

E X A M S T U D Y G U I D E

1st Edition

CRMA[®]

CERTIFICATION IN RISK MANAGEMENT ASSURANCE™



The Institute of Internal Auditors
Research Foundation

CRMA®
CERTIFICATION IN
RISK MANAGEMENT
ASSURANCE™

Exam Study Guide
1st Edition

Francis Nicholson, CIA, CRMA

Chris Baker, CMIIA, CRMA



Copyright © 2013 by The Institute of Internal Auditors Research Foundation (IIARF).

All rights reserved.

Published by The Institute of Internal Auditors Research Foundation
247 Maitland Avenue
Altamonte Springs, Florida 32701-4201

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means—electronic, mechanical, photocopying, recording, or otherwise—with prior written permission of the publisher. Requests to the publisher for permission should be sent electronically to: bookstore@theiia.org with the subject line “reprint permission request.”

Limit of Liability: The IIARF publishes this document for informational and educational purposes and is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The IIARF and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN-13: 978-0-89413-736-5

18 17 16 15 14 13 1 2 3 4 5 6 7 8 9

CONTENTS

List of Tables

List of Figures

Preface

Acknowledgments

About the Authors

DOMAIN I: ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

I.A Assess Risk Management Processes in the Context of Alignment with Strategic Imperatives

I.A.1 Objectives of Risk Management Processes

I.A.2 Organization's Risk Culture

I.A.3 Risk Capacity, Appetite, and Tolerance of Organization

I.B Assess the Processes Related to the Elements of the Internal Environment in Which Organizations Seek to Manage Risks and Achieve Objectives

I.B.1 Integrity, Ethical Values, and Other Soft Controls

I.B.2 Role, Authority, Responsibility, etc., for Risk Management

I.B.3 Management's Philosophy and Operating Style

I.B.4 Legal/Organizational Structure

I.B.5 Documentation of Governance-related Decision-making

I.B.6 Capabilities, in Terms of People and Other Resources (e.g., Capital, Time, Processes, Systems, and Technologies)

I.B.7 Management of Third-party Business Relationships

I.B.8 Needs and Expectations of Key Internal Stakeholders

I.B.9 Internal Policies

I.C Assess the Processes Related to the Elements of the External Environment in Which Organizations Seek to Manage Risks and Achieve Objectives

I.C.1 Key External Factors (Drivers and Trends) That May Impact the Objectives of the Organization

I.C.2 Needs and Expectations of Key External Stakeholders (e.g., Involved, Interested, Influenced)

DOMAIN II: PRINCIPLES OF RISK MANAGEMENT PROCESSES

II.A Benchmark Risk Management Processes Using Authoritative Guidance

Combined Australian and New Zealand Standard

The National Institute of Standards and Technology (NIST)

ISO 31000:2009, Risk Management – Principles and Guidelines

COSO's *Enterprise Risk Management – Integrated Framework*

GAIT for Business and IT Risk

II.B. Evaluate Risk Management Processes

II.B.1 Setting Objectives at All Levels to Achieve Strategic Initiatives

II.B.2 Identifying Risks

II.B.3 Risk Analysis and Evaluation, Including Correlation, Interdependencies, and Prioritization

II.B.3.i Risk Classification

II.B.3.ii Risk Analysis

II.B.3.iii Risk Criteria

II.B.3.iv Risk Level or Severity

II.B.3.v Risk Mapping and Prioritization

II.B.3.vi Risk Registers

II.B.3.vii Risk Psychology

II.B.4 Risk Response (e.g., Avoid, Transfer, Mitigate, Accept), Including Cost/Benefit Analysis

- II.B.5 Developing and Implementing Risk Mitigation Plans**
- II.B.6 Monitoring Risk Mitigation Plans and Emerging Risks**
- II.B.7 Reporting Risk Management Processes and Risks,
Including Risk Mitigation Plans and Emerging Risks**
- II.B.8 Periodic Review of Risk Management Processes to Aid
in Continuous Improvement**

DOMAIN III: ASSURANCE ROLE OF THE INTERNAL AUDITOR

- III.A Review the Management of Key Risks**
- III.B Evaluate the Reporting of Key Risks**
- III.C Provide Assurance that Risks Are Adequately Evaluated**
- III.D Provide Assurance on Risk Management Processes**

DOMAIN IV: CONSULTING ROLE OF THE INTERNAL AUDITOR

- IV.A Facilitate Identification and Evaluation of Risks**
 - IV.A.1 Understand the Needs of the Client**
 - IV.A.2 Confirm the Scope and Objectives with the Client**
 - IV.A.3 Plan the Facilitation Exercise**
 - IV.A.4 Facilitate the Activity**
 - IV.A.5 Review the Effectiveness of the Activity**
 - IV.A.6 Report Outcomes**
 - IV.A.7 Make Recommendations/Propose Further Actions**
- IV.B Coach Management in Responding to Risks**
- IV.C Coordinate Risk Management Activities**
- IV.D Consolidate Reporting on Risks**
- IV.E Maintain and Develop the Risk Management Framework**
- IV.F Advocate for the Establishment of Risk Management**
- IV.G Develop Risk Management Strategy for Board Approval**

APPENDIX A: SAMPLE CRMA EXAM QUESTIONS

APPENDIX B: SUGGESTED SOLUTIONS TO SAMPLE CRMA EXAM

QUESTIONS

APPENDIX C: CRMA EXAM SYLLABUS

APPENDIX D: REFERENCES

APPENDIX E: SUGGESTED READING

GLOSSARY

LIST OF TABLES

- | | |
|--------------|--|
| Table I.1. | Domain I Outline |
| Table I.2. | Organizational Structure Comparisons |
| Table I.3. | Effective Decision-making |
| Table I.4. | Internal Stakeholder Needs |
| Table I.5. | Analysis of the External Environment |
| Table I.6. | External Stakeholder Needs |
| Table II.1. | Domain II Outline |
| Table II.2. | COSO's ERM Components |
| Table II.3. | Measures of Severity |
| Table II.4. | Risk Severity Definitions |
| Table II.5. | Risk Prioritization |
| Table II.6. | Risk Profile Responses |
| Table III.1. | Domain III Outline |
| Table III.2. | Distinguishing Internal Audit Roles in ERM |
| Table III.3. | Information-gathering Actions |
| Table IV.1. | Domain IV Outline |
| Table IV.2. | How Consulting and Assurance Differ |

LIST OF FIGURES

- Figure I.1. Risk Management Processes
- Figure I.2. The Cyclical Nature of Risk Management Processes and Their Contribution to Increasing Risk Maturity and Improving Organizational Effectiveness
- Figure I.3. Requirements for Effective Risk Management
- Figure I.4. Levels of Risk Maturity
- Figure I.5. Response Manages Inherent Risk to Within Risk Appetite
- Figure I.6. Benefits of Defining Risk Appetite
- Figure I.7. Approach to Risk Appetite
- Figure I.8. McKinsey 7S Hard and Soft Elements
- Figure I.9. McKinsey 7S Framework
- Figure I.10. The 4 V's Model of Ethical Leadership
- Figure I.11. COSO's Internal Control – Integrated Framework
- Figure I.12. The Three Lines Of Defense
- Figure I.13. Roles of the Three Lines of Defense
- Figure I.14. Blake and Mouton's Managerial Grid
- Figure I.15. Blake and Mouton's Managerial Styles
- Figure I.16. Dimensions of Organizational Structures
- Figure I.17. Differences in Legal Forms of Organizations

- Figure I.18. The Decision-making Process
- Figure I.19. Adding Value to Inputs
- Figure I.20. Porter's Value Chain
- Figure I.21. Activities in Porter's Value Chain
- Figure I.22. Capabilities and Measures
- Figure I.23. Competing Stakeholder Interests
- Figure I.24. Overlapping Stakeholders
- Figure I.25. Porter's Five Forces
- Figure II.1. Cyclical Processes of Risk Management
- Figure II.2. Mnemonic for SMART Objectives
- Figure II.3. Four Primary Types of Objectives
- Figure II.4. The 8 Model for Strategy Execution
- Figure II.5. The Extended 8 Model for Strategy Execution
- Figure II.6. Shaping the Risk Universe (COSO).82
- Figure II.7. Sample Classification of Risks
- Figure II.8. Bow-tie Diagram
- Figure II.9. High-priority Risk Map
- Figure II.10. Threat/Opportuniy Risk Map
- Figure II.11. Risk Attitude
- Figure II.12. Optimal Risk-taking
- Figure II.13. Basic Risk Responses
- Figure II.14. Risk Level/Severity and Response
- Figure II.15. Controls for Treating Risk

- Figure II.16. Likelihood and Impact
- Figure III.1. Cornerstones of Corporate Governance
- Figure III.2. Important Interrelationships
- Figure III.3. ERM and Internal Auditing
- Figure III.4. Lead and Lag Indicators
- Figure III.5. Advantages of Key Risk Indicators
- Figure III.6. Types of Key Risk Indicators
- Figure III.7. Management of Key Risks
- Figure III.8. Information-gathering Methods
- Figure III.9. Steps to Assurance
- Figure III.10. A Strategic View of Assurance
- Figure III.11. Assurance-provider Classes
- Figure III.12. Areas of Interest
- Figure III.13. Assurance on Risk Management Processes
- Figure III.14. Seven Process Elements
- Figure III.15. Key Principles Approach
- Figure III.16. Risk Management Maturity Timeline
- Figure IV.1. Internal Audit's Role in Enterprisewide Risk Management
- Figure IV.2. Common Elements of Assurance and Consulting Engagements
- Figure IV.3. Facilitation Stages
- Figure IV.4. Consulting Engagement Scope
- Figure IV.5. Facilitation Session Elements

- Figure IV.6. Benefits to Individual Managers
- Figure IV.7. Benefits to Management as a Whole
- Figure IV.8. Coaching Steps
- Figure IV.9. Overview of Risk Management Coordination.
- Figure IV.10. Goals of Risk Management Coordination
- Figure IV.11. Purposes of Risk Reporting
- Figure IV.12. Risk Management Framework Evolution
- Figure IV.13. Advocacy Steps for Risk Management
- Figure IV.14. Risk Management Strategy

PREFACE

When Tony Hayward became CEO of BP in 2007, he vowed to make safety his top priority. Among the new rules he instituted were the requirements that all employees use lids on coffee cups while walking and refrain from texting while driving. Three years later, on Hayward's watch, the Deepwater Horizon oil rig exploded in the Gulf of Mexico, causing one of the worst manmade disasters in history. A U.S. investigation commission attributed the disaster to management failures that crippled "the ability of individuals involved to identify the risks they faced and to properly evaluate, communicate, and address them." Hayward's story reflects a common problem. Despite all the rhetoric and money invested in it, risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them. Many such rules, of course, are sensible and do reduce some risks that could severely damage a company. But rules-based risk management will not diminish either the likelihood or the impact of a disaster such as Deepwater Horizon, just as it did not prevent the failure of many financial institutions during the 2007–2008 credit crisis.

Kaplan and Mikes (2012)

You don't have to look very hard to find evidence of the importance of risk management. Unfortunately, it is usually when something has gone wrong—sometimes spectacularly so—that our attention is drawn to what can happen if internal controls are not up to the job. And for every high-profile disaster, a multitude of CEOs around the world heave a sigh of relief that it wasn't them or their organization.

It is regrettable that this only serves to reinforce a wholly negative view of risk management—that it is there to reduce or eliminate risk and stop things from going wrong. It can also create a suspicion that it is all a waste of time. Bad

things happen *despite* risk management. And, it might be asked, in the wake of another epic failure, what were the internal auditors doing?

However, both these views—the negative and the cynical—are too narrow, even misguided. Risk is inevitable, but it is also desirable. Risk management is not infallible, but it can add significant value to an organization. And internal audit, through its unique position, provides another vital layer of protection by offering a critical eye and constructive proposals.

This is what we will learn through the course of this book. *Risks* are impacts—both positive and negative—on objectives, arising from uncertainty. *Risk management* is the attempt to minimize the number of surprises, enabling an organization to exploit opportunities when they arise and be prepared for potentially damaging events and circumstances when they materialize. *Internal audit* delivers independent and objective evaluation and expert insights into risk management. *Risk management assurance* is the means by which the degree of reliability that can be given to risk management is evaluated and confirmed, complemented by intelligent advice for improvement.

An important model underpinning this view of risk and control is the *three lines of defense*.

- The first line of defense is operational management, which owns and manages risk and is responsible for implementing corrective actions for addressing weaknesses in internal controls.
- The second line of defense is risk management and compliance to help build and monitor the first line of defense.
- The third line of defense is internal audit, delivering independent assurance on the effectiveness of internal controls and advisory services on the development and improvement of risk management.

Underpinning all of this is senior management and the board, who are ultimately responsible for ensuring that risk management is in place and is effective by approving the risk management strategy and seeking assurance on its effectiveness.

To be able to deliver assurance on risk management processes and provide useful consultation for their continuous improvement, the internal auditor needs a thorough understanding of the client organization and the whole subject of risk management. Hence, the first two domains of the Certification in Risk Management Assurance (CRMA®) and of this book address the following key questions:

- Domain I: what is risk management and how does it fit within an organization?
- Domain II: how does risk management work?

Risk management does not operate in a vacuum but resides in living, breathing organizations that are unique. It must develop as the host develops in ways that are sympathetic and complementary. This means that risk management systems need to be customized to match the character of the organization and evolve as internal and external factors lead to an ever-changing environment. Readers will discover a wealth of information in these first two chapters in preparation for the second half of the book, where the understanding gained is applied to delivering assurance and advice. The latter two chapters focus on the following:

- Domain III: how does internal audit provide assurance on risk management?
- Domain IV: how does internal audit provide advice on improving risk management?

Assurance and advice have important similarities and differences. These topics are framed by the provisions of The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) and, in particular, the *International Standards for the Professional Practice of Internal Auditing (Standards)*, which are referenced throughout.

The structure of the book is organized to follow exactly the syllabus of the Certification in Risk Management Assurance (CRMA) and practice questions are included to help candidates prepare for the exam. The authors have provided plenty of context to the material to engender a sound grasp of the subject, and on

that basis it is hoped that the general reader of risk management, internal auditing, and assurance will find much that is of interest as well.

ACKNOWLEDGMENTS

We want to thank our colleagues and fellow members of the Chartered Institute of Internal Auditors (serving the UK and Ireland) for helping us produce this *CRMA® Exam Study Guide*. Everyone is a member of a team and—like Isaac Newton and Bernard of Chartres before him—we are all standing on each other's shoulders.

We would also like to express our sincere thanks to The Institute of Internal Auditors Research Foundation's Committee of Research and Education Advisors (CREA) review team for its guidance throughout this project. We particularly want to thank Selma Kuurstra, project manager, for her enthusiasm, patience, encouragement, and kind words—and for keeping us to task.

Francis Nicholson, CIA, CRMA

Chris Baker, CIIA, CRMA

ABOUT THE AUTHORS

Francis Nicholson, CIA, CRMA, has worked as the education director for the Chartered Institute of Internal Auditors for more than six years, taking care of membership and professional development services for both individuals and employers. His background is predominantly in education, having delivered, developed, and managed adult and professional training programs for colleges and universities. His primary field is business studies, spanning accounting, finance, economics, and management studies. He works with practitioners, chief audit executives, and academics to ensure that the guidance, support, and resources provided raise the skills and status of the individual and the standards of professional practice.

Chris Baker, CMIIA, CRMA, has been the technical manager for the Chartered Institute of Internal Auditors since November 2007. His role at the Institute is to promote and develop the professional practice of internal auditing and build upon the body of knowledge that is available to members in the UK and Ireland. He has more than 30 years of practical experience in governance, risk management, control, and internal auditing that includes a detailed understanding of our International Professional Practices Framework (IPPF). Since February 2011, Chris has developed and coordinated the UK and Ireland External Quality Assessment (EQA) Service.

DOMAIN I

Organizational Governance Related to Risk Management

Table I.1. Domain I Outline		
Topic/subtopic	Explanation	Reference # in study guide
A. Assess risk management processes in the context of alignment with strategic imperatives.	<p>The principal purpose of risk management is to help an organization achieve its strategic objectives. It does so by assisting management in:</p> <ul style="list-style-type: none"> Identifying and assessing the sources and nature of uncertainties that may impact positively or negatively on organizational objectives. Determining how much risk stakeholders are prepared to tolerate. Establishing and maintaining appropriate responses, including controls, to keep risk at a tolerable level. <p>Any assessment of whether</p>	I.A

	risk management processes are effective must include the extent to which those processes are aligned with organizational objectives.	
1. Objectives of risk management processes	The purpose of risk management and its processes is not always to eliminate or even minimize risk. Instead, the primary aim is to <i>understand</i> risk so that management can make informed decisions. Risk is unavoidable and, to an important extent, desirable. The key processes relate to reviewing strategic objectives, and then risk identification, risk analysis, risk response, monitoring, reporting, and review.	I.A.1
2. Risk culture	Risk culture refers to the overall attitude and approach an organization takes toward risk. Organizations may be described as being more or less risk mature. As the risk culture becomes more mature, greater importance is attached to understanding risk and considering it in planning and decision-making throughout the organization.	I.A.2
	<i>Risk capacity</i> refers to how much risk an organization is	

	<p>3. Risk capacity, appetite, and tolerance of organization</p>	<p>able to take with respect to its resources and capabilities. <i>Risk appetite</i> is a measure of how much risk an organization is prepared to take, from being risk averse to tolerating higher levels of risk (temporarily or on a long-term basis) in exchange for potential benefits.</p>	I.A.3
	<p>B. Assess the processes related to the elements of the internal environment in which organizations seek to manage risks and achieve objectives.</p>	<p>Risk management processes are set in a framework that must be understood and developed in the context of the organization's internal environment. The approach and implementation of risk management should be sympathetic to and mesh with the organization's resources and capabilities, and serve to reveal and manage the risks that exist in the internal environment.</p>	I.B
	<p>1. Integrity, ethical values, and other soft controls</p>	<p>Unethical behavior has the potential to create significant reputational and financial risks, while acting with integrity may generate positive opportunities. Organizations need to address business ethics with leadership from the highest levels. Risk management processes themselves must be delivered with integrity and support the organization's resolve for</p>	I.B.1

	<p>compliance with its codes for professional conduct and ethical behavior.</p>	
2. Role, authority, responsibility, etc., for risk management	<p>Organizations function effectively when there is a clear division of labor with well-defined roles and lines of authority that usually flow down the various structural tiers. Risk management equally requires an appropriate structure together with the necessary resources and channels of communication. From such arrangements, it gains its authority.</p> <p>The <i>three lines of defense</i> model makes a sharp distinction among the roles of:</p> <ul style="list-style-type: none"> • Operational management. • Risk management oversight. • Internal auditing (independent and objective assurance on the effectiveness of internal controls and risk management). <p>In addition, as primary stakeholders, senior management and the board have a critical role to play in ensuring that these three lines</p>	I.B.2

	<p>of defense are in place and working.</p>	
3. Management's philosophy and operating style	<p>The organization has a way of doing things that forms a large part of its culture. The “tone at the top” should drive that culture and be reflected by the approach management takes and the style that is adopted across all operational areas.</p> <p>Organizational culture makes a significant impact on the risk culture.</p> <p>Risk management processes must consider the attitude and style of management generally, and aim to be consistent with the prevailing philosophy while moving the organization toward greater risk maturity.</p>	I.B.3
	<p>The structure of an organization is determined by the way it distributes its responsibilities and resources and the manner in which the various divisions interact. Strategic goals, internal capabilities, and its response to the external environment are all determining factors of the structure. As these may change over time, it is sometimes necessary to alter</p>	

	<p>4. Legal/organizational structure</p> <p>the structure, whether organically or through a more substantial readjustment.</p> <p>Risk management processes should recognize the risks and benefits of different organizational structures as well as the current configuration.</p> <p>In addition to structure, organizations may use one of a number of legal forms that are available to reflect the needs of the organization in terms of its size, ownership, control, sources of capital, liability for losses, stakeholder interests, and reporting requirements.</p>	I.B.4
5. Documentation of governance-related decision-making	<p>Corporate governance arrangements exist to ensure that the interests of the stakeholders—especially those of the agent (management) and the principal (owner)—remain in balance with transparency and accountability. Documentation is used in support of decision-making and as an audit trail that can be accessed and referenced to ensure openness. The board (or equivalent) and its subcommittees collectively form the principal mechanisms</p>	I.B.5

	<p>for oversight and governance. In addition, other external functions may contribute to this process. Risk management plays a major role in corporate governance.</p>	
6. Capabilities of people and other resources (i.e., capital, time, processes, systems, and technologies)	<p>An organization adds value by taking various inputs and transforming them in some fashion. The extent to which this is possible depends upon the capabilities represented by the staff, equipment, systems, processes, etc. An organizational advantage is gained by meeting customer demands or service-user expectations better than the competition. Each of these capabilities should be evaluated in order to identify risks and opportunities.</p>	I.B.6
7. Management of third-party business relationships	<p>Organizations can extend their capabilities significantly by engaging with third parties to pursue goals of common interest and the mutual benefits of shared resources. Such relationships carry both risk and opportunity. Risk management processes should extend to cover such relationships and consider the internal arrangements for managing risks by those third parties.</p>	I.B.7

8. Needs and expectations of key internal stakeholders	<p>The key internal stakeholders are staff, managers, and the owners of the organization. They have significant stakes (or interests) that must be taken into account when considering any new initiative or strategy. Stakeholders contribute greatly to the success or failure of an enterprise. At times, the interests of different groups may be in competition. Therefore, management of stakeholder interests needs to be an integral part of strategic and operational planning.</p>	I.B.8
9. Internal policies	<p>To ensure consistent operational activity in a way that serves to deliver strategic objectives, it is necessary to set organizational policies. These provide the rationale and guidelines for procedures and are likely to form part of internal controls. Their operation should be considered by risk management processes to determine whether they are working and having the desired effect.</p>	I.B.9
C. Assess the	<p>Organizations operate in an external environment in which multiple influences are a</p>	

	<p>processes related to the elements of the external environment in which organizations seek to manage risks and achieve objectives.</p>	<p>continual source of changeable threats and opportunities. Risk management processes should protect the organization from surprises by monitoring the external environment for signs of change to be exploited, resisted, or endured.</p>	I.C
	<p>1. Key external factors (drivers and trends) that may impact the objectives of the organization</p>	<p>External factors are often analyzed under the headings of political, environmental, social, technological, economic, and legal (PESTEL). This provides a convenient framework in which to identify risks and opportunities that may have an impact on organizational objectives. It is important to understand the forces that drive change in the external environment and identify the underlying trends.</p>	I.C.1
	<p>2. Needs and expectations of key external stakeholders (e.g., involved, interested, influenced)</p>	<p>There are many external stakeholders (including customers, suppliers, investors, banks, the government, regulators, local communities, and the public at large) who can be powerful allies or strong adversaries to organizational efforts. Identifying them and anticipating their reactions are part of the process of</p>	I.C.2

determining risk and enabling management to establish suitable strategies for stakeholder engagement.

Introduction to Domain I

Where there are *objectives*—intended or desirable outcomes—there are *risks*. Success is never 100 percent guaranteed and new opportunities can occur unexpectedly. In short, the future is inherently uncertain. Risks and opportunities arise out of uncertainty in both everyday life and organizational endeavor. There is no guarantee even that the future will be like the past. Just as chaos theory tells us that the flap of a butterfly’s wings in some part of the world could produce a storm somewhere else, so even small changes in the organizational environment can bring about significantly different results tomorrow.

We should not regard all risk as negative or bad. In fact, organizations exploit the uncertainty of the future (the fundamental riskiness of existence) to their advantage, applying the maxim *no risk, no reward*. In this sense, risk management is the process of taking full advantage of opportunities that deliver clear benefits to the organization. This may be less true of public sector and charitable organizations whose purpose is to deliver services rather than profit, and as such, tend to be more risk averse in the pursuit of delivering the best value for their service users. However, such organizations need to be attuned to the negative effects of risk to service delivery. They also may have some commercial operations that seek to maximize profits or surpluses, and for these, they may accept greater levels of risks with a view to greater gains.

Risk management, as a well-defined and coordinated enterprisewide endeavor, is a relatively new area of interest for organizations. Over the past few decades, risk management has become more sophisticated and has enjoyed steadily increasing prominence and resources. Initially, the principal focus was on entrepreneurial risk (that the organization would not generate projected gains) and the main response to such risk was to transfer it through insurance. Now it is common to consider the full gamut of risks (both positive and negative, or “upside” and “downside”) as they arise to frustrate or enhance strategic and

operational objectives. The range of risk responses applied is also increasingly varied.

Risk management processes focus on the identification and assessment of risk followed by response, monitoring, and reporting. These processes (the full details of which are covered in domain II) form part of a risk management framework that is applied enterprisewide in more risk mature organizations. As both the environment (internal and external) and organizational objectives are subject to change over time, it is necessary to make regular checks to ensure that the responses to risk and control remain effective and continue to serve the needs of the organization. To do so, the whole approach must be aligned with strategic priorities. While risk management processes will be set up to achieve this, it is also of great value to gain independent and objective assurance on the effectiveness of those processes and risk management as a whole. This is a role for which internal audit is ideally suited and uniquely placed to fulfill.

The focus of this domain is to understand risk management processes as a whole—the risk management framework—in the context of the organization served. First, we will consider the alignment between risk management and the strategic aims of the organization (I.A). Second, we will explore the features of the internal environment to ensure that risk management processes take full account of these and integrate with them (I.B). Finally, we will make a similar exploration of the external environment to ensure that risk management processes provide sufficient assessment of the threats and opportunities so that the organization can control or exploit them accordingly (I.C).

Domain I counts for 25–30 percent of the CRMA examination.

I.A Assess Risk Management Processes in the Context of Alignment with Strategic Imperatives

According to Nicholson and Turner (2010):

Strategic management is the art of defining where you want to go and then making sure you get there. It requires a continuous process of reinvention, so that the goals are pushed further into the future the more

closely they are within reach. There is always a drive toward improvement and greater success.

It is in this context that risk management processes need to operate to ensure that, throughout the endless striving of strategic ambition, the risks and opportunities remain firmly in view. Risk management, as a structured approach to addressing the full range of risks faced by an organization, has developed considerably over the last 30 years. Operational and strategic plans may fail because events occur or conditions arise for which the organization was unprepared. Similarly, losses may arise if resources are irreversibly committed to one opportunity when a better opportunity presents itself. Risk management processes aim to help management by identifying and analyzing potential threats, vulnerabilities, and opportunities; agreeing on effective strategies; and providing regular updates to confirm risks are being managed effectively. There are many highly sophisticated tools, models, frameworks, and resources that organizations can adopt. However, since risk management exists to serve the needs of the organization, it is very important that the approach used is tailored to particular requirements based on its goals, culture, internal and external environments, and overall risk maturity. Therefore, any assessment of risk management processes—the first stage in providing risk management assurance—must consider how well those processes support organizational aims.

There is no single definition of risk that is accepted and universally used. The Institute of Internal Auditors' (IIA's) definition, taken from the glossary of the International Professional Practices Framework (IPPF), is as follows:

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. (IIA, 2013)

Risk management standards developed by a joint committee of Standards Australia and Standards New Zealand known as AS/NZS 4360:2004 were a forerunner of the International Standards Organization's (ISO's) risk management standard ISO 31000 and define risk as “the chance of something happening that will have an impact on objectives.” Similarly, ISO, in its risk management standards (ISO 31000), defines a risk as “the effect of uncertainty on objectives.”

KEY TERM

Risk: The possibility of an event occurring that will impact objectives.

Despite the difference in wording and emphasis, there are numerous features that these definitions have in common:

- Risks are considered in relation to their ability to impact an organization and its objectives. If there is no potential for an event to have such an impact, then it is simply irrelevant and not a risk for the organization.
- Risk assessment and risk processes more generally must be contextualized. Risks cannot be understood without considering their potential to disrupt a given activity or plan. Likewise, the effectiveness and appropriateness of risk responses can only be properly assessed for a particular set of circumstances.
- Risks are not the same as weaknesses or issues. A weakness is a flaw or a propensity for something to go wrong while an issue describes something that has gone wrong. Risks are about the future rather than the present, and are most commonly understood to be a product of likelihood and consequence or impact. This is often referred to as the *risk severity*. When numerical values can be used, a meaningful answer may be generated. For example, if there is a 10 percent chance that a loss of \$1,000 may be incurred, then we might say the value of the risk is \$100. Otherwise, we may apply a more arbitrary graded scale from less to more likely, and from lesser to greater impact.
- Risks arise out of the natural uncertainty of future events. They are an unavoidable feature of any endeavor.
- Not all risks are to be regarded as damaging. The same inherent uncertainty of the future is the basis for speculation and opportunity. The definitions quoted above refer to an impact or effect, but it remains open as to whether this is positive or negative. Negative impacts are sometimes referred to as the *downside* and benefits as the *upside*.

To distinguish whether we are referring to upside or downside risk, we often use *opportunity* to refer to positive risk and *risk* to mean negative risk.

The main processes of risk management relate to:

- *Analysis:* Risks (both current and emergent) must be identified and assessed for relevance to the organization, its context, and its objectives, and evaluated, leading to a determination of the key risks—the ones requiring most urgent attention by management.

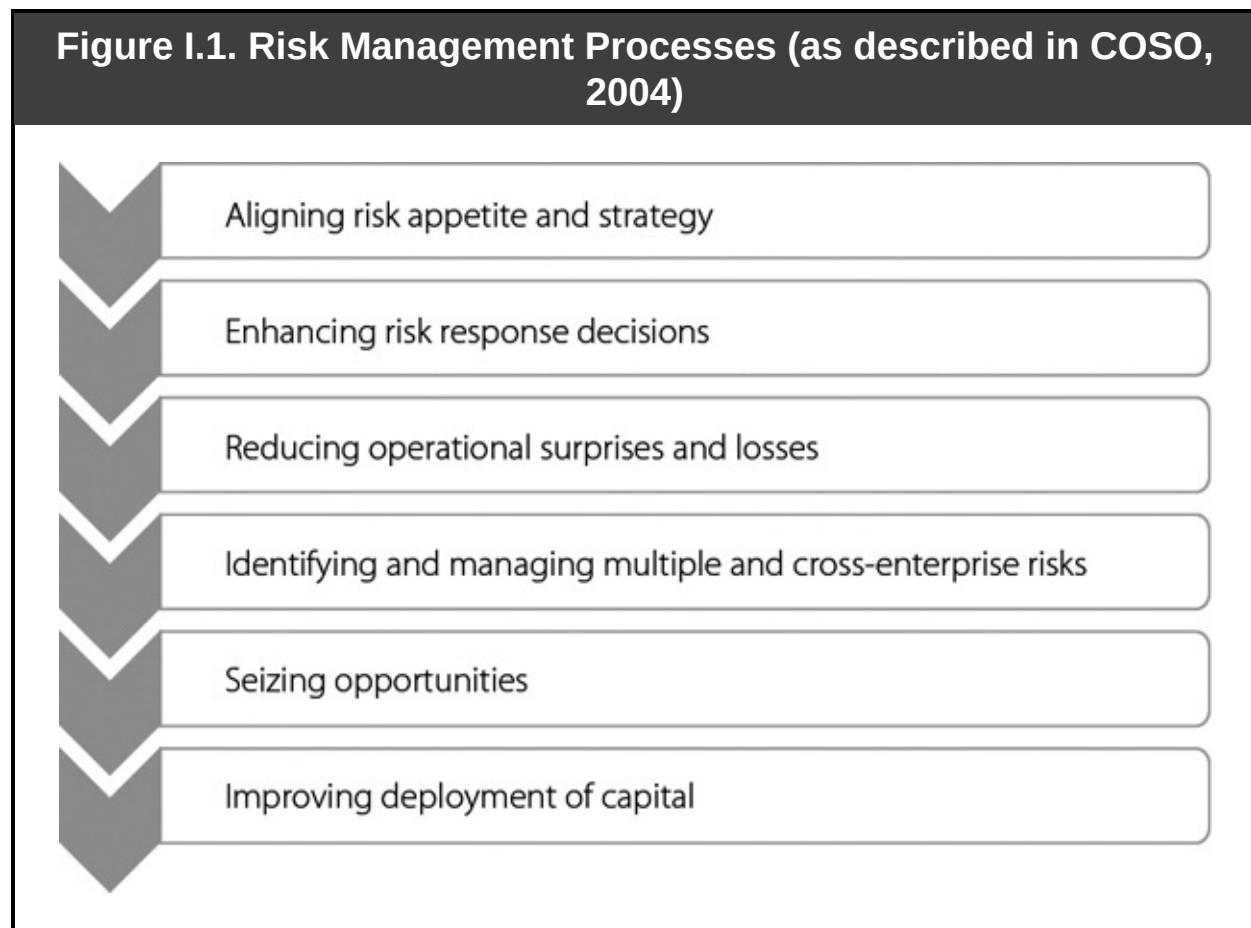
KEY TERM

Risk severity: The product of likelihood and impact.

- *Risk response:* There are a number of ways to respond to identified risks, depending on the risk *appetite*, available resources, and perceived priorities.
- *Monitoring:* The potential for change requires routine monitoring with regard to:
 - The system of internal controls and other responses to determine whether they remain relevant, and whether the required measures are in place and are having the intended effect with respect to the risks or opportunities (sometimes referred to as the *control objectives*).
 - Changes to the internal and external environments that may alter the risk profile, making some less severe while raising the severity of others; or introducing new and previously unanticipated risks, each requiring a new response.
 - Adjustments to the strategy of the organization, causing objectives and risks to change.
- *Reporting:* Management and the board (directly or via the audit committee or other similar body such as a risk committee or combined

audit and risk committee) will require updates and assurance on the risk profile of the organization and its state of preparedness with respect to internal controls.

Risk management processes may be described in other terms. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) model for an integrated framework for enterprise risk management lists key components as shown in [Figure I.1](#).



Enterprise risk management (ERM) is defined by COSO as:

A process, effected by an entity's board of directors, management, and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. (COSO, 2004)

This is similar to The IIA's definition of ERM in the 2009 Position Paper, Role of Internal Auditing in Enterprise Risk Management, according to which ERM "is 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." (IIA, 2009)

KEY TERM

Risk management framework: The sum total of the arrangements by which risk management operates.

From this it should be clear that, in addition to running its routine processes, risk management does other things:

- It establishes and maintains a risk management framework that is aligned to organizational objectives as well as coordinated, integrated, and enterprise-wide (where "risk management framework" refers to the sum total of all elements of risk management). The framework helps less risk mature organizations to move toward this desired status.
- It helps management determine:
 - Risk appetite.
 - Responses to particular risks.
 - The overall risk culture of the organization, enabling it to be progressively more risk mature.
- It enables organizations to prepare for risks and opportunities before they arise to maximize operational effectiveness and strategic gain.
- It allows organizations to deploy their resources according to need and potential for advantage.

While risk management can report on the risk profile, internal audit's analysis

of risks and internal control effectiveness provides independent and objective assurance by virtue of its unique role and position. The effectiveness of the risk management framework and processes is often reflected in terms of the organization's overall risk maturity.

I.A.1 Objectives of Risk Management Processes

In addition to a review of the organization's objectives, it makes sense to define and describe the objectives of risk management itself. Naturally, there should be a close alignment between these two sets of objectives. It is important not to lose sight of the fact that risk management processes are designed to fulfill a particular role. Sometimes, when the focus is very heavily on implementation and operation, it is possible to become too dogmatic about what is right for risk management rather than what is right for the organization. The COSO framework for enterprise risk management makes this point very clearly.

Enterprise risk management is not an end in itself, but rather an important means to achieving [an entity's] objectives. It does not operate in isolation in an entity, but rather is an enabler of the management process. Enterprise risk management is interrelated with corporate governance by providing information to the board of directors on the most significant risks and how they are being managed. (COSO, 2004)

A further point to bear in mind is that, because risks and opportunities may arise in all areas of activity, risk management should be enterprisewide.

The objective is to achieve maximum sustainable value from all the activities of the organization. Risk management enhances the understanding of the potential upside and downside of the factors that can affect an organization. It increases the probability of success and reduces both the probability of failure and the level of uncertainty associated with achieving the objectives of the organization. (AIRMIC, Alarm, IRM, 2010)

This brings us to a third point: risk management's breadth calls for a coordinated and consistent set of processes to ensure that its contribution is maximized.

A systematic, timely, and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results. (ISO 31000)

A common misconception is that the role of risk management is to act as a brake on strategic growth and ambition. On the contrary, successful risk management enables an organization to achieve its objectives and fulfill its potential by maximizing the value delivered to the primary stakeholders. Although they will vary as organizational objectives vary, risk management process objectives are likely to include the following:

- To contribute to the long-term survival of the organization.
- To maximize the value delivered to all stakeholders.
- To link growth, risk, and return.
- To safeguard the assets and reputation of the organization.
- To facilitate greater operational effectiveness and efficiency.
- To increase the likelihood of achieving strategic and operational objectives.
- To comply with legal and regulatory requirements.
- To improve organizational learning and resilience.
- To be better placed to take advantage of opportunities as they arise.
- To help an organization become more risk mature by considering its current and future risks in a coordinated manner within an enterprise-wide framework.
- To improve the understanding an organization has of itself and its activities to enable better decision-making, operational management, and deployment of capital and resources.
- To reduce uncertainty and volatility in those areas of organizational activity that do not benefit from being risk-laden. In other words, if there

is not a reason to accept a risk or to incur the costs associated with controls, the risk should be minimized or removed.

Risk management follows a cyclical and iterative process that uses monitoring as a feedback loop to maintain alignment with strategic objectives, improve the effectiveness of identification and response, and continually raise the level of risk maturity (see [Figure I.2](#)).

Figure I.2. The Cyclical Nature of Risk Management Processes and Their Contribution to Increasing Risk Maturity and Improving Organizational Effectiveness



The summary of the key requirements for effective risk management is shown in [Figure I.3](#).

Figure I.3. Requirements for Effective Risk Management



Risk management exists to serve the organization, not vice versa.

It needs to be enterprisewide.

It requires a coordinated and consistent framework.

It is not designed to be a brake on ambition.

It needs to be cyclical and iterative.

I.A.2 Organization's Risk Culture

The *risk culture* of an organization is its overall attitude and approach to dealing with risks—either more or less mature or risk aware. *Risk maturity* takes time to evolve as greater awareness and understanding, processes, and skills are steadily developed. An organization is generally guided by its vision and mission, set by senior management and approved and monitored by its governing body. (See II.B.1.) It also is responsive to changes in its internal and external environments. Although these factors impact risk culture, the culture is brought into being by the individual and collective behavior of those who make up the organization. According to the Institute of Risk Management (IRM), the culture of an organization “arises from the repeated behavior of its members.... [It] is more than a statement of values—it relates to how these translate into concrete actions.” (IRM, 2012).

KEY TERM

Risk maturity: A measure of the level of risk culture.

Risk culture can be defined as “the system of values and behaviors present throughout an organization that shape risk decisions. Risk culture influences the decisions of management and employees, even if they are not consciously weighing risks and benefits.” (Farrell and Hoon, 2009) This demonstrates that risk culture applies to everyone and that it can be working (either constructively or otherwise) even when the members of the organization are unaware of it.

In 2012, the IRM produced a booklet offering risk culture guidance to boards of directors. The following 10 features are listed as essential parts of a successful risk culture (IRM, 2012):

- Leadership and commitment from the highest levels of the organization.
- Adherence to ethical principles and concern for all stakeholders.
- Organizationwide recognition of the need for effective risk management.
- Ready access to reliable information relating to risk at all levels.
- Active encouragement to share information when things go wrong so that the lessons can be learned.
- Application of risk management to all activities, even those considered to be complex, remote, or too hard to understand.
- Encouragement and reward for appropriate risk-taking as well as sanctions for reckless or negligent approaches.
- Ready access to support and resources for the development of risk management skills.
- Acceptance of multiple perspectives to challenge the approaches adopted.
- Alignment of risk culture with the organizational culture.

These can be regarded as the characteristics of a *risk mature organization*. This list confirms a strong connection among risk culture, ethics, and integrity (I.B.1), as well as concern for wider stakeholder groups (I.B.8 and I.C.2).

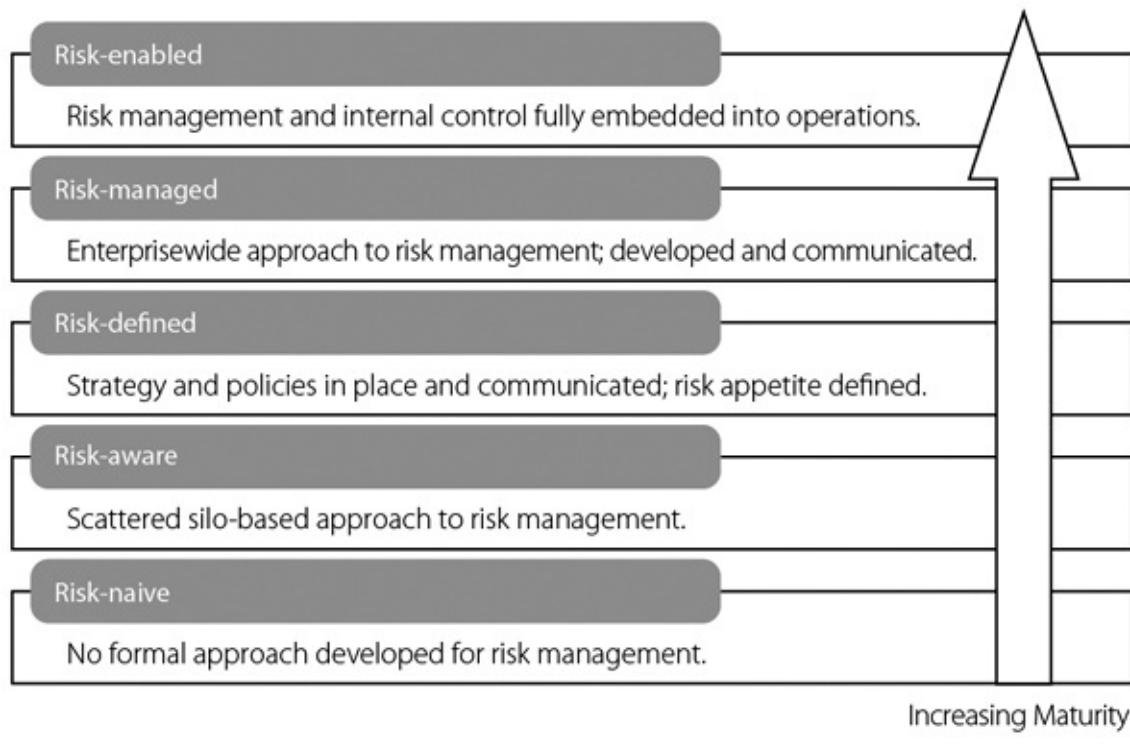
KEY TERM

Risk culture: The prevailing attitude and approach to risk.

Risk culture is revealed in a number of ways. The *risk appetite* (I.A.3) is an expression of how much risk the organization is prepared to accept or tolerate. This in turn is related to its *risk capacity* (I.A.3), which reflects the ability to accept risk as a consequence of the skills and resources at the organization's disposal. More than being just the totality of risk appetite, capacity, framework, and processes, however, risk culture determines whether there is genuine buy-in at all levels to address risks and opportunities that arise out of the uncertainty of events.

The risk culture can be assessed as more or less mature. [Figure I.4](#) illustrates how risk culture may evolve over time through five levels of maturity.

Figure I.4. Levels of Risk Maturity (adapted from The IIA, 2005)



More generally we define organizational culture as the way things are done, the style and values that underpin actions, the symbols and artifacts that are used to represent the organization, the stories and myths that are retold to reinforce intrinsic truths about the organization, and even the language that is adopted. It is as much about the informal structures—that is, the networks that employees and other stakeholders build and use—as it is about the formal structure. There may even be multiple subcultures among teams or ethnic groups or at particular locations that are distinct from the overall culture. The beliefs that people hold about the organization are valid even if they are based on inaccuracies or falsehoods. There is usually some truth in what people choose to think about an organization because this is how it appears to them.

Risk culture is very much a part of organizational culture. Risk management processes should reflect the same general way of doing things. However, risk management impacts the culture by making it more aware of the risks it faces, clearer about the levels of risk it is prepared to accept, more accountable for the risks that are integral to routine activity, and more open and transparent in discussing and reporting on risk. Just as the organizational culture may not be as management would like or claim it to be, the risk culture might sound better in theory than it is in reality. Culture generally is notoriously difficult to change, but it is important for management to maintain a realistic appraisal of it and commit to the kind of culture that it would like to see in place. This applies equally to risk culture.

I.A.3 Risk Capacity, Appetite, and Tolerance of Organization

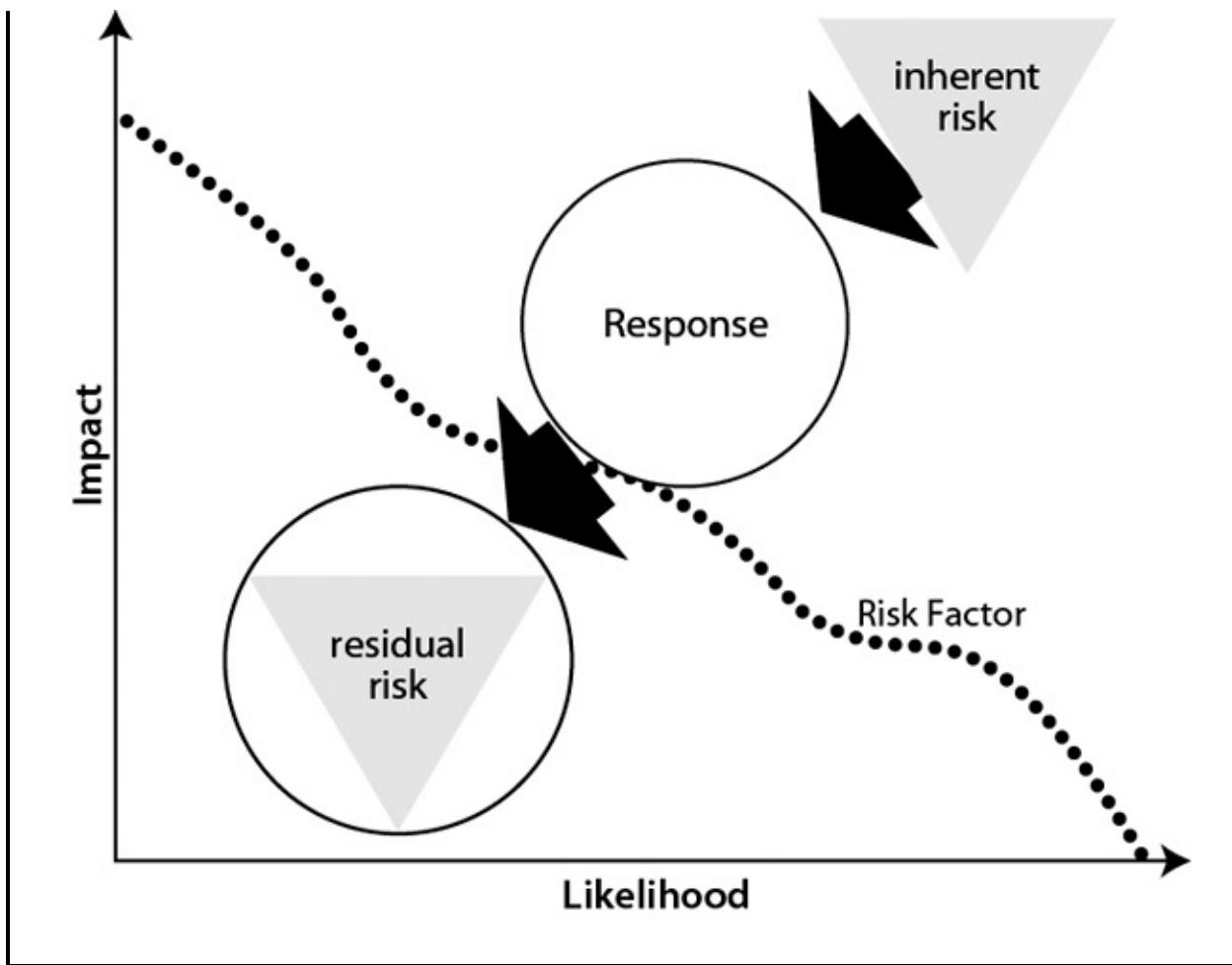
As has been stressed elsewhere, it is not the function of risk management always to minimize or eliminate risk. Risk is necessary and even desirable, as the uncertainties of future conditions and events are a source of opportunity. Risk management processes help the organization identify and assess current and emerging risks and opportunities. The board or equivalent body must determine how much risk the organization is able and prepared to accept or be exposed to.

KEY TERM

Risk appetite: The amount of risk an organization is prepared to accept or be exposed to.

