AUDITING THE RISK MANAGEMENT PROCESS
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

Preface xiii
List of Abbreviations 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
Chapter 4  Risk Appetite

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

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

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

Introduction 177
Poor Practice Model: Phase One 178
Poor Practice Model: Phase Two 184
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

Appendix A  Applying an ERM Diagnostic Tool  225

Index  265
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
does the organization respond to ensure that any damage is limited and opportunities are exploited through using gaps in the market thrown up by new risks. In fact, the main feature of a successful enterprise is its ability to anticipate and deal with global risks more efficiently than other similar organizations. In this scenario where the stakes are so high, the role that is carved out by the internal auditor becomes all the more important. If ERM is to be a key driver for success, the various parties that affect the ERM framework that is built to address risk across the business become a fundamental concern. Where each party has a clear role, there is a need to discharge the precise responsibilities of each of these roles. Any shortfalls may lead to problems. The choices made by the Chief Audit Executive, in the context of the audit approach to ERM, are likewise important, and nothing should be left to chance.

If organizations faced no risk, there would be no need to employ internal audit staff. The organization would always be in complete control, and there would be no need to review, adjust, realign, or even implement internal controls. The auditor exists because plans do not always go as intended, and things don’t always appear as they really are. The auditor is needed to ensure that the organization understands its risks and has taken steps to both handle foreseeable problems and seize potential advantages. Advising, helping, cajoling, and issuing warnings are all tools that may be employed by the auditor to put risk on the agenda and ensure that it is given proper consideration. This combination of effort to achieve a risk-smart workforce means that the auditor is fast becoming what some now refer to as a critical friend to executives, management, and employees generally.

Before we launch our first model, we need to outline the formal definition of internal auditing from the IIA:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.2

As is clear from this definition, internal auditing is firmly rooted in the risk management, control, and governance agenda. Dave Richards, President of the IIA, presented at the IIA’s Enterprise Risk Management and Control Self-Assessment* Conference in Las Vegas, Nevada, on September 9, 2004, which is reported as follows:

*Control Risk Self-Assessment (CRSA) is also called Control Self-Assessment (CSA); the two terms are interchangeable.
Richards highlighted key ERM and CSA trends, including legislative movements around the world emphasizing the need for risk management as well as signs that internal auditors are becoming more proactive in the use of risk-assessment processes. Although CSA has not been fully embedded in many organizations, he said ERM is becoming known as a key ingredient to good governance, and internal auditors should promote its adoption and progression. In Richards’ closing comments he encouraged the audience by saying, “It couldn’t be a better time to be in the internal audit profession,” and challenged participants to advocate risk management processes within their organizations while keeping internal audit standards and basic principles at the forefront of their audit activities.³

This sets the challenge: To help and support management as they struggle with establishing good risk management in the organization, while ensuring that the rigorous provisions of audit standards are retained. Risk management is defined by the IIA as:

A process to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization’s objectives.⁴

Enterprises include all public and private-sector organizations, and enterprise risk management is described as:

A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.⁵

We will also be devoting some time to a landmark document on ERM, which was launched by the Committee of Sponsoring Organizations (COSO) on September 29, 2004. COSO consists of five major professional associations in the United States and was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. All further references in this book to COSO ERM relate to the 2004 COSO ERM framework. Further information on COSO and their publications can be viewed on their Web site at www.coso.org. COSO provides the following commentary in its foreword to ERM guidance:

The need for an enterprise risk management framework, providing key principles and concepts, a common language, and clear direction and guidance, became even more compelling. COSO believes this Enterprise Risk Management—Integrated Framework fills this need, and expects it
will become widely accepted by companies and other organizations and indeed all stakeholders and interested parties.  

**RISK MANAGEMENT FRAMEWORK MODEL: PHASE ONE**

Our first model looks at the way risk management resides in an organization. We start at the top of an enterprise with the position of the CEO and the board and the way they respond to the pressure to ensure good corporate governance in Figure 1.1.

![Risk Management Framework Model: Phase One](image)

Each aspect of the model is described below.

