information and Communication 101
- Overall Evaluation of Information and Communication 104
- Monitoring 105
- Overall Evaluation of Monitoring 108
- Summary Assessment 109
- Overall Assessment of Internal Controls 110

Appendix 6B: Accounts Payable: Preliminary Controls Assessment Questionnaire 111

- Purchasing Controls Questionnaire 111
- Internal Control Assessment 112

Appendix 6C: Fraud Risk Factors: AU Section 316 114

- Risk Factors Relating to Misstatements Arising from Fraudulent Financial Reporting 114

Chapter 7: Ongoing Compliance Overview 120

- Origin of the Sarbanes-Oxley Act 120
- Generating Value from Compliance 121
- Moving Beyond Initial Compliance 123
Reevaluating the Compliance Program 125
Summary 131

Chapter 8: Ongoing Compliance Challenges 132
Future State Opportunity: Compliance Optimization 133
Issues to Consider When Optimizing Compliance 136
Ongoing Compliance Plan 138
Role of Internal Audit: Balancing the Compliance and
Audit Functions 143
Evolving Role of the Audit Committee 145
Summary 148

Chapter 9: Addressing Compliance and Risk Management Challenges through Automation 149
Software Can Add Value Beyond Compliance 151
Monitoring Software 152
Utilization of Continuous Monitoring: Control Testing and Control Automation 153
Benefits of Continuous Monitoring 154
Continuous Monitoring Tool Considerations 155
Continuous Monitoring Process 155
Risk Management Software 157
Unifying Financial Statements, Close Tasks, and SOX Controls 159
Determining the Right Solution 159
Summary 161
Note 161

Chapter 10: Ongoing Compliance and IFRS 162
International Financial Reporting Standards 162
Communicating the Impact 164
Preparing for IFRS 166
Comprehensive IFRS Transition Approach 167
Key Elements of an Effective IFRS Implementation 170
Summary 172

About the Author 173

Index 175
ANY ORGANIZATIONS STRUGGLE with the development and implementation of an enterprise risk management (ERM) program. Most are overwhelmed by the task. They believe they do not possess the expertise, resources, time, and/or dollars required to effectively design and build an effective risk management program. In addition, there is minimal perceived value in this activity.

My objective for this book is to demystify ERM and the risk management process in order to eliminate implementation apprehension. The goal is to simplify the explanation of related concepts and provide guidance that demonstrates a practical, cost-effective process that can be utilized by any organization.

The material addresses the development of programs in two major areas: ERM and ongoing compliance. Chapters 1 through 3 provide an introduction and overview of ERM including important components of the process as well as a corporate governance/organizational framework and definitions of roles and responsibilities.

Chapter 4 provides a detailed description of the ERM process and includes suggestions regarding implementation. Chapters 5 and 6 present an in-depth review of financial controls, including an example of the application of the risk assessment process relative to this risk category.

Chapters 7 through 10 address ongoing compliance challenges and provide insight into cost minimization and control optimization including the effective use of technology as well as future International Financial Reporting Standards considerations and implications.

It is my hope that this consolidation of information will be a useful guide through the risk management process. In addition, it is my intention to provide explanations and the basis for a solid understanding of critical components of an effective ERM program that will assist with strategy execution and achievement of overall entity objectives.
Overview of Enterprise Risk Management

ERM INTRODUCTION

Enterprise risk management (ERM) includes the methods and processes used by organizations to minimize surprises and seize opportunities related to the achievement of their objectives.

ERM is an approach to aligning strategy, process, and knowledge in order to curtail surprises and losses as well as to capitalize on business opportunities. Many individuals associate risk with negative outcomes. However, there is a potential value component to risk assessment and management. Risk management is about balancing risk and reward. A well-designed risk management program encourages and allows an organization to take intelligent risks. It involves assessing quantitative factors and information as well as considering management experience and judgment. An effective risk management program entails balancing people and processes. Ultimately, an entity’s risk profile
is affected by the actions and decisions of its board of directors, management, and employees.

One cannot talk about risk management without discussing risk assessment. The vast majority of organizations conduct some type of informal risk assessment process. As a result, these organizations have some form of risk management plan. This plan, in most cases, is not documented.

Initial introduction of formal risk assessment and risk management within an organization is critical to the ultimate success of the initiative. An entity must consider its culture and develop an approach that is most likely to result in success. The organization should take care not to overcomplicate or overwhelm individuals with technical terminology. Initial discussions should focus on the importance and the benefits of risk management. Employees should be encouraged to think and talk about the business and what could go wrong that might result in failure to achieve entity objectives and, as a result, have a negative effect on performance and/or perception.

Good risk management is essentially choice management. It is a continuous work in progress. An entity must identify risks and subsequently determine how it will address each one. The organization must decide the degree of risk it is willing to assume and address other identified risks, likely through mitigation. It is important to consider both tangible consequences, such as loss of revenue or drop in stock price, as well as intangible possibilities, such as public perception. Perception often is a major consideration in assessing positive or negative consequences. Organizations often evaluate risks in somewhat of a siloed process—considering the risk consequence to a single area of the business. Risks are inherently dynamic and interdependent. Consequences of unforeseen or unpredictable events typically affect multiple areas of a business. Therefore, aggregate entity consequences should be considered when conducting a risk assessment and designing a risk management program. Risks should not be separated into components and managed independently. Such an approach is rarely effective or successful. A holistic view of risk should be taken, including the contemplation of interdependencies.

Every organization is faced with uncertainty and risk. The challenge for management is to determine how much uncertainty to accept as it strives to improve stakeholder value.