The ability to accept risk is known as *risk capacity* and the preparedness to accept it is the *risk appetite*. There is no right risk appetite, and the board and senior management must make choices understanding the trade-offs of higher and lower risk. One major problem that led to the financial crisis in 2008 was that, although objectives had been created, there was no articulation of risk appetite or identification of those responsible when risks were incurred. *Risk tolerance* relates to risk appetite but differs in one fundamental way: risk tolerance represents the application of risk appetite to specific objectives. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that it will achieve its objectives. While risk appetite is broad, risk tolerance is tactical and operational. Risk tolerances guide operating units as they implement risk appetite within their individual sphere of operation.

Figure I.5. Response Manages Inherent Risk to Within Risk Appetite



Source: Chartered Institute of Internal Auditors, 2009. Reprinted with permission.

A complete risk management framework should assess a risk as both inherent and residual. An *inherent risk* represents the impact and likelihood of a risk event if no responses have been applied to manage the risk. *Residual risk*, meanwhile, is the impact and likelihood of a risk event after responses have been applied. In ISO 31000 residual risk is defined as “the risk remaining after risk treatment.” The difference between the inherent risk and the residual risk is the effect of the response. (See [Figure I.5](#).) The risk response may be designed to reduce the likelihood or impact, or both. Where quantitative methods are used to assess the risk, this effect can be stated as a number and known as the “response score” or “control score.” (This is discussed further in domain II. See II.B.3.)

KEY TERM

Inherent risk: The level of risk in the absence of any response.

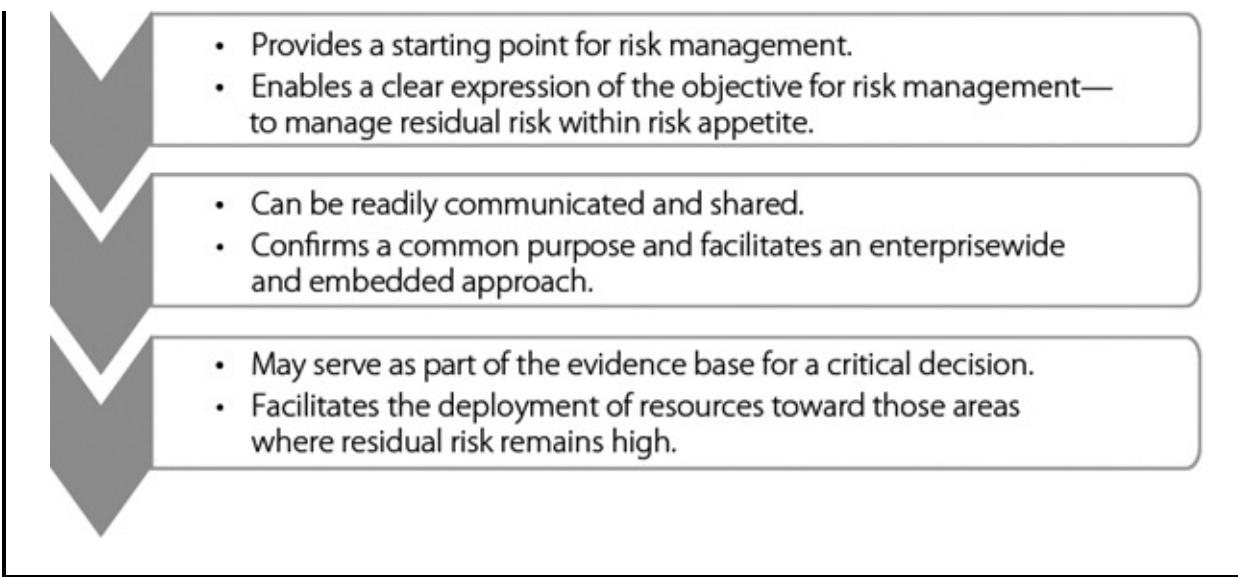
In a green-field situation, such as a new enterprise or a new project, it may be relatively easy to focus on the inherent risk because there are no existing responses in place. However, in an established organization that is introducing risk management for the first time, it can be difficult to disregard existing responses and focus on the underlying risk. For example, an inherent risk facing every economic entity is that the invoices received are wrong in some way. For example, they could be for goods or services not received or incorrectly priced. As a result, most organizations will have some existing accounting procedures that operate as responses so that the inherent risk is rarely, if ever, the prevailing risk. Similarly, manufacturing operations with an inherent risk that products will be produced in the wrong size or shape will have production control processes in response. Therefore, although it is very important to understand the inherent risk in order to develop and review the appropriateness of the response, the notion of what the risk would be like if there was no response is most often academic. (This is discussed further in domain II. See II.B.3.)

KEY TERM

Risk tolerance: Acceptable variance from risk appetite.

There are several reasons why it is important to define risk appetite. For one thing, it is a formal starting point for risk management. Without a clear expression of the willingness to tolerate risk, it is not possible to clarify the objectives of risk management processes. Once appetite is defined, we can say that risk management's role is to establish internal controls and other measures necessary to ensure that *residual risk* (or the level of risk remaining after the *inherent risk* has been mitigated by internal controls) falls within the risk appetite. In this way, measures of risk appetite can be used to determine the success of risk management processes.

Figure I.6. Benefits of Defining Risk Appetite



Risk appetite also can be readily communicated. Having a clear expression of the appetite makes it easier for members of the board, management teams, and staff to share a common view on acceptable risks. It also demonstrates how each separate part of the organization contributes to the overall risk management strategy. This shared understanding can then be embedded in planning and operational activities, leading to an overall culture that is more risk-aware and more risk-mature. Existing and potential investors want to know that risks are being managed, and will be able to compare their own risk appetite with that of the organization when it has been defined and communicated.

KEY TERM

Residual risk: The level of risk remaining after risk treatment.

Risk appetite may be expressed in general terms. For instance, we may say that one organization is risk averse while another is risk hungry. The appetite also may be expressed for particular types or classes of risk or even individual risks. In this case, it is appropriate to express appetite in the same form as the severity of the residual and inherent risks, as being a product of likelihood and impact or consequence. Sometimes these are assigned descriptive terms, such as moderate, medium, medium-high, and catastrophic. In other cases, the levels may be purely numerical. For example, if both likelihood and impact can be

assigned a value of 1, 2, or 3 (for low, medium, or high), then severity and appetite may take values of 1, 2, 3, 4, 6, or 9 (or low/low, low/medium, etc.). These values may then be readily compared.

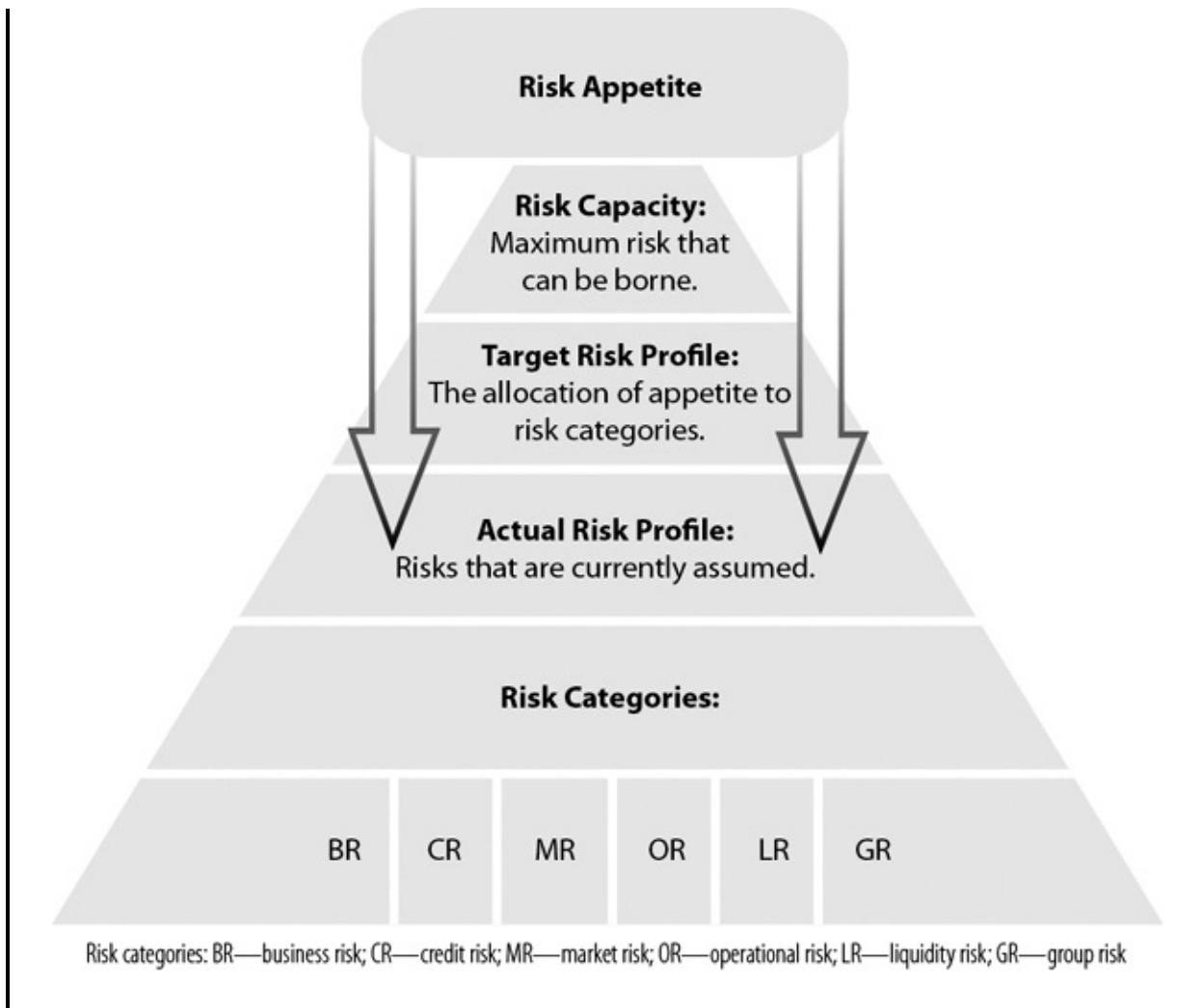
KEY TERM

Risk profile: The overall picture of risk across a range of categories.

As well as supporting decision-making, risk appetite can also be taken as part of the evidence base and a reference point for the future as the organization seeks to improve transparency and evaluate the effectiveness of decisions. More directly, risk appetite focuses the attention to areas in which residual risk remains above tolerable levels and may facilitate the allocation of additional resources to better control risk or exploit opportunities. In some cases, the risk may need to be removed altogether. A summary of the benefits of defining risk appetite are illustrated in [Figure I.6](#).

[Figure I.7](#) illustrates how *risk appetite*, in combination with *risk capacity* (the maximum risk the organization is able to bear, given its resources and capabilities), informs the target *risk profile* (the desired balance of risks across the defined risk categories or classification of risks). Finally, a comparison between the target profile and the actual profile identifies areas that require either further mitigation or some relaxation of controls.

Figure I.7. Approach to Risk Appetite (adapted from Barfield)



Risk categorization is part of the process of risk identification and analysis. These topics are covered in I.B.2 and II.B.3.

I.B Assess the Processes Related to the Elements of the Internal Environment in Which Organizations Seek to Manage Risks and Achieve Objectives

When assessing an organization's present position, it is useful to consider the internal and external environments separately. The *S* and *W* of the widely used SWOT analysis refer to *strengths* and *weaknesses*, and are features of the internal environment. The *O* and *T* are the *opportunities* and *threats* found in the external environment. SWOT is also a convenient way of reviewing potential

sources of risks and opportunities.

The two environments interact very strongly with each other. The internal environment is strongly influenced by the external environment. The supply of available skills in the labor market impacts human resources and payroll. The activities of marketing need to be informed by customer habits and changing social customs and norms. External events affecting suppliers can create difficulties for production. Similarly, the internal environment can influence the external environment, as we will see in I.C. However, organizations have greater and more direct power over their internal environment. Within the constraints of regulatory and legal requirements, ethical behavior, availability of capital and resources, and sheer practicality, managers may determine objectives and how to achieve them.

Choices around systems, processes, structure, communication, planning, and allocation of resources each represent a potential strength or weakness, as well a source of risks or opportunities. They also may form part of the risk response, including internal controls. Risk management processes need to fit in with the rest of the organization, and processes for identifying, analyzing, responding to, and reporting on risks are required to operate in such a way that they successfully manage risks across all elements of the internal environment.

In the sections that follow, we will consider each of the key components of the internal environment individually. However, it is important to recognize that they do not operate in isolation. Together, they form an integrated whole that we recognize as the organization. In fact, those separate dynamics are interrelated in such a way that it is hard to adjust one without impacting others. A famous description of this is made by the McKinsey 7S model, which lists seven interplaying dimensions. This is particularly useful as a tool for management when trying to bring about change. It also can serve as an indicator that risks and opportunities may arise not just within one area, but as a result of separate components working together.

In the 7S framework, the seven dimensions are described as *hard elements* that are readily grasped and manipulated by management, and *soft elements* that are much less tangible and more difficult to change. These are listed in [Figure I.8](#). For example, it is relatively easy to issue a new strategy or introduce a revised system. However, to make either of these things work requires

adjustments to other elements such as skills and shared values, which present a much greater challenge to manipulate.

The seven elements of the McKinsey 7S framework all interact, forming a connected mesh as shown in Figure I.9. The element of *shared values* is placed in the middle to emphasize the importance of collective goals and a common sense of purpose.

Figure I.8. McKinsey 7S Hard and Soft Elements

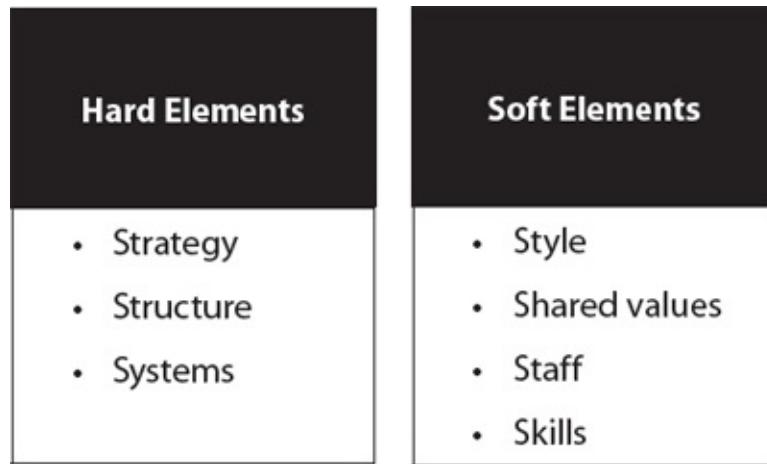
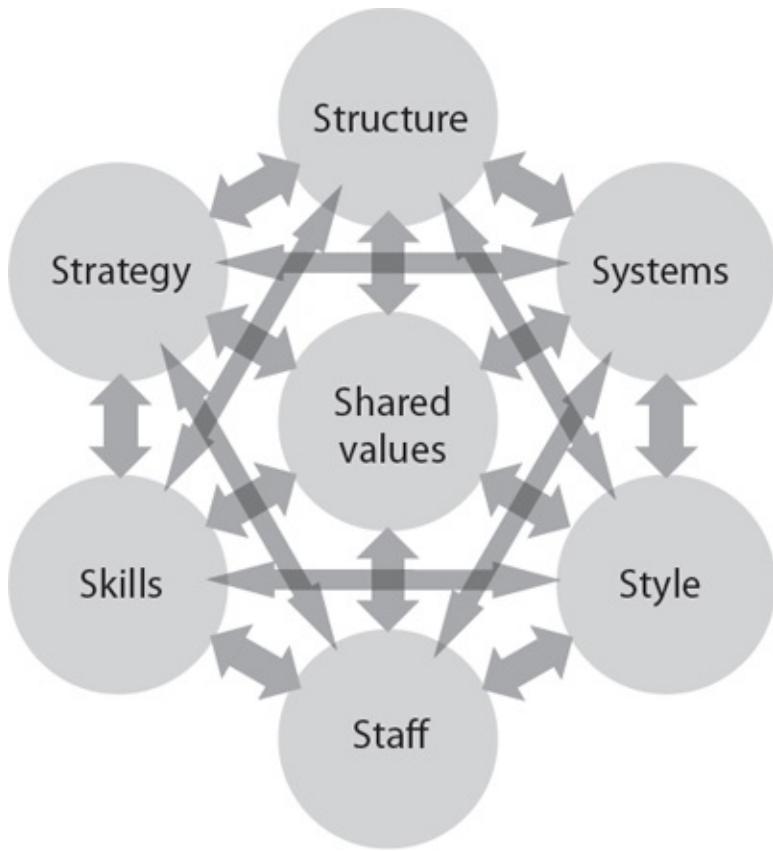


Figure I.9. McKinsey 7S Framework



One of the processes employed in risk management that seeks to analyze the internal environment is *root cause analysis*. This is an attempt to locate the underlying cause or causes of a given situation so that it will be better understood and the risk response can be more effective in the long term with corresponding improvements to business processes. According to IIA Practice Advisory 2320-2:

Without the performance of an effective root cause analysis and the appropriate remediation activities, an issue may have a higher probability to reoccur. Root cause analysis helps prevent additional rework and proactively addresses future recurrences of the issue(s). Root cause analysis may be considered in any number of situations, such as those involving a surprise risk event, process failure, asset damage or loss, production stoppage, safety incident, quality degradation, or customer dissatisfaction. It is important to recognize that there are often multiple related or unrelated causes of an issue. (IIA Practice Advisory 2320-2: Root Cause Analysis)

This further serves as a reminder of the interconnected nature of these features and how they may collectively contribute to a risk event, weakness, or failure.

I.B.1 Integrity, Ethical Values, and Other Soft Controls

Investors, shareholders, regulators, employees, and customers alike want to know what the organization stands for—its ethics, values, and intentions. They want to know that it can be trusted to do the right things in view of increasing concerns about—among other issues—bonuses, bribery, bullying, corruption, fraud, and failures in data security. As a consequence, boards are keenly interested in understanding and managing reputational risks stemming from unethical behavior at any level. All stakeholders want to know that management is responding to these risks to achieve common objectives for long-term value and sustainability. Stakeholders also need assurance that this message is understood throughout the organization and is driving appropriate behaviors. Assurance (the main focus of domain III), therefore, has a critical role to play in strengthening the culture of integrity by demonstrating top-level interest and commitment.

Organizations in many jurisdictions are required to comply with legislation designed to promote ethical conduct. Examples include the U.S. Sarbanes-Oxley Act of 2002, U.S. Federal Sentencing Guidelines of 2004, EU Accounts Modernization Directive of 2005, the UK Companies Act of 2007, and the UK Bribery Act of 2010.

Since the 1970s, the importance of corporate or business ethics has been strongly recognized, with increasing emphasis over the last 20 years. Some organizations have been able to establish their reputations around a concerted ethical position—such as the Body Shop—but this is no longer regarded as the province of just a minority. The expectations of stakeholders and the public at large are seemingly much higher and steadily growing. We expect honesty, transparency, decency, fairness, and respect from organizations and the individuals within them. Some elements may be required by law, but ethical behavior goes beyond this. With the heightened expectations of stakeholders has come the recognition, from all sides, of stakeholder power through whistleblowing, industrial action, political lobbying, and informing the media—all of which are made even more powerful through ready access to information and mass communication. Stakeholders are much more influential now than they

were in the past.

The string of corporate scandals that stretches back as far as you are prepared to look has heavily prompted the interest in integrity and ethical values. The public has been repeatedly shocked, disappointed, and angry as dishonesty, greed, self-interest, and a sense of entitlement and being above the law have been revealed at the highest levels of organizations they previously trusted. The risks associated with behavior that is—or is seen to be—unethical are considerable, threatening reputational damage and subsequent loss of confidence, trust, earnings, and jobs with the potential for total failure. Hence, measures or controls that can be taken to mitigate such behavior are an important part of the internal environment. More positively, there are also examples of organizations that have demonstrated moral integrity and gained a commercial or organizational advantage by demonstrating strong principles and ethical conduct.

Real integrity is sometimes hard to gauge. There is evidence that being seen as ethical can have reputational, financial, and competitive advantages. Whether the actions of individuals or organizations as a whole stem from genuinely held principles, legal requirements, peer pressure, the fear of being found out, or an assessment of the potential gains cannot readily be measured. Cynical adherence to a set of values, however, will be found wanting in the long term. It is likely that at some point there will be an apparent mismatch between what is said and what is actually done. Therefore, it is critical that organizations are clear about the importance of an authentic attempt to establish and maintain an ethical environment.

KEY TERM

Business ethics:

A set of moral principles applied to organizational activity.

What is meant by business ethics? The Institute of Business Ethics (2013) defines the term as:

The application of ethical values to business behavior. It applies to any and all aspects of business conduct, from boardroom strategies and how companies treat

their employees and suppliers to sales techniques and accounting practices. Ethics goes beyond the legal requirements for a company and are, therefore, about discretionary decisions and behavior guided by values. Business ethics are relevant both to the conduct of individuals and to the conduct of the organization as a whole.

It is clear that this definition applies equally to individuals and organizations. The development of the concepts of *corporate governance* and *corporate social responsibility* has a strong association with business ethics. Business ethics can be regarded as expressions of the personal integrity of the individuals that make up the organization and the desire to operate ethically at all levels.

If you explore the reasons why individuals act unethically, you'll find some interesting answers, such as:

- I didn't realize it was unethical.
- I didn't think I would be caught.
- I believed my employer sanctioned such behavior. (I was following the organizational culture.)
- Everyone else was doing it, why shouldn't I?
- I believed I was entitled to do it (because in some respects my employer treated me badly).

A set of moral principles applied to organizational activity.

- I believed the organization deserved it, as it was lax in preventing me.

A common control for unethical behavior is a set of espoused values and a code of ethical behavior. Many organizations define a set of values that they adhere to as an integral part of their strategic approach. The list is designed to help crystallize what the organization stands for and how it intends to operate. Ideally, the values should be easy to remember so that staff at all levels can refer to them when faced with an ethical dilemma. There is a danger that such statements by organizations can sound trite, merely stating the obvious (like motherhood and apple pie) that hardly needs mentioning. In any case,

organizational values, if they are to have a positive effect, should be relevant, clearly communicated, and refreshed from time to time.

KEY TERM

Code of ethics: Staff guidelines for instilling ethical behavior.

Ethical codes can be used as a means of fleshing out the values and providing more detailed guidance to staff on what is expected. Such codes can be adopted from elsewhere or produced for an individual organization. Professional bodies, such as The IIA, usually create codes to regulate the behavior of their members. Others are available for specific sectors.

According to the Ethics Resource Centre, in Carroll and Buchholt, 2008, codes of professional conduct or ethical behavior typically cover the following areas:

- Employment practices.
- Confidentiality relating to employee, client, and vendor information.
- Public information and communication.
- Conflicts of interest.
- Relationships with suppliers.
- Environmental issues.
- Political involvement.

KEY TERM

Values: Simple statements of what an organization stands for.

Closely related to these are policies on whistleblowing, anticorruption, human rights, environmental protection, and ethical investing. Taken as a whole, ethical values and codes of ethics or professional conduct alone will not guarantee that individuals and organizations behave with integrity. They are, at best, statements of intent to be regarded internally and externally as a declaration that the organization is serious about ethics. However, to gain any real benefit from such initiatives, it is necessary to supplement the values and codes with:

- Support for them at the highest levels of the organization.
- Clear and consistent communication relating to the values and codes.
- Integration of ethics into strategic planning and operational delivery.
- Staff training and development linked to ethical matters.
- Involvement of staff in the development and implementation of ethical frameworks.

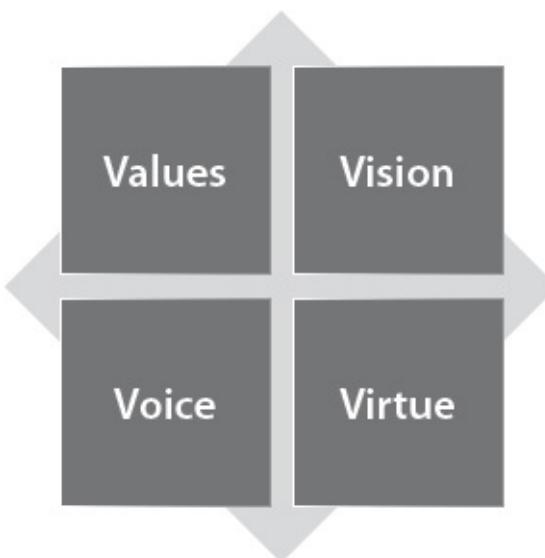
Above all, the values need to be shared, both in the sense of being communicated and of being held in common.

It is clear that risk management processes need to take into account ethical risks and the measures used for control. Codes of ethical behavior and organizational values play several important roles:

- First, they act as a way of describing what the organization regards as ethical behavior. They clarify the expectations the organization has of its staff and what external stakeholders can expect. They are intended to raise standards of behavior.
- Second, they can be a way of demonstrating ethical leadership from the top down. Unless there is a clear commitment from the boardroom, staff is unlikely to be convinced and may be less willing to comply. The 4-V model developed by the Centre for Ethical Leadership (2013) focuses on the importance of:
 - Values—Ethical leadership starts with personal conviction.

- Vision—It must be able to inspire others to adopt similar values.
 - Voice—Clear expression is required to communicate the vision and share the values.
 - Virtue—The important thing is that all of this has an impact that leads to a more virtuous way of thinking and behaving. (See Figure 1.10.)
- Third, codes and values should help resolve ethical dilemmas. In other words, they need to offer practical assistance by providing an answer to the question, “What should I do in this situation?” Sometimes this can be resolved by asking a number of questions about the considered course of action appealing to the individual’s personal integrity:
- Is it legal?
- Does it take a balanced account of the interests of all those affected?
- How will it look?
- How will it make me feel about myself? (See Peale and Blanchard, 1988.)

Figure I.10. The 4 V's Model of Ethical Leadership



A code of ethics (according to Schwartz, 2004) may be regarded as:

- A book of rules.
- A signpost.
- A mirror.
- A magnifying glass.
- A shield.
- A smoke detector.
- A fire alarm.
- A club.

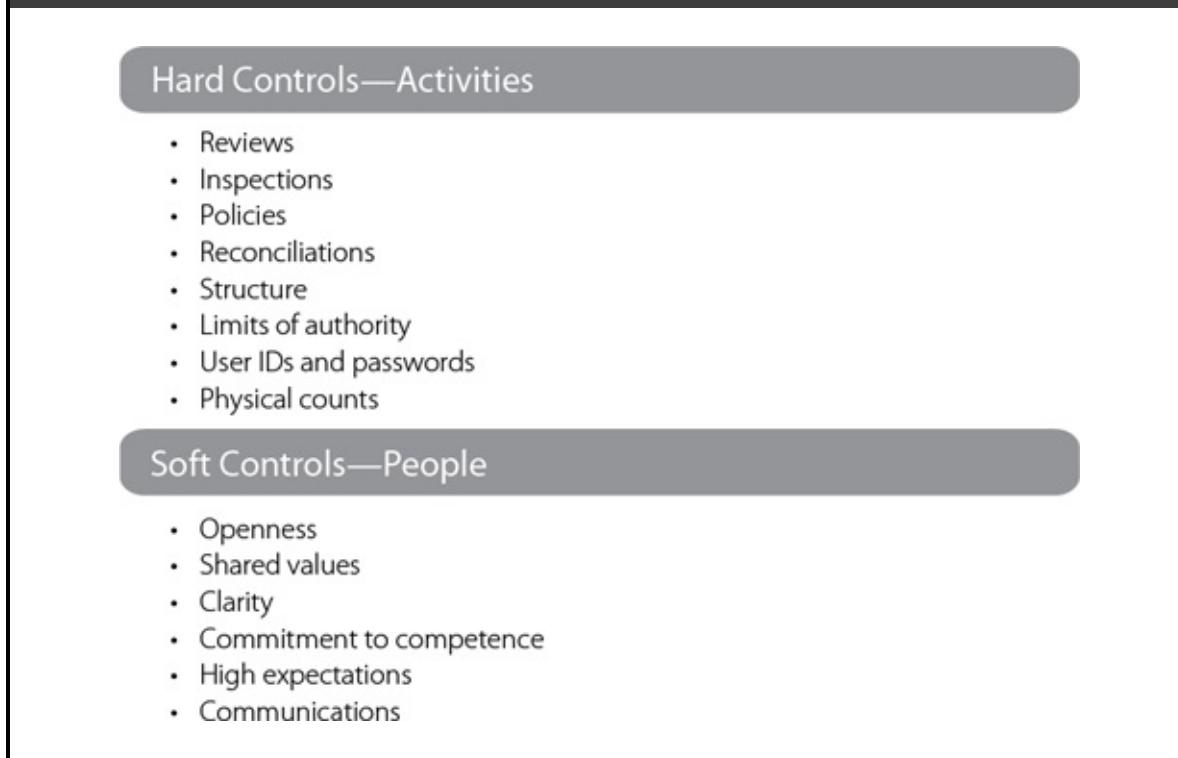
These metaphors reveal that the introduction of codes of ethics may be accompanied by feelings of fear, suspicion, or resentment. Therefore, management needs to be sensitive to the possible reactions and resistance that can be generated.

KEY TERM

Soft controls: Controls that rely on behavior and attitude.

Regarding internal controls as part of risk management that mitigates unethical behavior, we can follow COSO's distinction between soft and hard controls (see [Figure I.11](#)), which is similar to the distinction made by the McKinsey 7S model. (See [Figure I.8](#).) The *hard controls* are the ones that are relatively easy to introduce, monitor, and manage. They relate to policies, processes, and structure and include specific measures such as password protection, physical counts of stock, and bank reconciliations. *Soft controls*, on the other hand, relate to behavior and attitude. Both kinds of controls are important and work with each other to deliver overall control.

Figure I.11. COSO's *Internal Control – Integrated Framework*



I.B.2 Role, Authority, Responsibility, etc., for Risk Management

Because of its importance and analytical stance, risk management plays a *critical* role within the organization's structure and operations. The management team is responsible for running the business, which includes *risk management*, by identifying anything that might affect the success of the organization and taking action to mitigate threats and exploit opportunities. Ideally, all risk management actions and decisions will become embedded in the organization's normal direction and management, rather than operating as a separate process.

Since the financial crisis of 2008, there has been an ever greater emphasis on board responsibilities for overseeing an organization's risk management activities. For example, the corporate governance rules of both the New York and London stock exchanges require boards of listed companies to engage in regular and meaningful discussions about the nature and extent of the significant risks they are willing to take in achieving their strategic objectives. Similar responsibilities are placed on the boards of public sector organizations.

Requirements for improved corporate governance are clearly being driven by

risk and the need for its effective management. As Dr. Roger Barker, head of corporate governance at the Institute of Directors (IOD), said, “A board of directors is a legal requirement for any corporate enterprise. However, the justification for a board of directors in a modern quoted company owes more to considerations of risk than the need to comply with regulation or statute.” (IOD, 2012)

To some extent, the board can be seen as a direct response to a key risk posed by the structure of the organization, namely the risk that decision-making becomes dominated by insiders, particularly the chief executive and top management, whose interests are not necessarily aligned with those of stakeholders. A large number of corporate disasters over the last two decades highlight the saliency of this risk. The potential divergence of interests of the principal (the owners or stakeholders) and the agent (the board and managers) is the crux of the so-called *agency problem*, which finds its classic expression in Jensen and Meckling (1976). Corporate governance codes may be seen as an attempt to ensure the correct balance between responsibility and accountability.

It is important that there is clarity among the respective roles played by all those who contribute to the overall framework of risk management and control. According to The IIA:

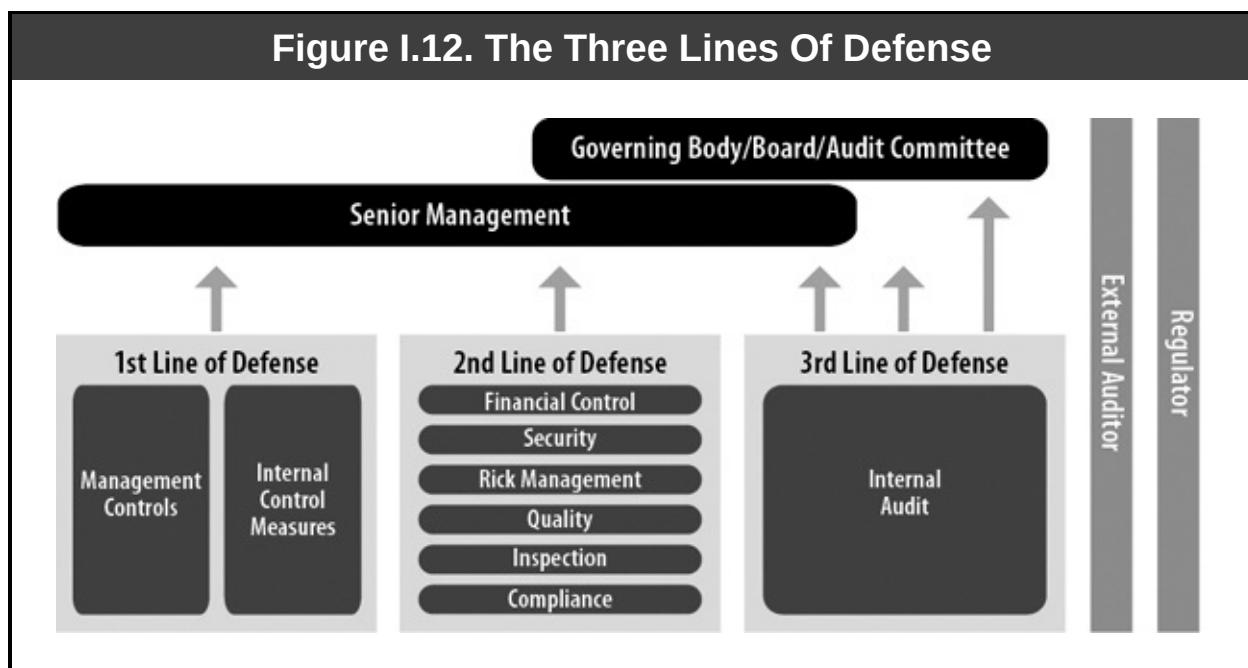
The board has overall responsibility for ensuring that risks are managed. In practice, the board will delegate the operation of the risk management framework to the management team, who will be responsible for completing the activities below. There may be a separate function that coordinates and project manages these activities and brings to bear specialist skills and knowledge. Everyone in the organization plays a role in ensuring successful enterprisewide risk management, but the primary responsibility for identifying risks and managing them lies with management. (IIA Position Paper, The Role of Internal Auditing in Enterprise Risk Management, 2009)

The picture is potentially very confusing as there may be a number of different groups acting both internally and externally in support of closely related organizational objectives, including:

- Senior management.

- Risk managers.
- Business unit managers with risk management responsibility.
- Compliance officers.
- Fraud specialists.
- Quality inspectors.
- Internal auditors.
- Consultants.

Overlaps and gaps need to be avoided and activities should be carefully coordinated to avoid deficiencies and inefficiencies.



Source: The Institute of Internal Auditors, 2013. Reprinted with permission.

The purpose of this model is to define and keep distinct the roles and responsibilities of each line of defense (see [Figure I.12](#)). The first line is operational management control, the second is the risk and compliance oversight functions, and the third is the independent assurance provided by internal audit.

While senior management and the governing body (the board) are outside the three lines of defense, they play essential roles as primary stakeholders and those best placed to ensure the three lines model is operating effectively. The respective roles are illustrated in [Figure I.13](#). Other bodies outside the organization (notably the external auditors and regulators) provide additional support to control, especially in regulated industries such as financial services.

Figure I.13. Roles of the Three Lines of Defense			
Primary Stakeholders	First Line	Second Line	Third Line
Senior management and governance body: To ensure the three lines of defense model is operational and effective	Operational management: To own and manage risks	Risk management and compliance functions: To provide risk oversight	Internal auditors: To provide independent assurance.

Although it is not the job of the directors to manage risk activities, they do set the tone at the top through their commitment to risk management and to overseeing what management has designed and implemented to manage top risk exposures. It is the board's responsibility to ensure that management is devoting the right level of attention and sufficient resources to risk management. What is more, the board should be comfortable that management has put in place an effective risk leader who is widely respected across the organization and who has accepted responsibility for overall leadership, resources, and support to accomplish the effort. The board of directors and senior management must work together to ensure the appropriate focus, resources, and activities are in place for effective risk management.

The board of directors exists as a distinct layer of governance, sandwiched between management and the organization's stakeholders. In most countries, corporate governance codes or regulations stipulate that a majority of board members should be independent, non-executive directors. In addition, it is

increasingly seen as best practice for the board to be chaired by someone independent of the organization.

KEY TERM

Autocratic: A highly centralized style with little or no consultation.

One of the board's most important contributions to effective risk management is likely to be its choice of chief executive. If the wrong person is appointed to lead the organization, all of the board's subsequent efforts toward effective risk management will be severely compromised. A second basic issue for the board involves defining the nature and extent of the risks that the organization is willing to take. This is not just a question of listing activities that should be undertaken or avoided. It is also about defining an attitude to risk, part of the process of establishing the risk culture, as discussed in I.A.3.

I.B.3 Management's Philosophy and Operating Style

The operating style and philosophy of management are often characterized by the phrase *tone at the top*. The example set by the upper levels of an organization will be mirrored throughout as an expression of and a contributor to organizational culture. Employees will mimic good behavior or alternatively behave badly as a justification for their own misdeeds.

It can be said that the tone at the top sets the tune to which the rest of the organization dances. It is not enough for managers to expect staff to *do as I say, not as I do*, but they must, instead, lead by example. For insight into the importance of leadership, consider how risk management operates in extreme environments such as waging a war. Strategy, planning, training, rehearsal, and operational excellence are vital. This is equally true in business, but unless the chief executive and senior managers display the same understanding of how to lead hearts and minds, they will fail, in spite of how good the risk management processes and systems might be.

KEY TERM

Laissez-faire: A “hands-off” style with little or no intervention.

The importance of character was revealed by, among others, the *Walker Review*, regarding the corporate governance of banks following the 2008 banking crisis. For the first time, the character of bank directors and senior managers was identified as a major factor. The review concluded that the fundamental failure of governance that precipitated the banking crisis was not caused by a lack of understanding of financial risk. Instead, it was caused by failures of personal integrity, responsibility, and judgment. (Walker, 2009)

There are many ways of characterizing the style and philosophy that management adopts. One way is to consider the approach taken to decision-making. An *autocratic* style is one with little or no consultation, while power and control are held centrally. By contrast, a *democratic* style is more inclusive, taking account of the views and inputs of others and including them in some form of collective responsibility. When the style is *laissez-faire* (from the French, meaning to let happen), power is highly decentralized. Things are allowed to run their course with only limited intervention from management.

KEY TERM

Democratic: Highly decentralized style with plenty of consultation.

None of these styles can be said to be better than the others, as it very much depends upon circumstances. With new staff having limited experience or where rapid change is required, an autocratic style may be appropriate. A democratic style can be adopted when there is more time and staff can contribute their ideas. Laissez-faire works when routines are very settled and staff members are highly experienced.

A well-known model used to analyze the style of management is Blake and Mouton’s managerial grid, which organizes management styles along two axes—concern for people and concern for tasks. (See [Figure I.14](#) and [Figure I.15](#).)

Figure I.14. Blake and Mouton's Managerial Grid (1964, in Boddy, 2011)

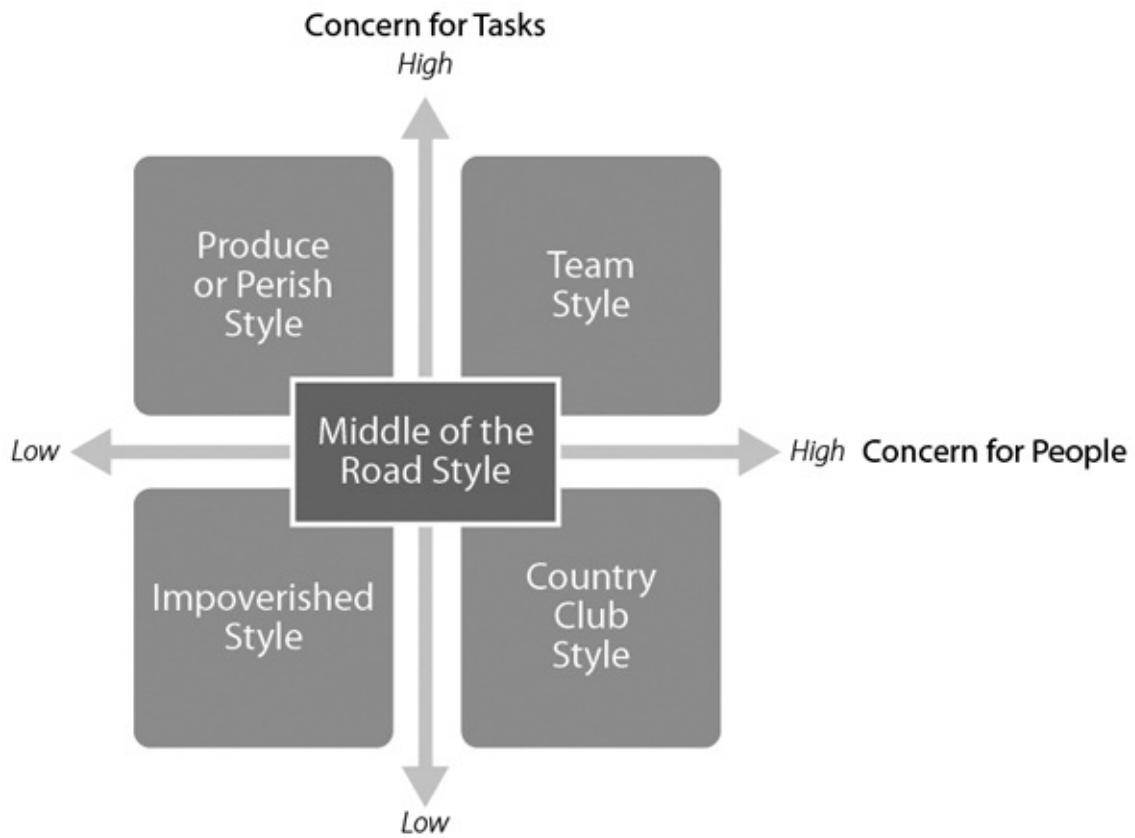


Figure I.15. Blake and Mouton's Managerial Styles

Team Style

- A high focus on both people and tasks.
- Participative and proactive leadership style.

Produce or Perish Style

- A high focus on tasks, but less on people.
- Performance is the primary focus.
- Management tends to be formal and authoritative.

Country Club Style

- High concern for people, but less for tasks.
- Democratic and inclusive.

Impoverished Style

- Limited focus on either tasks or people.
- Very laissez-faire "hands off" approach.

Middle of the Road Style

- A balanced view of tasks and people.

An important part of the philosophy of management is its approach toward employees. It is commonly said that people (or at least the right people) are the most valuable resource that an organization possesses and certainly one of the most expensive. It is not surprising, therefore, that management seeks to gain maximum value from the deployment of human resources. The methods adopted are often very revealing about management attitudes.

Individuals gain three main types of reward from working:

- Financial rewards (in the form of wages, salaries, bonuses, contributions to pension schemes, etc.).
- Nonfinancial rewards, fringe benefits, or perks (such as staff development, flextime, health insurance, paid leave, etc.).
- Psychological and social rewards (through status, networking,

recognition, acceptance, and friendship groups).

The great philanthropists of the nineteenth and twentieth centuries recognized that these rewards were intrinsically good and provided better working conditions, longer breaks, housing, and other perks out of a sense of moral duty. Undoubtedly, recognition of the importance of such rewards can be used to increase motivation and improve performance. Simply paying people higher wages in the long term is not usually enough. More effective compensation systems combine a variety of motivators.

A simple difference of approach that management may take regarding motivation can be described with reference to McGregor's well-known Theory X, Theory Y model. A Theory X manager makes the following assumptions about a subordinate's attitude toward work:

- Most people are naturally lazy.
- Most people are primarily motivated by money.
- Most people would choose not to work if they did not need to and will do the minimum necessary to get paid.
- Most people need to be monitored and directed in order to keep them working, and they prefer being managed to taking responsibility.
- The way to maximize performance is through a system of close supervision, coercion, rewards, and punishments.

On the other hand, a Theory Y manager is much more open to diverse motivational strategies that prompt individuals to perform well and are characterized by the following assumptions:

- Most people enjoy working.
- Most people want to learn and develop their skills.
- Most people welcome responsibility.
- Most people are willing to apply their skills toward achievement of group

or organizational goals.

- The way to maximize performance is to develop individuals, give them more responsibility, and give them the opportunity to contribute toward corporate objectives.

McGregor argued in favor of the more enlightened Theory Y approach as being both morally preferable and more effective in long-term practice. We can draw a parallel with soft and hard controls. To mitigate the perceived risk of under-performance by subordinates, a Theory X approach depends almost exclusively on hard controls. Theory Y, however, makes much greater use of soft ones. (See I.B.1.)

I.B.4 Legal/Organizational Structure

Organizations usually start small and grow and develop over time. Periodically, it is necessary to question whether the resources of the organization are arranged in such a way as to maximize the achievement of strategic objectives. As objectives change and as features in the external and internal environments change, structural adjustments may be required to maintain the optimal arrangement of the various blocks of activity. At some point, this may require increasing or reducing the headcount of staff; consolidating or expanding; redefining teams, departments, and business units; or even adopting a different legal form. Structural changes may be brought about organically over time or through step changes in the form of restructuring. After a merger or acquisition, it is likely that some form of redistribution of internal resources will be required.

The characteristics of an organization can be understood as responses to the external environment. This is particularly apparent in the way it structures itself.

Structures should be designed to reduce risk and exploit opportunities. In this sense, they are a kind of risk response, but they also introduce their own set of risks.

Because structure may be seen as an expression of both strategy and culture, these features certainly need to be aligned. For example, an organization may declare democracy in its values but demonstrate otherwise in the way it makes

decisions, which in turn depends heavily on structure. Similarly, where strategy dictates the need for agility and responsiveness to changes in the external environment, the physical structure is what makes that possible or not.

According to Turner and Nicholson (2012), a number of questions should be considered when deciding on an appropriate structure:

- What kind of culture does the organization want to create or maintain?
- What are the strategic objectives that the organization wishes to achieve?
- What will be the most effective way of assigning the tasks necessary to accomplish those objectives across the organization?
- What is the best way of arranging the resources and staff around those objectives and tasks?
- For maximum clarity, efficiency, and effectiveness, what subdivisions of the structure are required (units, divisions, departments)?
- How can these subdivisions integrate their activities *where it counts* to ensure a coherent organization?
- How does the organization need to communicate internally and externally?
- Where do the lines of accountability and responsibility need to be drawn?

One of the most influential thinkers on organizational structure is Max Weber. Drawing upon his 1925 *Theory of Social and Economic Organization* and similar works, many subsequent writers have sought to define the different dimensions of organizations to be able to analyze them more effectively. Hatch (2006), for example, outlines a number of features.

Figure I.16. Dimensions of Organizational Structures

Size as measured by employees, capital, turnover, or production	Management and administration (line and staff functions)	Horizontal differentiation - divisions in roles across levels
Vertical differentiation - the number of levels of hierarchy	Integration among segments of the organization	Centralization/decentralization of decision-making and power
Standardization of procedures	Formalization of documentation (bureaucracy)	Specialization of individuals and teams

There are a number of ways in which an organization may be subdivided. For example, Boddy (2011) highlights five common approaches:

- *Functions* separate the different discrete and focused areas of activity (such as finance, marketing, production, research and development, human resources, etc.).
- The creation of *divisions* uses features such as product lines, geographical regions, or customer types as the basis for organizing activity and resources.
- In *matrix* structures, staff and other resources are line-managed vertically, but organized in cross-organizational teams for specific projects or on a permanent basis.
- Other kinds of *teams* can be created within structures to give activities a particular focus and staff a sense of belonging.
- *Networks* are an increasingly common feature of endeavor, joining together organizations in pursuit of common objectives for mutual gain.

Organizational structures are commonly illustrated in charts or organograms. These visually represent levels of hierarchy, main divisions, lines of authority, communication (up and down the organization), and the span of managerial control (the number of people under direct line management). (See [Figure I.16](#) and [Table I.2](#).)