**External Global and Market Developments**

Risk is inherent in the way global events shift in the economy, including changing interest rates, international developments, and the fluctuating movement of capital. Meanwhile, markets are constantly changing as consumer demand alters and competitors enter or leave the marketplace. Public-sector services are also affected by constant changes in the demands...
and expectations of society. This sense of uncertainty has been summed up by COSO:

Enterprises operate in environments where factors such as globalization, technology, restructurings, changing markets, competition and regulation create uncertainty.7

**Statutes, Regulations, Codes, and Guidance**

Governance codes and company legislation can be generic or industry specific, and they create additional demands on enterprises—normally in response to heightened expectations from society, or as a result of corporate scandals that revealed a need to tighten up on existing regulations. The most famous of the more recent laws arrived several years ago in the guise of Sarbanes-Oxley, with the resulting impact on companies listed on the New York Stock Exchange and NASDAQ. An assortment of local state laws also add to the compliance framework within which enterprises must operate. Some professions, such as law, medical practice, and accounting, provide various codes of conduct and specific regulations that must be adhered to by their practicing members. Within this context, governance is about the way organizations conduct themselves and administer their affairs. The IIA’s definition of governance is:

The combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organization toward the achievement of its objectives.8

Most significant organizations understand the need to respond properly to the wider demands of society as expressed through the regulators. The foreword to the COSO ERM addresses this important point:

The period of the framework’s development was marked by a series of high-profile business scandals and failures where investors, company personnel, and other stakeholders suffered tremendous loss. In the aftermath were calls for enhanced corporate governance and risk management, with new law, regulation, and listing standards.9

Business performance goes hand in hand with regulatory performance, as described by one large retail company:

Our size and global reach present extraordinary opportunities, but also present additional complexity in dealing with an ever-changing variety
of laws and regulations. Keeping pace with changes in the regulatory environment is a challenge for management, but we are committed to do so. We continually monitor our legal and regulatory performance, and will upgrade internal systems or change the way we do business when necessary in order to assure compliance.10

The Mission

The risk management framework is driven by what the organization is trying to achieve, which, at its highest level, is the overall mission. For example, the mission of the Ford Motor Company is stated as:

We are a global family with a proud heritage passionately committed to providing personal mobility for people around the world. We anticipate consumer need and deliver outstanding products and services that improve people’s lives.11

Meanwhile, the company’s future vision is:

To become the world’s leading consumer company for automotive products and services.12

Many corporate governance codes argue that corporate objectives should be enriched by ensuring that they also address wider societal concerns:

In addition to their commercial objectives, companies are encouraged to disclose policies relating to business ethics, the environment and other public policy commitments.13

The reality of private, public-sector, and not-for-profit environments means that there can never be total certainty that the mission will always be fully achieved and make the vision a reality. Risk is about this lack of certainty, and it has been defined as follows:

Risk is the chance of something happening that will have an impact on objectives. Therefore, to ensure that all significant risks are captured, it is necessary to know the objectives of the organization function or activity that is being examined….Organizational success criteria are the basis for measuring the achievement of objectives, and so are used to identify and measure the impacts or consequences of risks that might jeopardize those objectives.14
The CEO and Board

The driving force for the enterprise is the CEO and board of directors. This is where the key decisions are made regarding the strategy that will transform the mission into firm results. The IIA defines a board in the following way:

A board is an organization’s governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee, to whom the chief audit executive may functionally report.\textsuperscript{15}

The board formulates strategy and employs executives, managers, staff, and appropriate resources to implement this strategy. The need for sound boards has been remarked on in the past:

The three main problems at Enron were that the company had an accommodating and passive board, an unhealthy drive to meet earnings targets and—probably the most damaging quality—a penchant for hiring only the best and brightest and rewarding them lavishly if they proved they could innovate, innovate and innovate. Unfortunately, the dark side of innovation is fraud.\textsuperscript{16}

Moreover, the board has a key role in overseeing the risk management process. COSO ERM has provided some direction in clarifying this role by suggesting the following oversight responsibilities:\textsuperscript{17}