Risk identification is a process designed to identify first both the strategic objectives and goals and then the potential internal and external events that can adversely affect the enterprise’s ability to achieve those objectives and goals.
Each entity should strive to build an integrated risk organization. This would include three components: (1) centralized risk management reporting to the chief executive officer and the board of directors, (2) an integrated risk management strategy that takes a holistic view of all types of risk within the organization, and (3) integration of risk management into business processes.

It is not easy to accomplish these stated objectives. The method and processes for execution may vary significantly based on the size, structure, and culture of the organization. Each company must determine the most practical method of implementation. However, this integrated approach will allow risk management to become an offensive weapon for management rather than the more common defensive reaction to incident occurrence.

Organizations should take a proactive approach to optimizing their risk profiles. Minimal investment in risk assessment and subsequent risk management program development and implementation can improve efficiency and reduce losses.

**GUIDANCE: HISTORY AND RELATIONSHIP**

Due to the heightened scrutiny and concentration on risk and risk management, there is a great deal of guidance available. Prior to exploring ERM design and implementation details, it is beneficial to examine various frameworks and standards. There will be extensive reference to these guidance documents in this book. The frameworks and standards discussed here are not the only sources of information available. The publications presented are commonly referenced and have been suggested for use by many industry-specific organizations. Some of the guidance, by nature of the issuer, is intended primarily for auditor use; some is directed to management. Certain publications provide broad advice regarding risk management; other documents specifically concentrate on risks and controls over financial reporting. However, examination of all of the recommendations, regardless of the source or intended audience, is valuable when undertaking a risk management initiative.

In 1992, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission first issued a conceptual framework entitled *Internal Control—Integrated Framework*. COSO originally was charged with studying and reporting on factors that can lead to fraudulent financial reporting. The COSO Framework was intended for broad use by any organization, and it provides evaluation tools that can be utilized for comprehensive evaluation of control
systems. This is evidenced in the general nature of the COSO definition of internal control:

A process, affected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Subsequently, with the passage of the Sarbanes-Oxley Act (SOX) in 2002, the Securities and Exchange Commission (SEC) suggested management use of the COSO Framework specifically for the design, build, and/or analysis of internal control over financial reporting. Details of the components of the COSO Framework and its use in the risk management and risk assessment process are presented in Chapters 5 and 6.

SOX established the Public Company Accounting Oversight Board (PCAOB), a private, nonprofit corporation whose mission is to oversee the auditors of public companies. To date, the PCAOB has issued five auditing standards (ASs); the most recent is AS No. 5, An Audit of Internal Control over Financial Reporting that Is Integrated with an Audit of Financial Statements. This standard directs auditors to adopt a top-down risk-based approach to internal control and compliance during the audit process. It points auditors toward initial review of entity-level controls and emphasizes the significance of strength at this level. In addition, the standard reinforces the importance of auditor focus on high-risk areas and situations and provides auditor guidance regarding the confirmation of risk mitigation in those identified areas.

In 2004, COSO published the ERM—Integrated Framework. It was issued to assist organizations to identify, assess, and manage risk effectively. The document establishes key risk management principles, concepts, language, and guidance with a goal of aiding an entity in formally establishing or improving its risk management. Details of the components of the Integrated Framework and its use in the risk management and risk assessment process are presented in Chapter 4.

The Auditing Standards Board has issued several Statement of Auditing Standards (SASs), commonly referred to as the Risk Assessment SASs (SAS 104–111), that outline auditor requirements, including documentation specifically associated with risk assessment. This guidance includes auditor requirements
for understanding and documenting management’s risk assessment process as well as documentation of the auditor’s own risk assessment process as part of audit planning.

All of the standards and frameworks contain detailed guidance that is valuable to an entity when designing, building, and/or analyzing its internal control and risk management program. The remainder of the text refers to these documents extensively because of their definitions, concepts, and advice. Risk management involves risk assessment, which results in risk mitigation, which occurs through the existence or implementation of control activities. All of these are interrelated and defined as well as referenced in one or more of the documents mentioned.

**Organization View**

Figure 1.1 illustrates an organization view of risk management and its role and relationship to overall corporate governance and compliance. Each entity should seek to build its organizational structure to support a top-down approach that begins with consideration of overall corporate governance, progresses to risk management and assessment, and ultimately considers the achievement of all compliance requirements. SOX Section 404 compliance requirements created an inverted pyramid effect. Many organizations focus primarily on compliance and secondarily on risk management and governance. More recently, there has been emphasis from governing bodies, guidance, and standards regarding the appropriate top-down focus and process. Thus, entity attention has shifted in this direction.

Executive management in tandem with the board of directors should develop and document a strategy that outlines what the organization expects to accomplish—its goals—as well as the objectives it must achieve in order to realize the desired results. When determining a strategy, the board of directors and senior management may ask: How are we going to create value for our stakeholders? The answers manifest themselves in a strategic plan and associated objectives. A clearly documented strategy and associated objectives are critical to the development of an effective ERM program. An outline in these areas allows the organization to focus on opportunities presented in the strategic plan as well as to minimize the potential impact of threats. From a practical prospective, this may be a single-page document that outlines organization goals in terms of areas such as the customer, financial expectations, and products/services. The strategic plan, at the highest level, will aid in the
facilitation of all future discussions regarding risk and risk mitigation. The organization should consider the strategy from a financial and an operational perspective. The absence of a documented strategy and objectives, including related policies and job descriptions that outline overall expectations and define roles and responsibilities, significantly impairs an entity’s ability to design and implement an effective ERM program.

Once the entity has documented and can articulate its strategy and related objectives, it can then develop and implement an ERM program. Doing this includes performance of a risk assessment, which includes considering what could go wrong that might prohibit the entity from achieving its objectives. Therefore, it is extremely difficult, if not impossible, to execute this process effectively if the strategy and objectives are not defined initially.

Part of the risk assessment process should include consideration of entity compliance with all applicable laws and regulations.