Table I.2. Organizational Structure Comparisons		
Tall/Hierarchical Structure		
Features	Benefits	Potential Risks
<ul style="list-style-type: none"> • Many layers of hierarchy. • High vertical differentiation and high degrees of vertical specialization. • Long lines of communication. • Smaller spans of control. • Tend to be autocratic with high degrees of formalization and standardization. • Centralized control. 	<ul style="list-style-type: none"> • Closer monitoring of teams possible by managers. • Clear and easily understood structure. • Employees “know their place.” • Clear demarcation of roles and responsibilities by teams and individuals. • Clear routes for career development and promotion. 	<ul style="list-style-type: none"> • Employees may feel more restricted and less likely to develop independent skills. • Low innovation likely. • Communication and decision-making can be slow, as chains of command are long. • Higher numbers of managers and higher salary costs (financial risk). • Not responsive to changes in the external environment. • High reliance on few key individuals.
Flat Structure		

Features	Benefits	Potential Risks
<ul style="list-style-type: none"> • Fewer levels of hierarchy. • Low vertical differentiation. • Shorter lines of communication. • Wider spans of control. • Greater horizontal integration. • Greater decentralization. 	<ul style="list-style-type: none"> • Greater personal autonomy and motivation. • Greater cooperation and collaboration. • Shorter chains of command. • Quicker communication and decision-making. • More responsive to changes in the external environment. 	<ul style="list-style-type: none"> • Fewer opportunities for promotion and so potential for higher staff turnover. • Management is more remote with larger teams and lighter touch with the potential for performance issues.

Matrix Structure

Features	Benefits	Potential Risks
<ul style="list-style-type: none"> • Comprising related cross-functional and cross-hierarchical teams. • High decentralization. • High degrees of individual autonomy. 	<ul style="list-style-type: none"> • Very flexible and responsive to external changes. • Can be very motivating for individuals and teams, leading to greater productivity. 	<ul style="list-style-type: none"> • Can be very disorienting for individuals familiar with more traditional structures. • Requires careful management to ensure operational effectiveness.

Risk management processes need to be accommodated within the organizational structures and will be subject to the same potential risks and benefits. One of the options for introducing greater flexibility in any given structure is *delegation*. Managers may pass the responsibility for completing a task to a subordinate, while retaining the overall responsibility for it being completed. This has various potential benefits:

- Staff can be motivated by taking on more responsibility.
- The manager may be freed up to complete other tasks.
- Subordinates will increase knowledge and experience, thus providing for succession planning.

KEY TERM

Delegation: The passing of authority but not the responsibility for certain tasks to a subordinate.

However, there are also potential risks with delegation:

- Staff members may feel they are being “dumped on” if it is not done properly.
- The tasks may be passed to someone who does not have the skills to complete them.
- Lines of responsibility may become blurred, making performance management more of an issue.

New structures are enabled by IT and globalization. Increasingly, organizations are networked with others to create larger virtual entities that are joined together for specific tasks with common goals and complementary resources. Modern forms can be organic, dynamic, and less likely to have boundaries.

The types of legal forms available for organizations depend on the particular

economy, culture, and regulatory framework of the country. (See [Figure I.17](#).)

Figure I.17. Differences in Legal Forms of Organizations

Ownership

Ranging from a single person or sole trader to multiple partners or shareholders (as in the case of public sector organizations, the public holds ownership), the organization is held and managed on its behalf by government and its appointed agents.

Organizational Control

It may be directly by the owners (the principals), but in many cases, especially larger organizations, limited liability companies, and public sector bodies, there may be no direct involvement of the owners, and control is maintained by directors and senior managers (agents).

Governance Arrangements

With the separation of ownership and management, there is a need for oversight, transparency, accountability, monitoring, reporting, and other measures to ensure that respective interests remain aligned. (For more on governance, see I.B.5.)

Available Sources of Finance

Organizations need capital (the financial investment made by owners and investors), as well as a supply of cash for ordinary operations.

Liability for Losses

In general, the owners of an organization share in the profits and in the responsibility for losses, but in the case of limited liability organizations, the limit of the responsibility to cover debts is the amount invested (capital), and the creditors of a company cannot call upon the personal assets of shareholders.

Reporting Requirements

These are linked to governance and ensure that the owners and investors, as well as other stakeholders, have access to consistent, reliable, and timely data.

Taxation and Other Financial Obligations

Governments require organizations to pay taxes on their profits and administer pay and other benefits in accordance with the law.

Other Forms of Regulation and Oversight

These may be general (health and safety, data protection) or specific to particular industries.

There is a broad distinction between *public sector organizations* (held in common and controlled on behalf of the people by government and their appointed agents to provide a socially desirable service) and *private sector organizations* (owned by one or more individuals for the purpose of making a profit). There is also a *third or charitable sector* (bodies that operate in the service of specific or general causes but are not part of the public sector). A legal form gives an organization an identity and certain privileges under the law but also brings with it various duties and legal obligations. As with structure, the right legal form for an organization depends upon its size, objectives, culture, capabilities, and competitive environment.

KEY TERM

Private sector: Organizations owned privately primarily for profit.

I.B.5 Documentation of Governance-related Decision-making

Corporate governance arrangements exist to ensure that organizations are properly managed. Management is appointed by the owners to operate the organization on their behalf and governance is necessary to ensure that things operate according to the interests of the owners. As stated in Nicholson and Turner (2010), “There is a natural asymmetry between the principal and agent in terms of information, skills, influence, and motivation.” In other words, managers are in a privileged position and could readily exploit this without the moderating influence of governance.

KEY TERM

Public sector: Organizations held by the state for public service.

To safeguard the interests of the owners and other stakeholders, the governance structure needs to provide oversight of strategy implementation while steering clear of making executive decisions and impinging on the role of the senior managers. This usually involves the participation of independent, non-

executive directors as part of the board. The requirements for governance are specified in some detail for companies—especially those that may be listed on the stock exchange—through a combination of governance codes and legislation.

Keys to effective governance include integrity, transparency, and accountability. The aim is to ensure that interested parties (stakeholders) remain clear about important decisions through openness and sharing information, while those in executive control are held accountable for their actions. Above all, there should be a prevailing attitude of honesty. According to the UK Department of Business Innovation and Skills (2013), requirements to achieve this include:

- Timely, high-quality information provided by the organization.
- A clear and credible decision-making process in the organization.
- Stakeholders giving proper consideration to the information provided and making considered judgments.

There is strong linkage among governance, decision-making, and documented information. Because it contributes to openness, documentation plays an important role in governance. In fact, documentation serves a number of different purposes:

- It provides information that can support an activity's decision-making, planning, analysis, and data input.
- It provides a historical record that can be used for reference purposes in the future.
- It contributes to openness and transparency in that the documentation is available for public scrutiny.
- It provides an audit trail for regulators and investigators to reconstruct the past.
- It defines authorities and responsibilities to enable accountability.

Governance operates generally by a combination of internal and external mechanisms. Internal governance mechanisms include:

- A governing body.
- Balance of power.
- Risk management.
- Internal auditing.
- Rewards and remuneration.

An organization's main oversight or governing body is its board of directors. The role of the board is to approve strategy and appoint the most senior executives, including the CEO. The board often has subcommittees, including the audit committee (or audit and risk committee), remuneration committee, and nominations committee. In most jurisdictions, the board of a listed company is required to include non-executive directors who are independent and provide a counterbalance to the views of the executive. Non-executive directors are at a disadvantage in that, because they are not employed full-time by the organization, their knowledge and expertise in daily matters is considerably less than that of senior management. The need for information is critical to ensure that non-executive members know what they must know in order to make effective decisions.

An appropriate balance of power is often maintained by ensuring that the chair of the board is not also the CEO. This practice limits the amount of power any one individual can wield.

Decision-making is an intrinsic part of management and governance. Each situation yields a variety of options that are mutually exclusive. Resources are scarce, time is finite, choices must be made at every turn, and future options are dependent on previous decisions. Even deciding to do nothing is a decision and closes off other options.

Documentation is necessary to foster transparency and support effective decision-making. Key documentation is likely to include minutes of board meetings and its various subcommittees, roles and responsibilities, policies and procedures, financial statements, internal audit reports, management accounts, other kinds of performance monitoring, compliance records, and the external

auditors' reports.

To enable effective decision-making (rather than random guessing), it is necessary to have a certain amount of information that is:

- Relevant.
- Timely.
- Accurate.
- Usable.
- Detailed.

In familiar and uncomplicated situations, decisions can usually be made fairly rapidly, especially when the outcome is not critical. Greater analysis and care are needed when there is no comparable situation from the past and the issues are complex. The decision-making process can be broken down into a number of discrete steps. (See [Figure I.18](#).)

Figure I.18. The Decision-making Process



A number of simple techniques are commonly used to assist the decision-making process, including those illustrated in [Table I.3](#).

Table I.3. Effective Decision-making	
<i>Five Whys</i>	This is a very simple method that repeatedly asks the question, “Why?” This leads to the root of a problem for easier decision-making. Parents of young children will be familiar with this technique.
<i>Chunking</i>	Often, it is useful to break a problem down into manageable chunks that can be more easily analyzed. A series of decisions may be required before an overall solution is reached.
	Drilling down to progressively more detailed levels can support decision-making. In essence, the issue is repeatedly analyzed at a greater degree of detail. This can be completed using a table with a number of

<i>Drill-down Technique</i>	columns, each of which breaks down a portion into its constituent components. Revealing sufficient detail facilitates a clear basis on which to make the required decisions. This also can be achieved using a spider diagram or flowchart.
<i>Cause and Effect</i>	Resembling a fish skeleton, the cause and effect diagram can be used after a problem has been analyzed into its constituent parts. The process seeks to find how the parts are interconnected as a series of causes and effects, thus increasing our understanding of relationships and enabling effective decision-making about actions needed to achieve the desired outcome.
<i>Decision Trees</i>	Decision trees weigh the relative likelihood and value of each possible decision. Sometimes there are chains of choices with multiple branches of subsequent choices. Each of the main branches can be assigned a cumulative value, so the option with the greatest potential value (or least potential loss) can be chosen.
<i>Cost Benefit Analysis</i>	Cost benefit analysis considers both the internal and external costs and benefits to produce a rounded picture. The internal costs and benefits relate to those enjoyed and incurred by the organization, while the external view takes into account the impact on external stakeholders and the public at large. A simple two-column, two-row table can be used to itemize all costs and benefits internally and externally so the totals can be compared. This assumes that all of these dimensions can be assigned a numerical figure, which is not always the case.
<i>Systems Diagrams</i>	Systems diagrams offer a very sophisticated analysis of how all relevant factors are interrelated. It helps with the decision-making process because it reveals the likely impact of changes to any part of the system. Within the system there may be feedback loops, balancing loops,

	<p>and reinforcing loops to consider, as well as gaps, delays, and the impact of and influence on external factors.</p>
<i>80-20 Rule</i>	<p>Pareto analysis takes advantage of a commonly observed asymmetrical effect. For example, roughly 80 percent of the world's resources are owned by 20 percent of its population. This ready approximation can help with initial analysis. We may make a rough assumption, for instance, that 80 percent of our customer inquiries are handled by 20 percent of the resources applied. The remaining 20 percent is far more complex and time-consuming and requires 80 percent of the resources. In trying to decide where to apply our limited resources, the 80-20 rule may help us maximize the impact by focusing on the 80 percent of things we can more readily change.</p>
<i>Force Field Analysis</i>	<p>There are forces in support of and in opposition to virtually any decision made. The positive benefits—willing acceptance among those affected and expected financial gains, for example—push in favor of the decision. On the other hand, the increased work required, the changes needed to systems, the resistance anticipated among some people, and the costs involved pull in the opposite direction. Force field analysis weighs these opposing forces and depicts arrows of different lengths, depending on their force and direction, either for or against the decision. This analysis helps to determine whether there is more value in moving one way or the other.</p>
<i>Paired Comparison</i>	<p>Paired comparison analysis methodically compares each of the alternative options against every other to determine which is preferable and by what factor. For instance, in determining the best way to fill a temporary shortfall of skills on a particular team, we may choose among appointing a temp, drafting someone from another team, or training an existing team member. We</p>

<i>Analysis</i>	may decide that the temp option is better than training by a factor of two, and better than seconding by a factor of three. Although this is not scientific, it does enable us to prioritize options systematically and reveal the preferred choice.
<i>Grid Analysis</i>	Grid analysis is a more sophisticated version of paired comparison analysis. Rather than attributing a single value to a preferred option, grid analysis takes into account all of the relevant factors in turn. To continue the previous example, relevant factors may include cost, time, impact on the team, and impact on other activities. Every available option can be scored against each of these factors. The other feature of grid analysis is to weigh the relative importance of each of these factors. The time constraints might be the overriding factor, with costs as secondary. The relative weighting can be expressed numerically with each of the elements multiplied accordingly to determine an overall value for each option. The one with the highest value indicates that it is the most appropriate choice.
<i>Thinking Hats</i>	Edward de Bono devised a famous scheme for helping teams come to a conclusion when faced with a difficult decision. One of the difficulties experienced in group discussions is that individuals focus on different aspects of a situation, making it hard to come to a consensus. In this model, team members are invited to move through six thinking modes together to ensure a collective and comprehensive approach. Starting with the red hat, participants are invited to give their purely emotional response, such as "I like it" or "I don't like it." Then, moving to a yellow hat, everyone considers all the positives associated with the proposal. Next, in the black hat mode, they review all of the negatives. The white hat is for logical assessment and the green hat is for creativity. Finally, the blue hat is worn by the chair of the meeting to keep focus and to summarize the exercise.

Moving through a problem in this constructed fashion makes it easier to get all of the salient responses out on the table and requires everyone to think about it from all points of view.

It is important to remember that such methods do not negate the need for gut reaction, experience, and instinct. Any technique for decision-making should be moderated by both qualitative and subjective measures, rather than being blinded by purely mechanistic processing alone.

Often, there is pressure for a quick decision. This may be driven by the desire to hit targets and maximize results, the need to report progress, or a reaction to an unexpected event. Some managers may believe that making decisions quickly is a sign of authority and being in control as part of an autocratic style. (See I.B.3.) Sometimes this is the right thing to do, when timescales are short and there is a limited amount of available information. Managers get paid to make difficult decisions and to be accountable for the outcomes. For the long term, however, knee-jerk reactions may result in arbitrary decisions and poor outcomes—perhaps requiring additional costs to put matters right. Therefore, in general, it is good practice to base decisions on sound evidence, careful analysis, and a methodical process. A more democratic approach draws upon multiple perspectives and garners support for the ultimate decision.

ISO 31000 states that risk management should be part of an organization's decision-making process. What is more, it facilitates better decision-making. Risk management helps decision-makers make informed choices, prioritize actions, and distinguish among alternative courses of action. Using risk management in decisionmaking allows others to be involved in the process and reaps the benefit of a greater spread of experience and insight, as well as greater support for the decision.

For example, there is a world of difference between calculated risks taken with foresight and judgment and risks taken carelessly. The identification and analysis of risk can have a major influence on the decision to launch a new product line, when to launch it, which markets to develop, the level and focus of investment in marketing, and after-sales. This will all be done within the boundaries of the organization's risk appetite to maximize reward and minimize

potential losses.

I.B.6 Capabilities, in Terms of People and Other Resources (e.g., Capital, Time, Processes, Systems, and Technologies)

The competencies or capabilities of an organization are the activities that it is equipped to undertake. From individuals they include skills, knowledge, experience, networks, and personal qualities; and from the rest of the organization they include resources, processes, networks, reputation, and goodwill. The *core capabilities* (following a distinction made by Henry, 2007) enable an organization to deliver its products and services to customers at a price they are prepared to pay, gaining access to key markets and making it hard for others to imitate. *Distinctive capabilities* give an organization its unique selling point and make the greatest contribution to its competitive advantage when compared with its closest rival. Public sector organizations may be said to have organizational (rather than competitive) advantage derived from their core capabilities in a similar way.

KEY TERM

Capabilities: Activities an organization is equipped to undertake due to its resources.

According to Boddy (2011), an organization's core capabilities arise from:

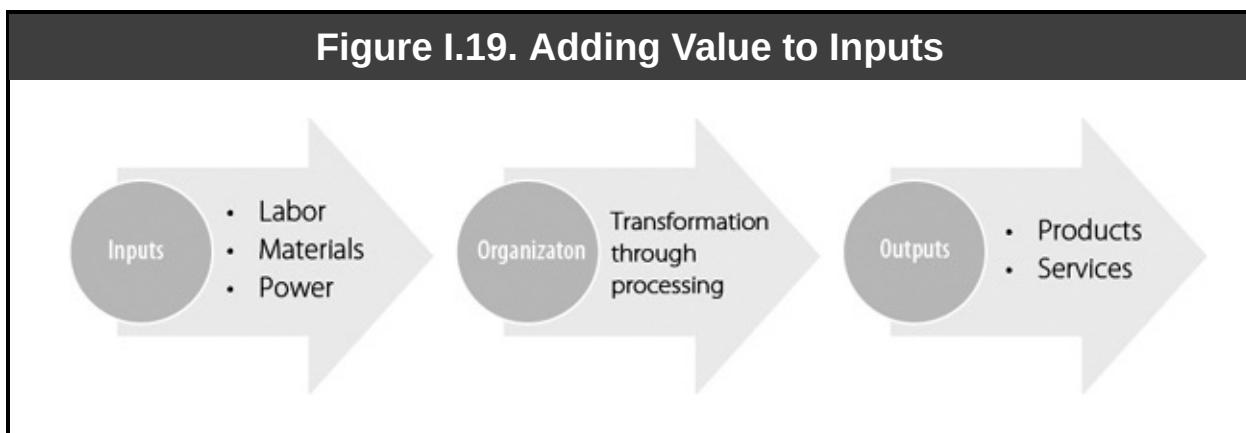
- Its unique range of products and services.
- Its resources (human, physical, financial, and intangible).
- Its processes.

We can analyze the capabilities further by considering the assets of the organization that cover both tangible and intangible items. The following list is taken from Hooley et al. (1988, in Drummond et al. 2001):

- Financial.

- Physical.
- Operational (including equipment, processes, and know-how).
- People.
- Patents, copyrights, etc.
- Systems (including MIS).
- Marketing.

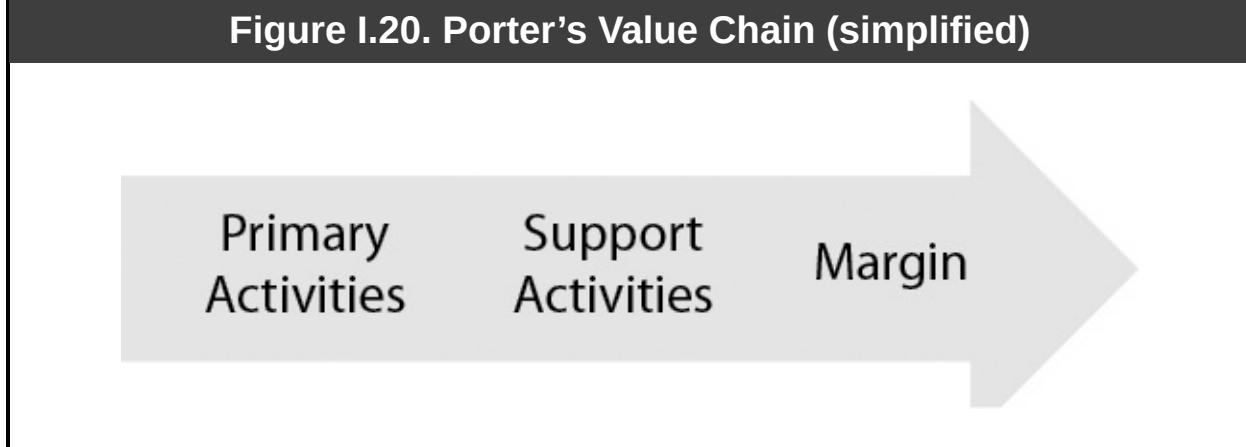
The critical (or essential) capabilities of an organization are the *value drivers*, as they add value to inputs that are subsequently transformed into outputs for customers and service users. (See [Figure I.19](#).)



A more detailed model of the value chain showing the contribution of the various capabilities of an organization is offered by Porter's model (Porter, 1983). (See [Figure I.20](#).) Knowing how the capabilities of an organization contribute to value enables managers to make decisions about their best deployment, as well as questions as to the appropriateness of outsourcing. The sequence of activities and the application of resources transform the inputs and, at various points, value is added for the benefit of the owners of the organization. The transformation is achieved by applying skills, adding new components, and using other kinds of processing. The aim is to maximize the value with the greatest efficiency. There is no necessary connection between cost and the amount of value. The things that customers are prepared to pay for and that add value for the shareholders may, in fact, be the cheapest processes (such as adding

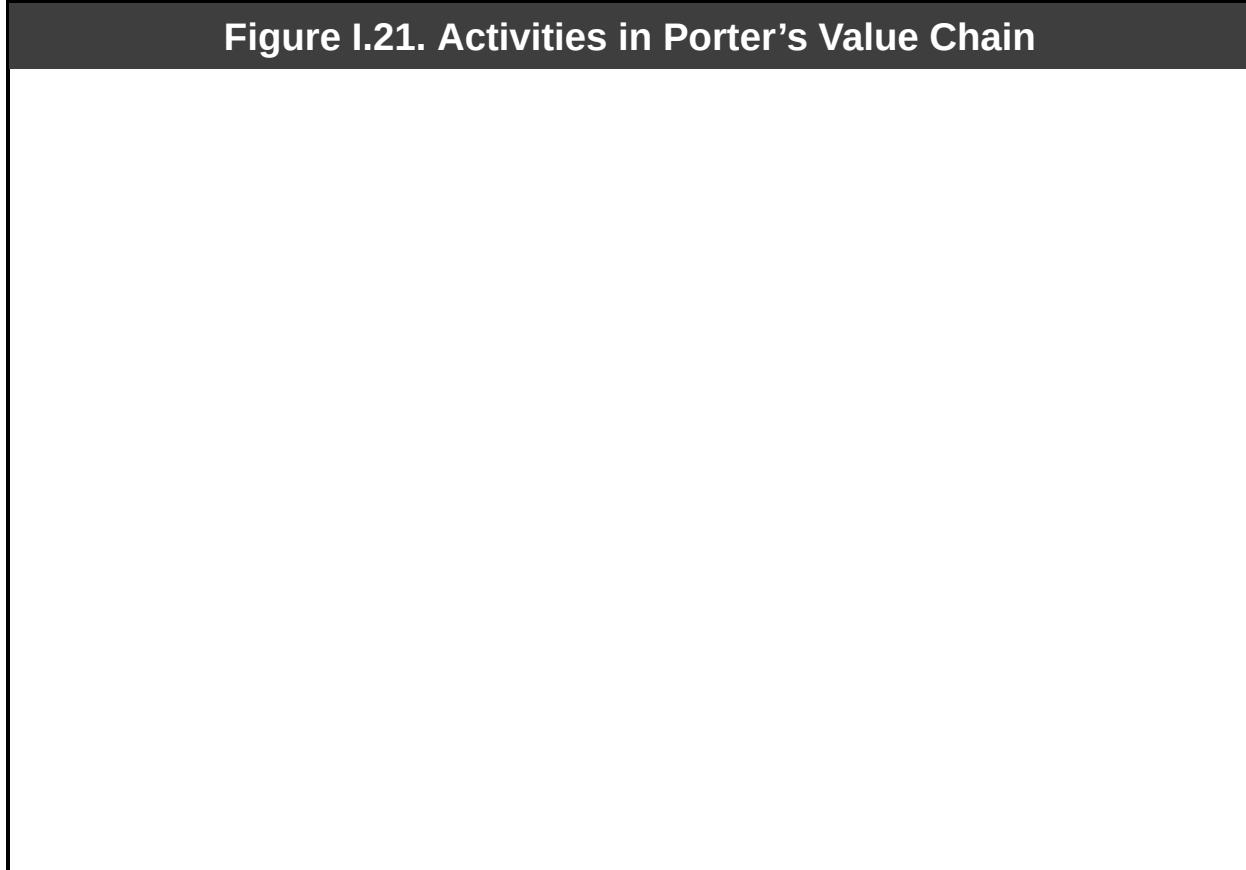
a logo).

Figure I.20. Porter's Value Chain (simplified)



In the value chain, the capabilities that contribute to the transformation of inputs and generate margin are divided into two groups. The *primary activities* have a direct bearing on adding value, while the *support activities* are additional things the organization needs to do to facilitate the primary activities. (See [Figure I.21](#).)

Figure I.21. Activities in Porter's Value Chain



Primary Activities

- **Inbound logistics** (all of the elements of the supply chain of goods and services received)
- **Operations** (all of the main activities needed to create the product or service, such as production, assembly, processing, etc.)
- **Outbound logistics** (the channels of distribution to deliver the product or service to the customer)
- **Marketing and sales** (including raising awareness, creating desire, and making the goods and services accessible)
- **Services to customers** (such as maintenance and after-sales care)

Support Activities

- **Administration**
- **Human resources**
- **Technology**
- **Procurement** (processes needed to set up and manage inbound supply chains)

As organizations become larger and more complex, it is harder to keep track of their capabilities. Using a checklist such as Hooley's or Porter's may assist in maintaining a comprehensive account. It may also be necessary to undertake some kind of routine and systematic check that covers a number of different areas to ensure that such records are accurate. (See [Figure I.22.](#))

Figure I.22. Capabilities and Measures

Finance

- To ensure the proper handling and reporting of financial processes and position.
- Measures: Borrowings, earnings reserves, credit rating, debt-to-equity ratio, and return on net assets.

Physical Assets

- To safeguard the investment placed in them and the activities that depend on them.
- Measures: Cost, age, net present value, condition, replacement cost, remaining years of useful life, and scrap value.

Skills

- To inform human resource development plans.
- Measures: Relevance to current and future tasks, costs, market value, and availability.

Marketing

- To ensure that the organization continues to maximize its competitiveness and remains vigilant to new opportunities and threats.
- Measures: Customer acquisition costs, lifetime value of customers, and marketing costs as a proportion of income.

Innovation

- To promote creativity and stimulate new ways of thinking and novel solutions to opportunities.
- Measures: Active encouragement for creative solutions, exchange of ideas among teams, and rate of adoption of new methods.

Knowledge

- To facilitate effective knowledge management and protect and maximize the value of the knowledge held by individuals in the organization.
- Measures: Processes for capturing implicit knowledge, validation processes for new knowledge, and arrangements for succession planning.

I.B.7 Management of Third-party Business Relationships

Third parties are a stakeholder group comprising individuals or organizations that have been engaged to undertake an activity on behalf of or in partnership with the contracting organization. (See I.B.8 and I.C.2.)

There are significant benefits of working this way. Indeed, it is difficult to

avoid entering into a range of relationships with third parties. However, when working with others, the risks must be considered carefully.

Third parties include:

- Suppliers.
- Contractors.
- Subcontractors.
- Consultants.
- Strategic allies.
- Business partners.
- Subsidiaries.
- Agents.

There should be a good reason for collaborative efforts, such as a way of increasing efficiency, sharing risk, gaining additional capability, or exploiting new opportunities. Sometimes, however, organizations are presented with the chance to work with another party and then attempt to create activity to exploit the opportunity. While this can be successful, it also can result in unfocused activity that falls outside the strategic plan, and ultimately serve as a distraction from achieving core objectives.

Clarifying the nature of the relationship through a formal agreement or memorandum of understanding (MOU) is one way of confirming expectations at the outset and avoiding misunderstanding later. Such agreements may specify the period the relationship is intended to endure, the objectives to be achieved, the roles and responsibilities of each party, how financial commitments and rewards are to be shared, and the options for terminating the agreement.

Once initiated, such relationships rely on effective communication and good working relations. It is important to agree on a schedule for making contact, holding meetings, sharing information, and issuing reports.

The engagement of a third party to undertake some activity does not absolve the organization of responsibility for risk. The organization's own risk management processes need to extend to the exposure to risks presented by the use of third-party contractors, subcontractors, vendors, affiliates, and partners. While the appropriate response to any of these risks may be through various legal and financial protections, it is important to recognize the full range of potential risks. Third-party risks tend to be greater when:

- The relationship is new.
- The relationship is entered into quickly.
- The services provided are critical to the organization's operations.
- The financial value of the arrangement is significant.
- The duration of the relationship is extensive.
- The nature of the undertaking is complex.
- The third party is also engaged in other activities or relationships that may be in direct competition or conflict.
- There are several parties involved.
- The third party is planning to subcontract some or all of the work.

The potential for risk in third-party relationships is significant, stemming from failures by the third party or of the relationship itself. These risks include:

- Operational risk due to the complexities of two or more organizations working together with different systems and strategic priorities.
- Reputational risk through association with another organization's shortcomings.
- Financial risk involving delays, disruptions, underperformance, and penalties.

- Compliance risk where expectations are unclear and no party within the alliance has full oversight of all activities and related regulatory duties.
- Legal risks arising from a partner's breaches in regard to regulation and statutory requirements.
- Strategic risk through the potential for the relationship with the third party to soak up additional time and resources, divert the organization away from its primary goals, and result in the failure to achieve major objectives.

To use a high profile example, BP's exposure to third-party risk proved to be substantial when the Deepwater Horizon oil rig, owned and operated by Transocean but supervised by BP, exploded in the Gulf of Mexico in 2010. Eleven lives were lost and the ensuing devastation to the region has been described as the worst manmade environmental disaster in history. The cleanup, legal battles, fines, and penalties have cost BP tens of billions of dollars (estimated at \$40 billion overall), but the reputational damage is almost impossible to calculate.

Risk management processes, therefore, need to consider the exposure to risk that such relationships bring. The following measures are commonly used to mitigate these risks:

- Using clear policies and procedures for procurement and tendering.
- Due diligence to ensure that the third party can deliver the required level of service for the required period.
- Detailed agreements with stated objectives and itemized responsibilities for each party.
- A schedule of regular communications and reports.
- Oversight by an individual or panel that may include representation from internal auditing or a non-executive director to provide an independent and objective view.
- Penalty clauses, indemnities, and insurance as part of the formal

agreement to provide financial protection should the third party fail to deliver.

I.B.8 Needs and Expectations of Key Internal Stakeholders

A *stakeholder* is defined as anyone who has a stake or an interest in some activity, project, or enterprise; or in this case, the organization as a whole. Stakeholder theory offers a more enlightened perspective, compared with a narrower focus on the immediate beneficiaries, such as shareholders. Being aware and taking account of those interests enables managers to secure support as required and to anticipate resistance to an initiative. This analysis is an extremely important management activity.

KEY TERM

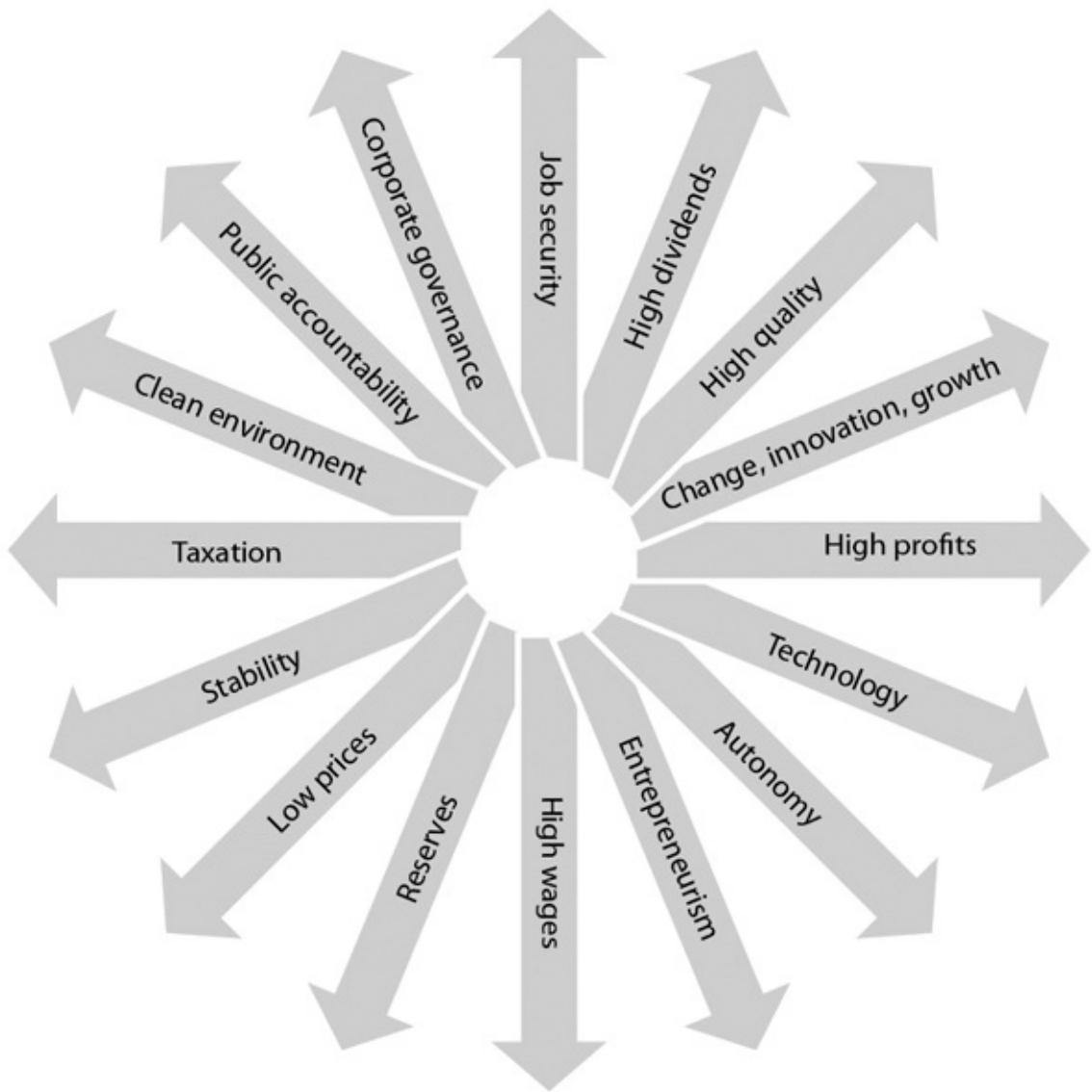
Stakeholder: Party with an interest or stake in the organization or venture.

Organizations exist to serve the needs and interests of their stakeholders by:

- Delivering a sought-after service or product to customers.
- Providing financial returns on an investment to investors and owners.
- Paying amounts that are due in a timely fashion to suppliers.
- Creating a safe, attractive work environment.
- Providing accurate and timely data on pay to tax authorities.

Sometimes these interests can be in conflict. (See [Figure I.23](#).) One party's efficiency gain might be another's cut in income, and one party's enhancements to product quality and service might be another's erosion of profit. Two primary stakeholders—the owners and management—sometimes can be in conflict, as the managers might seek personal or short-term gain, while the owners desire long-term returns on their investment.

Figure I.23. Competing Stakeholder Interests



Organizations are challenged to address a series of overlapping interests by various stakeholders. (See [Figure I.24](#).) Organizational boundaries are often indistinct. For example, where does the organization end and the stakeholder begin? Managers are quick to realize that stakeholders wield great power. Customers may withhold their business, investors may withdraw their capital, employees may take industrial action, the government may raise taxes and increase regulation, pressure groups may lobby for greater environmental protection, and the public may demand greater transparency and ethical

leadership.

Figure I.24. Overlapping Stakeholders



Like other organizational endeavors, risk management processes should be designed to reflect a balanced response to the needs and interests of stakeholders. This requires careful analysis, but it is not always easy to identify the stakeholders and their interests, and even when they are known, they may be subject to change. Often, an individual may span several stakeholder groups (an investor who is also a customer, an owner, or shareholder who is also part of the executive team). However, despite these problems, the analysis is still very valuable as it leads to greater sensitivity to potential sources of conflict or opportunities for support.

Stakeholder analysis can be applied to any planned activity and development, including strategic planning. When developing and reviewing risk management processes, asking key questions will help give due consideration to the needs and expectations of stakeholders:

- Whose interests will be affected (positively or negatively) by risk management?
- What are the interests or stakes (objectives) of these stakeholder groups?
- How could these groups impact (positively or negatively) on our ability to implement risk management?
- What strategies can we adopt to anticipate, mitigate, and exploit the reactions of stakeholders to make risk management processes more successful?

Simple measures, like involving stakeholders in the development of risk management processes and keeping people informed, can deliver the greatest benefit in stakeholder management.

Stakeholders may be categorized as being *internal* or *external*. Some refer to *connected stakeholders*, such as non-executive directors who cross organizational boundaries between internal and external stakeholders, and *peripheral stakeholders* who only have limited and intermittent interests.

Staff interests may be promoted by official or unofficial representatives, trade unions, and similar kinds of associations. Managers and directors may be considered to be part of staff as employees of the organization, but they are also likely to have other personal, financial, and professional stakes in it. The owners in a private sector organization look for a financial return on their investment and have an interest in seeing their vision come to fruition. All of these groups are internal stakeholders.

In the public sector, the government department, body, or agency manages the organization on behalf of the public at large or specific groups within it, and these too become internal stakeholders with a greater or lesser degree of direct influence, depending upon the decision-making structures.

Risk management processes must serve the interests of the organization and enable it to achieve its objectives. It is important to understand the impact risk management processes have on internal stakeholders. (See [Table I.4.](#))

Table I.4. Internal Stakeholder Needs		
Internal stakeholder	Stake in organization	Needs and expectations of the stakeholder with respect to risk management processes
Staff	<ul style="list-style-type: none"> • Secure employment. • Safe working conditions. • Efficient payment of wages. • Confidentiality of personal data. • Opportunities for promotion and personal development. • Social acceptance. 	<ul style="list-style-type: none"> • Being involved in the development of risk management processes in order to understand them and have ownership. • Having clear instructions on what is required of them and training as new skills are needed. • Being able to accommodate the requirements that risk management processes place on them within the time and other resources available. • Gaining recognition for any additional responsibilities they take on with regard to risk management. • Having the opportunity to provide feedback on the operation of risk management processes and being given credit for the expertise and experience they can add.

Internal stakeholder	Stake in organization	Needs and expectations of the stakeholder with respect to risk management processes
Managers and Directors	<ul style="list-style-type: none"> • Personal reward and status. • Short-term returns. • Influence and control. • Networking with others. 	<ul style="list-style-type: none"> • Being confident that risk management processes are providing them with the information they need to execute appropriate decisions and manage the organization effectively and efficiently. • Being confident that risk management processes will contribute to the effectiveness and efficiency of their areas of responsibility. • Receiving support from risk experts to facilitate risk identification and the development of effective risk management processes. • Receiving assurance that the internal controls are working effectively. • Increasing their personal reward by demonstrating that risk management processes add value to operations. • Being able to satisfy the owners that risks are being managed effectively.
	<ul style="list-style-type: none"> • Long-term sustainability. • Financial 	<ul style="list-style-type: none"> • Being confident that management has correctly identified the key risks and that

<p>Owners</p> <ul style="list-style-type: none"> • rewards from investment. • Personal satisfaction from development of the business. 	<ul style="list-style-type: none"> • they are being managed effectively. • Being confident that risk management processes contribute to the value generated by the organization.
--	--

I.B.9 Internal Policies

Although policies and procedures are often referenced together and are closely related, they are actually two distinct things. *Policies* may be described as a course of action or something an organization is supposed to do. They are likely to include the reason or rationale for doing something, and for doing it in a particular way with reference to agreed strategic objectives. Policies can be statements of what the organization stands for. *Procedures* provide the steps by which the policies will be met.

KEY TERM

Policy: Description of the approach or attitude adopted by an entity or activity.

KEY TERM

Procedure: Steps required to undertake an activity in accordance with policy.

Policies and procedures together are used by organizations to explain, justify, and codify expected practice. They serve to provide guidelines for activity and to set boundaries on what is acceptable. They are often developed as new activities are introduced and become stable. They can be used as the basis for staff training and development. They are also part of knowledge management, as a way of

capturing intellectual capital that may be lost if a person leaves the organization.

Policies are advantageous because they:

- Explain and justify a position on a particular issue, such as stating that the organization is an equal opportunity employer.
- Facilitate staff induction and training.
- Capture organizational knowledge.
- Ensure consistency of practice.
- Translate regulatory and legal requirements into operational procedure.
- Satisfy inspectors and regulators that appropriate arrangements and controls are in place for key activities.
- Act as a point of reference for performance management.
- Serve as a risk response, enabling an organization to keep the residual risk within the levels of appetite while exploiting opportunities as they arise.

Organizations differ in their requirements for internal policies and procedures. The need varies, according to the size, age, culture, and degree of formalization. Policies may be either lengthy formal documents or simple statements. Sometimes what is meant by a policy is simply what is accepted custom and practice. Policies and procedures may sometimes be captured in a single document.

The potential for a myriad of policies is great. For example, within the area of human resources, an organization may have policies and procedures covering:

- The hiring and firing of staff.
- Staff induction.
- Grievances.

- Job evaluation.
- Confidentiality.
- Promotion.
- Notice periods.
- Disciplinary action.
- Annual leave.
- Expense claims.
- Recording and reporting of sickness and injuries.
- Performance monitoring and appraisals.
- Whistleblowing.
- Union recognition.
- Retirement.
- Severance.
- Forced loss of employment.
- Harassment.

Given that there is extensive legislation covering all elements of employment, it is not surprising that organizations establish firm policies and procedures in this area to ensure compliance. This applies similarly to other areas such as finance, health and safety, and data protection.

Risk management processes may also be guided by policy documents that include a description of the objectives of risk management and an account of how it is to be effected within the organization. Defined procedures will serve to itemize the application of the policy linked to all key stages in the process. (Refer to II.B.) Because internal policies are part of the control environment, it is

important to review the risk management processes for relevance, timeliness, and effectiveness.

I.C Assess the Processes Related to the Elements of the External Environment in Which Organizations Seek to Manage Risks and Achieve Objectives

Having reflected on the internal dimensions of organizations, we now turn our attention to the external environment—everything outside the organization and its control. The external environment is also the principal source of opportunities and threats.

Managers and analysts use a number of models to help identify relevant features of the external environment that may introduce uncertainty. Increasingly, it is necessary to take the widest possible view, including global as well as local forces. Risk management processes need to be responsive to changes that could precipitate new risks or fluctuations in the severity of existing ones. It is also important to be mindful of the interplay among risks, whether internal and external. Often, it is the unexpected concurrence of two or more risks that takes organizations by surprise.

I.C.1 Key External Factors (Drivers and Trends) That May Impact the Objectives of the Organization

Because organizations do not operate in a vacuum, it is necessary for them to consider the impact that the external environment has when developing risk management processes. Organizational boundaries are not only hard to define but also, in some sense, “porous.” In other words, the external environment influences the organization internally, while the organization impacts the external environment.

The external environment is not only the organization’s physical surroundings, it covers everything that is outside, including technology, physical resources, and more intangible, softer issues such as prevailing ethical values, religious beliefs, political ideologies, social attitudes, and other influences. One way of understanding the external environment is to see it as a mesh of overlapping

influences engaging with and affecting each other. To put it another way, the organization itself is “a response to its environment, the pearl that grows out of the ‘irritations’ of opportunity, threats, personal ambitions, demand, etc.” (Turner and Nicholson, 2012)

One of the most familiar ways of analyzing the external environment uses the acronym PESTEL to represent influences that are:

- Political.
- Environmental.
- Social.
- Technological.
- Economic.
- Legal.

Each of these influences has varying impacts on the objectives of the organization and are likely to introduce a mixture of opportunities and threats. (See [Table I.5](#).)

Table I.5. Analysis of the External Environment	
Features of the External Environment	Risks, Opportunities, and Threats
Political	Current and developing government policy, especially attitudes toward interventions in the economy, including interest rates, taxation, subsidies, state ownership, tariffs, business grants, and foreign trade.
Environmental	Factors relating to sustainability and the physical environment, including pollution, climate, availability and distribution of natural resources, renewable

	sources of energy, global warming, and the supply of power and water.
Social	Trends in public attitudes, buying habits, and customs as well as demographics such as birth rates, morbidity, health and migration, and other features such as class mobility and education.
Technological	Development of new technologies as well as the obsolescence of older technologies as they impact new product development and production methods, performance management, reporting, market research, communication, social networking, etc.
Economic	Variations in financial dimensions, including standards of living, inflation, exchange rates, national expenditure and debt, balance of payments, unemployment, interest rates, and taxation.
Legal	Changes in legislation, especially in relation to labor law, health and safety, data protection, financial reporting requirements, public procurement, consumer protection, and civil liberties.

Risk management processes need to be alert to the complex and changeable external environment. Current and emerging risks, opportunities, and threats can stem from any one of these influences or from a combination of events. What if there are unfavorable exchange rate fluctuations at the same time that new trading tariffs or restrictions are introduced? What if the customer demands a more environmentally friendly product, as new technology makes it possible to reduce waste cheaper and more effectively? What if black market trading begins to influence demand and the pricing policy?

When considering the external environment, it is increasingly important to think globally. Information and communications technologies have significantly increased the effective proximity of organizations, creating vast new opportunities as well as potential threats. In the PESTEL analysis, it should be recognized that there may be multiple legal jurisdictions and political

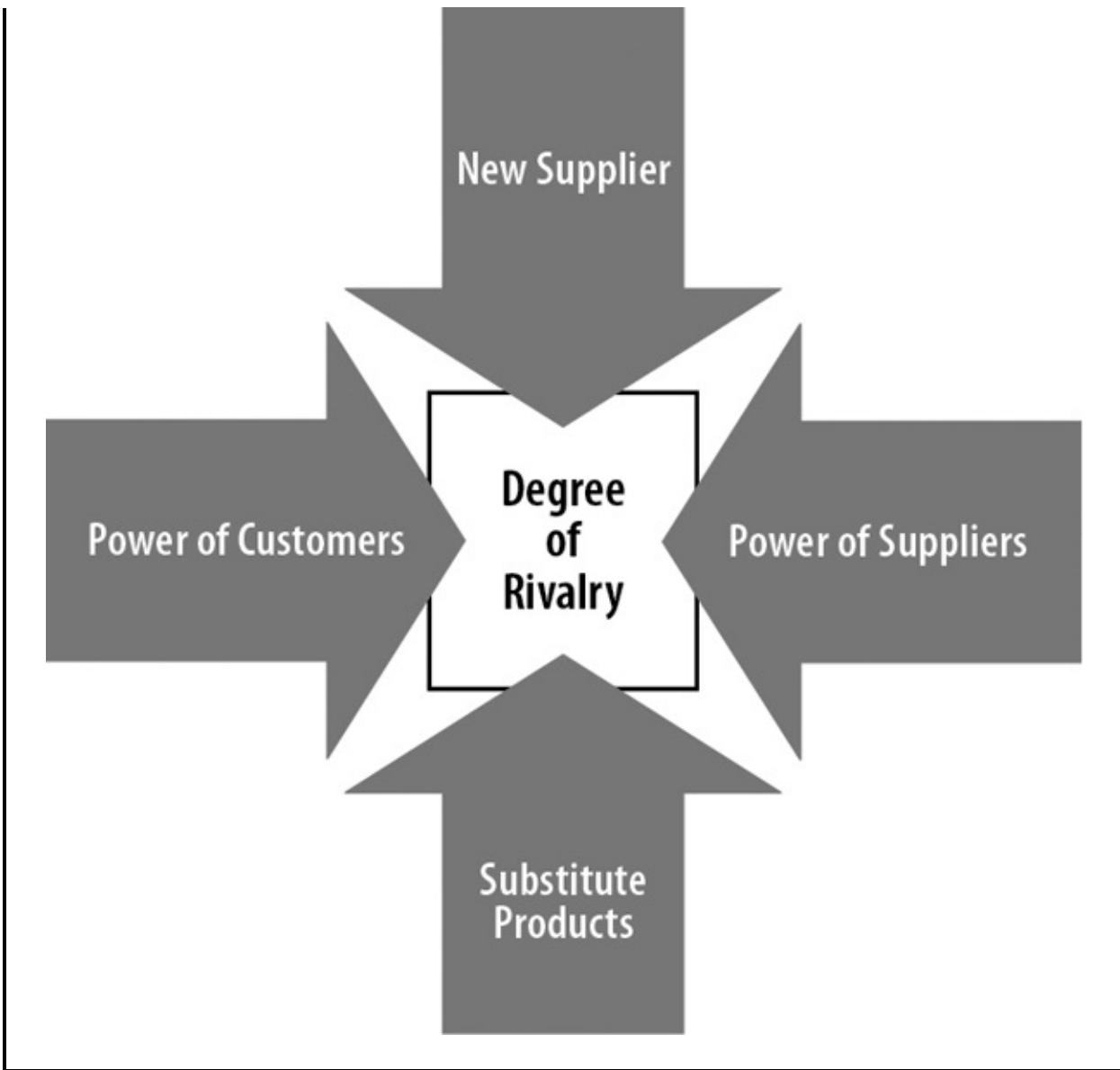
administrations to consider. Social trends progress at different paces around the world, and although there are global economic factors, there are also highly variable local ones too.