- Knowing the extent to which management has established effective enterprise risk management in the organization
- Being aware of and concurring with the entity’s risk appetite
- Reviewing the entity’s portfolio view of risk and considering it against the entity’s risk appetite
- Being apprised of the most significant risks and whether management is responding appropriately

Strategy Formation

Our model suggests that the context for the development of a formal strategy is found within the global market forces and the relevant regulatory
framework for each individual organization. One short example of strategy formation comes from CalPERS, the California Employees’ Retirement System, which provides retirement and health benefits:

Our Strategic Plan provides our organization with a road map for meeting the retirement and health benefits needs of more than 1.4 million members and participating employers. It guides our business relations and interactions. Our business philosophy is straightforward. We are customer-focused, and our decision-making process is guided by value and quality.¹⁸

**Senior Management**

The next aspect of the model relates to senior management (i.e., the people who sit in the firing line to get the job done). The corporate strategy will result in various objectives that will need to be delivered to ensure that the organization is successful (i.e., the overall mission is achieved). Senior management run the business lines and are responsible for meeting key performance targets, commonly known as Key Performance Indicators (KPIs). COSO ERM builds on this theme and goes on to locate key responsibilities to senior managers:

Managers guide application of ERM components within their sphere of responsibility, ensuring application is consistent with risk tolerances. In this sense, a cascading responsibility exists, where each executive is effectively a CEO for his or her sphere of responsibility.¹⁹

**Strategy Implementation**

Managers are responsible for ensuring that their staff, systems, and budgets are applied to delivering the set strategy. They do this by breaking down the longer-term corporate strategy into more manageable shorter-term chunks that are handed out to their workforce and associates. The workforce is in effect the engine room of the organization. Empowering organizations allow people to make decisions on the front line and flex their responses to the needs of customers and clients. In terms of implementing solutions, the responsibilities of senior management have been outlined in the banking operational risk management framework, BASEL:

Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors.²⁰
RISK MANAGEMENT FRAMEWORK MODEL: PHASE TWO

So far we have described an overall corporate arrangement that has a basic view of setting strategy and then implementing the various aspects of a more detailed plan to keep the workforce busy and productive. This rather one-dimensional version of the way businesses operate needs to become much more layered and colorful. The additional dimension that has emerged over the years relates to the need to isolate and understand risk. Our model is further enhanced in Figure 1.2 in recognition of this fact.

Each new aspect of the model is described below.

Active Stakeholders

Over the years we have come to accept the role of stakeholders in corporate life. Active stakeholders have a direct influence over an organization, and in incorporated companies, this relates to shareholders who can vote on the board members and what they are paid for their services. Investors,
lenders, associates, partners, bankers, employees, and other parties each have an important influence on the organization. Likewise, institutional investors have a major role in holding a batch of voting shares in many large enterprises, whereas public-sector organizations are beholden to their public to ensure they deliver and deliver well. Stakeholders, in the context of risk management, are described in the Australian/New Zealand risk management standard:

Those people and organizations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.21

Passive Stakeholders

There is a growing band of stakeholders that sits just outside of direct interfaces with specific enterprises, and this is what we mean by passive stakeholders. Local communities, the media, environmental groups, and people who are concerned about the behavior of large organizations may have no obvious influence over the board, but they do have some collective sway in the way the organization is seen by others. Increasingly, such pressure groups are able to influence businesses that are behaving badly or have not made a full assessment of their impact on local communities. The Australian/New Zealand risk management standard has something to say on this matter:

Communication and consultation are important considerations at each step of the risk management process. They should involve a dialogue with stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision maker to other stakeholders.22

There is an emerging theme based around the concept of corporate social responsibility that is starting to enhance the importance of all types of stakeholders.

Strategic Risk

Our model places strategic risk firmly on the corporate agenda. The risks from changing markets and the risk of failing to comply with various laws and rules, or meeting the needs of stakeholders, may mean the stated mission will not be achieved. Strategy takes on board these diverse risks and