Another approach to analyzing the external environment focuses on competitiveness. Porter's Five Forces model from 1980 is still widely used to determine the degree of rivalry that exists within segments of a given market or the market as a whole (see [Figure I.25](#)). The model's five forces include:

- The likelihood of a new supplier joining the market, threatening to take a slice of the action.
- The bargaining power of customers and their ability to dictate prices or switch suppliers.
- The bargaining power of suppliers and their ability to dictate prices and keep customers locked into their product or service.
- The threat of substitute products or services becoming available, thereby undermining the market or market segment.
- The degree of competition and rivalry, which is the net result of the other four forces.

When developing strategy and risk management processes, the model helps focus the attention on the dynamics of the competitive environment and may suggest particular responses to the threats and opportunities. For example, some firms use extensive promotion as a means of keeping new entrants out of the market, especially in the fast-moving consumer goods sector. Generous credit terms, extensive after-sales service, and even technological solutions can tie customers to a given supplier and make it hard for them to switch.

Figure I.25. Porter's Five Forces



I.C.2 Needs and Expectations of Key External Stakeholders (e.g., Involved, Interested, Influenced)

In I.B.8, we examined the power that stakeholders have and the importance of considering their needs and interests, exploring in detail those relating to internal stakeholders. In this section, we will turn our attention to the needs of external stakeholders.

The key external stakeholders of an organization generally include:

- Non-executive directors.

- Customers.
- Suppliers.
- Investors.
- Government and regulators.
- Pressure groups.
- The local community.
- The public at large.

Non-executive directors may alternatively be considered to be *connected* stakeholders or *internal* stakeholders, depending on how their position and influence are regarded with respect to the organization.

Being outside the organization, external stakeholders do not have direct control over strategy and operations. However, their ability to exert influence on such matters is considerable. They may not be as directly interested in the mechanics of risk management processes as internal stakeholders, but they will be affected in various ways if these fail.

An analysis of stakeholders often helps determine the best approach to managing expectations and addressing potential opposition or resistance. One common type of analysis identifies the degree to which stakeholders are engaged with a particular issue or the organization as a whole. A simple scale illustrates levels from being merely *interested* to being *involved* and to exerting an *influence* and being *influenced by* the organization. Similarly, stakeholders may fit into one of the following categories:

- *Promoters*—those who are keen advocates of the organization or the initiative under consideration, and are likely to encourage others to support it.
- *Supporters*—those who have a positive view about the initiative or organization but are less likely than promoters to encourage others to adopt a similar viewpoint.

- *Latents*—those who have the potential to become a supporter but are presently unaware or uninterested.
- *Apathetics*—those who do not have any strong opinion and lack any motivation to get involved.

An organization may use various strategies to move stakeholders from one group to another to gain the backing it requires. Another common form of analysis considers two dimensions: importance and influence. Stakeholders differ in relation to how much importance they attach to a particular issue, which depends upon the size of their stake (financial investment, means of earning a living, source of essential supplies, and so on). They also differ with respect to how much power they have either to influence other stakeholders or to impact directly on the organization. This helps an organization identify different strategies for different categories of stakeholders. (See [Table I.6](#).)

Table I.6. External Stakeholder Needs		
External stakeholder	Stake in organization	Stakeholder needs and expectations with respect to risk management processes
Non-executive Directors	<ul style="list-style-type: none"> • Personal reputation and status. • Future career prospects. 	<ul style="list-style-type: none"> • Receiving assurance that risk management processes are working effectively, are identifying all the key risks, and are having the intended effect on control and the exploitation of opportunity. • Being confident that risk management processes deliver the information needed to effectively challenge the executive team.
		<ul style="list-style-type: none"> • Being confident that risk management processes will

Customers	<ul style="list-style-type: none"> • Product and service quality. • Reliability of delivery. • Stability of prices. 	<p>contribute to the quality, safety, and value of the product or service.</p> <ul style="list-style-type: none"> • Being confident that risk management processes will not add unnecessary costs to the product or service they are buying. • Being confident that the risk management processes will ensure continuity of service and delivery.
Suppliers	<ul style="list-style-type: none"> • Predictable and ongoing demand. • Efficient receipt of monies due. 	<ul style="list-style-type: none"> • Being confident that risk management processes will contribute to the efficient processing of invoices and payments to support their need for good cash flow. • Being confident that the risk management processes will ensure continuity of the organization as an ongoing concern.
Investors	<ul style="list-style-type: none"> • Financial return on investment. • Security of investment. • Accurate and timely data. 	<ul style="list-style-type: none"> • Being confident that risk management processes will improve sustainability and long-term profitability.
		<ul style="list-style-type: none"> • Being confident that the

Government and Regulators	<ul style="list-style-type: none"> • Compliance with legislation and regulations. • Contribution to the national economy. 	<p>organization is meeting its statutory and regulatory requirements with regard to risk management.</p> <ul style="list-style-type: none"> • Being confident that risk management processes will contribute to compliance in other areas (taxation, health and safety, and labor laws).
Pressure Groups	<ul style="list-style-type: none"> • Raising the profile of particular social issues and getting positive reactions. • Recruiting others to the cause. 	<ul style="list-style-type: none"> • Having the ability to influence risk management processes so that they take account of and address the particular areas of concern promoted by the pressure group.
The Local Community	<ul style="list-style-type: none"> • Stability of local jobs and services. • Protection of the local environment. 	<ul style="list-style-type: none"> • Being confident that the organization is aware of and protecting the community against health, safety, and environmental risks. • Being confident that the organization is a stable provider of employment and local services and is a champion of local needs.
The Public	<ul style="list-style-type: none"> • Social welfare 	<ul style="list-style-type: none"> • Being confident that risk management processes ensure fairness across all similar

at Large

and fairness.

organizations in terms of how they are treated by governments and regulators and how they treat employees and customers.

Summary

It is essential that risk management processes are aligned to and embedded within the organization. Risk management is a part of organizational governance, providing stakeholders with clear information about risks and opportunities. In fostering a better understanding and appreciation of risk (both positive and negative), risk management is able to raise the level of risk maturity and contribute to the greater success of the organization.

Risk management processes are not only required to provide management with insights into the riskiness of the organization's internal environment, they are also very much part of that same environment, intrinsically linked to the ethical values, culture, structural arrangements, policies and procedures, and capabilities that operate in the organization. The real strength of an embedded, enterprisewide approach is that risk management processes are working consistently along with routine activities to shine a spotlight on uncertainties that are always present and to help the organization understand them.

As an organization can only be understood in its environmental context, risk management can only truly enable an organization to understand itself by providing a view on current and emerging risks. There are key drivers in play that create an endlessly changing set of conditions. By analyzing the underlying causes and likely trajectory of these changes, risk management processes are able to help the organization prepare its responses. It has been said that *forewarned is forearmed*. By eliminating surprises, organizations are better able to resist, endure, and exploit the threats and opportunities that come along.

Having set the scene for risk management, the next stage is to evaluate its effectiveness. This is the focus of domain II.

DOMAIN II

Principles of Risk Management Processes

Table II.1. Domain II Outline		
Topic/subtopic	Explanation	Reference # in study guide
A. Benchmark risk management processes using authoritative guidance.	<p>It is common practice to use recognized frameworks and sets of standards to help establish risk management processes in an organization and then refer to those standards as a basis for evaluation. Many such standards exist, whether at the organizational, sector-specific, national, or international level. The two most widely used and frequently referred to are COSO's <i>Enterprise Risk Management – Integrated Framework</i> and ISO 31000:2009 <i>Risk Management – Principles and Guidelines</i>.</p> <p>In addition, The IIA's <i>GAIT for Business and IT Risk</i> methodology is an excellent framework for IT general controls and their potential for impacting financial reporting.</p>	II.A

	Benchmarking against given criteria can be extremely beneficial, but it also requires a pragmatic approach. This is essential to ensure that, above all else, the risk management processes in place remain relevant to the organization, rather than slavishly adhering to a given convention.	
B. Evaluate risk management processes related to:	In the previous domain, we stressed the importance of aligning risk management processes with organizational objectives and the organization's internal and external environments. In this section, we examine these processes in more detail. This is to provide a basis on which risk management processes can be evaluated so that adequate assurance can be provided. (This is the focus for domain III.)	II.B
1. Setting objectives at all levels to achieve strategic initiatives	Objective-setting focuses activity and provides a way to assess organizational success. Risk management processes are designed to help the organization achieve its objectives by helping it understand opportunities and risks, and by removing surprises as a result of those risks.	II.B.1

2. Identifying risks	<p>Having defined an organization's objectives, risk management processes can identify upside and downside risks that may enhance or prohibit that achievement.</p> <p>There are various methods used to identify risks. It is good practice to involve key people in the organization with diverse perspectives as a way to raise the level of risk knowledge and embedding risk management. Having a structured approach helps to ensure that all important elements of activity and exposure are considered.</p> <p>It is worth stressing that a risk is not the same as a weakness or an issue. The total of all risks identified constitutes the <i>risk universe</i>.</p>	II.B.2
3. Risk analysis and evaluation, including correlation, interdependencies, and prioritization	<p>Once risks are identified, they must be understood so they can be managed. Analysis and evaluation require an appreciation of the factors giving rise to the risk, and likely trends that underpin them. In addition to likelihood and impact, risks can be analyzed against other criteria, such as volatility and velocity. This helps with <i>prioritization</i>. In addition to regarding risks individually, it is</p>	II.B.3

	necessary to appreciate relationships that exist among them, how materialization of one risk may precipitate another, and how the concurrence of multiple risks may give rise to new and less manageable ones.	
4. Risk response (e.g., avoid, transfer, mitigate, accept), including cost/benefit analysis	A detailed understanding of each risk facilitates decisions regarding an appropriate response, taking account of risk appetite, capacity, profile, and culture. Control measures require resources. Even when the response is only to tolerate the residual risk, it is likely that measures will be necessary to mitigate the inherent risk and to monitor the position for signs of change. In all cases, there should be an assessment of costs versus the benefit of the treatment.	II.B.4
5. Developing and implementing risk mitigation plans	Having determined the appropriate responses for risks, it is essential to record and implement the actions required to establish necessary controls and other measures. As the organization becomes more mature in the risk management process, it will recognize how a single control or suite of controls can be used to treat multiple related risks. Risks with the potential to	II.B.5

	<p>threaten the survival of the organization are likely to form the basis of a separate and well-defined business continuity/disaster recovery plan.</p>	
6. Monitoring risk mitigation plans and emerging risks	<p>Once established, risk mitigation plans (like all plans) require close monitoring to determine that the agreed-upon actions to establish and improve internal controls are being undertaken. It is important that the mitigation plans are well-defined with measurable success criteria. Risk profiles can change, new risks can emerge, and existing risks may become more or less acute. It is just as important to determine when controls are no longer needed as it is to identify where additional measures are required.</p> <p>Risks with high volatility or high velocity require the closest monitoring, as they are prone to changeable probability and can quickly impact the organization. In addition, it is important that the organization closely monitors emerging risks whose nature and potential for opportunity or threat may not yet be well understood.</p>	II.B.6

<p>7. Reporting risk management processes and risks, including risk mitigation plans and emerging risks</p>	<p>Internal and external stakeholders require regular updates to inform them about risk management processes and to advise them of changes in the risk profile. When risks materialize (i.e., when there is a risk incident), a process of escalation up through the chain of command is necessary so that any required remedial action can be taken and contingency plans can be implemented timely.</p>	<p>II.B.7</p>
<p>8. Periodic review of risk management processes to aid in continuous improvement</p>	<p>The approaches of both COSO and ISO 31000 involve continuous improvement. The entire risk management process is a cycle in which periodic reviews provide feedback to the system. They enable faults to be corrected and adjustments to be made in response to changes in the risk universe. At the same time, these reviews contribute to improving the risk culture and maturity of the organization.</p>	<p>II.B.8</p>

Introduction to Domain II

To assess risk management processes, we need to understand the processes and what they are supposed to achieve. The glossary to The IIA's *Standards* describes risk management 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." The *Standards* requires the internal audit activity to evaluate the effectiveness of risk management and contribute to the improvement of its processes. The interpretation of Standard 2120 outlines the features necessary for risk management processes to work properly:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities. (IIA, 2013)

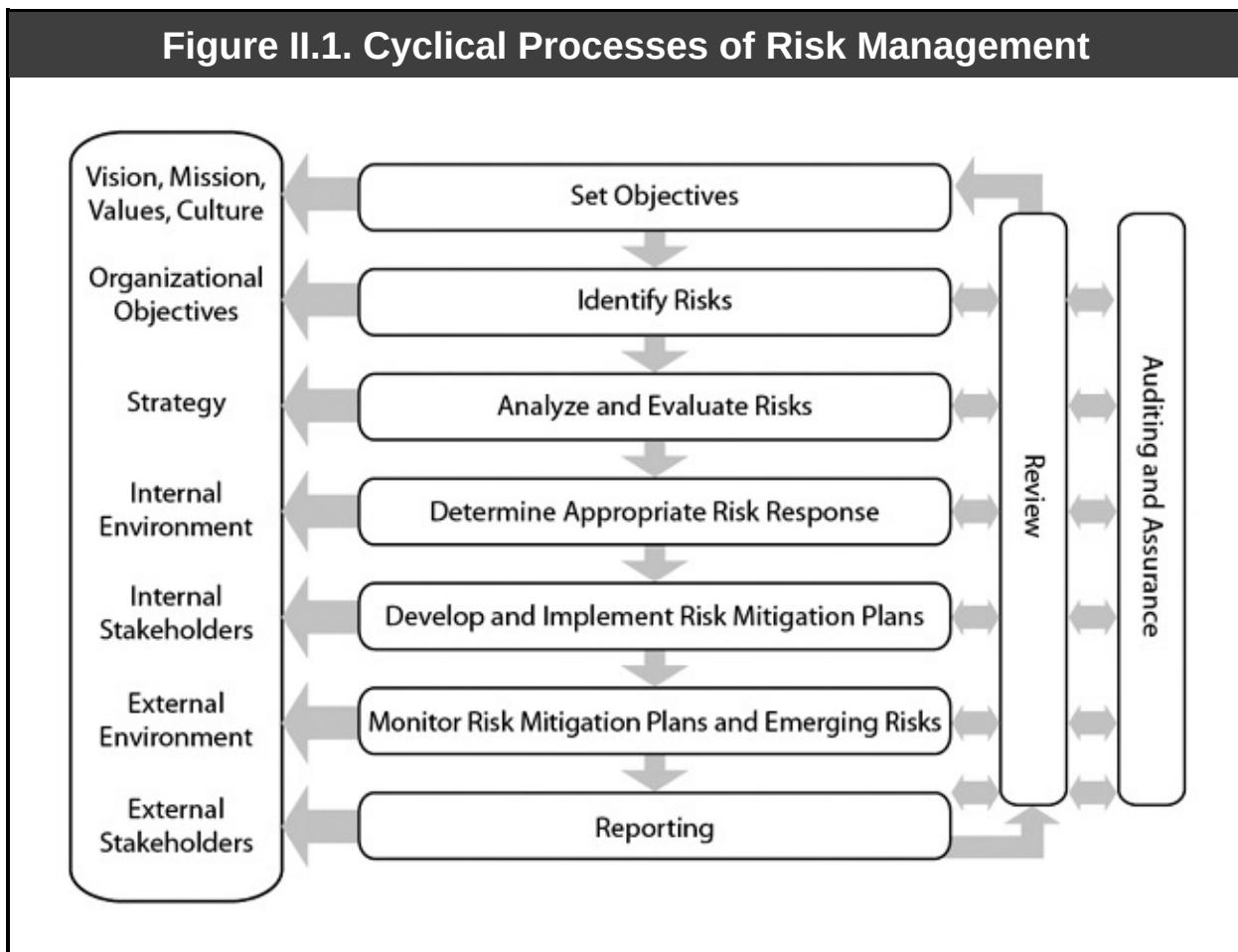
These elements of risk management form the main focus of this domain.

In domain I, we set the context in which risk management processes operate, making it clear that they can only be understood within the context of the organization. Risk management is part of an organization, and it holds up a mirror so that the organization may better understand itself and the risks (both positive and negative) that it faces. In evaluating risk management, we need to ask, "How do we know whether the risk management is good?" We can answer this question through a series of related inquiries:

- Are risk management processes aligned to the organization's strategy?
- Do the processes provide a comprehensive view of the internal and external environment?
- How effective are the processes in identifying and assessing risks?
- Are the risk responses the appropriate ones?
- Are the controls working?

- Above all, does risk management contribute to the organization's success by preparing it for upside and downside risks?

These are the considerations that underpin risk management assurance, and this domain paves the way to delivering that assurance. [Figure II.1](#) provides an overview of risk management processes, their alignment to the needs and characteristics of the organization, the cyclical nature of monitoring, review, and continuous improvement, and the role of internal audit and assurance in providing an independent and objective view on the overall effectiveness and contribution of risk management. These processes are considered one at a time in this domain and the next. In practice, however, the process is integrated with regular movement forward and backward among the steps, facilitating a deeper understanding of the risks and opportunities faced by the organization.



An organization's risk management framework and all the processes that work within it do not come into being at once. Pickett (2005) makes this point very

clearly by showing the evolution of risk management models and processes through a number of phases. This is important when applying benchmarks and choosing appropriate solutions for the organization. Risk management has to grow with increasing maturity. Those responsible for risk management and those providing assurance on it must be diligent to see that the risk management approach advances in a way that best serves organizational interests at all stages.

Domain II counts for 25–30 percent of the CRMA examination.

II.A Benchmark Risk Management Processes Using Authoritative Guidance

In guidance produced by COSO (2012), *benchmarking* is defined as “a collaborative process among a group of entities that focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities.” It involves comparing and evaluating individual performance against a set of standards that may be derived from competitor analysis, industry averages, or perceived best practice. It is possible to do this on a qualitative basis, determining whether the standard has been met or partially met. This requires an appropriate evidence base to support the judgment, although it may depend ultimately on a subjective opinion. Quantitative metrics make it easier to objectively assess whether the actual performance matches the standard. However, the data must be prepared on the same basis for a true comparison.

Rather than sticking with what may be an ad hoc, custom-built approach, the organization can benchmark against recognized standards in a well-established, comprehensive framework. Widely accepted and well-regarded models such as COSO and ISO (described below) have been thoroughly developed and tested over many years. An organization that uses these models can rest assured that the comparisons made are truly against best practices. Many additional resources are available to provide further support for improvement.

KEY TERM

Benchmarking: Systematic comparison of actual activity with a set of standards.

Benchmarking provides a challenge to management, highlights gaps and weaknesses in the current system, and establishes targets for development. However, a benchmarking exercise needs to be approached with care. Even though a set of standards is right for some organizations, it might not always be right for all, especially in totality. The scope and complexity simply may be inappropriate for or incompatible with a particular organization's culture, and using it could result in unwarranted activity and costs. Another danger is that the organization may take undue comfort, falsely or arrogantly believing that everything is okay just because the benchmarking against a set of standards says so.

Therefore, a balanced approach is required, along with a healthy degree of scepticism and pragmatism while aspiring to the highest quality within organizational capability. Overall, the key is to strive for continuous improvement.

There are a number of risk management standards regarded as authoritative guidance that may be used as the basis for benchmarking. They have many similarities, as new standards often adopt and build upon features of earlier models. Sometimes, one body formally adopts the standards of another body. For example, the Federation of European Risk Management Associations (FERMA) adopted its standards directly from the Institute of Risk Management (IRM).

We already have discussed The IIA's Standard 2120 and will make repeated references to the *Standards* throughout this book. In addition, there are a number of other high-profile risk management standards and frameworks commonly used, including:

- AS/NZS 4360:2004 risk management standard.
- National Institute of Standards and Technology (NIST).
- ISO 31000.

- COSO's *Enterprise Risk Management – Integrated Framework*.
- The IIA's *GAIT for Business and IT Risk*.

This guidance can be integrated within a wider internal control framework, such as:

- COSO's *Internal Control – Integrated Framework*.
- Criteria of Control Framework (CoCo).
- UK Corporate Governance Code.
- ISO 9000.

Other risk management standards exist for geographical regions, particular sectors, or individual organizations. For example, the IRM has a very simple and easy-to-use risk management framework, and CAN/CSA-Q850-97 was developed for Canada. Some frameworks focus on specialty parts of risk management. PAS 56 (2003), for example, deals exclusively with business continuity, and COBIT (Control Objectives for Information Technology) is a widely used framework for managing IT risk. The two most important general risk management standards, however, are undoubtedly those issued by COSO and ISO.

When considering whether to adopt a set of standards formally or simply take valuable parts from different sets, each organization must make its own decision based on its own circumstances and organizational culture. Formal systems are usually comprehensive and their detailed guidance and support can be very useful. However, they also can be cumbersome and may not fit well with the quality systems and other standards already embedded in the organization. The advantage of taking what you want from a framework is that it can be tailored readily to suit the particular requirements of the organization. On the other hand, this simplified approach carries the risk of missing important elements by taking shortcuts rather than adopting a more detailed approach.

Combined Australian and New Zealand Standard

One of the first sets of standards for risk management was the 1995 combined

Australian and New Zealand Standards, referred to as AS/NZS 4360 and subsequently revised in 1999 and 2004. These standards recognized that a coordinated approach is an integral part of effective risk management. They describe a framework that is embedded within general organizational operations, policies, and culture to create “... a risk management process involving establishing the context and the identification, analysis, evaluation, treatment, communication, and ongoing monitoring of risks.” (AS/NZS 4360:1999)

AS/NZS 4360 quickly gained international acceptance with formal adoption by such notable organizations as the UK National Health Service. The framework, which was designed to be used by organizations of any type and at any level of activity—from discrete operations to an enterprisewide view—comprises seven key steps:

- Establish the context.
- Identify risks.
- Analyze risks.
- Evaluate risks.
- Treat risks.
- Monitor and review risk management processes.
- Communicate and consult with key stakeholders.

This is described as a continuous process in which ongoing monitoring and review ensure an up-to-date understanding of the context in which risk management takes place. Contextualization and responsiveness to the needs of a given organization and its environment are central to the effectiveness of risk management processes.

The National Institute of Standards and Technology (NIST)

NIST 800-37 is an example of a risk management framework for a specific sector. It is a U.S. Department of Defense “guide for applying the risk management framework to federal information systems.” Although specifically

designed for information systems, it has many similarities to more generic frameworks. Promoting an organizationwide view of risk, its principal steps are:

- Categorizing information and information systems.
- Selecting security controls.
- Implementing security controls.
- Assessing security-control effectiveness.
- Authorizing the information system.
- Monitoring security controls and information system security on an ongoing basis.

ISO 31000:2009, Risk Management – Principles and Guidelines

The International Organization for Standardization (ISO) provides an extensive suite of standards that are widely regarded as definitive within their sphere. Covering virtually all aspects of organizational activity, ISO 31000 was launched in 2009, and largely superseded AS/NZS 4360. It “provides principles, a framework, and a process for managing risk” and is applicable to organizations, regardless of their size or sector. Its focus is to help organizations to:

- Increase the likelihood of achieving objectives.
- Improve the identification of opportunities and threats.
- Effectively allocate and use resources for risk treatment.

Many of the ISO standards provide a basis for certification, although this is not the case with ISO 31000. Its main role is to serve as an authoritative international benchmark. Although it can apply to individual aspects, it is geared toward enterprisewide risk management. The target audience for ISO 31000 is:

- Executive-level stakeholders.

- Appointment holders in the enterprise risk management (ERM) group.
- Risk analysts and management officers.
- Line managers and project managers.
- Compliance and internal auditors.
- Independent practitioners.

ISO 31000 views risk as related to uncertainty rather than loss and, therefore, conforms to our definitions of both threat and opportunity. The process of adopting the ISO standards helps ensure that:

- There is clear commitment to and accountability for enterprise-wide risk management.
- The broader provisions for governance are in alignment with the ISO standards.
- There are well-defined key performance indicators that can be measured and tracked.
- Monitoring and reporting mechanisms are in place and are harmonized with the organization's performance management systems.

COSO's *Enterprise Risk Management – Integrated Framework*

COSO's *Internal Control – Integrated Framework*, with its multicolored cube, is a very popular and widely recognized approach to effective internal control. Essential for effective internal control, the framework's five interrelated components are:

- Control environment.
- Risk assessment.
- Control activities.
- Information and communication.

- Monitoring activities.

However, COSO's *Enterprise Risk Management – Integrated Framework* goes a stage further to provide a more extensive focus on risk. As a result, the *Internal Control – Integrated Framework* is incorporated by reference within the ERM framework.

A key objective of the ERM framework is to help managers of businesses and other entities better deal with the wide range of risks that threaten organizational objectives. One of COSO's goals in designing the model was to integrate various risk management concepts within a framework in which a common definition is established and components are identified. This framework is designed to accommodate most viewpoints and to provide a starting point for assessment and enhancement of ERM.

The objectives of risk management processes as defined in the COSO model are covered in II.B.1.

GAIT for Business and IT Risk

In 2007, The IIA introduced the GAIT (Guide to the Assessment of IT Risk) methodology. Its purpose was to provide organizations with a top-down approach to identifying the IT general controls that need to be tested so that assurance on the management of IT risks can be provided. GAIT places particular emphasis on how those risks impact financial reporting in the context of sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002. The framework is based on four key principles:

- The failure of technology is a risk that only needs to be assessed, managed, and audited if it represents a risk to the business.
- Key controls should be identified as the result of a top-down assessment of business risks, risk tolerance, and the controls (including automated controls and ITGCs [IT general controls]) required to manage or mitigate business risk.
- Business risks are mitigated by a combination of manual and automated key controls, and key automated controls must be assessed to manage or

mitigate business risks.

- ITGCs may be relied upon to provide assurance of the continued and proper operation of automated key controls.

II.B Evaluate Risk Management Processes

As explained in domain I, risk management should be understood and undertaken in the context of the organization it serves and the environment in which it operates. Clarifying organizational goals and the goals of risk management is an essential first step in the process. The scope of the organization—its capabilities, activities, and ambitions—determines the proper focus of risk management processes. Risk management and organizational objectives share a symbiotic relationship. The purpose of risk management is to enable the organization to achieve its objectives. Therefore, organizational objectives set the scope of risk management. Failure to achieve one of these objectives is a risk that should be managed. We can only identify risk and set the appetite for it with reference to the goals and approaches adopted by the organization.

Because a process may be considered effective if it produces the desired results, it is essential to understand what risk management processes are designed to achieve. This domain examines the detailed processes of risk management, one step at a time, so that their effectiveness can be adequately evaluated.

In I.A.1, we examined the objectives of risk management. Let's briefly revisit the intended goals with reference to the two key risk management frameworks.

ISO 31000 standards establish the following 12 principles that risk management should follow:

- Create value, as the gains are greater than the resources required for risk responses.
- Be integrated within routine organizational processes.

- Be integrated into ordinary decision-making processes.
- Provide a focus for identifying and understanding uncertainty.
- Be well structured and systematic.
- Be founded on accurate and reliable information.
- Be flexible to accommodate the features of the organization.
- Be reflective of the human element of activity.
- Be open and transparent.
- Be responsive to change through close monitoring of the organization's environment.
- Be focused on continuous improvement.
- Be subject to cyclical review.

According to COSO's ERM Framework:

Determining whether an entity's risk management is effective is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. (See [Table II.2](#).)

Table II.2. COSO's ERM Components	
Internal Environment	The internal environment comprises many elements, including an entity's ethical values, competence, and operating style incorporating how it assigns authority and responsibility. As part of the internal environment, management establishes a risk management philosophy and the entity's risk appetite, forms a risk culture, and integrates enterprise risk management with related initiatives.
	Objectives must exist before management can

Objective Setting	identify events with the potential to impact their achievement. Enterprise risk management ensures that management has a process in place to set objectives that are aligned with the entity's mission/vision and are consistent with the entity's risk appetite.
Event Identification	Event identification refers to management's consideration of external and internal factors that create threats and uncertainties. This includes events that potentially have a negative or positive impact, or both.
Risk Assessment	Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses events from two perspectives: likelihood and impact.
Risk Response	Management identifies risk response options and considers their effect on event likelihood and impact (in relation to risk tolerances and costs versus benefits), and designs and implements response options.
Control Activities	Control activities are part of the process by which an enterprise strives to achieve its business objectives. They are the policies and procedures that help ensure risk responses are properly executed.
Information and Communication	Information is needed at all levels of an organization to identify, assess, and respond to risks. Information comes in a variety of forms from many sources—internal and external, and in quantitative and qualitative forms—and allows enterprise risk management to respond to changing conditions in real time. Communication should raise awareness about the importance and relevance of effective enterprise risk management.

Monitoring	Monitoring of enterprise risk management involves an assessment of both the presence and functioning of its components and the quality of their performance over time. Monitoring can take place through ongoing activities or separate evaluations.
-------------------	--

These standards can be applied to any enterprise or area of activity. However, complex and unique areas such as IT require specialist schemes. Chief among these is COBIT. The GAIT-R methodology (IIA, 2008), suggests eight steps that mirror many of the stages of general risk management assurance. The GAIT-R steps are:

1. Identify the business objectives for which the controls are to be assessed.
2. Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved.
3. Identify the critical IT functionality relied upon for key business controls.
4. Identify the significant applications where ITGCs need to be tested.
5. Identify ITGC process risks and related control objectives.
6. Identify the ITGCs to ensure they meet the control objectives.
7. Perform a reasonable holistic review of all key controls identified.
8. Determine the scope of the review and build an appropriate design and effectiveness-testing program.

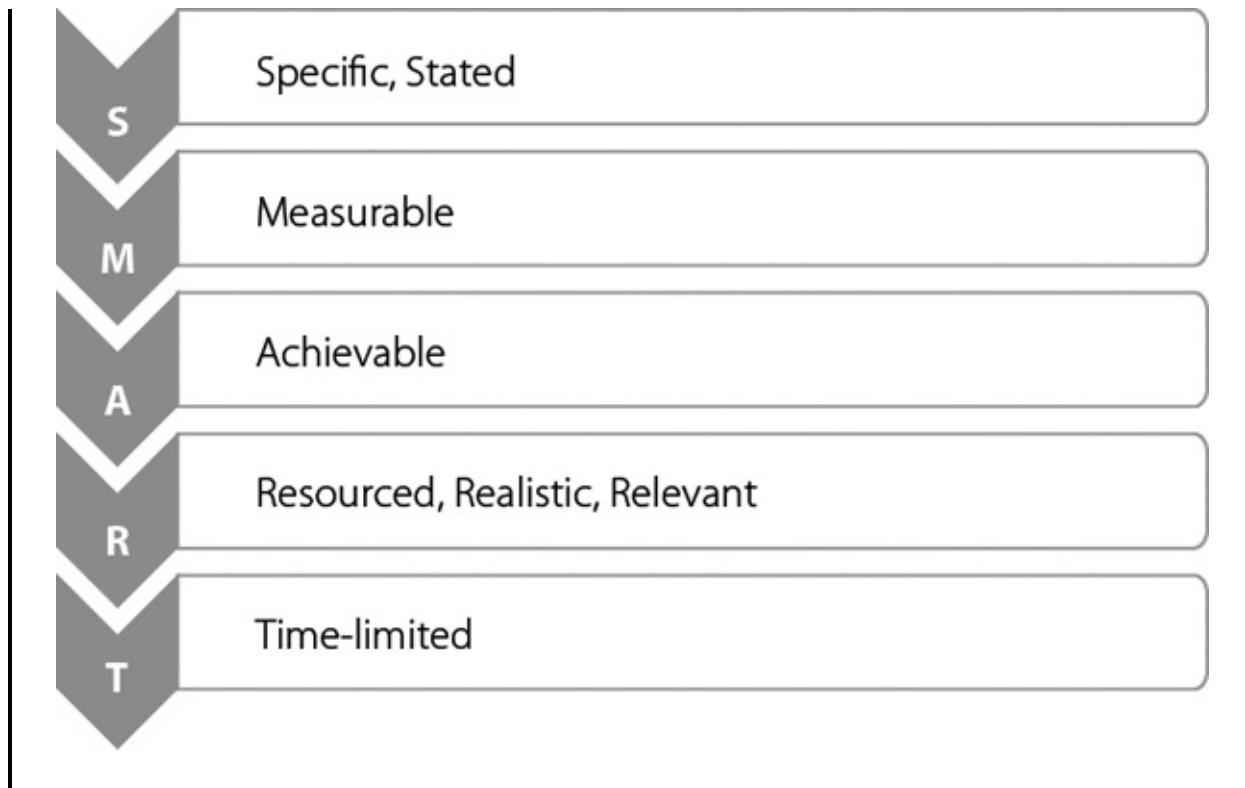
With the help of these various standards and guides, either individually or together, organizations can build their risk management processes. These tools also can be used as a framework for measuring the effectiveness of risk management processes once they have been introduced.

II.B.1 Setting Objectives at All Levels to Achieve Strategic Initiatives

Considering risks as unpredictable and essentially unmanageable accidents and disasters that exist *out there somewhere* is an outmoded viewpoint. As we recognized in our various definitions, a more sophisticated view is to regard risks as those things that add uncertainty to our objectives. Therefore, it is not only desirable, but also necessary to begin the building of risk management processes by considering organizational objectives.

Strategic objectives vary considerably among organizations. Strategy represents a choice from a number of options. The vision, mission, and objectives should consistently express what the organization is trying to achieve; and the resources—people, cash, and other organizational assets—should be dedicated to making those goals a reality. High-level, long-term strategic objectives apply to the organization as a whole, cascading down to lower levels in the organization where they become more operational. Every team and every individual should understand what is expected with regard to contributing to the goals of the organization. SMART objectives, as illustrated in [Figure II.2](#), help ensure clarity and effective performance management.

Figure II.2. Mnemonic for SMART Objectives (with allowances for different variants of this model)



As organizations develop their risk management process, the potential for uncertainties to impact objectives becomes more apparent. The processes described below (risk identification, risk analysis, risk mitigation, monitoring, reporting, and review) are steeped in strategy and its underpinning analysis (providing challenge to the process of strategic thinking), followed by a review of the resulting objectives. Risk management starts by asking the question, “If these are our goals, what might go wrong and what other opportunities might arise?”

Organizations exist for a purpose. As we discussed in I.B.8 and I.C.2, the needs and expectations of various stakeholders may vary considerably. That is one of the reasons it is useful to define the organization’s purpose. Having a purpose is one of the things that differentiates an organization from a random collection of people and resources. Another reason for defining the purpose is that (in a quote variously attributed), “If you don’t know where you are going, you usually end up somewhere else.” In other words, defining where you want to go is the first step to getting there.

KEY TERM

Objective: A sought-after result.

We may consider that the overriding aim of organizations tends to be survival. Unless the organization continues to exist, it cannot achieve any of its other goals. While this is generally true, it is not always so. For example, an organization that exists to achieve a particular time-limited goal (e.g., to host a tournament at a given moment or bring about a change in the law) may happily disband once that goal is achieved. In any case, the aim is not usually survival *at any cost*. There will be other important goals and values.

In I.B.4 we observed a general differentiation among public, private, and third-sector organizations. As well as differing in ownership, the distinction is also characterized by principal objectives. Private-sector organizations seek to maximize the return on investment for the owners; public-sector organizations aim to provide a valuable service to sections of the public; and charities seek to promote and support a socially desirable cause not adequately covered by the public sector.

In giving expression to their goals, organizations often establish a vision, a mission, and a set of strategic objectives. The *vision* is a statement of where the organization wants to be or a state of affairs it wishes to bring about in the future. For example, Walmart's vision is:

If we work together, we'll lower the cost of living for everyone and give the world an opportunity to see what it's like to save and have a better life.

A *mission* is a statement of the primary purpose of the organization. Walmart's mission statement is, "We save people money so they can live better." Not all organizations separate their mission and vision. The mission of McDonald's is "to be our customers' favorite place and way to eat."

The mission of the Walt Disney Company is:

KEY TERM

Mission: Statement of an organization's purpose.

To be one of the world's leading producers and providers of entertainment and information. Using our portfolio of brands to differentiate our content, services, and consumer products, we seek to develop the most creative, innovative, and profitable entertainment experiences and related products in the world.

These statements are most effective when they are memorable and can be used by staff, managers, customers, and other stakeholders as a ready point of reference.

Objectives may be set at various levels of the organization. [Figure II.3](#) paraphrases Sobel and Reding (2012) and COSO to depict the four main types of objectives.

Figure II.3. Four Primary Types of Objectives

Strategic Objectives

Relate to the way the organization intends to fulfil its mission and achieve its mission.

Operational Objectives

Relate to the effective and efficient deployment of resources in achieving strategic objectives.

Reporting Objectives

Relate to the communication of information internally and externally.

Compliance Objectives

Relate to those activities designed to align actual practice with regulatory and contractual requirements and organizational policy.

KEY TERM

Strategic objective: A high-level, long-term goal likely to impact the

whole organization.

To turn the vision and mission into a reality, organizations must align their strategic and operational objectives. *Strategic objectives* tend to be longer term (usually three or more years) and relate to significant initiatives that are likely to impact much or all of the organization or have high costs, risks, and potential for opportunity. *Operational objectives* tend to be shorter term (usually within 12 months) and focus more on the ways routine activity will deliver the strategy. *Reporting objectives* are those that provide the framework for delivering communications to internal and external stakeholders. The content of those communications relates to activities required to achieve strategic and operational objectives. Finally, *compliance objectives* are met through efforts to satisfy the formal requirements of legislation, regulation, internal policy, and contractual obligations.

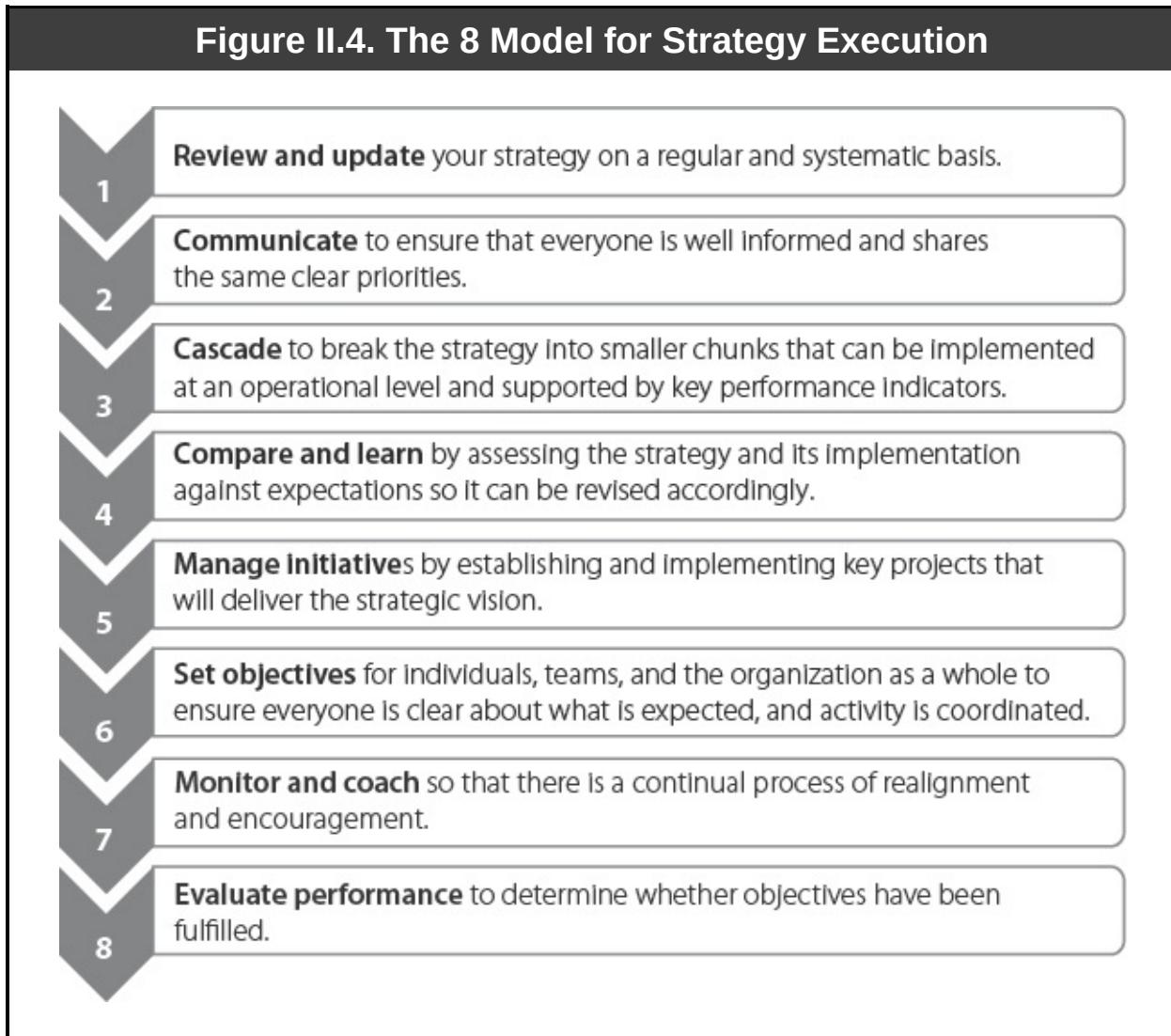
KEY TERM

Operational objective: Shorter term, activity-focused goal required to deliver strategy.

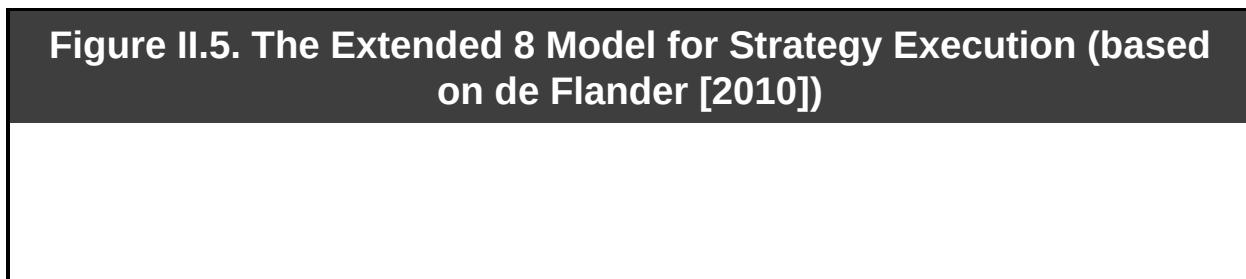
Sometimes it is not clear whether an objective is strategic or operational. What is important to note is that strategy cascades from the vision and mission down to operational objectives. At each stage (and there may be many), the larger strategic objectives are broken down into smaller chunks of operationally focused activity. This process can continue down to the level of the individual, ensuring that staff members are aware of what is required of them and that their personal objectives are aligned with those of the organization.

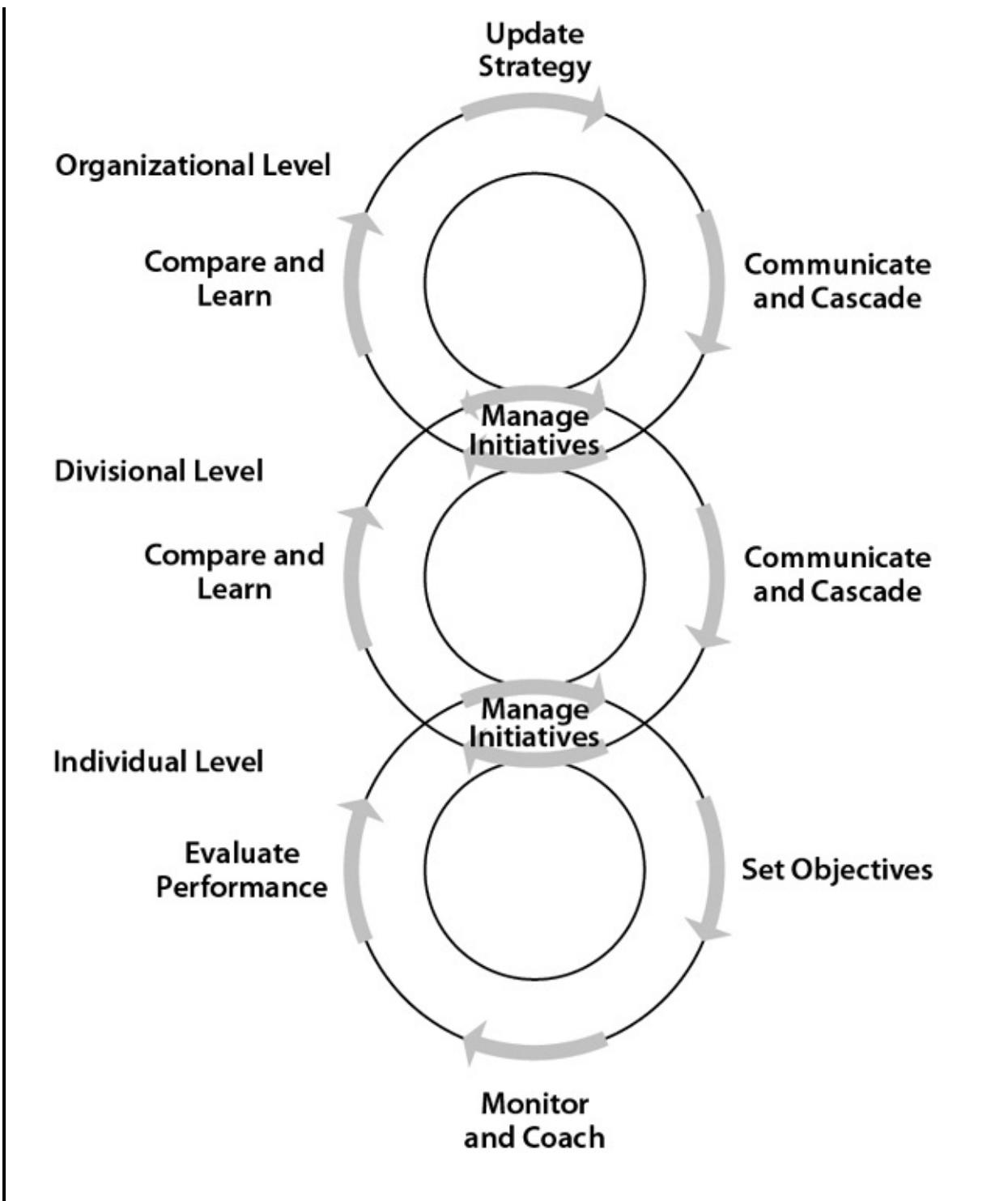
This alignment of objectives—horizontally and vertically—is critical for organizational effectiveness. Consider an organization whose capabilities are provided by a team of horses. To pull more weight, go faster, and travel further, the horses must face the same direction. To continue the analogy, risk management processes are required to check the horses for signs of fatigue or misalignment, anticipate changes in the road, prepare for the awkward bumps, and maximize the potential of any downhill stretches.

A useful model for the integration of strategic, operational, and individual objectives (see [Figure II.4.](#)) is referred to as The 8 Model for Strategy Execution (de Flander, 2010). It is named after the building blocks of strategy.



The model also gets its name from a diagrammatic representation (see [Figure II.5](#)) that resembles the number “8.”





Understanding the integration and cascading of objectives from strategic to individual levels enables risk management to define the *risk universe* (the full scope of its interest) and ensure that its own objectives are fully aligned.

KEY TERM

Risk universe: The totality of risks that may impact an entity.

According to COSO's *Internal Control – Integrated Framework* (2012), "an effective system of internal control reduces to an acceptable level the risk of not achieving an objective." According to COSO, objectives of risk management processes (see I.A.1) may be classified under the headings of:

- Operations.
- Reporting (broadened in 2012, from the internal control framework's earlier terminology, *financial reporting*).
- Compliance.

In COSO's internal control framework model, strategic objectives define the sphere in which risk management is to operate but are not regarded as part of internal control. Setting objectives is fundamentally important, as the effectiveness of internal control is measured against objectives.

II.B.2 Identifying Risks

Having considered what an organization is trying to achieve, its internal capabilities, and the environment in which it operates, the process of identifying risks and opportunities may begin in earnest. To ensure that all key risks are considered, a structured and systematic risk identification process should be in place. The process includes developing a comprehensive list of risks and then evaluating the risks, locating their origin, and assessing their likelihood, potential impact, and other characteristics.

Identifying risks is a matter of removing surprises and losses. Anticipating risks and opportunities helps an organization to be prepared. The identification of risk needs to be led by the board or its equivalent. Unless risk identification is being undertaken for the first time, it involves a periodic and systematic review of the strategic risk register to determine whether the most recent assessment captures all relevant and significant risks. In addition, it is necessary to scan

internal and external factors that may have changed and may now present new or emerging risks. Finally, it is important to reflect on the possible impact of a combination of particular risks crystallizing at the same time, as well as considering each risk individually. It is often the unexpected simultaneous occurrence of risks that takes organizations by surprise.

The process of risk identification is described as follows:

Risk identification establishes the exposure of the organization to risk and uncertainty. It requires an intimate knowledge of the organization, the market in which it operates, the legal, social, political, and cultural environment in which it exists, as well as an understanding of strategic and operational objectives. This includes knowledge of the factors critical to success, and the threats and opportunities related to the achievement of objectives. **It should be approached in a methodical way** to ensure that all value-adding activities within the organization have been evaluated and all the risks flowing from these activities have been defined. (AIRMIC, Alarm, IRM, 2010) [emphasis added]

For organizations with greater risk maturity, the principle is that risk management is embedded within ordinary activities so that risks are naturally identified as part of the process of objective-setting and business-planning at each level. Ideally, it should not be seen as an additional or burdensome task that is separate from day-to-day management. Chesshire (2010) states that (to be successful) risk identification needs to:

- Be supported and promoted from the highest levels of the organization.
- Be carefully planned with a clear briefing for all participants.
- Be adequately resourced.
- Be led by someone with specialist skills in risk management and risk identification.
- Involve a cross-section of individuals with the right blend of skills and knowledge regarding organizational activities.
- Operate according to an agreed-upon set of rules.

- Have clear objectives.
- Communicate its outcomes clearly.
- Make appropriate reference to good practice frameworks.
- Take account of cross-departmental risks as well as those that fall within a single area.
- Ensure that agreed-upon actions are recorded and subsequently implemented.

The identification of risk is defined in ISO 31000 as “the process of finding, recognizing, and describing risks.” These risks are both current and emerging. Just as the internal and external environments discussed in I.B and I.C are subject to continuous change, so are organizational objectives, the strengths and weaknesses that may precipitate risk, and the opportunities and threats that may arise. As depicted in [Figure II.6](#), COSO lists seven potential sources of change that could impact risk identification:

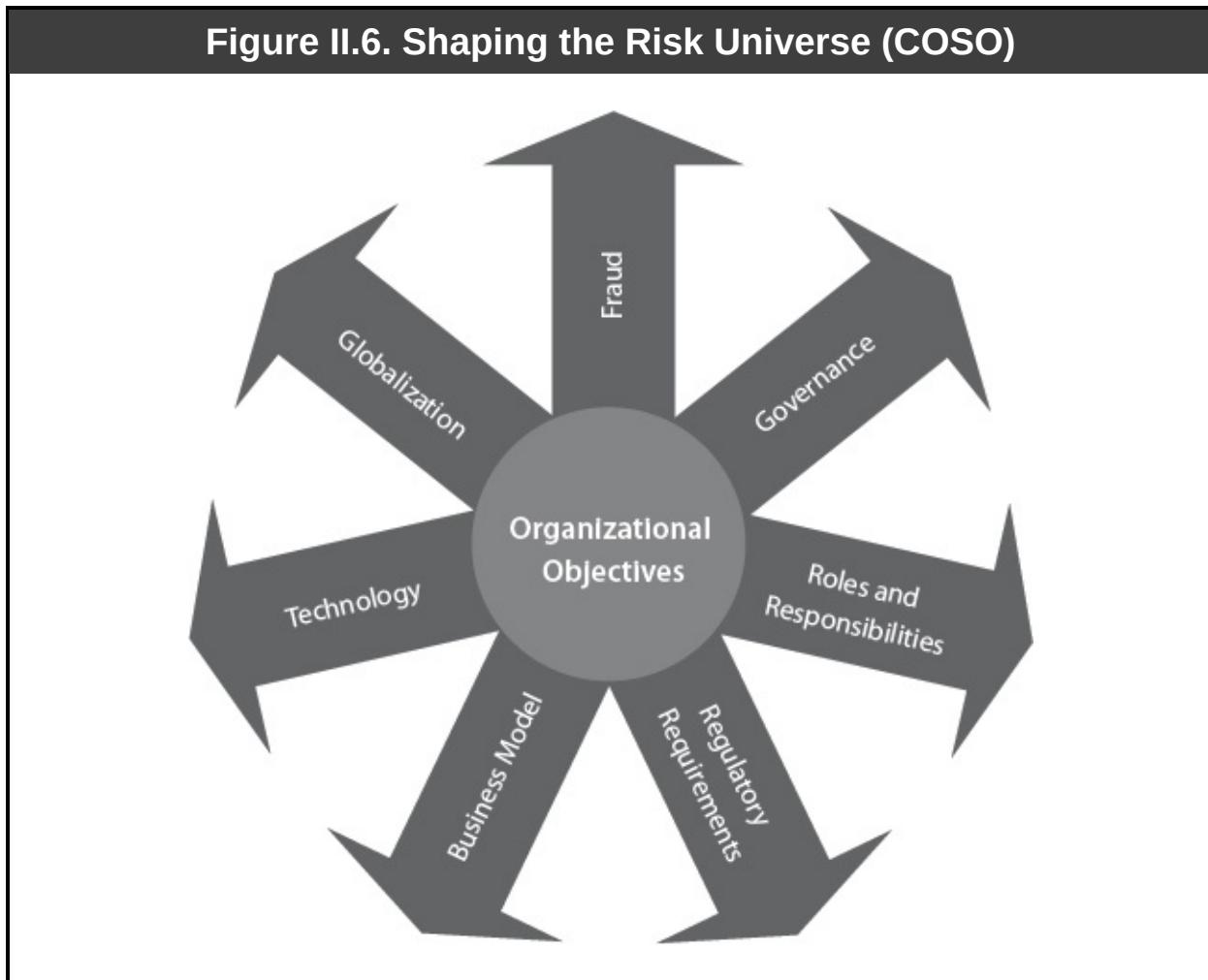
- Expectations for governance oversight.

KEY TERM

Risk identification: The process of finding, recognizing, and describing risks. (ISO 31000)

- Globalization of markets and operations.
- Changes in business models.
- Demands of complexity in laws, rules, regulations, and standards.
- Expectations for competencies and accountabilities.
- Use of and reliance on evolving technologies.

- Expectations relating to preventing and detecting fraud.



The board may require help, such as special training and development, to facilitate the understanding and identification of risks. Then it will be in a position to fulfill its role of providing challenge and adding value to the strategic plan. Middle managers should regularly draw upon the board's knowledge and secure its buy-in, thereby strengthening the risk culture. The relationship between risk identification and planning helps ensure that strategic and operational thinking are appropriately aligned.

To support the process of risk identification, there are plenty of templates, tools, and toolkits available. However, the process may be carried out perfectly well without such assistance. A number of relatively simple methods and activities commonly used are outlined below and may be used either in isolation or conjunction with each other (with reference to Chesshire, 2010).

- *Checklists*: Checklists are a good starting point for risk identification when they relate to similar organizations in the same sector or for particular areas of activity. However, organizations and their circumstances are unique, and something considered to be a relevant risk to one organization may not be so to another. In II.B.3, we will review some common classifications of risks that can be used as checklists.
- *Benchmarking*: A more detailed comparison with other bodies or industry norms can be achieved through a benchmarking exercise, as discussed in II.A. This may be facilitated by individuals from a similar organization sharing their own insights and analysis. Benchmark data also may be obtained through a number of sources. Although benchmark data can be very useful, it is unlikely to provide a perfect fit for any given organization.
- *Scenario planning*: “What if …?” scenarios are a useful way to consider a range of possible events or circumstances and determine their impact. Managers may be able to undertake such an exercise internally, or the organization may wish to employ a team of business analysts.

Vulnerability assessments: By reviewing in detail each process or activity the organization undertakes, it is possible to identify the points at which it is vulnerable to failure or, alternatively, where new opportunities may arise. Vulnerabilities may occur, for example, where there is a bottleneck in a system, an overreliance on an individual or piece of equipment, or a highly changeable environment. These are often referred to as *single points of failure* or SPOFs. This analysis of processes and activities may be represented visually by a cause-and-effect or fishbone diagram. (See I.B.5.)

KEY TERM

Vulnerability assessment: The process of identifying and evaluating risks by examining the potential for failure.

Risk brainstorming (thought-shower) sessions: The key feature of a brainstorming (or thought-shower) session is that ideas can be freely suggested

without worrying whether they are right. This encourages everyone to participate and creates an environment in which the thinking can flow without inhibition. For such a session to be really useful, the facilitator needs to be skilful enough to keep the discussion focused and highlight the important points raised. Although this is a good technique, it is not sufficient on its own to ensure all relevant risks are identified.

KEY TERM

Control risk self-assessment: An exercise to assess risks and control strengths against a control framework.

- *Control risk self-assessment (CRSA), alternatively referred to as risk and control self-assessment, or simply control self-assessment (CSA):* As a process, CRSA can follow a number of formats, including questionnaires and workshops. It is more highly structured and more rigorous than a brainstorming session, and its most important feature is its participative approach that includes staff from all levels. Those who are most closely involved with the day-to-day activity under review are the people best suited to support the identification of risks and controls. CRSA can be implemented for any activity, from discrete areas of operation to the organization as a whole. The basic approach requires participants to:
 - Identify the objectives for the area under review (or review the objectives that have already been developed through strategic and operational planning); and determine how actual events may vary due to the degree of uncertainty.
 - Evaluate the responses that exist or are needed to ensure that the likelihood and impact of the risks identified are consistent with the risk appetite (or to take advantage of opportunities that may arise).
 - Check the effectiveness of the controls to determine that they are working as required.

As well as identifying risks, a CRSA or series of events has the

advantage of articulating the organization's approach to risk management and involving many people in the process. This fosters awareness and understanding, leading to a greater degree of ownership.

- *Questionnaires or surveys:* A questionnaire may be used to maximize the level of participation because it can be circulated across all business units. It also serves to reinforce a standard approach. The quality of the questions is critical.
- *Risk identification workshops:* Although a face-to-face workshop is more time-consuming, it is essential that objectives are clear; this provides the benefit of checking and reinforcing understanding. The same workshop can be extended to consider risk responses and implementation plans.

It is important to focus on risks that are *relevant and significant*. It is possible to imagine all kinds of hypothetical risks that may or may not have any impact on the organization. Generating a long list of such risks would prove to be counterproductive. Therefore, the emphasis should be on the risks that require the board's attention. The process of prioritizing risks and identifying the significant ones forms an overlap with II.B.3. As stated above, these processes are not completed in clinical isolation but are integrated and often iterative. This does not mean that lesser risks can be ignored; however, there should be an appropriate allocation of effort. The board should focus attention on high-level strategic risks that expose the organization to potentially major disruption and large-scale losses, as well as opportunities for significant gain and strategic advancement. Together with risk management, those closer to operations must be aware of operational risks and opportunities, as well as the impact they may have on more routine activity.

Sobel and Reding (2012) condense the process for risk identification down to a number of pragmatic steps. First, they suggest looking for the events that may precipitate risks by:

- Following a structured and systematic process.
- Involving people who bring a range of different perspectives using research to enhance understanding.

- Utilizing brainstorming activities to gain maximum input from all participants with a focus on:
 - Upside and downside risks.
 - Events that impact individual and multiple objectives.
 - Events that can trigger other events.
- Considering the impact of events with respect to desired objectives.

Second, the process requires the development of the *risk universe*. This moves us beyond a list of events that might arise to a set of defined risks. The level of detail included in the risk universe depends on the needs and, to some extent, the maturity of risk management processes across the organization. Too little detail can be detrimental for practical purposes, but too much detail can be overwhelming. In the risk universe, risks are grouped into categories using appropriate classifications. As suggested by Sobel and Reding, the steps for moving from events to a risk universe are to:

- Consider the possible outcomes of the events identified.
- Group these together according to similar sources, causes, or related impacts.
- Analyze groups and label each cluster with an appropriate name.
- Write a definition that explains each group of related risks.
- Organize the risk universe under major headings to reflect the needs of the organization.

We should remember that risk identification is not a one-time process. Instead, like the rest of risk management, it requires regular monitoring and review to ensure that the organization remains alert to internal and external environmental changes that may affect the risk profile.

KEY TERM

Risk register: A structured record of all the key risks and their analysis.

As risks are identified and the risk universe is defined, it is common to collate them all on a *risk register*. As outlined in I.B.5, documentation plays an important part in governance because of its contribution to openness and decision-making. Therefore, it is important to record the results of risk identification, and there are many format variations and plenty of software solutions available to help. As the register grows, it also can be used to track the subsequent stages in the process (i.e., analysis, response, and planning). Information that should be noted on the register includes:

- A description of the risk event (the event precipitating the risk).
- The risk owner (the individual or team responsible for monitoring, responding, and reporting).
- The inherent risk assessment impact, likelihood, and score (if quantitative), according to the organization's measurement method. (See II.B.3.)
- Information on the responses currently applied to the risk. (See II.B.4.)
- The residual risk assessment, using the same method as for inherent risk.
- A conclusion, regarding acceptability of risk.
- Information on any actions to be taken. (See II.B.5.)
- Monitoring controls to be applied. (See II.B.6.)

Risk registers may be compiled and held in different parts of the organization. We will revisit the risk register in the following sections.

Organization of risks under various clusters and major headings may rely on the classifications to be considered in II.B.3, but it also may be of the organization's own devising.

II.B.3 Risk Analysis and Evaluation, Including Correlation, Interdependencies, and Prioritization

Risk analysis and evaluation can be undertaken in a number of stages. The level of complexity adopted at each stage should reflect the needs of the organization. In the following pages, we will describe the processes that may sometimes appear to be bureaucratic. It is important to remember that risk management is not an end in itself, but something designed to assist an organization in the achievement of its objectives.

We will consider this topic under the following headings:

- II.B.3.i Risk classification
- II.B.3.ii Risk analysis
- II.B.3.iii Risk criteria
- II.B.3.iv Risk level or severity
- II.B.3.v Risk mapping and prioritization
- II.B.3.vi Risk registers
- II.B.3.vii The psychology of risk

II.B.3.i Risk Classification

The first step toward analysis and evaluation can be a simple classification of risks under various headings. Such classifications have various benefits. In general, the descriptions of different types or aspects of risk help us to comprehend risk. When used as checklists, they can help with the identification of risk as described in II.B.2. In addition, they are helpful in analyzing risks and structuring the risk register.

In domain I, we introduced a number of fundamental definitions of risk and the distinction between *inherent* and *residual risk*. This section will build upon and expand what has already been discussed.

KEY TERM

Speculative risk: Opportunity.

There is no universal classification of risk. Instead, organizations tend to tailor their language to reflect their understanding and preferences. Classifications are useful to help group the related risks, and may make it easier to determine the appropriate risk response. Distinctions can be made on a number of different bases. The following relate to classifications that are based on the nature of risks:

- As we have already seen (I.A.3), risks may be classified in terms of the natural risk that exists (theoretically) in the absence of any response (*inherent risk*), and the remaining risk (*residual risk*) that prevails when the response is in place.
- Risks also may be distinguished on the basis of their benefits. Risks that are purely destructive or negative may be referred to as *pure risk* (or downside risk), and those that can be exploited for gain can be called *speculative risk* (or upside risk or opportunity).

KEY TERM

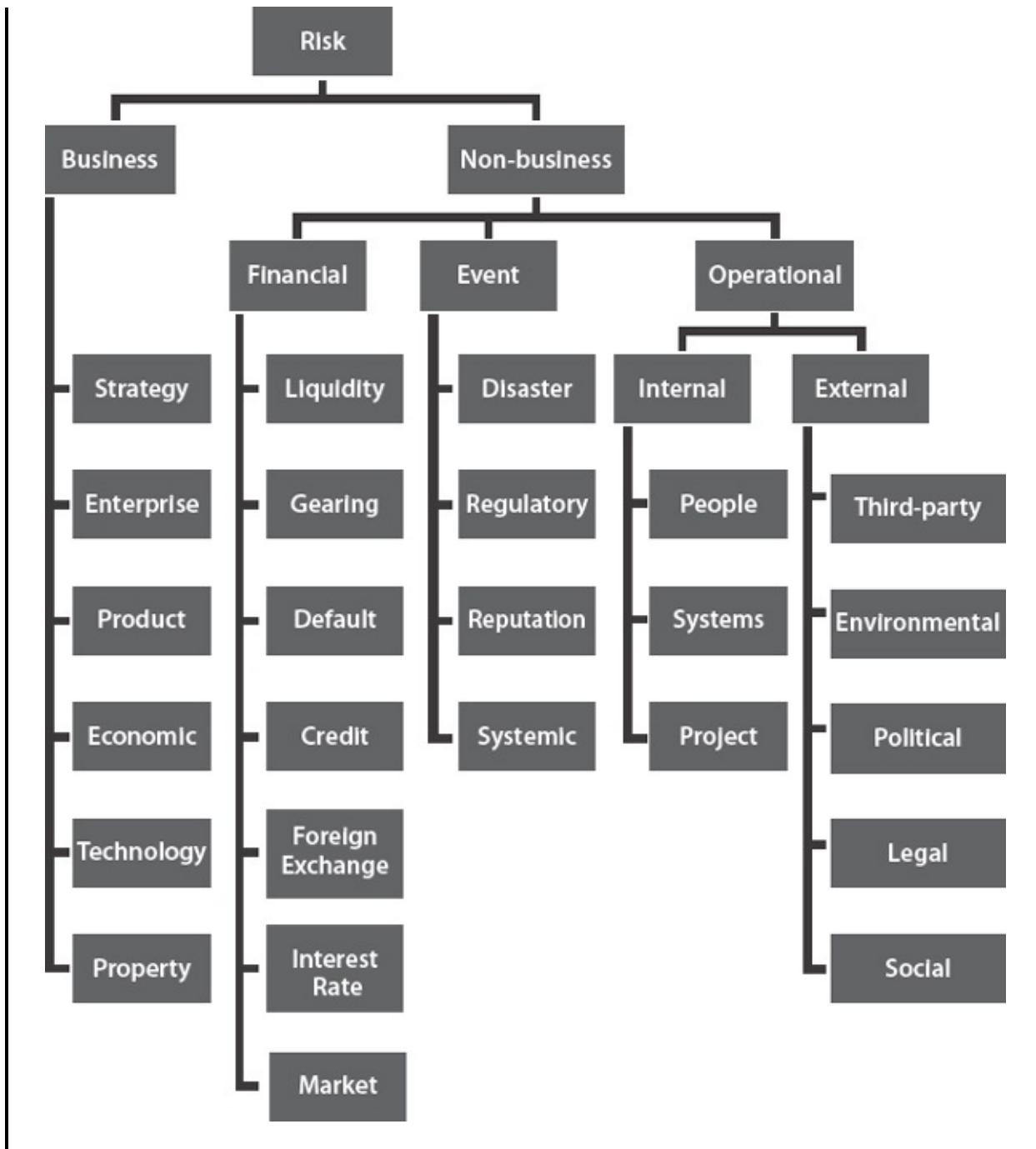
Pure risk: Wholly negative risk.

- We can separate risks according to how well they are understood. *Well-known risks* are based on strong knowledge. *Hypothetical risks* are based on incomplete or uncertain knowledge. *Unknown risks* are based on an absence of knowledge. As we learn more about the circumstances surrounding a risk, it may move from being unknown to being hypothetical or well-known.
- *Foreseeable risks* are those that are known or (at least) knowable, provided we have good intelligence. *Unforeseeable risks* cannot be understood or predicted with any degree of accuracy.

- *Theoretical risks* are those that exist, but are so unlikely or will have such little impact that they are not worth considering. On the contrary, *significant risks* are the ones that have the ability to frustrate strategy or offer valuable new opportunities.

It is also common and highly useful to classify risks according to their origin or source. [Figure II.7](#) depicts one potential classification, although it is neither definitive nor exhaustive.

Figure II.7. Sample Classification of Risks (Nicholson and Turner, 2010)



Typically, a distinction between business and non-business risks is made. Business risks (positive and negative) stem from the nature of the business itself, the way it operates, the goods and services it delivers, and the resources it uses. Business risks include:

- *Strategy risks* associated with the choice of strategy and its

implementation.

- *Enterprise risks* associated with selecting and undertaking business activities.
- *Product risks* associated with trying to meet customer needs and to predict and satisfy demand.
- *Economic risks* inherent in general trading conditions.
- *Technology risks* that new technology brings to all aspects of activity.
- *Property risks* associated with the use or misuse of property, its development, and deterioration.

Non-business risks cover any other type of risk not arising directly from the nature of the business. These risk categories often are subdivided into financial risks, event risks, and operational risks.

Financial risks arise from sources external to the business, including:

- *Liquidity risk* relating to the availability of cash.
- *Gearing risk* (arising from leverage) relating to the balance between owners' capital and other investment, with a corresponding impact on volatility of earnings and insolvency.
- *Default risk* relating to the possibility of debtors failing to pay all that they owe on time.
- *Credit risk* relating to access to borrowing.
- *Foreign-exchange risk* relating to fluctuations in the rate of exchange.
- *Interest-rate risk* relating to rises and falls in interest rates.
- *Market risk* relating to changes in the value of the stock (share price).

Event risks are risks stemming from events that are largely outside the organization's control, including:

- *Disaster risk* that threatens business continuity through acts of nature, accidents, or sabotage.
- *Regulatory risk* arising from changes in legal requirements that impact the organization.
- *Reputation risk* that often occurs as a result of other risks crystallizing and impacting the standing of the organization.
- *Systemic risk* relating to operations and processes, such as the supply chain.

KEY TERM

Risk profile: Overall distribution of risks across an organization.

Operational risks relate very closely to risks in the internal and external environments explored in domain I. (See I.B and I.C.) Among the internal risks, two are often given high prominence: *fraud risk* arises from the intent to deceive for personal or organizational gain, and *IT risk* represents all of the opportunities and vulnerabilities associated with information systems.

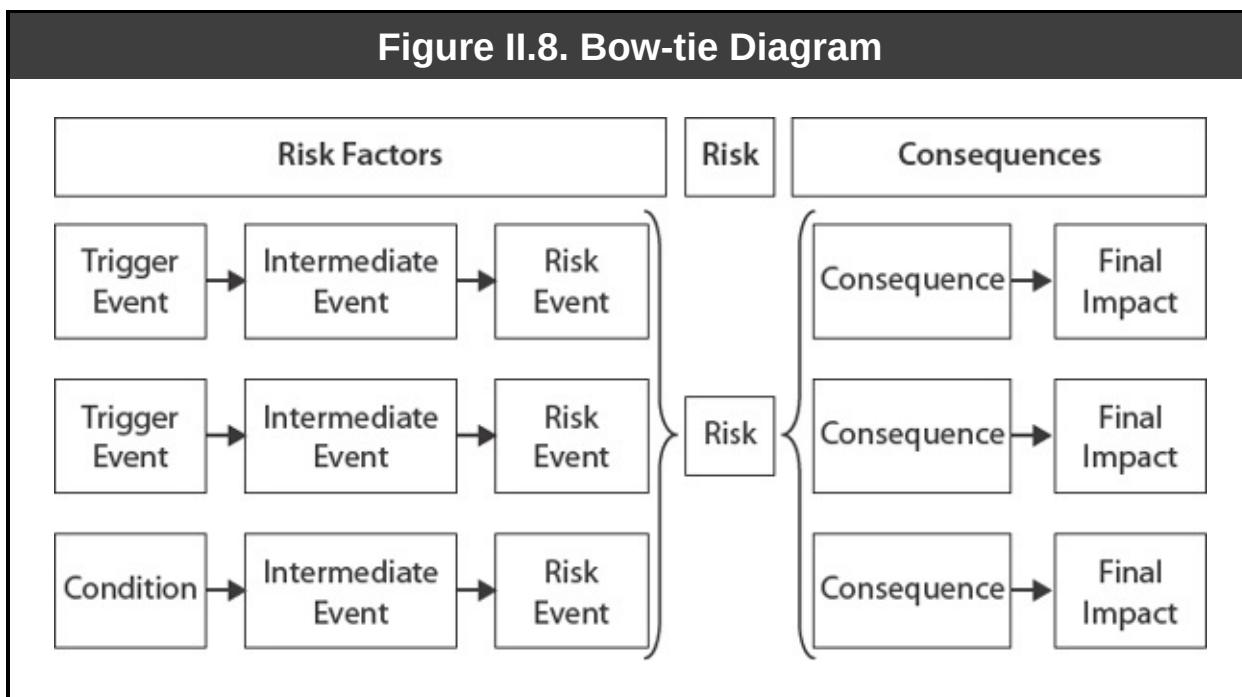
These classifications overlay and are always open to interpretation. In spite of which scheme is used, it must suit the needs of the organization and help with the risk identification and analysis.

To avoid getting bogged down in the detail of individual risks, we should routinely take several steps back and consider the overall picture. In evaluating risk at the highest level, the board (or its equivalent body) should determine how each threat or opportunity presents a *value risk*. This helps the organization to focus on what is relevant and significant. Value risks may be assessed as either a risk to *earnings* or to *assets*. To clarify matters further, the organization should assess its overall *risk profile*.

II.B.3.ii Risk Analysis

As well as identifying the classification of risk in terms of the broad area of activity to which it relates, it is essential that its true nature is understood. How does it arise? What are the trigger events or conditions that can precipitate it?

Often, there are several intermediate steps between the trigger event and the risk itself. For example, cost-of-living risk (inflation) may not have direct impact on an organization, but it will trigger a series of related events (i.e., unemployment may rise, individuals may have less to spend, and demand for certain products may fall). Hence, more than one trigger event may be required for the risk to materialize. A combination of rising inflation and a bad harvest might have an impact on a food manufacturer, even though one of these events alone might not. A series of causes and effects can result in significant consequences when combined, and such events can impact the earnings of the organization dramatically. Diagramming correlations, interdependencies, and conditions that could lead to a risk event (see [Figure II.8](#)) can help clarify the potential effect or danger.



II.B.3.iii Risk Criteria

KEY TERM

Risk level or severity: The relative seriousness or value of a risk.

Having classified risks in various ways and broken down the chain of events to reveal their true identity, we now can consider how the risks may be analyzed and evaluated. To do so, it is necessary to determine appropriate *risk criteria*. These criteria are defined in ISO 31000 and then quoted in Sobel and Reding (2012) as “terms of reference against which the significance of risk is evaluated ... [and] are based on organizational objectives, and external and internal context.” These criteria can be grouped under two main headings: *governance risk* and *assessment risk*. Governance risk criteria set the framework in which risk management takes place and covers the four key factors—risk capacity, risk attitude, risk appetite, and risk tolerance—which we explored in domain I. Assessment risk criteria are those that are needed for analysis and evaluation. (See Sobel and Reding, 2012, chapter 4.) The overall *risk level* or *severity* that helps determine risk *prioritization* is a function of all the criteria that an organization chooses to use in its assessment. Criteria may include:

- Likelihood (or probability).
- Impact (or consequence).
- Vulnerability.

KEY TERM

Risk criteria: Factors or dimensions that may be used to analyze risks.

- Velocity (comprising the speed of reaction and the speed of recovery).
- Volatility.
- Interdependency.
- Correlation.

There is some variability on the use of terms associated with risk, and it is crucial that there is a common understanding among all individuals engaged. We will begin our discussion on terminology with the two most commonly used criteria for the assessment of risk—impact and likelihood.

Impact

Impact or consequence is a measure of projected organizational effect of materialized risk. According to Sobel and Reding (2012), it may make its presence felt in a number of different ways, including:

- Financial impacts affecting earnings, access to credit, availability of cash flow, operational expenditure, and levels of reserves.
- **Financial reporting impacts**, including making erroneous statements or faulty judgments that may make the position or performance appear better or worse than it actually is.
- **Reputational impacts** leading to changes in the way the organization is perceived by stakeholders.
- **Environmental impacts** that result in an improvement or deterioration of the natural world, affecting access to resources, resource availability, and consumption.
- **Safety impacts** with consequences for the working conditions of employees, customers and others exposed to unsafe goods and services, and the general environment of the public.
- **Legal impacts** that may enable or restrict the organization and may lead to litigation, reward, or punishment.

Likelihood

There are different ways of analyzing likelihood, taking into account the probability and frequency over given time periods. In its simplest form, we assume that the likelihood is fairly stable within a given time frame. However, this is certainly not always the case, and measures—such as volatility—will help refine our assessment of likelihood.

Vulnerability

Vulnerability is a measure of how susceptible the organization is to a given risk. This depends on the organization's state of readiness, its agility, and its adaptability. Given this description, it is clear that there is a close relationship between vulnerability and impact: the greater the vulnerability, the greater the likely impact will be. This analysis is useful, however, and helps with understanding the risk and identifying an appropriate response.

Volatility

In some cases, the probability of a risk varies, depending on the *volatility* of the situation. When conditions vary greatly, it is harder to predict the likelihood of a given event. It is likely that such a risk would be a higher priority for risk management because of its high unpredictability.

Velocity

Some analyses include the criterion of *risk velocity* (or speed of onset). This is a measure of how much prior warning and preparation time an organization may have between the event's occurrence and impact. This, in itself, can be split into *speed of reaction* and *speed of recovery*. The time from the event occurring and the impact on the organization is sometimes known as *proximity*.

Interdependency

KEY TERM

Risk interdependency: The causal relationship between two or among more risks.

It is important not just to consider risks in isolation, but also in various combinations. The materialization of two or more risks might impact the organization differently, depending on whether the events occurred simultaneously or concurrently. For instance, nuclear power stations in Japan are prepared for earthquakes and tsunamis. However, the concurrence of these events may allow a wave to breach defenses that are already weakened by

ground tremors. Consider another example: routine financial controls usually require the segregation of key duties to prevent an employee from ordering goods for personal use. However, if two or more individuals decide to collude on such a fraud, it is much harder to detect.

Correlation

Correlation is similar to interdependency in that it relates to the connection of two or more risks. In this case, rather than mutual dependency of risks precipitating new and potentially unexpected risks, the impact or likelihood of the risks varies. For example, weaknesses in a national economy may precipitate foreign exchange risks and result in additional costs to goods and services traded internationally. These costs may add to the need to increase borrowing. The underlying economic factors that led to exchange-rate fluctuations also may be associated with higher interest rates and greater difficulty securing credit.

KEY TERM

Risk correlation: The interdependency of two risks.

Possible interactions between risk events (both interdependencies and correlations) may be mapped on a square grid with each risk as a heading for all columns and all rows. When two risks intersect on the grid, there is potential for an even greater risk. We may find, for example, that an economic downturn is likely to precipitate, add to, or coincide with a whole range of other risk events, such as increased costs of borrowing, rises in the cost of raw materials, and diminishing demand.

II.B.3.iv Risk Level or Severity

After choosing the appropriate criteria for the purpose, it is possible to undertake the assessment and evaluation of the identified risks by applying the criteria to each risk. The evaluation uses the assessment to determine the acceptability of the risk in comparison with the appetite, and will be used to determine an appropriate response. Risk assessment and evaluation include:

- Assessing the likelihood (frequency and probability) of the risk occurring.
- Assessing the impact (or consequence) of the risk occurring, when impact or consequence of a risk is defined as an *outcome of an event affecting objectives*. (ISO 31000)
- Assessing other dimensions of the risk (such as velocity, volatility, and interdependencies).
- Measuring the severity or level of the inherent risk, defined as the *magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood* (ISO 31000). This usually consists of the product of the likelihood and the impact of the risk, but also may include other dimensions.
- Comparing the severity of the risk with the related risk appetite.
- Determining an appropriate response when the residual risk is outside the boundaries of the risk appetite. (II.B.4)

This description assumes an ideal natural state in which risks are not currently treated. In practice, there is usually some degree of response (internal control or other measure) already in place. The assessment and evaluation of risk is often repeated for the *inherent* and the *residual* risk, and the severity of the latter is compared with the appetite to determine whether further action is required.

Risk level or *severity* is often taken as a function of likelihood and impact. With numerical values assigned to each, the risk severity can be taken as the product of these two numbers.

To measure the true value of the impact, it is necessary to isolate the damage or positive opportunity the risk event would precipitate from other unrelated occurrences. Impacts may be assigned a financial value by computing the damage to assets, loss of earnings, additional costs, or new benefits that the risk would cause. There are practical difficulties with this assessment unless it relates to similar incidents from the past, or the anticipated effect can be easily isolated. As an alternative, impacts may be assigned a numerical value to present their

relative weight, as compared with other risks (such as a simple 1 to 3 scale from low to high). Another option is to assign a descriptive term—such as *negligible*, *disruptive*, or *catastrophic*. These terms, however, often are converted into numerical values for ease of comparison.

It sometimes is possible to attach a meaningful value that is based on available details from similar events in the past. In this case, a given percentage indicates the chance that the risk event will occur during the time interval under consideration. Otherwise, we can assign a value based on relative likelihood or a qualitative term such as unlikely, possible, probable, or highly likely. It is often quite hard to know whether the assigned value of likelihood is the right one, even if the risk materializes. From time to time, even a low-probability event will occur. [Table II.3](#) illustrates an example of risk severity measures based on a more descriptive estimation of impact and likelihood, and [Table II.4](#) provides definitions.

The purpose of calculating risk severity or level is that it enables us to compare and prioritize risks. For example, if the likelihood of the risk occurring is 50 percent and the financial impact calculated is \$3,000, we may show the risk level as \$1,500. However, when whole numbers are assigned to the risk criteria, it is more customary to use the relative values of each factor, such as 1 to 3, yielding values of 1, 2, 3, 4, 6, and 9 for the severity.

Table II.3. Measures of Severity

Impact	Likelihood		
	Unlikely	Possible	Likely
Catastrophic	High	Very High	Extreme
Disruptive	Medium-low	Medium	High
Problematic	Very Low	Low	Medium-low

Table II.4. Risk Severity Definitions

Dimension	Size	Definition
		It requires nearly all of the management

	Catastrophic	team to focus all of their attention on responding to the problem, such as the destruction of the main premises, or financial losses that threaten total reserves.
Impact:	Disruptive	It requires some of the management team to focus the majority of their attention on responding to the problem, such as a financial loss that threatens to reduce annual earnings by over 50 percent.
	Problematic	It requires a few of the management team to focus some of their attention on responding to the problem, such as the website crashing, or a financial loss that threatens to reduce annual earnings by more than five percent.
	Likely	May occur more than once a year, such as being unable to access emails.
Probability:	Possible	May occur every few years, such as industrial action or terrorist incident.
	Unlikely	May occur only once in a working life, such as the premises being destroyed by fire.

Not all authors agree that the level or severity of risk should be assessed and assigned simple numerical values like this. (See, for example, Sobel and Reding, 2012.) The danger with such calculations is that they are a simplification of a more complex reality. Although a graphical depiction may be preferred, even this is a stylized representation of only a small portion of the big picture. We can extend the assessment of risk level or severity by adding other criteria such as velocity, volatility, and vulnerability. These can be used to add weight to a risk value, which may be important to prioritization.

II.B.3.v Risk Mapping and Prioritization

KEY TERM

Risk map: Graphical depiction of risks, usually on two axes of impact and likelihood.

Although risk assessment is undertaken piecemeal, it is very important to get an overview of the whole organization to compare the overall risk profile against the total risk capacity. For a number of reasons, it can be a complex and sometimes daunting undertaking to get a comprehensive and holistic picture of risks across the whole organization. Risk appetite is unlikely to be applied equally in all areas, and there even may be varying risk appetites in different divisions and units of the organization, as well as varying risk appetites for different classes of risk. However, to design and implement consistent enterprisewide strategies that deliver strategic objectives, it is necessary to have an aggregated profile of risk. In addition, although risk responses may be working to keep risks within appetite for individual classes and divisions, the organization needs to ensure it has a balanced profile or overall portfolio of risk that meets the general attitude. Finally, the organization needs to be able to communicate its risk profile to key stakeholders, especially owners and investors.

The usual approach is to produce a *risk map* that depicts all key risks and their relative severity graphically or in a table. [Figure II.9](#) illustrates a generic risk map or heat map where the highest priorities are usually colored red, amber is used to denote those that need to be kept under close supervision but are not as critical as those in red, and green is used to denote those that require no special additional monitoring (although all key risks need planned and systematic monitoring). In [Figure II.9](#), light gray has been used to denote green, medium gray denotes amber, and dark gray denotes red. [Figure II.10](#) illustrates a risk map of possible threats and opportunities.

Such a view is helpful in communicating the organization's position with respect to risk exposure. It also can assist in risk prioritization and determining the appropriate allocation of resources as part of the risk response or treatment.

In addition, it may help identify how risks can be offset against each other to ensure that—despite some instances of bearing risk above appetite—the overall profile remains within risk capacity. Risks with the highest overall severity are likely to be those requiring the most urgent attention.

The risk map picture of the organization's risk profile is linked to *prioritization*. (See [Table II.5](#).) The more granular the measures for likelihood and impact, the greater refinement we can add to ordering the risks that require the most immediate and significant responses or treatments. If we choose to use a three-point scale for impact and likelihood, and measure severity or level of risk as a product of these two, we can readily determine priority levels.

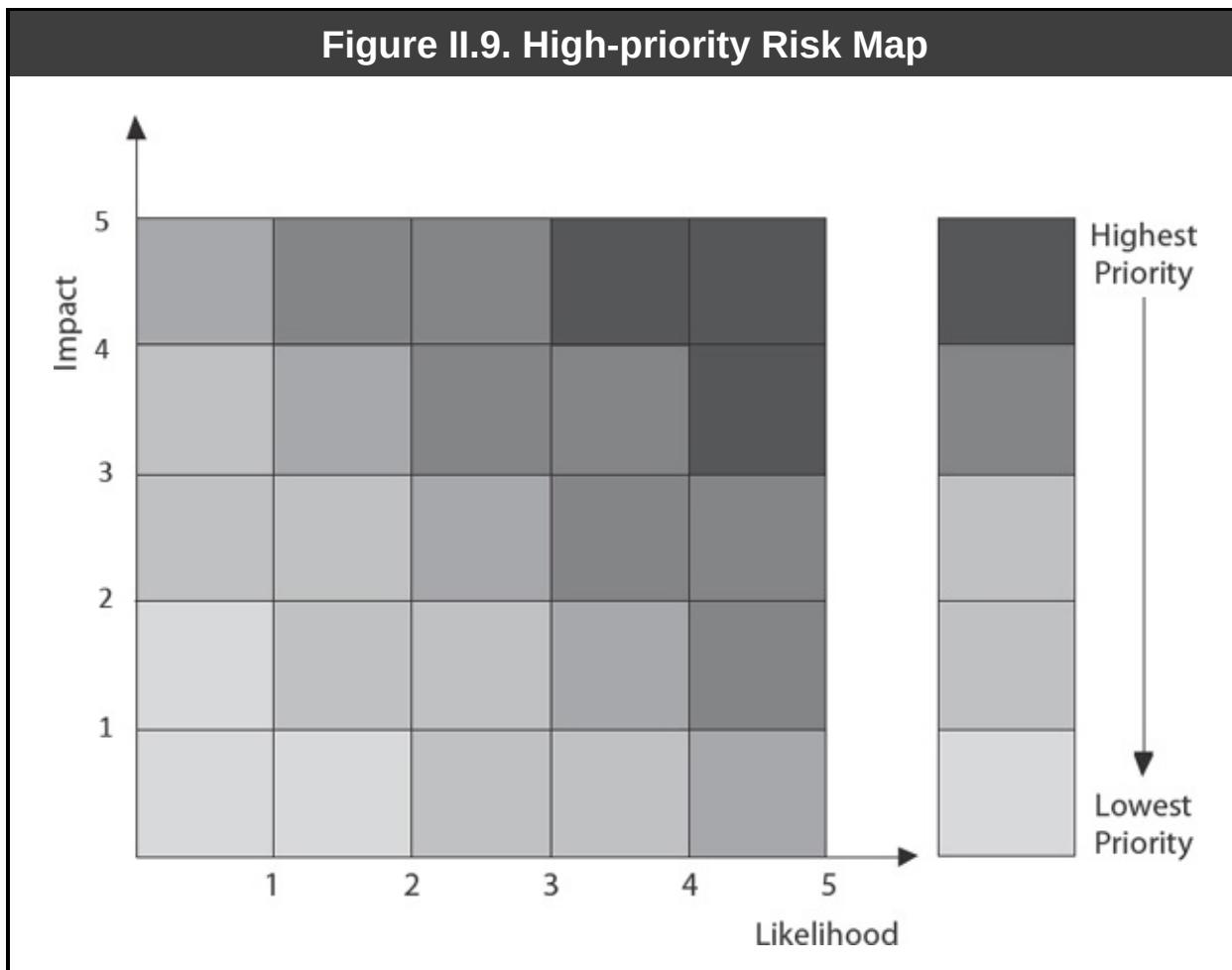


Figure II.10. Threat/Opportuniy Risk Map



Table II.5. Risk Prioritization

Likelihood x Impact	Severity or Level	Priority
High (3) x High (3)	9	1
High (3) x Medium (2) or Medium (2) x High (3)	6	2
Medium (2) x Medium (2)	4	3
High (3) x Low (1) or Low (1) x High (3)	3	4
Medium (2) x Low (1) and Low (1) x Medium (2)	2	5
Low (1) x Low (1)	1	6

However, we should bear in mind the points made earlier about the

oversimplification that such a model incorporates. First, it assumes that likelihood and impact have the same weight. For example, in this scheme, a risk with high likelihood and low impact has the same severity rating as a risk with low likelihood and high impact. This may be true, but not necessarily. We may consider, for instance, that something with the potential to cause a catastrophic blow to the organization—even if unlikely—requires more attention than something highly likely with only moderate consequences.

Another weakness is that the schedule is blind to other types of criteria, such as volatility and velocity. By introducing columns for these factors, it is feasible that prioritization levels would change.

Even when we attach numbers to measures of risk, a significant degree of subjectivity and judgment is required. We are attempting to formalize a process to come up with the important risks an organization faces. According to Sadgrove (2005):

Academics have mathematical formulae to assess risk. This type of risk is rarely understood in boardrooms, and still less so by shop-floor supervisors. Such calculations are of little help to management (unless they can be explained clearly and have practical implications for the business).

KEY TERM

Risk prioritization: Ranking of risks by level or severity.

It is important that those accountable for managing risks and their treatment have a high level of common sense and understanding of their responsibilities. At some point, it is worth asking, “Does it *feel* like these are the most important risks?” It is also worth reiterating that risk analysis, evaluation, and prioritization are processes that require regular refreshing and updates to ensure they remain aligned with the ever-changing organizational context.

Risk maps tend to focus on the two dimensions of likelihood and impact (partly due to the practical difficulties of drawing three-dimensional graphs);

however, we should not overlook the other criteria described above. When calculating values attached to a strategic choice, we may recognize several possible outcomes—some positive and some negative. If each of these is quantified and multiplied by its relative likelihood, the product will provide a value for the option. If the overall value is positive, we may decide that this is an acceptable risk to take, given the availability of resources.

II.B.3.vi Risk Registers

A *risk register*, as described in II.B.2, is usually compiled to keep a record of the risks identified together with the relevant information about them. It may be either electronic or a paper-based record, typically in the form of a table with multiple columns. These records vary considerably among organizations and should be customized to reflect particular needs and circumstances. The following common headings (extended from the now defunct UK Office of Government Commerce quoted in Sadgrove, 2005) are built upon the outline previously provided:

- A unique risk identification number.
- Risk type.
- Risk owner (i.e., the person responsible for the risk).
- Date identified.
- Date last updated.
- Description.
- Cost (if the risk materializes).
- Inherent risk probability.
- Inherent risk impact.
- Inherent risk level or severity.
- Other criteria (e.g., volatility, velocity, vulnerability).

- Risk appetite.
- Possible responses or treatments.
- Chosen treatment and action required to implement.
- Target date (for implementation of the treatment).
- Action owner (if different from the risk owner).
- Closure date.
- Cross-references to plans and associated risks.
- Risk (residual impact, probability, and severity) and action status.

II.B.3.vii Risk Psychology

KEY TERM

Risk response: Measures taken to address a risk.

Risk psychology is a fascinating field of research. There is an unavoidable, yet desirable, subjectivity to risk analysis and a natural inclination to focus on impact, because it is harder to comprehend likelihood in quite the same way. The result is that likelihood becomes exaggerated. Consider the insecurities many people have about flying. The consequences of an airborne disaster are easy and somewhat unsettling to imagine. This translates into a perception that flying is more dangerous (i.e., more risky) than it is—perhaps even more risky than driving. The fact that a passenger is more likely to suffer injury or death in the car on the way to or from the airport does not ease the *psychological weight* given to the risk level associated with flying. This has to do with the element of personal control. When driving a car, the driver feels—rightly or wrongly—that he can make a personal intervention to avoid an accident, but an airline passenger must rely on the pilot's actions, someone else's security arrangements, and the mechanical integrity of the plane.

Likewise, the psychological element is important when considering risk appetite. A group of managers may agree on the defined appetite of the organization, but each individual may vary when it comes to being either a risk taker or a risk avoider. The perceived level of acceptable risk depends on how it aligns with personal risk appetite.

In all situations, the role of risk management is to try to lead organizations toward an understanding of risk and objective appraisal while recognizing both the inevitability and value of subjective impressions. Armed with better information, the organization can make a more intelligent response.

II.B.4 Risk Response (e.g., Avoid, Transfer, Mitigate, Accept), Including Cost/Benefit Analysis

KEY TERM

Risk psychology: The subjective elements of risk assessment.

We have already begun to see how risk analysis helps with the process of prioritization, which in turn draws our attention to *risk responses*. Now that we can prioritize risks for management attention, what level of attention is needed? By using the very simplest risk map and a probability/impact matrix (see [Table II.6.](#)), it is easy to see how an organization can start to categorize its appropriate responses:

- For high-impact/high-probability risks, take immediate action.
- For high-impact/low-probability risks, build contingency plans.
- For low-impact/high-probability risks, consider adjustments to routine operations and other treatments.
- For low-impact/low-probability risks, keep under review.

Table II.6. Risk Profile Responses

Degree of Probability		Degree of Impact	
		Low	High
Low	Keep under review	Build contingency plans	
High	Consider treatments	Take immediate action	

The purpose of addressing risks is to turn uncertainty to the organization's benefit by constraining threats and taking advantage of opportunities. Determining the appropriate risk response is linked very closely to the overall risk attitude of the organization and its risk appetite (as discussed in I.A.3). Appetite may be expressed for classes of individual risks, while the attitude may apply to the philosophy of management and organizational culture.

As illustrated in [Figure II.11](#):

KEY TERM
Risk attitude: Aggregated risk appetite.

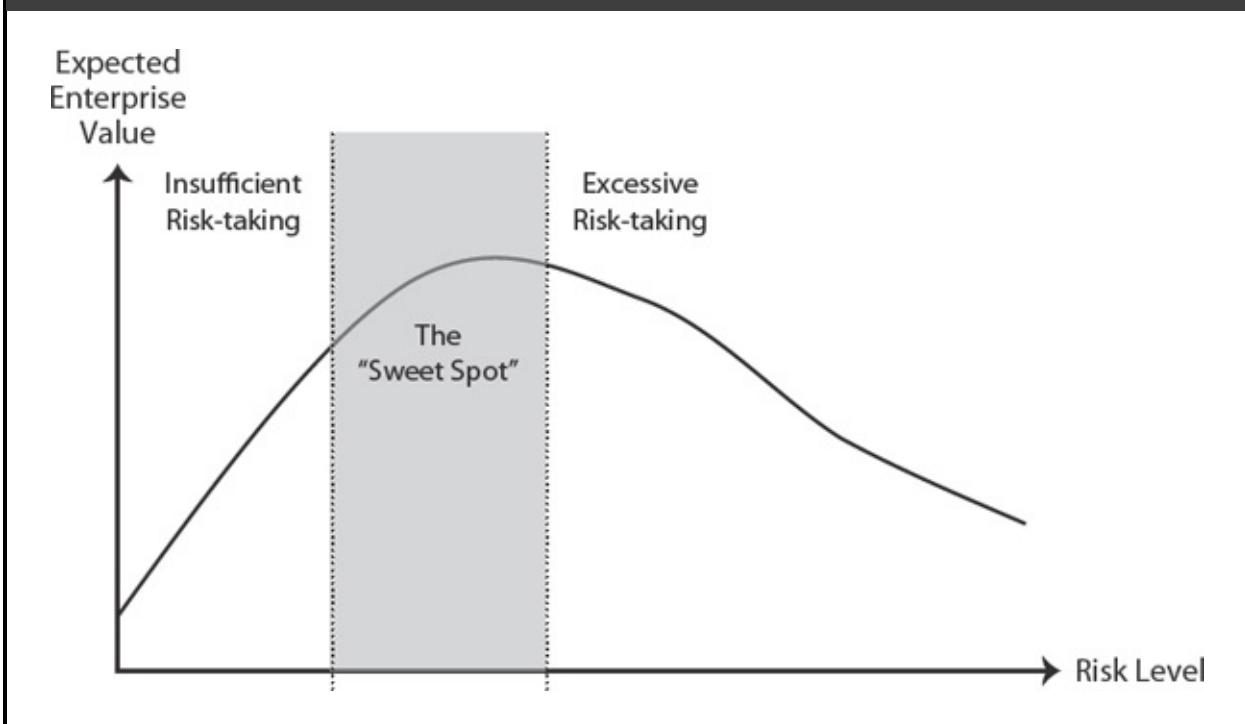
- A *risk-averse* attitude prefers options that offer the same or better return for a lower risk, or a higher return for the same or lower risk.
- A *risk-neutral* attitude prefers the highest return while being indifferent to risk.
- A *risk-seeking* attitude actively seeks high-risk strategies.

Figure II.11. Risk Attitude



In deciding how much risk an organization should take, remember that value is a function of risk and return. Typically, the net value gained by an organization and its stakeholders will increase as risk level increases to a point, after which the value will fall. (See [Figure II.12](#).) The optimum point (the “sweet spot,” says COSO’s guidance) provides the highest net gain. Finding the sweet spot and manipulating risk to keep it there is the purpose of risk management.

Figure II.12. Optimal Risk-taking (based on COSO, 2012)



Once the identification and analysis is complete, the next step in the process is to determine an appropriate response. The *risk response* refers to any actions taken to modify the risk, whether to maximize the potential benefits or mitigate

the negative effects. (See [Figure II.13](#).)

Risk response options include:

KEY TERM

Sweet spot: The position of optimal risk-taking that maximizes benefits to the enterprise.

- Treat—introduce or strengthen internal controls to mitigate the risk (reduce likelihood and/or impact).
- Tolerate—accept the risk based on a sound understanding of it.
- Transfer—apportion some or all of the risk to a third party, typically through some form of insurance, joint initiative, or outsourcing.
- Terminate—cease the activity or withdraw from the situation in which the risk arises.

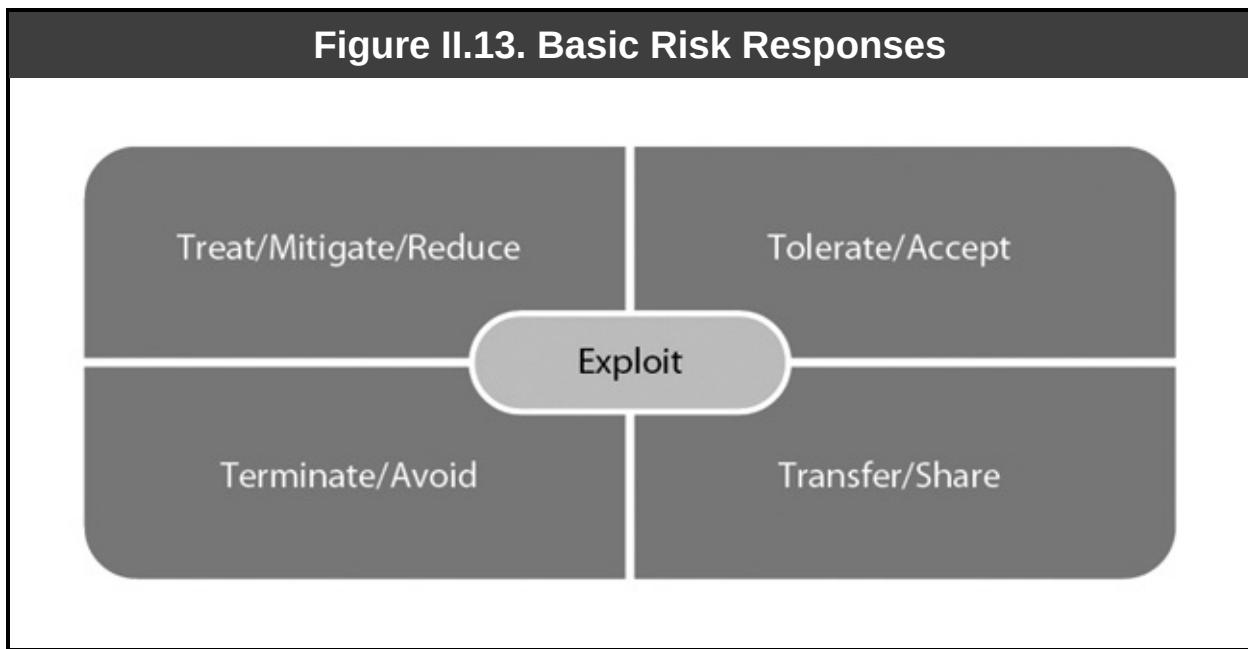
This is similar to the options listed in COSO's ERM framework, which also focuses on downside risks:

- Avoidance (terminate)
- Reduction (treat)
- Sharing (transfer)
- Accepting (tolerate)

The ISO 31000 framework suggests similar responses, but it also includes responses to opportunities:

- Avoiding
- Mitigating

- Sharing
- Accepting
- Exploiting (by accepting or increasing the risk to maximize the potential benefit)



Given these basic choices, how should our risk management processes guide us toward the most appropriate responses? The factors to take into consideration include:

- The risk attitude of the organization.
- The risk appetite for each class and individual risk.
- The risk capacity of the organization (i.e., how much risk it can accept overall).
- The risk profile of the organization (i.e., the present distribution of risks across the organization).
- The risk tolerance of the organization (i.e., the ability to accept risk, even temporarily, at a level above risk appetite).

- Whether the activity or situation (giving rise to the risk or under threat from it) is core to the purpose of the organization.
- Whether a single treatment or a combination of two or more is required.
- The level of confidence the organization has that the intended treatment or treatments will operate with the desired level of efficiency and effectiveness.
- The cost of treating the risk to keep the level within appetite by reducing the likelihood or impact or both, compared with the benefits to be gained from the activity.

In addition to the criteria used to assess and evaluate risks, an organization needs to take stock of its *risk capacity* (i.e., its ability to respond to risk). Sobel and Reding (2012) cite the following *capability criteria* that an organization may use to gauge how much risk it can take:

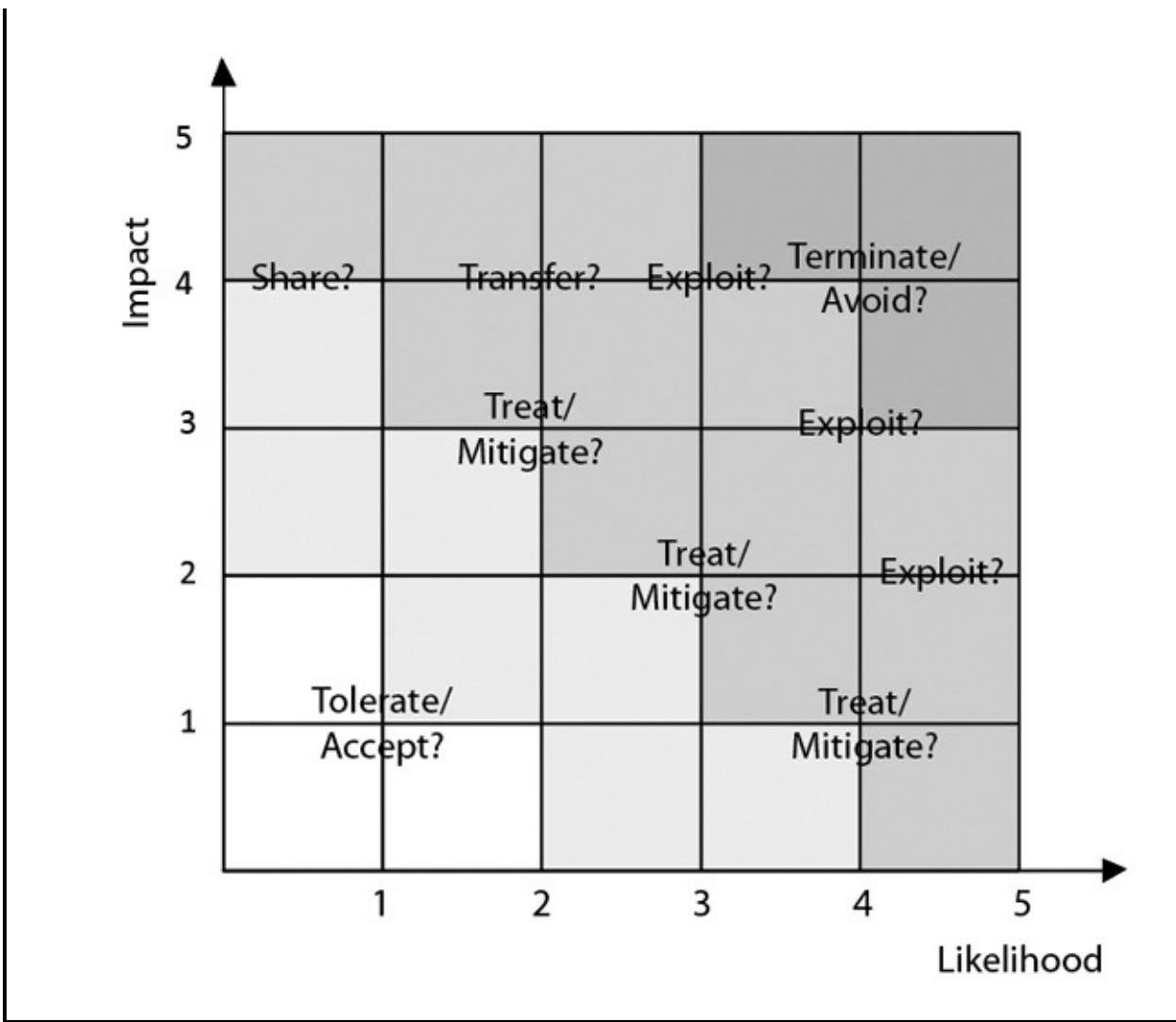
- *Readiness and preparedness* relate to how well the organization can mount its reaction and implement the desired treatment of risks as they arise.
- *Agility* relates to the ability to vary the response, especially if events are volatile and velocity is high.
- *Resilience* is a measure of the organization's ability to continue to mount its response in the context of a particular risk. The organization's resiliency to all risk determines its risk capacity.
- *Controllability* indicates how much influence the organization may exert over the risk. If the cause is ongoing, there is less controllability and the appropriate treatment is likely to focus on impact rather than likelihood.
- *Monitorability* is a measure of how closely the organization is able to track and receive accurate data on the risk. This is generally lower for external events, especially those with high volatility or high velocity.
- *Maturity*, as discussed in I.A.2, is an overall measure of an organization's approach to risk and is in part a reflection of the sum total of these

capability criteria.

- *Degree of confidence* reflects how well the risk is understood, varying among well-known, hypothetical, and unknown. (See II.B.3.)

Given the variability of these factors, there is understandably no standard way of responding to risks based purely on severity or level. As a general starting point, however, activities assessed to have both high-likelihood and high-impact risk are probably ones the organization would consider *terminating*, and those with low-likelihood and low-impact risk are likely to be *tolerated*. *Sharing or transferring* risks might be best suited for high-impact risks, when the likelihood is not high enough to consider terminating altogether. Everything else in between may fall under the heading of *treatment* or mitigation, assuming the risks relate to important activities, the controls are reliable, and the cost of controls does not outweigh the benefit of the activity. High-impact positive (upside) risks or opportunities may be considered for *exploiting*. (See [Figure II.14](#).)

Figure II.14. Risk Level/Severity and Response



Let's consider each of the major responses to risk in detail.

Terminate

The decision to terminate an activity or operation that exposes the organization to certain kinds of risk is usually based on the recognition that benefits to be gained are not worth the risk. Alternatively, it may mean that the risk cannot be treated economically to a tolerable level. For example, such risks may include the safety of staff (for instance, when operating in hostile geographical locations), the potential for large financial losses (when investing in high-risk options), or fundamental damage to the organization's reputation (when engaging in activities that would be poorly regarded by customers, even though they may be legal). These risks can be avoided by ceasing the activities.

This is sometimes an appropriate response to risks associated with continuing a project that is in danger of incurring additional costs, tying up resources, and over-running without delivering the desired benefits. Although organizations are reticent to abandon projects after time and resources have been applied, terminating an activity whose benefits now seem unlikely avoids the risk of incurring even greater losses. Private-sector organizations are usually able to pick and choose which activities to terminate or situations to avoid. In the public sector, however, there is often no option to terminate parts of a socially desirable service because of potential risks. For example, health workers and security forces may be exposed to abuse and potential violence in some settings, but the only available risk response is to treat, rather than terminate, because the private sector does not want to own the service.

Tolerate

Risks of low likelihood or low impact may be tolerated. For example, large retail outlets dealing with cash sales may tolerate a certain level of theft by staff because the cost of measures necessary to catch 100 percent of the incidents would be prohibitive. In the case of higher levels of risk, organizations with a higher appetite may tolerate such losses because of the potential advantages. Sometimes, risks are tolerated because there is no easy way to treat them. Risks should not be tolerated simply because they are not well understood. Such silent risks arise quite unexpectedly.

Transfer/share

Risks can be shared with or transferred to another organization that is more willing to tolerate them. Insurance companies can accept risks because they calculate the cumulative value of doing so, compared with the costs of paying claims. Businesses can outsource non-essential functions to others with specialist capabilities or economies of scale. There are other risks in both of these examples. Insurance companies are likely to expect an organization to suffer the first part of the risk and prove that it took adequate care to prevent the risk from becoming an event. Claims may be contested and some losses are uninsurable. Outsourcing will expose an organization to third-party risks (discussed in I.B.7), and these, in turn, require an appropriate treatment.

When deciding to transfer a risk, it is important to consider carefully what is

being done and if, in fact, the risk is genuinely being transferred. For example, outsourcing may not necessarily transfer the risk but merely change the person responsible for managing it. Consequently, the risk still needs to be treated in some way. Similarly, insurance does not transfer all risk—just some or most of the cost of the impact.

Treat

Most risks will be tolerated and some form of control will be applied to ensure that inherent risk is within appetite. Organizational activity is naturally risky (like all activity), as future outcomes are never absolutely certain. Simple controls—such as the segregation of duties, especially in financial processes—are often sufficient.

The IRM *Risk Management Standard* describes risk treatment as the process of selecting and implementing measures to modify the risk. By far, the greater number of risks will be addressed in this way. The purpose of treatment is to take action (control) to keep risk at an acceptable level. In I.B.1, we defined soft and hard controls. Internal controls can be subdivided further according to their particular purpose, and risk treatment can be categorized further under four different types of controls. (See [Figure II.15](#).)

Figure II.15. Controls for Treating Risk

Preventative Controls

- These controls are designed to stop or limit the possibility of an undesirable event from happening.
- Examples include segregation of duties, access controls, and authorization procedures.

Detective Controls

- These controls detect the occurrence of undesirable events.
- Examples include exception reports, error reports, reconciliations, control totals, closed circuit television, and inventory checks.

Directive Controls

- These controls encourage desired behaviors and outcomes.
- Examples include accounting manuals, training and supervision, and strategic plans.

Corrective Controls

- These controls restore normality after the occurrence of undesirable events.
- Examples include virus isolation, incident and complaint handling procedures, and business continuity plans.

It is important that the treatment is focused appropriately to ensure the desired effect. It is possible to fall into the trap of having controls (systems and procedures) that merely formalize a process without tackling the root cause. For this reason, some organizations define control objectives as a way of specifying the treatment's intended effect. This facilitates a better understanding of the treatment designed to address the origin of the risk, and serves to ensure better monitoring and review of its effectiveness.

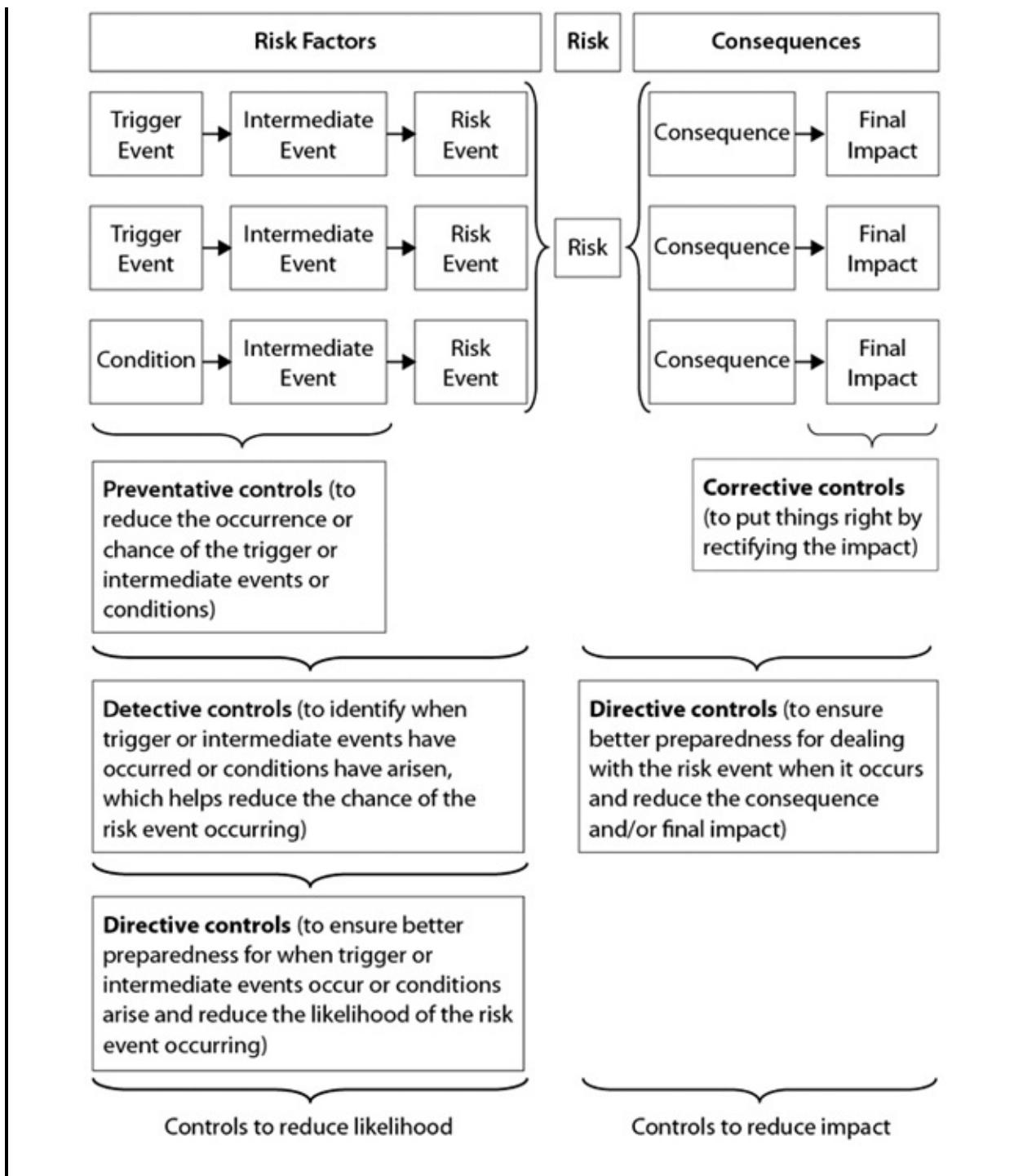
Risk treatment can be targeted at reducing the impact, reducing the likelihood, or a combination of the two. In general terms:

- Preventative controls are designed to reduce likelihood.
- Detective controls are designed to reduce likelihood.

- Directive controls are designed to reduce both likelihood and impact.
- Corrective controls are designed to reduce impact.

To target the treatment correctly, there must be a good understanding of the risk. The extended bow-tie diagram ([Figure II.16](#)) illustrates where different types of controls may be applied.

Figure II.16. Likelihood and Impact



Exploit

When an upside risk presents an opportunity that will add value to the organization's assets or earnings—or will provide better service to the public—an appropriate response is to take advantage of it. Favorable changes in

legislation, the introduction of new technology, and an increase in the availability of desirable skills can be exploited more effectively and more rapidly if the organization anticipates them and has plans in place to take advantage of them. Increasing the investment in a project that promises to yield a positive return also increases the risk and maximizes the potential payout. Unlike downside risk (with negative consequences in the absence of adequate control or intervention), opportunities—other than windfalls—do not normally fully materialize unless the organization takes action. Identification and analysis processes for upside and downside risks are very similar, and the organization must evaluate the expected return against the value of resources necessary to respond. It also is important to be aware of the danger of focusing on opportunities that divert attention and resources away from core strategic objectives.

Blended response

In practice, an organization will probably use a combination of responses to address each risk. Response decisions should be explicit and made at the appropriate level of authority. For example, the board should formally accept any risk that will be tolerated. The board needs to understand the size and nature of the risk, as well as the cost and likely efficacy of the proposed response, so that it can decide how to respond. If transferring or treating a risk is not possible or will cost too much, the organization may decide to tolerate the risk. However, if the risk is particularly large or the underlying activity is not particularly important to the organization, it might be prudent to terminate the underlying activity.

As the organization moves toward a truly integrated enterprise-wide risk management process, it will become more adept at applying the appropriate treatment to particular risks. It also will become aware of the relationships among the risks and how treatments may be used to address more than one risk.

IT controls

There are two main classes of controls applied to treat IT risks:

- *General controls* operate at the most fundamental level and ensure the integrity of IT outputs. With reference to some of the requirements of

Sarbanes-Oxley, examples include:

- The control environment.
 - Change management.
 - Source code/document version-control procedures.
 - Software development life-cycle standards.
 - Security policies, standards, and processes.
 - Incident-management policies and procedures.
 - Technical-support policies and procedures.
 - Hardware/software configuration, installation, testing, management, standards, policies, and procedures.
 - Disaster recovery/backup and recovery procedures.
- *Application controls* are fully automated to ensure correctness of processing throughout the system by:

KEY TERM

IT general controls: Controls designed to ensure the integrity of IT outputs.

KEY TERM

IT application controls: Automated controls designed to ensure correct IT processing.

- Completeness checks.

- Validity checks.
- Identification.
- Authentication.
- Authorization.
- Problem management.
- Change management.
- Input controls.

Risk strategy

As stated earlier, the purpose of risk management is to safeguard assets and maximize value for stakeholders. According to the results of a 2005 Deloitte study of UK companies:

Value is (and will always be) at risk from unexpected, unavoidable internal and external events.

The companies included in the research were found to be particularly vulnerable to risk from unexpected external sources, including:

- One-off shocks:
 - Financial market shocks.
 - Business-malpractice events.
 - Terrorism.
 - Environmental and health disasters.
- Global integration of markets.
- Government policy.

- Market liquidity.

The report highlights differences between companies that are successful in creating value for their shareholders and those that are not:

- Value-creating companies focus on long-term risks and develop far-reaching strategies to address them—usually by building resilience into intangible assets, including brand, reputation, goodwill, and unique organizational capabilities (knowledge, skills, assets, and processes). Such assets serve as a value cushion. These companies also are successful in communicating to key stakeholders about their long-term approach to risk.
- Value-destroying companies rely on short-term tactics that may provide protection from external risks but fail to build long-term value for shareholders. They tend to focus on short-term fluctuations in share prices, which results in being overly risk averse, leading to further volatility.

The report states that *risk avoidance* is not effective in protecting companies from external shocks. The best approach is through value-creation, which makes business less risky and more value-enhancing.

The same report defines risk as the impact an event has on value, and describes two different classes of events:

- *Exogenous events* are the external “one-off shocks” and other situations that can be anticipated but not controlled (i.e., terrorism or a flu epidemic).
- *Endogenous events* are internal occurrences caused by management practices and corporate governance.

Exogenous events affect other organizations and may be responsible for some general volatility in the market as a whole, while endogenous events are unique to a particular organization. The study demonstrates that *interdependency* is an important criterion when analyzing risks, pointing out that organizations with the largest negative impact on value are those that did not appreciate how risks are

related to each other and did not prepare for concurrent events. Such organizations also tended to be underprepared for significant one-off events.

The report concludes that the most effective strategy for the management of long-term risks is proactive creation of value, rather than reactive responses to events as they occur. Risk and value should be considered and monitored together.

II.B.5 Developing and Implementing Risk Mitigation Plans

According to the Project Management Institute (PMI):

Risk mitigation planning is the process of developing options and actions to enhance opportunities and reduce threats to project objectives. Risk mitigation implementation is the process of executing risk mitigation actions. (PMI, 2013)

KEY TERM

Risk mitigation: Treatment of risks.

Risk mitigation employs the processes of risk identification, analysis, prioritization, and response. The plan records what is required to implement the intended response or make amendments to existing responses. Such a plan may include all actions required for all the risks, but the prioritization of actions should naturally align with the prioritization of risks. Therefore, responses to risks of high criticality (i.e., those whose residual level is beyond the risk appetite) need to be addressed first. We noted in II.B.4 that prioritization is based on risk level or severity derived from selected criteria. The criteria usually comprise likelihood and impact but also may involve consideration of velocity (or proximity), volatility, and other factors.

Plans are necessary for developing and implementing controls that will mitigate a risk or a number of risks, but it is important not to ignore risks that fall within the level of risk tolerance. Even those risks should be tolerated only *for now*. They should remain in view and be vigilantly scrutinized from time to time

for changes. This is part of the monitoring process. (See II.B.6.)

Implementation plans need to align with the purpose of the operating area, as organizational activity must continue while controls are being developed and implemented. Understanding the needs of those involved in delivering the processes from which the risks arise is essential to devising effective control-implementation plans. Those closest to the action will most likely be the experts on what actually happens. In most cases, they also are the risk owners and the ones responsible for making controls operate effectively. Their support is critical for the success of the risk treatment. Embedded risk management seeks to administer controls within routine activity as much as possible, rather than by creating additional processes. Reengineering an existing process to mitigate the risks and improve operational efficiency is a two-part goal worth pursuing. There is likely more than one way to satisfy control objectives, and the method adopted must be the right one for the team most directly affected.

The steps to developing a risk mitigation plan include:

- Understanding the nature of the risk.
- Reviewing interdependent and correlated risks so that control may be achieved by the same treatment.
- Identifying the risk owner.
- Developing control objectives by carefully describing the control's intended effect on likelihood, impact, and other dimensions of the risk.
- Breaking down the action required in manageable steps with clear criteria, responsibility, resources needed, and deadlines for completion.

Clarifying the steps required, target deadlines, and criteria for success (ways of knowing the task has been completed correctly) makes the process of monitoring much easier.

II.B.6 Monitoring Risk Mitigation Plans and Emerging Risks

Monitoring plays a key role in all leading risk management frameworks. ISO 31000 refers to “continual checking, supervising, and critically observing or

determining the status,” while COSO suggests “ongoing monitoring of activities, separate evaluations, or a combination of the two.” To clarify the importance of these requirements, Sobel and Reding (2012) add their own definition of monitoring as “the assessment of the organization’s context, ERM system, and business performance over time.”

Regardless of how we define it, monitoring helps ensure effective risk management processes by:

- Systematically checking risk mitigation plans to ensure controls are in place and working, while checking for changes to the risk universe.
- Reviewing risk management processes to achieve continuous improvement. (See II.B.8.)

Monitoring risk mitigation plans helps facilitate assurance that the agreed-upon risk treatments have been established, are operational, and are having the desired effect.

For risk treatment or control-remediation plans relating to higher potential exposures (especially in long-term situations), it may be appropriate to monitor performance against the plan. As a minimum, management should receive an assessment of progress against milestones, and the board should receive validated risk treatment plan status reports.

In addition, monitoring can assess the plan structure, resources, accountabilities, project management, etc., and provide recommendations and considerations to enhance the likelihood of plan success. (IIA, 2010)

Responsibility for risk treatment must be clearly understood. Usually, the manager responsible for implementing the response is also required to ensure its effectiveness and report on its status at regular intervals. In practice, the risk owner may have to rely on responsible delegates who are working closest to the source of the risk and/or the location of the control.

Monitoring risk mitigation plans may lead to an updating of the risk register. It

may be necessary to revise the original analysis and assessment to amend the response. In some cases, new risks that were previously unknown or unrecognized will need to be added. It is equally possible (but often overlooked) that controls sometimes can be reduced in the light of experience or due to circumstance changes, and certain risks can be removed from the register altogether. All changes should be communicated to those required to implement them.

Monitoring risk mitigation plans should include considering the cost-effectiveness of the treatments in place. It is useful to challenge what has been established and assess whether resources are still warranted to maintain the controls. The benefits gained, as well as the value of the risk being treated, also are considerations in the monitoring process.

When monitoring implementation plans and scanning for emerging risks, it is beneficial to involve individuals who are directly engaged with implementing the controls and other measures in response to identified risks. Also helpful are independent views from those working in different areas or individuals outside the organization. This maximizes the effectiveness of the review and builds ongoing support for a positive risk culture.

A key extension to ERM is the identification and monitoring of emerging risks and opportunities. In a 2009 study by PricewaterhouseCoopers (PwC), organizations were urged to maintain a watching brief on new risks, because previously unknown risks cause the most damage.

KEY TERM

Emerging risk: A new risk that is not fully understood and has not yet fully revealed itself.

To address risks that are unknown or unknowable, organizations must adopt a systematic approach to identifying, assessing, and managing emerging risks. Effectively applying ERM principles can help business leaders think through informed, rational, and value-creating decisions regarding emerging risks. Organizations can better protect themselves

and even further their strategies and objectives by embedding this discipline into their risk management culture. (PwC, 2009)

The report suggests a number of steps organizations can take to address emerging risks.

- *Identify emerging risks relevant to the organization:* This is achieved in much the same way as risk identification but with an extra emphasis on scenario planning and projecting current trends into the future.
- *Assess the risk's significance and interconnectedness with other risks and implications to the business:* This requires risk analysis and a deep understanding of the string of events and conditions that we illustrated earlier in the bow-tie diagram.
- *Determine risk response strategies, considering collaboration with external parties:* All of the usual responses are available for emerging risks and should be selected based on the analysis we have already examined. However, given the uncertainty and potential volatility of such activities, it is worth focusing particular consideration on transferring and sharing.
- *Routinely monitor emerging risks through the effective use of indicators:* Emerging risks should be prioritized for monitoring until they are better understood. It is possible that the values for likelihood and impact will lessen as time progresses. However, they are just as likely to increase and, therefore, require close scrutiny.

Key conclusions of the PwC report are:

- Applying ERM principles to emerging risks represents an opportunity to fully capture the rewards of effective risk management as manifested in the organization's ability to detect and respond to large-scale risks. Such discipline should be embedded in the processes and tools used for planning, executing, and evaluating business performance.
- With the use of innovative approaches such as scenario analysis and event simulations (supported by a strong risk management culture),

organizations will be better able to identify and prioritize emerging risks to protect value and further the organization's strategy and objectives.

II.B.7 Reporting Risk Management Processes and Risks, Including Risk Mitigation Plans and Emerging Risks

The purpose of reporting on matters relating to risk management processes is to satisfy a number of requirements. Overall, the aim is to provide assurance to management and the board that risk management processes are effective in that they keep key risks in view, support management in its understanding of risk and its preparedness for risk events, and respond to changes in the risk profile.

KEY TERM

Risk incident: The materialization of a risk.

Risk management reporting should include communicating about:

- Changes in the risk register or new risks that arise from internal or external environmental changes or modifications to strategic objectives.
- Weaknesses identified in the internal control system (whether temporary or longer term) that elevate residual risks beyond the limits of the risk appetite.
- *Risk incidents* (risks that have materialized as events) and treatment effectiveness.
- Updates on actions taken to treat risks.

Reporting confirms success of the identification, analysis, and evaluation of risks. It provides a check on the appropriateness and reliability of the treatments in place. It also helps to integrate and embed risk management processes, contributes to an increasing understanding of risk, and prompts a steady advance of risk maturity.

KEY TERM

Risk maturity: A robust risk management approach adopted and applied, as planned, by management across the organization.

Reporting should consider the information needs of both internal and external stakeholders. The expectation for disclosures on risk and risk management processes increases almost daily. Effective reporting on risk management processes should occur at all levels of the organization to the required level of detail, and should be fully integrated within routine activity and other forms of reporting. This may include performance reviews, management accounts, appraisals, and project monitoring. The board needs to be kept aware of the integrity of risk management and internal control as a whole, and of significant changes in the risk universe—especially in the strategic-risk register. Managers require information that relates to activities and control resiliency within their areas of responsibility.

Like all forms of reporting, communication related to risk management processes needs to be evidence-based, timely, relevant, and in a format that facilitates assimilation and understanding. All organizations run the danger of information overload. Therefore, focusing on the salient points serves to enhance communication.

Information and communication technology (ICT) is increasingly used to support the exchange of useful information. This may start with risk profiling, tracking internal controls, and other structured approaches that provide up-to-the-minute data and handy reminders. There are many risk management and reporting software programs that yield user-friendly, high-impact outputs. It is important, however, to avoid being seduced by what the technology can do, rather than paying attention to what it reveals about organizational risk. The ability to report on risk management processes relies upon regular monitoring. (See II.B.6.)

As indicated in The IIA's Position Paper, The Three Lines of Defense in Effective Risk Management and Control (IIA, 2013), the second line (specifically, the risk management function) is responsible for monitoring management's implementation of effective risk management practices. This line

of defense also assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.

KEY TERM

Risk escalation: The process of reporting risk incidents up the line.

The reporting of risk incidents up the chain of command is known as *escalation*. The greater the threat (or opportunity), the higher up the chain the reporting should go—especially if it is apparent that the internal controls are ineffective. There should be a designated point at which escalation is required, starting with *risk capture*—the ability to recognize and record that a risk event has occurred. If the system is too sensitive and too many small risk incidents are escalated, the process becomes ineffective. At the right degree of criticality, the process needs to be sufficiently rapid for management to respond. The purpose of escalation is partly to keep managers informed of risk incidents, as well as to precipitate implementation of a *contingency plan*. This may be a combination of directly addressing the incident and considering some other action (including termination of the activity, at least temporarily) to prevent recurrence.

Management should be able to answer several key questions about risk incidents:

- Had we identified the risk correctly?

KEY TERM

Risk capture: The ability to recognize and record the materialization of a risk incident.

- Was our assessment of the risk adequate or did we lack the required information?
- Did we select an appropriate response?

- If the control failed, can it be improved in the future?
- Was there an unexpected combination of events that took us by surprise?
- What can be learned from this incident to improve risk management processes in the future?

Contingency planning should be considered at the point of determining the appropriate risk response. It may form part of the control itself or be a stand-alone option. An organization can usually tolerate a higher level of risk if it knows that there is a fallback plan that will recover the situation after an incident. The cost of developing and resourcing contingencies needs to be taken into account. For those risks that have the potential to be fatal to the organization, it is common practice to develop a separate *business continuity (or disaster recovery) plan*. This is a particular contingency plan for resuming normal operating activities as quickly as possible, with minimum disruption, following a catastrophic event. Given the importance of survival, significant resources are often allocated to such plans. Although this is often undertaken as a distinct element of planning, it should be properly regarded as a general risk management concern.

Risks that could severely impact the day-to-day operations should be identified from the register of risks and analyzed in detail. These usually include natural disasters (such as extreme weather or flu epidemics), malicious damage like terrorism and cyber attacks, systems failure, widespread industrial action, and sustained economic downturns.

KEY TERM

Contingency plan: Provisional plan for addressing the impact of a risk incident.

The status of a risk, particularly the residual risk following treatment, is often communicated using a RAG (*red, amber, green*) rating, denoting the acceptability of the current position. *Red* represents the most serious state, requiring urgent action to prevent a more serious issue. *Amber* is used to show

that, although there is no immediate danger of a risk causing significant problems, the situation needs to be monitored carefully. A *green* rating indicates that the controls in place are adequate and are working to maintain the risk within the agreed appetite.

In addition to reporting risk incidents, there is value in considering near misses. Often, there is much to be learned from materializing risks that did not produce the most detrimental outcomes. Cheshire (2010) provides examples of:

- Health and safety breaches that do not result in reportable injuries.
- A small fire that was extinguished before it could spread.
- A fraud that was detected early while the losses involved were relatively low.
- An entire board travelling together on an airplane that made an emergency landing with no injuries.

II.B.8 Periodic Review of Risk Management Processes to Aid in Continuous Improvement

Senior managers and the board need to work closely with operational managers and the risk management function to facilitate continuous improvement in risk management processes. The purpose of periodic reviews is to identify issues that may affect any of the elements of the adopted risk management approach, examine them carefully, and determine whether changes are required or improvements are possible. Such issues may be brought to the organization's attention through either internal or external review, or as a result of a risk incident.

Periodic review of risk management processes provides a way of checking that they are functioning correctly—from risk identification to implementing effective responses—and reporting to key stakeholders. There is always the potential that parts of any system may become weakened or fail altogether. Author John Gall (1978) wrote about the many reasons systems are prone to failure, including:

- All systems, especially complicated ones, naturally will fail, unless

adequately maintained.

- Systems designed to solve problems generate new problems.
- Issues or problems are changed by the systems that are designed to solve them.
- Systems are subject to “mission creep.”
- Complex systems become inherently unpredictable.
- Complex systems tend to defeat themselves.
- Individuals who are part of a system do not actually do what the system says they do.
- As systems get larger, they no longer achieve what they were designed to achieve.
- A system is only as good as the information it draws upon.
- Systems attract systems people.
- Large systems squeeze out individual interaction.
- Systems develop goals of their own.

The review of risk management processes has the following three aims (Sobel and Reding, 2012):

1. To identify and repair weaknesses and faults in risk management processes.
2. To identify changes in the organization’s objectives and environments, and to ensure that risk management processes remain in alignment.
3. To determine that the organization is achieving its goals (because risk management is working).

According to Sobel and Reding, each of these requires a different focus and a

particular approach.

1. To identify and repair weaknesses and faults in risk management processes

To achieve this aim, it is necessary to review the system of risk management processes themselves (from risk identification to reporting. This part of the review takes a critical look at the risk processes to identify, assess, evaluate, determine, and implement responses, and to report on risks. The review may seek answers to the questions:

- Is the risk management framework appropriately comprehensive, robust, and embedded?
- Are the processes being diligently applied?
- Are the processes working to achieve the aims of risk management?

As a check on the processes and their effectiveness, the review needs to undertake activities such as:

- A comparative evaluation of the risk register, the organization's strategic objectives, and internal and external environments.
- Appropriate benchmarking of internal controls to identify deficiencies.
- Reviewing records of risk incidents, identifying lessons to be learned, and checking to ensure these have been used for appropriate improvements.
- Testing controls in high-risk areas to ensure they are in place and operational.

2. To identify changes in the organization's objectives and environments, and ensure risk management processes remain in alignment

To achieve this aim, it is necessary to review the organizational context. This includes the content of domain I, in addition to II.B.1. Risks are defined as

unexpected events that may impact organizational objectives positively or negatively. Organizations operate within the capabilities of their internal environment. They also operate in—and are best understood as a reaction to—a changing external environment. This part of the review should encompass all organizational features explored in domain I. This understanding is critical to all risk management processes, from risk identification to implementing responses and reporting. Refreshing knowledge through review enables us to reconsider the same elements to determine whether adjustments are needed in response to changes.

To track developments in the organization's objectives, capabilities, and the environment in which it operates, the review needs to look for new or changing risk indicators. This may be achieved, for example, through:

- Horizon scanning across all elements of the external environment, using the PESTEL mnemonic as a guide through trade journals, quality newspapers, competitor analysis, market intelligence, and networking. (See I.C.1.)
- Performance monitoring and staff surveys.

It is also important to keep abreast of possible changes to risk appetite, as this does not remain fixed forever. Formal expressions of appetite may come from board papers and other internal documents.

3. To determine that the organization is achieving its goals (because risk management is working)

To achieve this aim, it is necessary to review business performance as defined for the organization. The fundamental aim of risk management is to help the organization achieve its goals. Therefore, if risk management is working, the organization will be performing well. It is often challenging to check on this, as an organization may succeed (at least in the short- to medium-term) not because of its risk management processes, but in spite of them. Failure in strategic planning and attainment of goals is easier to attribute to risk management's weaknesses than organizational success is to attribute to its strengths.

Reviewing business performance for this purpose requires considering the

organization's key performance indicators (through its balanced scorecard or a similar process). Analyses may include operating results from finance, production, HR, IT, marketing, and customer relations to identify potential weaknesses in internal controls. Underperformance, as measured against targets, reveals a failure of some kind—strategy, planning, targetsetting, forecasting, reporting, operational management, systems, or capability. In other words, these weaknesses produce unexpected surprises that risk management should have eliminated.

KEY TERM

Ongoing assessments: Regular or continuous embedded reviews.

In accordance with The IIA's Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000 (IIA, 2010), reviews may be accomplished via *ongoing* and *separate* assessments. *Ongoing assessments* operate within the risk management processes close to the activities being reviewed.

They may be periodic, at regular intervals, or continuous. This means that repairs to the system can be made quickly. *Separate assessments* are more likely to be done at more of a distance—both in time and proximity to the activity under review. They can provide a more objective view, as well as verify the findings made through integrated reviews.

KEY TERM

Separate assessments: Periodic and external reviews.

Roles are played by all levels of staff and management, and this requires careful integration to avoid overlap, gaps, or confusion.

With responsibility for monitoring and assurance activities traditionally being shared among various parties, including line management, the internal audit function, risk management specialists, and the compliance function, it is

important that assurance activities be coordinated to ensure resources are used in the most effective and efficient way. Without effective coordination and reporting, work can be duplicated or key risks may be missed or misjudged. (IIA, 2010)

Risk management and its contribution to governance belong to the senior team or board. These parties are ultimately responsible for ensuring that it is regularly reviewed and kept fit for purpose. In the three lines of defense model, the first line (operational management) is responsible for “ensuring that activities are consistent with goals and objectives.” (IIA, 2013) The second line, however, operates as a risk management and compliance function and plays a key role in any review activity to keep risk management processes in alignment with the needs of the organization. Identifying trends and shifts in risks and risk appetite are a key part of this second line. These views, however, can never be wholly objective or independent, as they are too close to the implementation of risk management processes and controls. The third line (the internal audit function) is able to offer an objective perspective that is a fundamental part of risk management assurance.

Building on guidance provided by the Treasury Board Secretariat of Canada (TBS, 2013), the following key areas are important components of a strategy for periodic review of risk management processes:

- Clear roles and responsibilities for monitoring and review to ensure all parties (including senior management) are aware of their expected involvement and contribution.
- Effective integration with other oversight and assurance functions (including internal audit and compliance) so that they are well coordinated without undue overlap or duplication.
- Careful consideration of the timing of reviews to facilitate participation of all key players, and avoiding clashes (as much as possible) with other cyclical activities that may present competing demands.
- Appropriate communication mechanisms that serve to promulgate lessons learned to all key stakeholders.

- Well-documented records of expected outcomes from risk management in terms of the desired effect on risks and opportunities to provide a basis for review.
- Other performance indicators and measures that are subject to periodic review to ensure they are challenging and achievable.

The TBS guidance outlines the focus of the review to:

- Confirm that risk management is adding value to decision-making, business planning, resource allocation, and operational management.
- Validate that an organization's risk management approach and process are appropriate for its risk management needs and remains responsive to its external and internal context, including its mandate, priorities, organizational risk culture, risk management capacity, and partner and stakeholder interests.
- Ensure ongoing relevance, effectiveness, and efficiency of the risk management approach and process (including relevant policies and supporting tools), in relation to its mandate, key outcomes, and evolving risk management principles and practices.
- Check for new approaches, tools, and ideas.
- Assess compliance with relevant laws, regulations, and policies. We should also add:
- Assess the allocation of resources in risk responses as part of a cost-benefit analysis.

Finally, to emulate best practice and current trends in risk management, consider the following. These are seven areas identified in Leitch (2008) in which risk management generally should aim to make progress (and is likely to do so, based on current trends):

- A greater focus on and investment in internal controls, and a move away from remediation and compliance measures (the prime example of the latter being the piecemeal and costly approach taken by many

organizations to meet the requirements of Sarbanes-Oxley).

- Continued movement toward convergence of internal control and risk management through the use of intelligent controls for the smaller, recurring internal risk events (that traditionally are the focus of internal control), as well as the big, nonrecurring risk events (that usually fall within the province of risk management).
- The development and adoption of better methods to quantify risk and move performance metrics away from the traditional high, medium, and low classifications.
- Less focus on the risk register as an end in itself, and more emphasis on improving controls, embedding risk awareness into projects and business practice generally, challenging complacency, and changing management's behavior.
- Greater understanding and application of psychological factors that impact risk identification, assessment, analysis, and reporting to improve risk management.
- Continued movement toward convergence of risk and performance management to remove the reliance on two separate systems and overlapping sets of records; and ultimately developing a *strategy map* that unites risk registers and the balanced scorecard.
- Greater use of a more technical approach to producing risk registers with additional reliance on mathematical models.

Summary

We have covered the detailed processes of risk management to prepare you for evaluating their effectiveness and subsequently providing assurance on them. Clearly, these processes can be very lengthy and even bureaucratic. There is a danger of becoming bogged down in the detail and forgetting what these processes are trying to achieve. It is good to take a step back and consider the bigger picture. Risk management exists to help an organization achieve its

objectives, protect its value, and avoid surprises. There are plenty of resources and standards to help with the task, but they must be appropriate for the organization in consideration of its culture, size, objectives, environment, and risk maturity. There are critics of risk management who believe it has become a self-serving industry, and—in its worst excesses—this is sometimes true. It is always important to ask of any tool, method, or framework:

- Will it help us manage our risks?
- Will we be able to identify, analyze, respond to, and report on risks more effectively?
- Does it add to our understanding of risk?

If the answers to these questions are not positive, the organization needs a different way of doing things.

Among the many definitions and technical content of risk management, terms sometimes can be used differently (or misused) by others. Therefore, a very useful starting point is a conversation with all involved parties to agree to a common language for discussing risk management processes.

Armed with detailed knowledge about risk management processes and how they may be assessed, we turn our attention to risk management assurance in domain III.

DOMAIN III

Assurance Role of the Internal Auditor

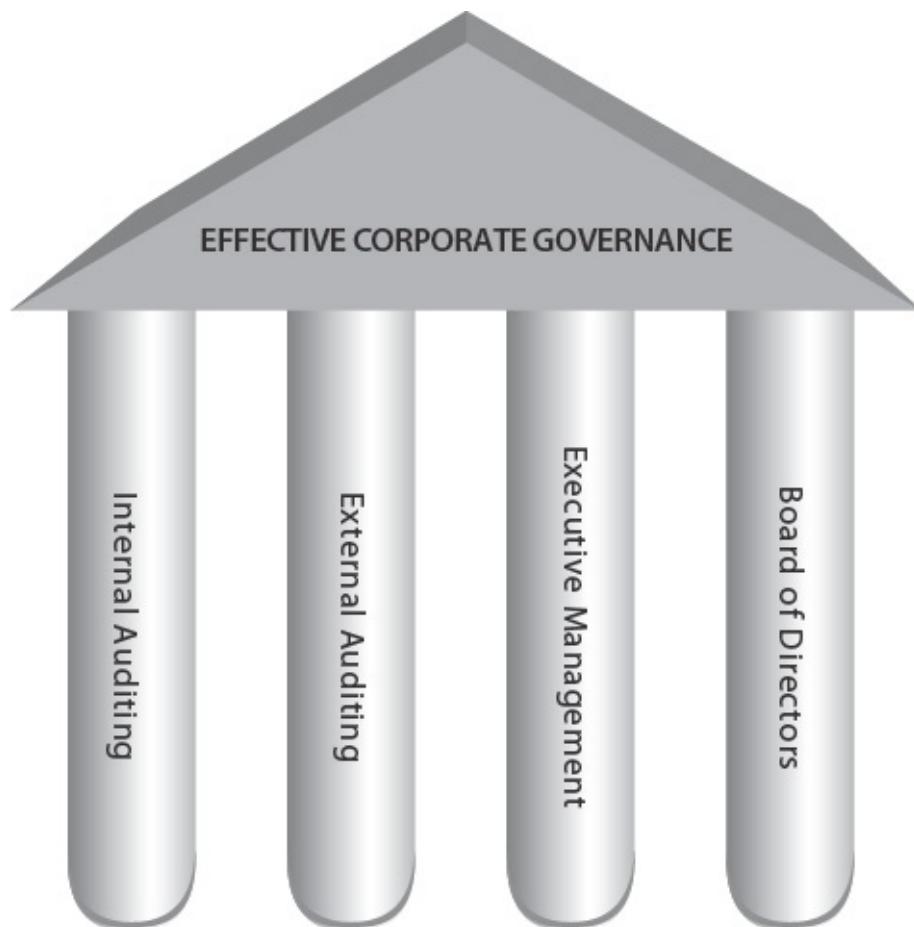
Table III.1. Domain III Outline		
Topic/subtopic	Explanation	Reference # in study guide
A. Review the management of key risks.	<p>Key risks are those that are the most significant to the organization and that have the greatest potential for negative or positive impact. Therefore, they warrant the closest attention to ensure they have been accurately identified, analyzed, and evaluated, and responded to in the most appropriate way. Plans for risk mitigation or opportunity maximization also require careful monitoring. Key risk indicators (KRIs) form an important role in the effective management of key risks. The internal audit activity can provide an independent and objective review of the management of key risks as part of its overall assurance role.</p>	III.A
B. Evaluate the	<p>Due to their potential for significant impact, key risks are a priority for all stakeholders. This evaluation includes an update on the current status of risk and the effectiveness of risk</p>	

reporting of key risks.	mitigation. It also requires close attention to new and emerging risks. Internal auditors evaluate the quality of reporting to ensure that management, the board, and others are getting a clear and accurate view about key risks.	III.B
C. Provide assurance that risks are adequately evaluated.	As discussed in domain II, this extremely important process requires a systematic and consistent approach, as prioritization, risk responses, and the allocation of resources for mitigation are all based on the evaluation of risk. The internal auditors may provide assurance by assessing the evaluation process and delivering an opinion on risk evaluation.	III.C
D. Provide assurance on risk management processes.	As described in domain II, risk management processes cover risk identification, analysis, response, mitigation planning and monitoring, and regular review for continuous improvement. The board and other stakeholders typically want assurance that these processes have been—and continue to be—operating effectively. The IIA's Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000, recognizes the three approaches described in this section.	III.D

Introduction to Domain III

Internal auditing is sometimes described as one of the four cornerstones of governance (see, for example, Adamec, 2005). The other three cornerstones are external auditing, executive management, and the board of directors (as shown in [Figure III.1](#)). Two key contributions that the internal audit activity makes to governance are included in the definition of internal auditing. First, internal audit provides *assurance* on the effectiveness of governance, risk management, and internal control. Second, it provides *advisory services* for improvement. In this and the next domain we will focus on how these two contributions apply, in particular, to risk management processes.

Figure III.1. Cornerstones of Corporate Governance



According to The IIA's Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000, “assurance and risk management are complementary processes.” (IIA, 2010) Clearly, internal auditing plays a very

important role in improving the maturity of risk management. In fact, according to Pickett (2005), the internal auditors may play a number of roles with respect to effective risk management, including:

- Raising the profile of risk in organizational decision-making and planning at all levels.
- Providing training and guidance to other managers and staff.
- Making recommendations for improvement to risk-based controls.
- Keeping up-to-date with the latest thinking and serving as a source of risk expertise for the organization.

KEY TERM

Audit universe: The summation of all possible internal audits.

- Ensuring risk management is consistent and well-coordinated on an enterprise-wide basis.
- Providing assurance on risk management and its processes.
- Reporting on the level of operational risk as part of routine audit work.
- Championing risk and advocating enhanced risk maturity.
- Leading risk identification workshops.
- Providing practical tools that may assist risk management processes.

Sobel (2011) points out that the internal auditors also can:

- Provide training for audit committees and management on all aspects of risk.
- Offer consulting services in support of those charged with risk management.

- Evaluate strategic risk management by determining whether strategic risks are known, responded to appropriately, and monitored accordingly.
- Develop the expertise of the internal audit function to maximize its competency in risk.
- Supplement risk-related skills of the internal audit team (as required) by drawing upon third-party support.

As enterprisewide risk management becomes established in organizations, the internal audit activity can progress from being risk-based to being ERM-based. Standard 2010 requires CAEs to establish risk-based audit plans. The interpretation of the standard makes this clear:

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

Why is it important for audit planning to be ERM-based rather than simply risk-based? Sobel and Reding (2012) provide some of the reasons. With an effective, integrated, enterprisewide approach to risk management, internal audit no longer needs to identify the risk universe. Management takes on that responsibility, and the internal auditors adopt it as the basis for describing the *internal audit universe* (the summation of all possible internal audits). [Figure III.2](#) illustrates how these roles relate to organizational objectives. As stated in

Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures, “The audit universe will normally be influenced by the results of the risk management process ... The CAE prepares the internal audit activity’s audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization.” Of course, this

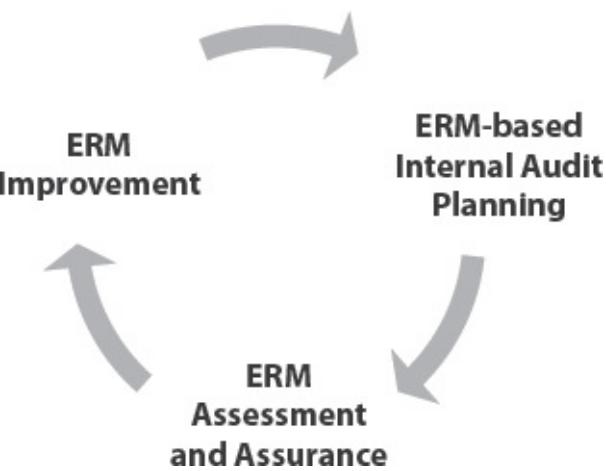
assumes the internal auditors are confident about the ERM processes used to develop the risk universe. ERM can help identify and prioritize the risks that may then direct risk-based audit planning. However, to maintain its independence and objectivity, the internal audit activity must never be wholly dependent on ERM, and the internal auditors must exercise their own judgment about internal audit priorities.

Figure III.2. Important Interrelationships



There should be a positive circular relationship—one in which internal audit draws upon ERM for its risk-based approach. (See [Figure III.3](#).) The internal auditors are responsible for assessing enterprise risk management—which is part of the risk universe—and providing assurance on it. To complete the cycle, this assurance informs ERM improvements.

Figure III.3. ERM and Internal Auditing



It is clear that the internal auditors have a considerable role to play in embedding good enterprise-wide risk management practices. Internal audit provides independent and objective assurance and advisory services with regard to governance, risk, and control. In fulfilling this responsibility, it is critical that the internal auditors maintain sufficient distance from risk management. To secure independence and objectivity, there are certain roles that internal audit should not play. [Table III.2](#) distinguishes between roles the internal auditors can and cannot undertake for risk management.

Table III.2. Distinguishing Internal Audit Roles in ERM

Core Internal Audit Roles with Regard to ERM	Legitimate Internal Audit Roles with Safeguards	Roles the Internal Auditors Should Not Undertake
<ul style="list-style-type: none"> • Providing assurance on the risk management process 	<ul style="list-style-type: none"> • Facilitating the identification and evaluation of risks • Coaching management in responding to 	<ul style="list-style-type: none"> • Setting the risk appetite • Imposing risk management

<ul style="list-style-type: none"> • Giving assurance that risks are correctly evaluated • Evaluating risk management processes • Evaluating the reporting of key risks • Reviewing the management of key risks 	<p>risks</p> <ul style="list-style-type: none"> • Coordinating ERM activities • Consolidating the reporting of risks • Maintaining and developing the ERM framework • Championing the establishment of ERM • Developing ERM strategy for board approval 	<p>processes</p> <ul style="list-style-type: none"> • Managing assurance on risks • Making decisions on risk responses • Implementing risk responses on management's behalf • Assuming the ownership of and accountability for risk management
---	--	--

When trying to distinguish between what the internal auditors should and should not do, the key factor is risk management responsibility. If the internal auditors do not take on any direct role for managing risks, they can independently and objectively perform any assurance or consulting assignment. It is management's responsibility to ensure that risks are adequately addressed, and ERM is recognized as the best way to do so. According to The IIA, if a role listed in the middle column of [Table III.2](#) is taken on by internal audit, it should be on a temporary basis only, safeguards should be in place, and there should be a plan for handing it over to management. The IIA (2009) recommends the following provisions:

- All parties should be clear that managing risk is the responsibility of management.
- If internal audit does undertake any of the roles in the middle column of [Table III.2](#), the audit committee should expressly approve it in advance as a temporary measure.

- Regardless of the circumstances, the internal audit function should never be required to take on risk management responsibility—even for individual risks—as its role is to *advise, challenge, and support*.
- Any internal audit roles—other than assurance—are considered *consulting*, to which relevant implementation standards apply.

It is a requirement of governance to seek assurance on risk management processes. For the board or equivalent (as the agent) to fulfill its responsibilities to the shareholders or owners (as the principal), it is important that an appropriate balance of interests be maintained between these two groups (an expression of the “agency problem.”) (See I.B.2.) Governance serves that purpose, seeking openness and transparency from the senior management team as it delivers the agreed strategy. After setting the risk appetite and agreeing to the risk strategy, both groups of primary stakeholders (the owners and the managers) need to be confident that risks are being managed as intended. According to The IIA (2010), the internal auditors provide that assurance across the key elements of risk management, including:

- Risk management activities (design and operating effectiveness).
- Management of key risks (including the effectiveness of responses).
- Verification of the rigor and reliability of risk assessments.
- Reporting on the status of risk and control.

Monitoring and assurance must be coordinated, as they are likely to be provided by various sources (including management, the risk oversight function, compliance, and the internal audit function). IIA Standard 2050 requires the CAE to coordinate assurance through *assurance mapping* and other techniques.

Ultimately, senior management must determine the role that the internal auditors play with respect to risk management processes. This is driven by culture, tone at the top, strategy, objectives, and internal audit competency.

The 2009 IIA Position Paper, *The Role of Internal Auditing in Enterprise Risk Management*, makes a case for three very specific areas in which internal audit can provide risk management assurance. Each of these is reflected strongly in

domain III, namely:

- Risk management processes—both their design and how well they are working (see III.D).
- Management of those risks classified as “key,” including the effectiveness of internal controls and other risk responses (see III.A).
- Reliable and appropriate assessment of risks (see III.C), and reporting of the risk and control status (see III.B).

KEY TERM

Assurance mapping: The act of coordinating all assurance activities to identify and eliminate gaps and overlaps.

IIA Standard 2120 is key to the review and evaluation of risk management and the process of providing assurance. Because it is so important and will be frequently referenced throughout this domain, we quote it in full:

2120 – RISK MANAGEMENT

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation: Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:

- Organizational objectives support and align with the organization’s mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization’s risk appetite.

- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

Domain III counts for 20–25 percent of the CRMA examination.

III.A Review the Management of Key Risks

Senior management teams and other stakeholders are naturally keen to monitor the performance of the organization to ensure that it is fulfilling its purpose. They want to know that the strategy is being achieved and value is being delivered—whether it's *value for money* in the public sector (maximizing the public good from taxpayer dollars) or *a financial return* on earnings and increasing assets. Various means are used to determine value, typically through a set of performance indicators. The balanced scorecard (Kaplan and Norton, 1996) is a well-known and widely used framework for keeping in view key measures across the four primary dimensions of the organization, including the:

- Customers.
- Internal processes.
- Learning and growth (i.e., information capital, organizational capital, and human capital).
- Finances.

KEY TERM

Lag indicator: A measure of something that has already impacted the organization.

The balanced scorecard and other models like it focus on strategic objectives. In developing the scorecard, Kaplan and Norton explain that a focus on purely historical financial measures is no longer adequate “for guiding and evaluating the journey that information-age companies must make to create future value through investment in customers, suppliers, employees, processes, technology, and innovation.” (Balanced Scorecard Institute, 2012)

The intention is to achieve balance—not just across segments in both financial and nonfinancial core activities, but also between *lag* and *lead indicators*. Lag indicators are those that reveal what is happening after the fact. For example, a lag indicator of decline in demand is a decrease in the volume of production and raw materials to fulfill customer orders. An even later indicator is a decrease in actual sales figures, as compared with previous periods. In both cases, trends included in the data show impacts that have already occurred.

On the other hand, lead indicators provide a sign of what will occur in the short- to mid-term. For example, these may include:

KEY TERM

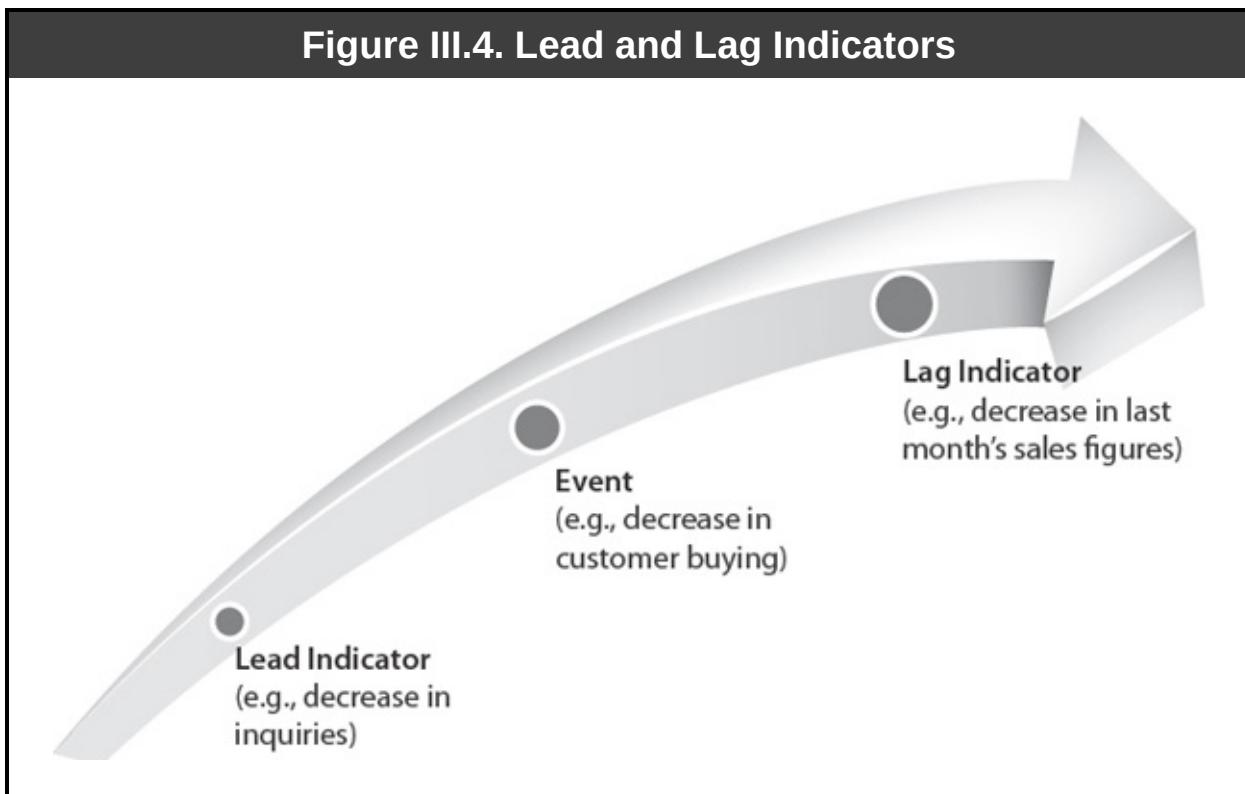
Lead indicator: A measure of something that will impact the organization.

- The number of orders being placed.
- The number of inquiries being received.

The amount of traffic on the organization’s website.

Another lead indicator might be declining sales in complementary goods (goods purchased in conjunction with other goods—such as computer games and computer consoles).

The relationship between lead and lag indicators is illustrated in [Figure III.4](#).



These indicators are particularly critical in regard to risks and risk management. While it is important to have systems in place to monitor, record, and report risk incidents, it is preferable to avoid materialization of risk. There is an even greater urgency with respect to the *key risks* to which the organization may be exposed.

KEY TERM

Key risk: A risk with the potential for significant impact.

We know that changes in the internal or external environment can precipitate previously identified risks and also may bring about new and emerging risks. Senior management must obtain early notice of likely trigger events or conditions to proactively prepare for a potential shift in the risk universe. Lead indicators enable risk owners to project likely trends and (if required) intervene much earlier in the process.

KEY TERM

Key risk indicator (KRI): A lead indicator of risk-triggering events or conditions.

Key risks are those with the highest severity rating and the potential (individually or in combination) for the highest impact. Metrics that may be used as lead indicators of exposure often are referred to as *key risk indicators*. They can play a significant role in strengthening ERM, lessening vulnerability, and improving agility. The value of key risk indicators is captured in the following quote:

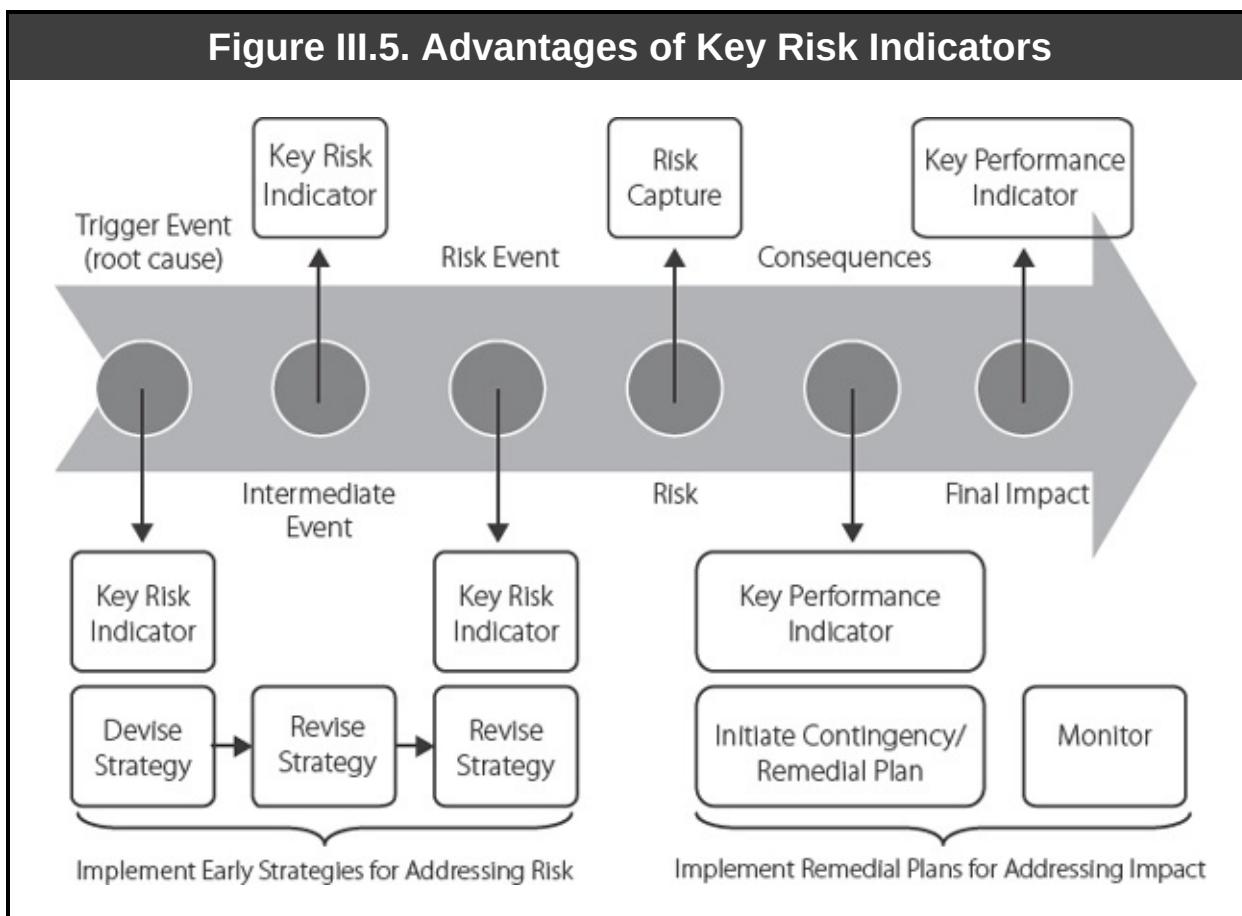
Measures of events or trigger points that might signal issues developing internally within the operations of the organization or potential risks emerging from external events (such as macroeconomic shifts that affect the demand for the organization's products or services) may provide rich information for management and boards to consider as they execute the strategies of the organization. (Beasley, Branson, and Hancock, 2010)

As an example, Beasley et al. consider the monitoring of accounts receivable. A key performance indicator of credit control might be the financial value of amounts written off as bad debts. Although Beasley et al. do not use the term, *lag indicator*, this value measures a risk that has already materialized—that customers will not pay what they owe. It is an important measure that should not be ignored. An accompanying key risk indicator or lead indicator might be a measure of the largest customers' liquidity, based on an analysis of their recent financial performance. This can help indicate that some customers may be suffering cash flow problems, which could make it difficult for them to satisfy their creditors.

We are applying the word *key* to two different terms: key risk indicators (KRIs) are key indicators of risk; and key risks are the most important risks. However, it is natural that the indicators are used by senior management to track those risks with the highest priority. “A goal of developing an effective set of KRIs is to identify relevant metrics that provide useful insights about potential risks that may have an impact on the achievement of the organization’s

objectives.” (Beasley et al., 2010)

There is an important link here with our previous discussions on risk analysis (see II.B.3), especially the bow-tie diagram, illustrated in [Figure II.8](#). Key risk indicators signal that trigger events, conditions, or intermediate events have occurred. The greater our understanding of a risk and the pre-conditions that could precipitate an event, the more apt we will be at identifying early signs of a risk event. The advantages of early warning indicators are illustrated in [Figure III.5](#).



The process of developing appropriate key risk indicators begins with the identification of *stress points*, which may require the input of specialists from the activity of interest. (See Beasley et al., 2010.) This is because the risk owners may be challenged to propose suitable metrics. It also is useful to consider the organization’s existing performance indicators. It may be possible to use some of this data to flag incidents or problems that indicate more serious emerging risks.

As with any metrics, there should be clarity and consensus on timing, means of measurement, and definitions. This may be problematic, however, when key threats have their origin outside the organization and it is necessary to rely on external sources of data. Even when trigger events are internal, it is not always easy to capture the right data at the right moment and recognize it as a risk indicator. Benefits from external data sources include their objectivity and ability to be used for categories of risk not previously encountered by the organization. However, they must be applied and interpreted with care because they have been gathered by others for different purposes.

Often, more than one indicator may be used as a sign of a trigger event, in what Beasley et al. refer to as a “mosaic of information.” This has the advantage of being richer and more sophisticated than a single measure. However, the more complex the indicators, the more skill they require to understand the implications.

Beasley et al. provide six design features that key risk indicators should emulate:

- They should be based on authoritative standards or benchmarks.
- They should be developed consistently across the organization.
- They should provide an unambiguous and easy-to-grasp picture of what is happening.
- They should facilitate measurable comparisons across the organization and over time.
- They should enable the measurement of the performance of risk owners.
- They should be designed and implemented in a cost-effective manner.

The same document also gives plenty of examples of key risk indicators. These indicators can be readily illustrated by a simple table in a “dashboard,” or by graphical means to provide a quick overview of the current status of key risks. Using a RAG (*red, amber, green*) rating is helpful to convey:

- The likely indications are that the key risk will materialize. (red)

- There are indications of possible problems. (amber)
- Everything is as expected. (green) Trends in these ratings can be denoted by arrows.

Key risk indicators (adapted from Mainelli, 2007) are important because:

1. By measuring probable risk over a given time period, they can be extremely powerful for risk oversight.
2. They can be used to help with decisions about resource allocation for risk treatment.
3. In some sectors (especially financial services), they may be used by business analysts and ratings agencies, such as Moody's or Standard & Poor's.
4. They may be used by regulators.

In Mainelli's model, there are four kinds of key risk indicators (see [Figure III.6](#)), each of which prompts a different type of response. The first is a *challenge indicator*, which reveals the root cause of a risk event and should encourage an organization to take appropriate action to prepare itself for the impact. The second is an *action indicator*, which provides feedback on actions taken to show that they have been implemented correctly. The third is a *health indicator*—the first indicator of *impact*—showing whether the action has restored the organization to normal health or whether further action is required. The fourth and final is a *risk incident indicator*, which records the final impact. When these indicators do not work properly, organizations receive misleading messages, take inappropriate actions at unsuitable times or no action at all, and treat the wrong risk in the wrong way. Ultimately, the organization suffers greater impact from the risk, or fails to reap the full benefit from an opportunity.

Figure III.6. Types of Key Risk Indicators (Mainelli, 2007)



How does internal audit evaluate the management of key risks?

According to Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning:

Internal audit planning needs to make use of the organizational risk management process, where one has been developed. In planning an engagement, the internal auditor considers the significant risks of the activity and the means by which management mitigates the risks to an acceptable level.

The internal audit charter normally requires the internal audit activity to focus on areas of high risk, including both inherent and residual risk. The internal audit activity needs to identify areas of high inherent risk, high residual risks, and the key control systems upon which the organization is most reliant. If the activity identifies areas of unacceptable residual risk, the internal auditors should notify management so the risk can be addressed.

The priorities for internal audit usually are:

- Areas in which the residual level of risk is above the appetite and management action is required.
- Key controls—those on which the organization depends most heavily (because they relate to business-critical activity).

- Areas in which there is the greatest difference between inherent and residual risk, as controls failure would precipitate significant risk exposure.
- Areas in which the inherent risk is very high, due to great likelihood or the threat of great impact.

Practice Advisory 2010-2 focuses the attention of the internal audit activity on key (or significant) risks and associated controls. As part of the planning process, the internal auditors should identify how they will provide assurance on the effectiveness of controls used to mitigate key risks and offer advisory services to help rectify or improve existing systems of control. Such activities include:

- *Control reviews/assurance activities*, through which the internal auditors review the controls of key risks and provide assurance on their adequacy, efficiency, and effectiveness; as well as provide assurance on the management of the key risks, themselves.
- *Inquiry activities*, whereby the internal auditors investigate the effectiveness of key controls, about which management is uncertain. By doing so, the internal auditors improve management's understanding of the current state of controls and the associated risks.
- *Consulting activities*, through which internal auditors offer advice to management about the improvement of internal controls to address unacceptably high residual and severity levels of key risks.

As a result of resourcing constraints and other priorities, the internal auditors may not be able to review all key risks. However—in some cases—the risk register will point to risks whose residual levels currently exceed the risk appetite, there may be no clear plans by management to ameliorate this, and the internal audit activity may not be in a position to evaluate it. This can be addressed partly by coordinating assurance for those risks from other providers, which will, of course, influence the audit-planning process. The internal auditors should report these areas to the board to ensure it is aware of the level of exposure.

As illustrated in [Figure III.7](#), the internal auditors are responsible for evaluating the management of key risks and verifying that necessary stages are in place.

Figure III.7. Management of Key Risks

Key risks are identified.

Emerging key risks are identified and monitored closely.

Key risks are analyzed, evaluated, and duly prioritized.

Responses for key risks are agreed, implemented, and monitored for effectiveness.

When reviewing the management of key risks, the internal auditors specify the scope and objectives of the audit and gather relevant evidence in accordance with the *Standards*.

Assurance services involve the internal auditor's objective assessment of evidence to provide an independent opinion or conclusion regarding an entity, operation, function, process, system, or other subject matter. The nature and scope of the assurance engagement are determined by the internal auditor. (IIA, 2012)

KEY TERM

Audit scope: The agreed purpose and limits of an audit.

With reference to Standard 2120, the evidence required to support a review may be gathered from either a single investigation or multiple activities. The key

is that the information must be, in the words of Standard 2310, “sufficient, reliable, relevant, and useful.” Within the context of the engagement’s objectives, the internal auditors must determine whether the evidence satisfies these criteria. This judgment further confirms the importance of effective planning and an agreement of objectives at the beginning of the investigation. Criteria for information are further defined in the interpretation of the standard:

- *Sufficient information* is “factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor.”
- *Reliable information* is “the best attainable information through the use of appropriate engagement techniques.”
- *Relevant information* “supports engagement observations and recommendations and is consistent with the objectives of the engagement.”
- *Useful information* “helps the organization meet its goals.”

When there is enough reliable and relevant evidence from which to draw conclusions, it is considered to be *sufficient*. Positive assurance is based on evidence indicating either conformance or non-conformance to agreed standards. Negative assurance (see III.B) is based on an absence of evidence that would indicate failure.

Evidence is *relevant* if it can be *properly* used to either support or negate a conclusion that helps achieve the audit’s objectives. By “properly,” we mean that its use must be in accordance with the principles of logic and valid inference. Of course, the greater the significance to the overall evaluation, the more relevant the evidence is.

The *reliability* of evidence arises from how it was acquired, its source, its currency, and the availability of other corroborative evidence. Direct observation generally is more reliable than reported information, and greater reliability is placed on evidence gathered by the internal auditor, rather than from other sources.

It is necessary to consider and analyze the full range of material gathered objectively to determine the overall picture and management of key risks. A further requirement to ensure the audit process is open and transparent is to maintain clear documentation of the processes followed, evidence gathered, analysis applied, and conclusions drawn.

There are a number of different ways to gather evidence about risk management. As is true for the nature and scope of the engagement, the internal auditor determines the approaches taken. It is usually preferable to employ a range of information-gathering methods. Then, the internal auditor can determine consistency through corroboration and validation. Based on Collins, 2012, [Figure III.8](#) illustrates methods commonly used to gather information.

Figure III.8. Information-gathering Methods



Table III.3 illustrates how these methods are used in the management of key risks.

Table III.3. Information-gathering Actions	
Documentary Analysis	<p>The internal auditor reviews the following documents and draws conclusions as to their accuracy, consistency, and completeness when compared with the risk strategy, risk framework, risk policy, and risk procedures:</p> <ul style="list-style-type: none">• Risk register.• Notes from CRSA and other risk identification and assessment exercises.• Minutes of board meetings at which risk was discussed, especially when risk appetite was agreed upon and key risks were considered.• Records of risk incidents.• Risk mitigation implementation plans.
Interviews	<p>To secure a representative picture, the internal auditor should consider gaining input from all key players in the risk management process, including:</p> <ul style="list-style-type: none">• Owners of key risks.• Specialist risk managers and compliance officers.• Senior management.• Non-executive directors.• Representatives of the risk committee.• Operational staff in key risk activities.
	Focus groups comprise relevant stakeholders (likely

Focus Groups	drawn from the same pool as those for one-to-one interviews) in the management of key risks. They may be a homogenous group or include different classes of stakeholders at varying organizational levels. The internal auditor can use a prepared set of questions that cover the main elements of the management of key risks. This includes gathering opinions on the effectiveness of risk management.
Testing	<p>Testing involves the active checking of controls through controlled experiments. By testing the systems in place, the internal auditor can get an answer to the question, “What would happen if ...?” A certain amount of artificiality is required to avoid putting the organization in any real danger of damage or loss. It may be possible, for example, to test what would happen if a key risk indicator alerted a risk owner to the early onset of certain trigger events. Would the risk owner follow through with the required action and escalation?</p> <p>IT tests are often conducted in a safe mode to see how much tolerance there is in the system until it fails.</p>
Observation	Observation is a very powerful source of evidence, as it is not filtered by the interpretation or bias of another individual. The internal auditor can make a direct assessment based on real-life activity. Care must be taken to determine both whether the observation represents routine activity and whether the internal auditor’s presence skewed the outcome. In the management of key risks, for example, it may be possible for the internal auditor to observe a board meeting in which strategic risks are analyzed, or a CRSA exercise designed to identify and evaluate key risks. This may reveal certain strengths or weaknesses in these important stages of the process.
	A walk-through is an attempt to recreate a process

Walk-through

from start to finish. The internal auditor selects examples of key risks—either randomly or from a representative sample. Alternatively, the internal auditor may investigate examples of risks incidents. By following through the various stages of the risk management process for individual key risks (using a combination of documentary evidence, observation, and other types of evidence), it is possible to recreate what has occurred and determine whether proper procedures have been followed.

When drawing conclusions, the internal auditor must compare the findings with what is expected by defined policies and procedures and recognized as good practice. Based on the system's existing risk tolerance, there can be room for a certain amount of tolerance or deviation from perfection. By the very nature of key risks, however, this is likely to be low.

III.B Evaluate the Reporting of Key Risks

Central to governance, risk oversight is one of the most important functions of the board. In the aftermath of the 2008 financial crisis, attention to oversight has increased and, in many cases, has needed significant strengthening. A central factor in this is the quality of the reporting of key risks, which is the reason an organization would turn to the internal auditors for assurance.

COSO's ERM framework assigns the board a number of responsibilities with regard to the effective reporting of key risks, including:

KEY TERM

Oversight: High-level continuous monitoring.

- Staying aware of the organization's key risks and how management is addressing them.
- Being familiar with the approach (framework, policies, and procedures)

adopted by the organization for risk management, including any changes and new developments.

- Knowing how well ERM is operating in the management of key risks.
- Regularly reviewing the key risks against risk appetite.

The board may rely upon a number of subcommittees to undertake some or all of the oversight on its behalf. Each respective committee must receive the information it requires, and all parties must stay aware of related activities to avoid overlap, duplication, and contradiction. Such arrangements should be carefully documented, as they increase the importance of effective reporting. Although division of duties among committees varies in different organizations (see Protiviti, 2010), it includes the following:

- *Audit committees* generally oversee financial reporting risks as a minimum, as well as all other key risks (unless there is a separate risk committee). They also review risk management policies and risk assessment.
- *Governance committees* focus on governance risks, such as the structure and operation of the board.
- *Risk committees* oversee key risks, as assigned.
- *Remuneration committees* have oversight of risks associated with bonus and reward systems, and how these systems drive behavior.
- *Strategy and finance committees* have oversight of strategic risks.

To discharge its responsibilities for ERM oversight, the board (or a similar body) relies on risk reporting. Although the oversight group is not responsible for managing risk, it is responsible for ensuring that risks are being managed effectively. Typically, the board is too far from the activities to monitor risks directly, evaluate the operational effectiveness of controls, respond to key risk indicators, and witness the present exposure in critical areas. Reporting on key risks, therefore, plays a very significant role in key risk management. ISO 31000 sets a requirement for internal and external risk reporting to “support and encourage accountability and ownership of risk.” The board is not the only

beneficiary of the reporting of key risks. The full list might include all stakeholders in some fashion, but the most obvious are:

- Senior management team.
- Business unit managers (risk owners).
- Risk management specialists.
- Investors (current and potential).
- Owners.
- Suppliers.
- Customers.
- Regulators.

The internal auditors also will make use of (and evaluate the effectiveness of) risk management reporting as part of their efforts to provide assurance on risk management processes.

Like all reporting, communication on risk needs to exhibit the good features of timeliness, reliability, intelligibility, and relevance. Risk reporting is usually a periodic process. As researched and evidenced by Walker, Shenkir, and Barton (2011), best practices in risk reporting include:

- Using a variety of risk reporting approaches.
- Tailoring reporting methods to suit the needs of the organization.
- Making reference to recognized risk management standards.
- Keeping it simple, by limiting the number of key risks to 5–20.
- Reporting regularly.
- Including updates on risk management action plans.

- Keeping all directors informed without duplicating the work of subcommittees.
- Training directors to understand their responsibilities, as well as comprehend the organization's risk profile and way of managing risk.
- Keeping risk oversight independent of the CEO.
- Ensuring information flows up and down.

With regard to risk management standards, Walker et al. (2011) quote ISO 31000 and its recommendations for reporting mechanisms:

- Key components of the risk management framework and any subsequent modifications are communicated appropriately.
- There is adequate internal reporting on the framework, its effectiveness, and the outcomes.
- Relevant information derived from the application of risk management is available at appropriate levels and times.
- There are processes for consultation with internal stakeholders.

As appropriate, these mechanisms should include processes to consolidate risk information from a variety of sources, and consider the sensitivity of the information.

Where risk management is integrated within routine organizational practice, “risk reporting is considerably simplified,” although Walker et al. detail some natural barriers to this, including:

- CEO reluctance to share too much negative information for fear of putting executive management in a bad light.
- A similar reluctance on the part of the internal auditors in case they are challenged about the details.
- The sheer volume of information that boards receive on risk and all other

matters that obscures what is critical. (For example, many boards receive updates on 50 or more risks.)

- A tendency toward infrequent reporting as a way for the CEO to steer clear of difficult topics.

Another problem encountered in this study is a trend among boards to delegate risk management oversight to a committee (such as the audit committee), only to receive from the committee a duplicative detailed report on all aspects of the board.

These findings (along with III.A and domain II—especially II.B.7) are helpful in the evaluation of risk reporting. In addition, use of key risk indicators is also highly relevant.

According to a 2010 study by Protiviti, boards are most likely to receive a regular update on key risks. This report, provided at least annually, typically includes:

- Summary information about the key risks as they apply to the organization as a whole, as well as the specific areas in which they arise.
- A review of risk management processes, especially with regard to identification, analysis, and prioritization.
- An assessment of emerging risks requiring a response from the board.
Less often, boards receive:
 - Analysis that reveals how the changing external environment is likely to impact the organization in the form of new risks and opportunities.
 - Reports of gaps or weaknesses in the management of key risks.
 - Reports of inadequate capabilities to manage key risks and how those risks are being addressed.

This second group is equally important for effective oversight and represents a common weakness in risk management reporting. When evaluating risk management reporting, the internal auditor ideally will find a system that is

suitably mature and robust, consistent, and reliable.

Information reported to the board should focus on the significant matters and be accurate and timely. Effective reporting tends to depend on well-defined processes, rather than something loosely specified.

According to Protiviti (2010), the features of a good report on key risks include:

- It is repeatable over time.
- It is well-defined.
- It is supported by a rigorous methodology and an analytical framework.
- It is applied periodically over time, as opposed to as needed.
- Process inputs and requirements, processes activities, and the expertise needed to execute them are articulated clearly; non-essentials are eliminated; and outputs are quantitatively determined, anticipated, and used for decision-making.
- The skills needed to undertake the analysis and deliver the report are in place.
- There are arrangements for the sharing of good practice and for continuous improvement.
- The reporting process is embedded within core management systems.

III.C Provide Assurance that Risks Are Adequately Evaluated

As stated in the introduction to this domain, the internal audit activity brings great value to their organization by providing assurance and advisory services. This comes directly from The IIA's Definition of Internal Auditing. We will consider advisory services (or consulting) in the next domain. In this section, as

well as in III.D, our focus is assurance and the support it provides for risk management. We will first consider assurance in general and then as it specifically relates to the evaluation of risk.

KEY TERM

Assurance: Confidence gained from an audit opinion on the reliability of given processes.

In the glossary of The IIA's *Standards*, assurance is defined as "an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization." The Chartered Institute of Internal Auditors provides a fuller definition, stating that assurance is:

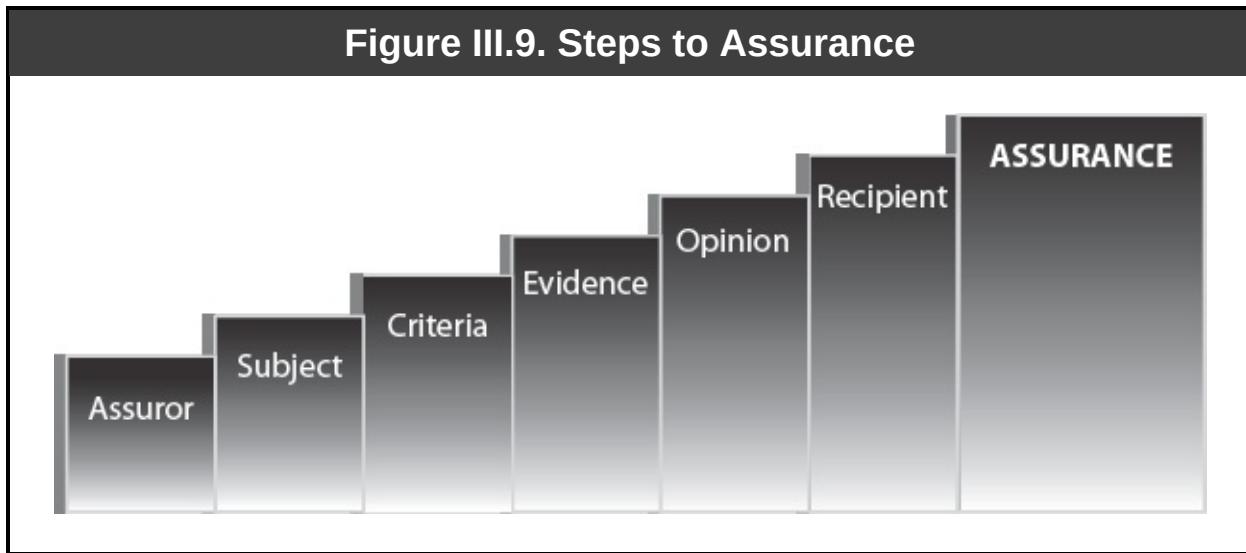
The delivery of an opinion or conclusion regarding the credibility of disclosed information and the process that delivers that information, or regarding the reliability of processes according to their conformity with certain criteria. The receiver of the opinion may or may not be assured, depending on other influences upon them.

This also relates to the internal auditors' role as the third line of defense. While assurance can come from a variety of sources, the position of the internal audit function is unique and, therefore, its opinion is of great value.

The key steps to assurance (see [Figure III.9](#)) are:

- An assuror (the party providing assurance).
- Specified subject matter on which assurance is being given.
- The application of criteria for evaluation.
- The consideration of evidence that is sufficient, relevant, and reliable.
- An independent and objective audit opinion.

- A target recipient for the audit opinion and assurance.



Assurance is an essential element in the board's oversight of risk, originating with strategy (see [Figure III.10](#)) and the objectives designed to deliver the strategy. We know that uncertainty gives rise to risk (both upside and downside) and the need for responses. Internal audit can provide an independent and objective view on the effectiveness of controls. Having this assurance from the internal auditors is vital to the board's role of risk oversight.



There are different types of assurance. According to Chesshire (2010), assurance may be given with respect to:

- Current financial position.
- The degree of compliance that exists with a given set of requirements.
- Operational performance against targets.
- The present state of IT security.

- Due diligence on a proposed procurement or merger.

KEY TERM

Audit opinion: The internal auditor's statement regarding the effectiveness of internal controls.

How is the internal audit activity able to provide assurance?

As a result of a systematic review and evaluation that reflects the risks associated with the area being audited, the internal auditors can reach an independent and objective conclusion (opinion) about the effectiveness of internal controls. In addition, they can provide assurance with regard to the likelihood that the area audited will continue to satisfy its objectives in support of organizational purpose and value. The provision of assurance is based on an audit *opinion*—a statement regarding the effectiveness of the internal controls over the key risks. Strictly speaking, it is the client who *draws* assurance from the audit opinion provided by the internal auditors. This distinction is clear in The IIA's definition of assurance.

There also are several levels of assurance:

Reasonable assurance: There is no IIA definition for reasonable assurance, but we could define it as strong (but not absolute) assurance that requires due professional care in accordance with the IIA's Definition of Internal Auditing, Standards, and Code of Ethics (integrity, objectivity, confidentiality, and competence).

KEY TERM

Reasonable assurance: Strong, but not absolute, assurance.

Absolute assurance: An opinion of total confidence that all controls are effective and will remain so *cannot be given*. An audit opinion is provided at a moment in time and usually is based on a sample. With the exception of

continuous auditing, it is not possible to view a complete record of everything that has occurred within an activity. Furthermore, there is always a human element to risk management, and controls may be deliberately or accidentally overridden. In any case, an audit opinion is based on the past for the immediate future—in which there will always be an element of uncertainty.

The outcome from the audit may be *positive assurance* that the risk management processes are operating as intended and in accordance with the agreed standards. Alternatively, there may be positive assurance that risk management processes are not operating correctly and fail to meet the standards.

KEY TERM

Positive assurance: Assurance based on a statement noting confirmed evidence of effective or ineffective processes.

The audit may result in *negative assurance* that there is nothing in the findings to indicate that risk management is not operating in accord with expected standards. Negative assurance, sometimes referred to as *limited assurance*, indicates that:

KEY TERM

Negative (or limited) assurance: Assurance based on a statement noting the absence of evidence to the contrary.

... nothing came to the auditor's attention about a particular objective, such as the effectiveness of a system of internal control, adequacy of a risk management process, or on any other specific matter. The internal auditor takes no responsibility for the sufficiency of the audit scope and procedures to find all significant concerns or issues. Such an opinion is generally considered less valuable than positive assurance and, therefore, auditors consider their value before rendering them. (IIA Practice Guide, Formulating and Expressing Internal Audit Opinions)

Internal auditors need to be confident that their audit opinions are genuinely independent, objective, and justified by the evidence. It is easy to be swayed by a single piece of information—especially if delivered by a persuasive manager—and not consider it fully in the context of all the available data. The provisions below help bring an appropriate conclusion to fruition:

- There should be a clear scope and a set of objectives for every audit, and all parties should be in agreement about what is under scrutiny, what falls within the review, and what is outside of scope.
- The objectives should be referred to throughout the evidence-gathering process, as “mission creep” (i.e., the accidental expansion of objectives) can easily occur—especially during longer engagements.
- Robust testing methods should include the right approaches and level of sampling for the particular project.
- Findings must be considered in turn, and conclusions must be drawn holistically, with a big-picture perspective, rather than being persuaded disproportionately by less significant data.
- Objectivity requires that the internal auditors follow the evidence without pre-conceived ideas or the desire to prove a point.

Of course, all internal audit work must be conducted in accordance with the IPPF, and general requirements, such as the need for appropriate skills, supervision, and the application of the Code of Ethics, are always of paramount importance. Providing an audit opinion requires a great deal of skill and professionalism, without which it is of little value.

As with any type of audit engagement, the evidence on which an opinion is based needs to be sufficient, reliable, relevant, and useful. (See III.A above.) The more positive the opinion, the higher the level of assurance and the greater the requirement for sufficiency and reliability. The testing carried out for an assurance engagement must look for and fail to find material weaknesses in the internal controls, and should reveal positive corroboration that the controls are working.

Even when expertly reached, opinions can be misinterpreted, so clear communication is essential. No matter what methods are used to convey the audit opinion—RAG rating (red/amber/green traffic lights), dashboard, numerical scale, symbols (i.e., smiley faces, arrows, or checks), or preset categories—there must be clear definitions and consensus on the conventions employed. There is a connection here with our previous comments on risk appetite and risk psychology (see II.B.3). Even when language is defined, it can mean different things to different people, depending on their personal views.

The internal auditors enjoy organizational independence, free from undue influence from both the owner of the area under review and the intended recipients of the audit opinion. Internal auditors achieve professional objectivity by being impartial and unbiased and avoiding conflicts of interest. They require appropriate competencies, are skilled in carrying out a review and reaching valid conclusions, and have an in-depth understanding of the organizational context.

The internal auditors are not the only source from whom the board will seek assurance. Regardless of the source, however, the CAE plays a role in coordinating assurance “to ensure proper coverage and minimize duplication of efforts.” (Standard 2050) Practice Advisory 2050-2: Assurance Maps distinguishes three broad classes of assurance providers (see [Figure III.11](#)) based on an analysis of the stakeholders they serve, as well as their level of independence and the reliance that may be placed on the assurance.

Figure III.11. Assurance-provider Classes



An assurance map shows the coverage offered by the three main classes of providers (internal auditors, external auditors, and others) for each class of risk or each significant risk. The internal auditors typically will provide assurance across the enterprise and its operations, with a particular focus on risk management processes and key risks. In planning its other activities, it will consider the coverage provided by others. The map can be used to identify gaps or overlaps and give confidence to the board that overall assurance is adequate and robust.

The internal auditors must decide how much reliance they will place on the assurance from other providers. (See IIA Practice Advisory 2050-3: Relying on the Work of Other Assurance Providers.) This is a necessary element of the internal auditors' independence. Being able to rely on such assurance avoids unnecessary duplication and may cover areas for which the internal auditors are inadequately skilled. The internal audit activity needs to be confident in the process followed by the other assurance provider. The level of reliance that can be placed on the assurance of others depends on an assessment of:

- Independence.

- Objectivity.
- Competence.
- Processes followed.
- Adequacy of coverage.
- Sufficiency of evidence.

IIA Practice Guide, Reliance by Internal Audit on Other Assurance Providers, identifies the benefits of adopting an integrated approach to assurance, including:

- Assurance based on a comprehensive and shared view of risk enables the board to identify its assurance needs effectively.
- Matching the board's assurance needs to the sources of assurance not only avoids gaps and overlaps, but also enables cost-effective delivery of assurance.
- The board has reduced workload, which enables it to focus on key risks, controls, and assurance.
- Strong first and second lines of defense can make internal auditing easier, allowing for more attention to important exposures or areas not well covered.
- When the internal auditors are required to express an opinion on the whole of management's framework of governance, risk management, and control, they may be able to rely on a well-structured management-assurance regime.

On the other hand, coordinated assurance is not an easy thing to deliver. As we have indicated, boards and their audit committees must have a clear view of their objectives and must identify and respond to risks before they can piece together their assurance needs. The situation is often complicated by myriad assurance providers who can be difficult to identify and group within an effective framework. In some cases, risk management processes will need to be

improved before an assurance framework can be put in place.

Organizations also need to share an understanding of what coordination means and a framework with strong leadership to pull the various resources and plans together to create a cohesive program of work with a risk-based approach. Fortunately, as with any jigsaw puzzle, it is possible to arrange all the pieces to see the overall picture.

The internal audit activity is the only part of the organization with the competence to evaluate the effectiveness and efficiency of the assurance provision arrangements. As such, it should encourage management to take the lead and ownership for the coordination of assurance work in the first two lines of defense. The internal auditors should work with management to build on the existing assurance activity and provide the most effective assurance coverage in support of the needs of the board and audit committee.

At the same time, coordination does not diminish internal audit's responsibility to express an opinion on the effectiveness of governance, risk management, and control. The internal auditors may rely upon the work of other assurance providers to form this opinion, but must assess their work periodically. They also must be free to review and comment on the effectiveness and reliability of other assurance providers. Any steering group or working committee should understand this.

In domain II (II.B.3), we analyzed in detail how risks are evaluated. We identified a number of key activities that make up this process, namely:

- Risk classification.
- Risk analysis.
- Selecting risk criteria.
- Assessing risk level or severity.
- Risk mapping and prioritization.
- Producing risk registers to document and track this information.

To assess how effective the evaluation has been for the purpose of providing assurance on this key risk management process, the internal auditors can consider a review under these same headings. Critical questions may include:

- From the evaluation of any given risk, what conditions or events will precipitate the risk event?
- Does the evaluation accurately reveal the impacts on the organization—bearing in mind that there may be several?
- Are any interdependencies with other risks similarly understood and accounted for?
- Is there a realistic measure of likelihood, taking into account previous occurrences of similar risks and data from other sources?
- In addition to likelihood and impact, have other relevant criteria (such as volatility or velocity) been considered and applied?
- Is the evaluation of both inherent and residual risk equally comprehensive?

Information sources needed to make a judgment in each of these areas are likely to include all of those discussed in III.A. To reach a conclusion, there should be consideration of the risk evaluation processes adopted and documented, the needs of the organization, and best practices.

III.D Provide Assurance on Risk Management Processes

In the introduction to this domain, we noted that the evaluation of risk management processes (see IIA Standard 2120) needs to consider:

- The alignment with organizational objectives.
- The success with which the processes identify and evaluate key risks.
- The degree to which appropriate risk responses are identified and

implemented.

- The effectiveness of risk-information recording and reporting to the relevant stakeholders.

The subject of this section—the provision of assurance on risk management processes—draws upon information in the previous sections as it all contributes to assurance. The IIA’s Practice Advisory 2010-2 makes a similar point—suggesting that an assurance engagement focusing on risk management processes should consider:

- The identification and assessment of inherent risks.
- The identification and assessment of residual risks.
- The establishment of mitigating controls, contingency plans, and monitoring activities; and the extent to which these are linked to the trigger events and risks
- The maintenance of risk registers and whether this follows a systematic, comprehensive, and accurate process.
- The completion of risk documentation.

As part of the necessary background information, the internal auditor should be familiar with the mission, strategy, and objectives of the organization, and understand the organization’s internal and external environments. Furthermore, as part of the process of evaluating the appropriateness of risk responses, the internal auditor requires knowledge of the risk appetite, risk capacity, and risk tolerance for the areas under review and for the organization as a whole. In fact, the setting and communication of risk appetite is arguably part of the risk management processes and should be included in the review. The evidence also includes how the organization documents and responds to risk incidents, as success or failure is really best assessed when the controls are tested by real events. Finally, there should be a review on risk management process reporting, so the internal auditors can opine in regard to assertions that have been made about risk management effectiveness.

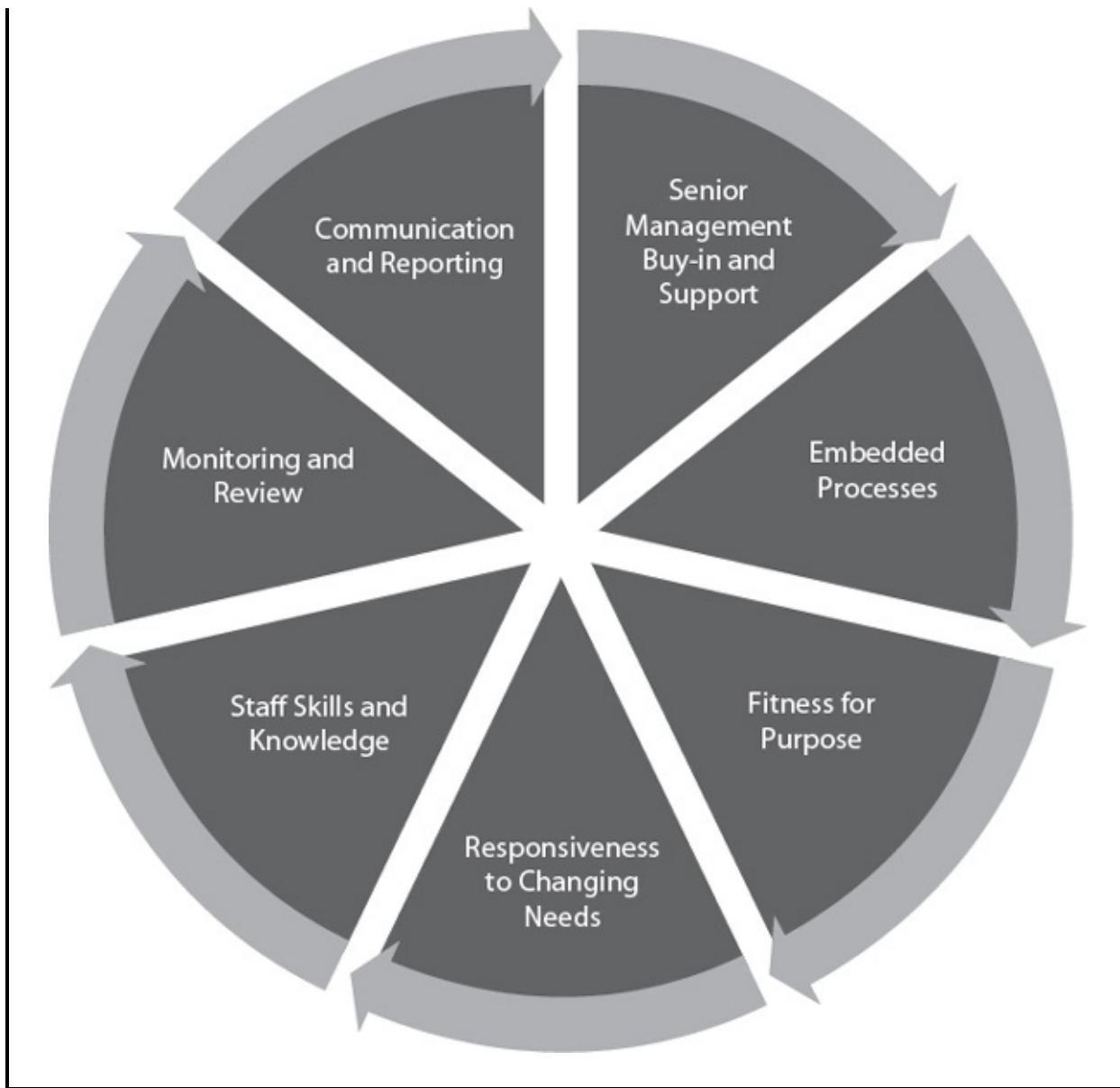
Assurance on risk management processes may be provided to senior

management to provide confidence in process design, delivery, and documentation. Key questions (adapted from IIA Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000, fall under several categories (see [Figure III.12](#)):

- Staff skills and knowledge:
 - Do those with responsibility for risk identification, risk analysis, risk evaluation, and risk treatment have the right knowledge and skills?
- Senior management involvement:
 - Is there adequate commitment at the highest levels of the organization for risk management, as evidenced by the recognition it receives and its level of resourcing?
 - Is the risk attitude established at the proper level on the governance structure of the organization?
- Embedded processes:
 - Is risk management embedded into organizational processes and decisionmaking processes?
- Fitness for purpose:
 - Is the risk management framework appropriate for the organization and its internal and external environments?
 - Are the criteria used to evaluate risks appropriate for the organization?
 - Are there clear roles and responsibility, adequate definitions of key terms, and sufficient levels of communication to support and maintain the risk management processes?
 - Are key principles (for risk assessment, appetite, response, escalation, etc.) applied consistently?

- Reporting:
 - Do key outcomes from risk management activities get communicated effectively, with an appropriate balance of sensitivity and transparency?
 - Do the reports to stakeholders adequately communicate the organization's risk attitude and risk responses?
- Monitoring and review:
 - Are adequate performance and monitoring measures in place?
 - Are risk mitigation plans monitored and communicated effectively?
- Responsiveness:
 - Are risk management processes responsive to changes in the organization and its needs?

Figure III.12. Areas of Interest



To provide assurance on risk management processes, the internal auditors must determine whether (IIA, 2010):

- Risk management processes have been applied appropriately and all elements are suitable and sufficient.
- Risk management processes are in keeping with the strategic needs and purpose of the organization.
- All significant risks have been identified and are being treated.

- Controls are being correctly designed in line with the objectives of risk management processes.
- Critical controls are adequate and effective.
- Review by line management and other non-audit assurance activities are effective at maintaining and improving controls.
- Risk mitigation plans are being implemented.
- There is appropriate progress on the risk management plan, as reported.

It is helpful if the internal auditors have access to documentary evidence related to the requirements above. The risk management framework should be clearly set out and described, normally as part of a formal risk strategy and policy together with operating procedures. The risk register is a useful tool, as it represents a current record of the relevant risks to which the organization is exposed. It may be subdivided into a number of separate accounts, representing key or strategic risks and more operationally focused risks, as appropriate. In addition to logging the risks, the register provides their classification, analysis, assessment, and evaluation. Most important, it also assigns ownership of risks. Linked to these details are the agreed risk responses, desired objectives of the treatments, and steps required to put them in place and keep them under review. Further details may form part of the risk register or, more likely, will be found in a risk mitigation implementation plan. Systems policies and procedures should clarify how to maintain controls that have been embedded in operations. Supporting documentation (such as working papers and notes from risk identification workshops) offers the internal auditors a basis for reviewing risk management processes.

As illustrated in [Figure III.13](#), IIA Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes, suggests a range of options for gathering the evidence required to obtain assurance on risk management processes.

Figure III.13. Assurance on Risk Management Processes

Analyze Sector Trends

- Research and review quality newspapers, business journals, statistical reports, professional body digests, training events, and similar sources.
- This will help determine alignment of risk management processes with developments in the sector and identify potential new exposures.

Identify Organizational Strategy

- Use policy documents, board papers, and other internal documentation to identify vision, mission, values, and strategic objectives.
- Identify risk culture, the risk management framework, and risk appetite.

Review Previous Risk Evaluation Reports

- These may have been issued by the internal auditors, management, the external auditors, or another external group.
- They can provide a rich source of information and may include improvements that should now be in place.

Carry Out Interviews

- These should be conducted with line managers and senior managers, among others.
- This will help identify business-unit objectives and associated risks, as well as how they are being addressed.

Assimilate Information

- This is necessary to enable the internal auditor to come up with an independent and objective opinion.

**Figure III.13. Assurance on Risk Management Processes
(continued)**

Assess Arrangements for Reporting

- Are the reporting lines clear?
- Are there clearly demarcated roles and responsibilities?
- Are reports adequate for the needs of the recipients?
- Are the reports delivered in a timely fashion?
- Are there adequate arrangements for mounting and reporting risks?

Review Risk Analysis

- This can be done by studying risk mitigation plans.
- It should provide a record of the agreed actions needed to respond to risks, so it can be determined whether those actions have been implemented.
- At the same time, the agreed actions can be assessed for their appropriateness. Did they deal with the root cause of the risk?

Observations and Testing

- This can be carried out to determine the effectiveness of the self-assessment processes used by management as part of its risk management arrangements.
- The accuracy of the information can be tested and controls can be observed and monitored.

Apply Standard 2600: Communicating the Acceptance of Risks

- This requires the CAE to advise senior management where it may have accepted an unacceptable level of risk.
- "Unacceptable" means it is inconsistent with the risk management strategy and policies, or inappropriate for the organization.
- If the response is inadequate, the CAE needs to communicate this to the board.

IIA Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000, recognizes three different models for delivering assurance on risk management. The practice guide points out that an external source should provide assurance if the individual internal auditor or the audit function is not wholly independent of the risk management function. The three assurance approaches identified are:

- Process elements approach.
- Key principles approach.
- Maturity model approach.

These models may be used in isolation as they each provide a rigorous approach. However, there is value in adopting multiple approaches over time or even concurrently as they offer different perspectives. Just as risk management processes must be customized to reflect the needs of the organization, its objectives, and internal and external environments, the most effective assurance process should be chosen and adapted to serve the organization.

Sobel and Reding (2012) describe only two methods for assessing ERM, namely:

- Comprehensive assessment approach.
- Maturity assessment approach.

In many ways, the comprehensive assessment approach operates like a combination of the process elements and key principles approaches.

The practice guide also stresses that, while each of the three approaches listed above and described below may be used as a *desk-based review*, they must be validated by supporting control-based assurance. According to the guide, the purpose of this additional validation is to provide assurance that:

- Risks are being effectively identified and appropriately analyzed.
- There is adequate and appropriate risk treatment and control.
- There is effective monitoring and review by management to detect changes in risks and controls.

Let's consider each of these three approaches individually.

Process Elements Approach

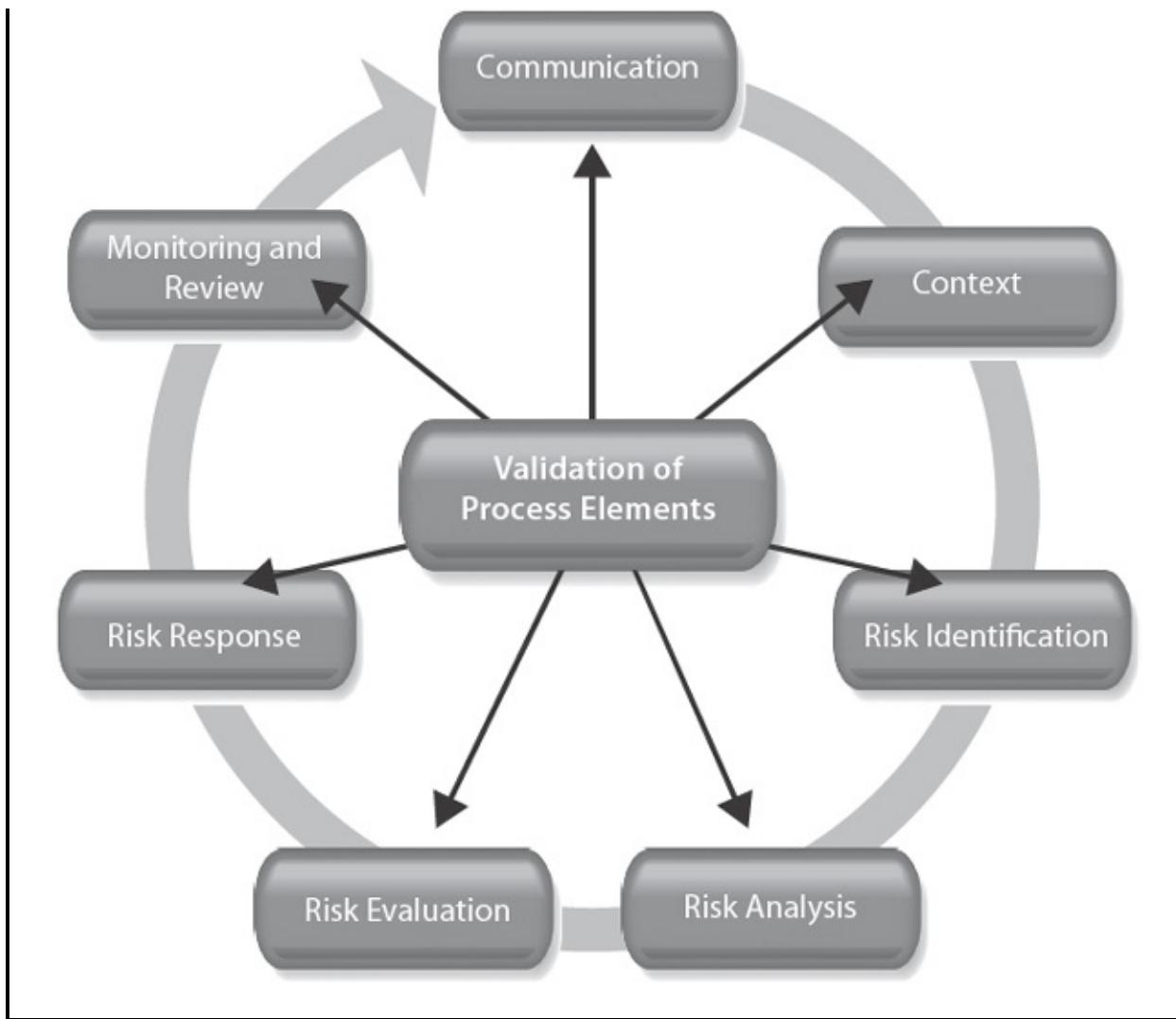
As the name suggests, this approach delivers assurance that is based upon validating each of the elements of the risk management process. These make up the key sections of domain II.B. As defined by ISO 31000, the elements (see [Figure III.14](#)) and accompanying questions include:

1. Communication—Are the key individuals and team (i.e., those

impacted by the activities and controls related to each risk) kept involved through regular communication?

2. Context—Are the internal and external environments and organizational purpose sufficiently understood to enable effective risk identification?
3. Risk identification—Is there a structured and comprehensive approach to identifying risk?
4. Risk analysis—Are risks well understood both in how they may occur (the trigger events and circumstances) and the impact they may have on the organization and its objectives?
5. Risk evaluation—Are risks evaluated to determine their importance to the organization and facilitate a means of prioritizing them and their responses?
6. Risk responses—Are appropriate responses selected and implemented to manage the risks within appetite, tolerance, and capability?
7. Monitoring and review—Are risk implementation plans monitored to discern whether actions are being undertaken, responses have been implemented and are working, and emerging risks are being tracked closely? Are all processes reviewed to check their effectiveness and inform continuous improvement?

Figure III.14. Seven Process Elements



In validating each element, sufficient audit evidence is necessary to confirm that it is operating effectively, as required. This may require a degree of triangulation among management's intentions, the views of those closer to the process element, and the performance of each element as viewed firsthand.

Key Principles Approach

The key principles approach evaluates risk management processes to determine whether they satisfy a minimum set of characteristics or principles. Risk management (as it actually is practiced in the organization) is compared against the selected principles. According to IIA Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000, ISO 31000 provides a set of principles (see [Figure III.15](#)) that can be used for this purpose. The principles

include:

- Risk management creates and protects value.
- Risk management is an integral part of organizational processes.
- Risk management is part of decision-making.
- Risk management is systematic, structured, and timely.
- Risk management is tailored.
- Risk management takes human and cultural factors into account.
- Risk management is transparent and inclusive.
- Risk management is dynamic, iterative, and responsive to change.
- Risk management facilitates continual improvement and organizational enhancement.

Figure III.15. Key Principles Approach

- Creates and protects value.
- Is integrated in organizational processes.
- Is central to decision-making.
- Addresses uncertainty.
- Is structured and systematic.
- Is customized to match organizational needs.
- Reflects social, cultural, behavioral, and psychological dimensions.
- Is open and involves key stakeholders.
- Is responsive to change.
- Encourages ongoing improvement and organizational change.

Maturity Model Approach

Risk management processes should evolve and develop along with the organization's understanding and attitude toward risk. The more mature the processes, the greater the benefit. We examined the development of risk culture in domain I (see I.A.2 and [Figure I.4](#)). As the risk culture evolves:

- The understanding of risk increases across the organization.
- The recognition of risk informs decision-making and planning to a greater extent.
- Risk processes become more embedded at all levels.
- There is greater focus on a broader range of responses, rather than simply mitigation.
- There is greater involvement by all staff in risk management.

- Risk reporting is more effective.
- There is less focus on compliance.
- More value is derived from risk management.

Risk management improvement and risk maturity advancement are confirmed when a plan successfully advances the culture features listed above. For evidence of risk maturity evolution, the internal auditors look for performance measures that demonstrate risk management progress. Typically, this involves having in place a risk management plan with suitable, tracked, and monitored performance indicators.

As illustrated in [Figure III.16](#), performance measures are used to gauge progress. They also help ensure continuous movement toward greater alignment with current and future organizational needs and increased risk maturity over time.



ISO/IEC 15504 Information Technology — Process Assessment, also known as Software Process Improvement and Capability Determination (SPICE), provides an alternative model to improve and develop the maturity of a process.

The standard, in nine separate parts, is primarily designed for technology organizations, but the approach has wider application. It assesses maturity, assigning one of five levels:

- Incomplete (0)
- Performed (1)
- Managed (2)
- Established (3)
- Predictable (4)
- Optimizing (5)

Given a choice of methods for providing assurance on the effectiveness of risk management processes, how does an organization know which one is the most appropriate?

There are no hard and fast rules and, as with risk management itself, the overriding criterion is to ensure that it is right for the organization. However, there are some general guidelines that may be used (based on Sobel and Reding, 2012).

A process elements or key principles approach (or, in Sobel and Reding, a comprehensive assessment) may be adopted when:

- ERM has been introduced fairly recently.
- ERM has been in place for a couple of years, but has not previously been assessed.
- There has been a significant risk event.
- There are other indications that ERM is not working effectively.
- ERM is well-established and seems to be working well, but (given its importance) a cyclical assessment is appropriate about once every three

to five years.

The same rationale may be applied to a partial or staged implementation of ERM.

- Alternatively, a maturity model approach may be taken when:
- A process elements or key principles approach (or comprehensive assessment) has been undertaken in the recent past and an alternative approach is chosen to provide a different, but complementary, perspective.
- ERM has been found to be effective, but the organization is ready and motivated to drive further improvements.
- ERM is effective for pure risk (downside risks) but is not yet maximizing potential opportunities (upside risks).

Summary

In this domain, we have looked at internal audit's contribution of providing assurance on risk management processes. In doing so, we have stressed that the internal audit function can make a unique contribution because of its independence and objectivity. Accordingly, it is imperative that the internal auditors maintain this position by not taking on roles that stray into the responsibility for managing risks. This must always remain the responsibility of management. Even when undertaking advisory roles, there are safeguards for preserving the internal auditors' independence and objectivity.

As a cornerstone of effective corporate governance and in its responsibility for risk oversight, the board of directors requires risk management assurance. The board typically remains too remote from operational activity to be able to judge for itself whether risk management processes are being implemented in accordance with risk strategy and for the benefit of the organization. It is essential to know that key risks are being identified and correctly analyzed so that resources can be allocated where they are needed. It is also critical to know that risk responses are being selected and implemented cost-effectively and in a

manner that maintains risks within appetite. By the same token, the board needs to be aware when controls are not working or there is an exposure in excess of appetite or one that is inappropriate for the organization.

The board and other stakeholders can derive assurance from other sources—notably management and external agencies. However, the opinion of the internal auditors—the third line of defense—adds great value.

In discussing the process the internal auditors use to evaluate and deliver an opinion from which assurance is drawn, we have paid particular attention to information gathering. Unless the evidence supports the conclusions, an opinion has no merit.

This domain has drawn heavily on domains I and II, as the task of evaluating risk management processes requires comprehensive knowledge of how risk management is intended to work and the added value it should provide to an organization. In the next domain, we will consider internal audit's other significant contribution—consultation.

DOMAIN IV

Consulting Role of the Internal Auditor

Table IV.1. Domain IV Outline		
Topic/subtopic	Explanation	Reference # in study guide
A. Facilitate identification and evaluation of risks.	To <i>facilitate</i> means to help make something possible or ease its occurrence. Internal auditors can apply their expertise and skills to provide a useful advisory service to management by helping identify and evaluate risks. This may be through a series of tasks, typically with groups of people in structured discussions and brainstorming exercises.	IV.A
B. Coach management in responding to risks.	Although instruction involves explaining and demonstrating what is required, coaching does not. Instead, the aim of <i>coaching</i> is to create conditions under which individuals can make important discoveries for themselves and grow personally. By coaching management on risk response, internal auditors help build a more effective understanding of risk, which will strengthen organizational capabilities for the	IV.B

	<p>future.</p>	
C. Coordinate risk management activities.	<p>With all consulting engagements, it is necessary to have safeguards that protect internal audit independence and ensure management owes the responsibility for managing risk. <i>Coordination</i> of risk management activities requires great care, as it moves the internal auditor very close to management responsibilities. Disparate activities must be pulled together and standardization must be adopted to improve reliability, consistency, and cost-efficiency.</p>	IV.C
D. Consolidate reporting on risks.	<p>Many stakeholders (both internally and externally) rely on effective reporting. The ability to <i>consolidate</i> reporting (i.e., bring it together under a single well-structured system) relies on effectively coordinating risk management activities and then recognizing the audiences for risk reporting and their particular information requirements.</p>	IV.D
E. Maintain and develop the risk management framework.	<p>Maintenance and development also are activities that are very close to managing and, once again, the internal auditor needs strong safeguards in place before undertaking such an engagement. To <i>Maintain</i> is to keep risk management operating—possibly in the temporary absence of an overall manager—by checking to ensure that each element is working properly and reporting exceptions to management.</p>	IV.E

	To <i>develop</i> the framework requires an analysis of the current arrangements, an agreement regarding intended improvements, and a proposed plan to management for delivering the required changes.	
F. Advocate for the establishment of risk management.	In <i>advocating</i> the establishment of risk management, the internal auditors promote their importance to a broad range of stakeholders and encourage management to increase the maturity of its risk management processes. There are many ways this may be achieved: the internal audit activity will conduct some within its assurance role and respond specifically to management's requests for advice on others. Internal audit is one of the beneficiaries of a well-established framework and mature risk management processes.	IV.F
G. Develop risk management strategy for board approval.	The board is responsible for ensuring risk management takes place and for approving the strategy. The internal audit activity is well-placed to help draft a new or revised strategy for risk management. Working with management, the internal auditor can help with the evolution of the overall approach and underpinning policies and processes. Involving others in the creation of the strategy is one of the ways to increase understanding, promote its importance, and secure enterprise-wide buy-in.	IV.G

Introduction to Domain IV

From The IIA's definition of internal auditing, we know that the activity adds value to an organization through assurance and consulting (or advisory) services. In domain III, we explored the internal auditors' role in providing assurance on risk management processes. In this final domain, we will look at the consulting role and how it contributes to the effectiveness of risk management.

The definition of internal auditing was amended with much debate in 1999 to include consulting as an explicit and distinct part of its role. Those opposed to broadening the definition in this way raised four main objections:

- Internal audit had always included a consulting element through the recommendations it delivers within an assurance engagement and, therefore, it is unnecessary, unhelpful, and perhaps even damaging to separate it out.
- Consulting is not a distinctive activity, as many other functions offer advice and guidance to management. The primary value of internal audit comes through the delivery of assurance.
- There is a potential conflict of interest if internal audit takes on a consulting role separate from the delivery of assurance.
- The new definition includes both assurance and consulting with no indication of which is more important—the natural conclusion is that there should be an even split between the two activities. However, while consulting may be a trendier or more attractive role, assigning it undue emphasis could damage the primary focus for internal audit, which is and should remain assurance.

Despite these arguments, it has proved tremendously helpful to the profession and its stakeholders for the definition to make clear the two ways in which internal audit adds value with independence and objectivity. This has been supported by the development of corresponding standards and guidance that provide much needed assistance for implementation. It is important to point out that the internal auditors can only *recommend*, as they are not in a position to *implement* such actions, and management is free to accept or reject any

proposals.

In addition to the features that consulting and assurance engagements have in common, there are some significant differences (see below). In practice, it may sometimes be hard to separate assurance and consulting. For one thing, it is common for an assurance engagement to address weaknesses in internal control and offer recommendations for improvement, and for a consulting engagement to contribute to an overall audit opinion. Indeed, it is a requirement of the *Standards* that information garnered through consulting be applied to the auditing of risk management:

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization’s risk management processes.

2130.C1 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization’s control processes.

Furthermore, it is often through assurance engagements that the need for consultation is identified in the first place, leading to discussions with management regarding actions. Consulting, on the other hand, can provide additional assurance by giving management detailed insights on a particular aspect of the organization. The internal auditor should take care when framing an opinion on the basis of a consultancy assignment to avoid any distortion regarding the materiality of the findings with respect to risk and control.

The glossary to the *Standards* defines consulting services as follows:

Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization’s governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

In addition, the introduction of the IPPF states that:

Consulting services are advisory in nature, and are generally performed

at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Consulting services generally involve two parties: (1) the person or group offering the advice—the internal auditor, and (2) the person or group seeking and receiving the advice—the engagement client. When performing consulting services, the internal auditor should maintain objectivity and not assume management responsibility.

Despite the origin of the consulting engagement, the skills and insights that enable an internal auditor to follow a risk-based approach in evaluating controls and delivering an opinion on their effectiveness are also highly valuable when providing constructive advice about systems development and business improvement. However, assurance and consulting are distinct. If an assurance engagement identifies the potential value that consulting may bring to the same area of review, the scope must not shift from assurance to consulting without setting out a new proposition. This is covered by Standard 2220.A2:

If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

In this domain, we will explore the contribution the internal auditors can make to risk management through consulting. While assurance engagements for ERM are generally delivered when everything needed is already in place, consultancy is likely to be required when there are no systems and processes or they are new, incomplete, or less than optimal. When serving as consultants, the internal auditors must adopt a different mindset from that of assurance, even though they will employ the same expertise and build useful knowledge. The nature and extent of consulting to be offered by the internal audit activity must be set out clearly in the charter (in accordance with Standard 1000.C1) and, like all activities undertaken by the internal audit function, must be limited to those tasks that can be performed competently by available capabilities. Standard 1210.C1 states that:

The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the

knowledge, skills, or other competencies needed to perform all or part of the engagement.

This is in contrast to assurance engagements, which are not to be declined if resources are lacking internally. (In such assurance cases, resources would be secured from other sources.)

Advisory work focuses on governance, risk, and control, which form internal audit's primary knowledge base. Consulting can take many forms. According to *Sawyer's Guide for Internal Auditing* (2012), the various kinds of consulting services the internal auditors may provide or contribute to include:

- Business process improvement.
- Continuous monitoring.
- Control self-assessment of risk and control self-assessment.
- Forensic auditing.
- Governance and ethics training.
- Internal control review.
- Internal control training.
- Participation on committees or task forces.
- Readiness.
- Review of a new product or service before implementation.
- Risk self-assessment.

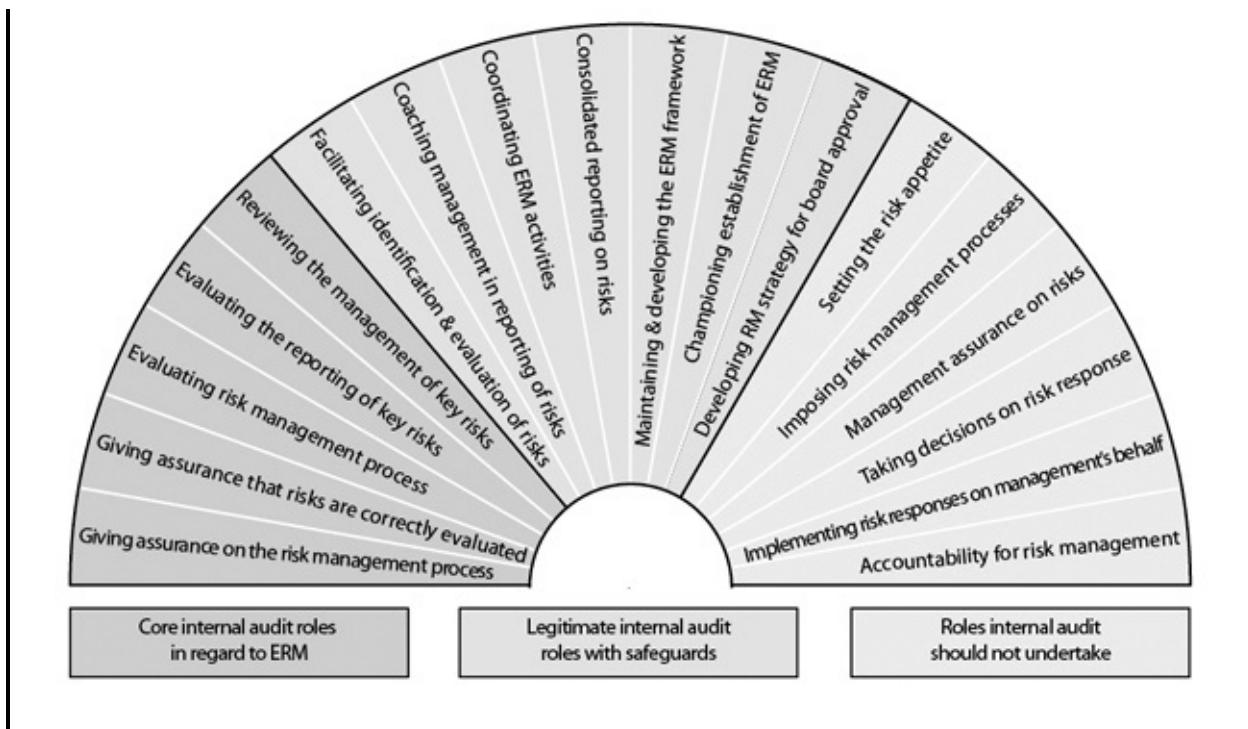
In this domain we will focus on seven types of consulting engagements related to risk management:

- Assisting in the identification and evaluation of risks through an analysis of strategy and the internal and external environments (IV.A).

- Developing management's capabilities in respect to risk responses by providing coaching (IV.B).
- Helping to draw risk management activities together across the organization in a more coherent, effective, and deeply embedded fashion (IV.C).
- Strengthening risk reporting by ensuring it is timely, relevant, and focused (IV.D).
- Maintaining and improving the risk management framework through a combination of testing, validation, and the offering of potential solutions to identified weaknesses (IV.E).
- Promoting risk management across the organization by acting as its champion (IV.F).
- Advancing the progression toward greater risk maturity by developing the risk management strategy (IV.G).

We will explore these principal topics one by one. First, however, let's review the range of activities the internal auditors may rightly undertake in support of ERM (see [Table III.2](#)). A fan is commonly used to depict this (see [Figure IV.1](#)).

Figure IV.1. Internal Audit's Role in Enterprisewide Risk Management



Source: The Institute of Internal Auditors

The third section of the fan in [Figure IV.1](#) comprises responsibilities that belong to management and should not be undertaken by the internal auditors. Consulting clearly falls within the middle section of the fan, and it is important that relevant safeguards are maintained to secure the objectivity and independence of internal audit. (These safeguards are highlighted in the introduction to domain III.)

There are several characteristics, as well as important differences, that assurance and consulting engagements have in common. The similarities arise from the simple fact that any activity carried out by the internal auditors should be delivered in accordance with high standards of professional practice. More specifically, both types of internal audit engagements must be:

- Defined in the internal audit charter.
- Delivered by the internal auditors with:
 - Due professional care.

- Independence and objectivity.
- Due regard to the safeguards (as itemized in the introduction to domain III). *Due professional care* is explained in Standard 1220.C1:

Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results.
- Relative complexity and extent of work needed to achieve the engagement's objectives.
- Cost of the consulting engagement in relation to potential benefits.

Furthermore, if it is clear at the outset that there are any impediments to independence or objectivity, they must be declared before accepting the engagement. This is also evident in the *Standards*:

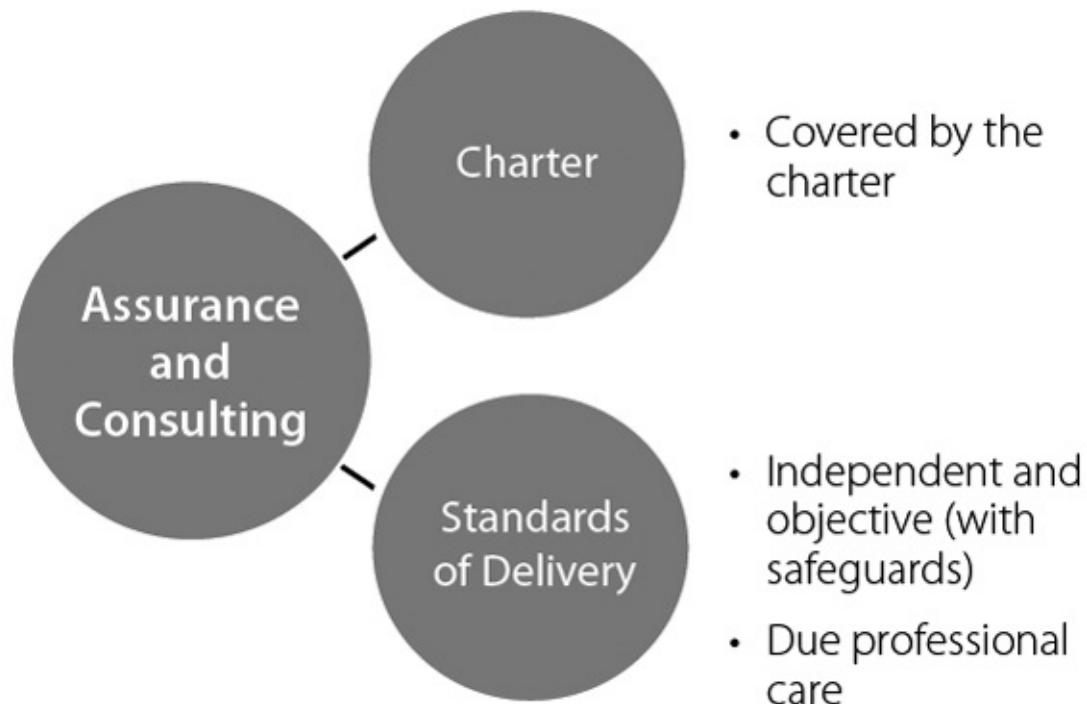
Standard 1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

The overriding safeguard is that, under no circumstances, should the internal auditors take responsibility for risk management. It is also clear that a consulting engagement should not be accepted simply because management requests it. It must be relevant and planned. This is clear from Standard 2010.C1:

The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

The common elements of assurance and consulting engagements are illustrated in [Figure IV.2](#).

Figure IV.2. Common Elements of Assurance and Consulting Engagements



Let's consider the differences between the two types of engagements. One distinguishing factor is that consulting is principally delivered for the benefit of management at its request, while assurance has a much broader value and is directed by the internal audit function. There are exceptions to this view of consulting, and the internal auditors may propose areas in need of advisory services—especially when significant new activities are introduced, major developments are taking place, or there is no risk management. For an overview of the major differences, refer to [Table IV.2](#), with reference to *Sawyer's Guide for Internal Auditors*.

Table IV.2. How Consulting and Assurance Differ

	Assurance Engagements	Consulting Engagements
	To offer an	

Main Purpose	independent <i>audit opinion</i> based on an objective assessment of evidence, from which assurance may be gained.	To offer advice, usually at the request of management.
Main Parties	(i) Internal auditor (ii) Owner of the activities being audited (iii) Recipient of the assurance (generally senior management and the board)	(i) Internal auditor (ii) Recipient of the advice (the client)
Objectives, Scope, and Approach	Determined by the internal auditor.	Agreed between the client and the internal auditor.
Objectives	Must be based on risk assessment and take into consideration error, fraud, and noncompliance.	Must be consistent with the organization's strategic aims.
Governance, Risk Management, and Control Processes	Must be included within the scope and addressed by the objectives.	May be included within the scope and addressed by the objectives as required by the client.
	If the skills are not available within the internal audit activity,	If the skills are not available within the internal audit activity, the CAE must either

Skills	the CAE must obtain the necessary skills to deliver the engagement.	obtain the necessary skills to deliver the engagement or decline the engagement.
Conflicts of Interest	Internal auditors must not audit areas of operation for which they had direct responsibility within the past 12 months.	Internal auditors provide consulting services with respect to any areas of operation, even if they had direct responsibility for them within the past 12 months (see Standard 1130.C1).

Throughout this domain, we refer to the importance of proper safeguards to ensure internal audit maintains its objectivity and independence. Practice Guide 2050, Coordination, provides useful commentary on measures for keeping the internal audit activity and risk management responsibility separated:

It should be clear that management remains responsible for risk management, even in those organizations where internal audit has been asked to facilitate the risk management program. Internal audit should not manage any risks on behalf of management, nor make final decisions regarding the enterprise's risk appetite or level of resource allocation to control or mitigate risk. Whenever internal audit acts to help the management team to set up or to improve risk management processes, the audit committee should approve its plan of work.

- The nature of internal audit's responsibilities should be documented in the internal audit charter and approved by the board. Any work beyond the assurance activities should be recognized as a consulting engagement, and the implementation standards related to such engagements should be followed.
- Internal audit should provide advice, challenge, and act as a support to management's decision-making, as opposed to making risk management decisions. Internal audit cannot give objective assurance on any part of the risk management framework for which it is responsible. Other

suitably qualified parties should provide such assurance.

Domain IV counts for 20–25 percent of the CRMA examination.

IV.A Facilitate Identification and Evaluation of Risks

KEY TERM

Facilitate: To help make something happen.

Internal auditors are well placed to facilitate risk identification and evaluation. A useful way to achieve this is through a brainstorming (or “idea shower”) session with the internal auditor (see II.B.2). The same knowledge and skills used for investigative inquiry can be used to draw responses from those in attendance, organize the responses, ensure comprehensive consideration of all likely sources of relevant risk, and summarize the findings. It is helpful to have a balanced group with a range of relevant expertise. Those closest to the activity or area for which risks are to be identified should be included, but other views also should be represented; i.e., business unit managers, risk management specialists, senior management, and other operational areas that have an interface or synergy with the area under review.

There is an important difference between facilitation and instruction. *Instruction* tells management what risks it faces and does the evaluation with the managers (or even *for* them). *Facilitation*, on the other hand, means acting as a resource for management, enabling the organization to identify its risks and arrive at its own conclusions about their value. This is an important difference, as it ensures that management maintains responsibility for risk and will be more able to identify and evaluate risks in the future without assistance.

To facilitate something is to ease its happening and help bring it about. The quality of objectivity (familiar to internal auditors) is very important. In this context, this means not bringing a pre-set solution or pre-conceived ideas to the facilitation exercise, but creating an environment in which those present can

come to well-reasoned judgments of their own. The operational and senior managers of the organization need to understand, own, and take responsibility for the risks.

An effective facilitator must be skilled in:

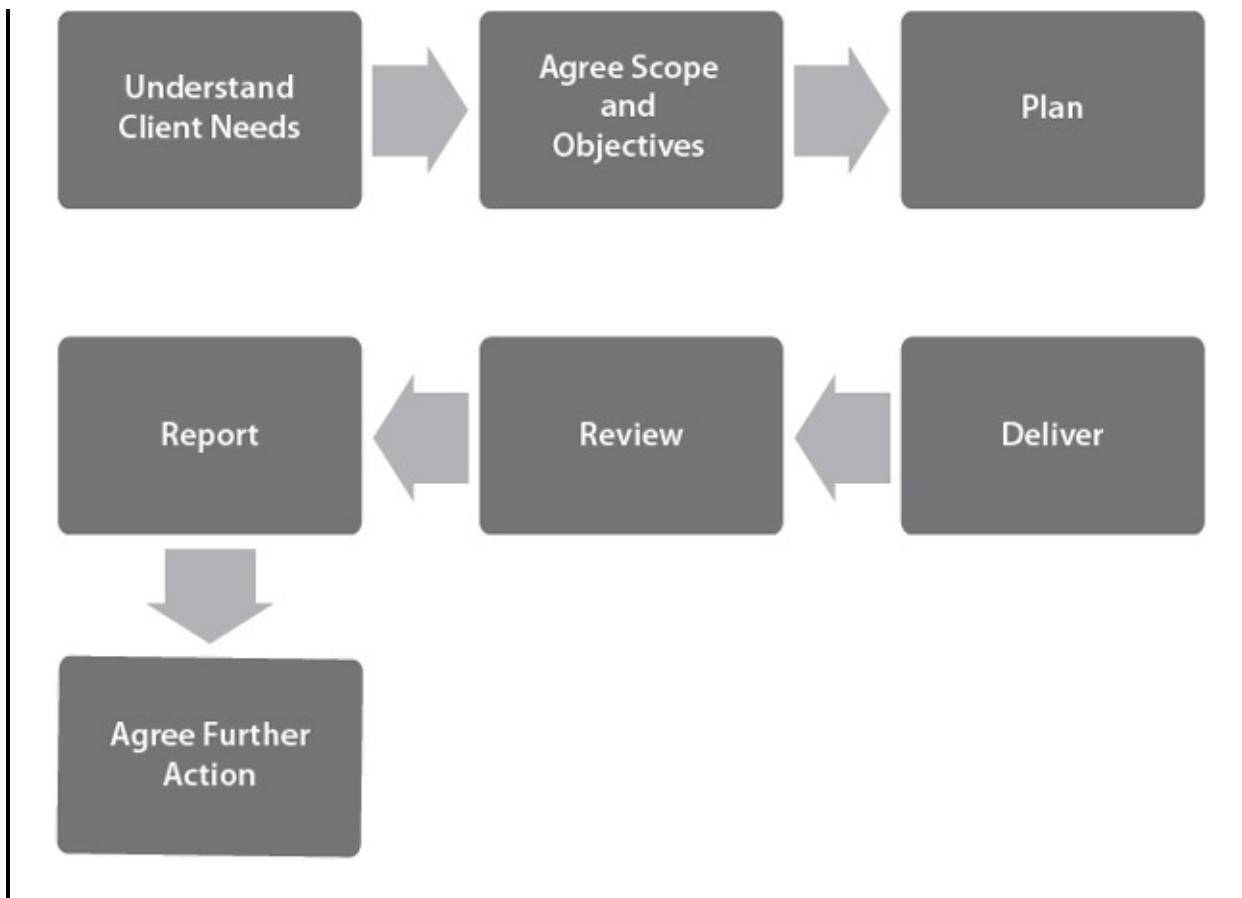
- Planning facilitation sessions.
- Guiding individuals through the facilitation objectively to reach their own conclusions after a thorough review of all relevant information.
- Managing people and time to ensure everyone has the opportunity to make a contribution, and keeping the session focused on the objectives.
- Critical thinking to process and summarize information, demonstrate connections, and highlight implications.

There are a number of tools and resources that the internal auditor can use to help prepare and deliver a facilitated session. (See, for example, www.mindtools.com.)

Several key stages (see [Figure IV.3](#)) to the facilitation process include:

- Understanding the needs of the client.
- Confirming the scope and objectives with the client.
- Planning the facilitation exercise.
- Facilitating the activity.
- Reviewing the effectiveness of the activity.
- Reporting outcomes.
- Making recommendations and proposing further actions.

Figure IV.3. Facilitation Stages



IV.A.1 Understand the Needs of the Client

The process begins with fully understanding the needs of the client. This requires a series of discussions to ensure that both sides are clear and have a shared understanding and common expectations of the desired outcomes. The internal auditor has a very good grasp on the process of risk identification and evaluation, but, as we saw in II.B.2 and II.B.3, there are many different options. It is necessary, therefore, to come to an agreement about the appropriate techniques, level of detail, reference material, and benchmarks to be used. This will depend upon the size, values, and culture of the organization, as well as the degree to which ERM already exists and is embedded. It could be very unhelpful to employ a highly sophisticated approach when neither the complexity of the operations nor the present maturity level of the risk management processes warrants it. A good starting point (which the internal auditor should already know) is risk management maturity. Considering a scale from risk-naive to risk-enabled (see [Figure III.6](#)), one can determine the maturity level of the organization or area of activity under review.

It is quite possible that the internal auditor understands the needs of the client better than the client does or, at least, is able to express those needs more clearly. Care and sensitivity should be exercised in discussions to prevent the internal auditor's views from taking undue precedence. It is acceptable for the internal auditor to help the client express what the requirements are for the facilitation, and this may be supported by asking a series of questions. This helps ensure that important considerations are taken into account, rather than simply ignored—whether deliberately or through lack of awareness. However, in the interests of independence, the internal auditor should not *tell* the client what the requirements *ought* to be. That is for management to decide.

IV.A.2 Confirm the Scope and Objectives with the Client

Although the internal auditors set the objectives for assurance engagements, the client is responsible for the objectives of advisory services, such as facilitation. This is made clear in the *Standards*:

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.

2210.C2 – Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

2220.C1 – In performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-upon objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the client to determine whether to continue with the engagement.

In summary, the *Standards* require that the objectives, scope, responsibilities, and expectations must be:

- Clear and agreed.
- Documented (for “significant engagements,” although documentation is good practice for all but the simplest engagement).

KEY TERM

Scope: The defined range and limits of the subject of inquiry for an engagement.

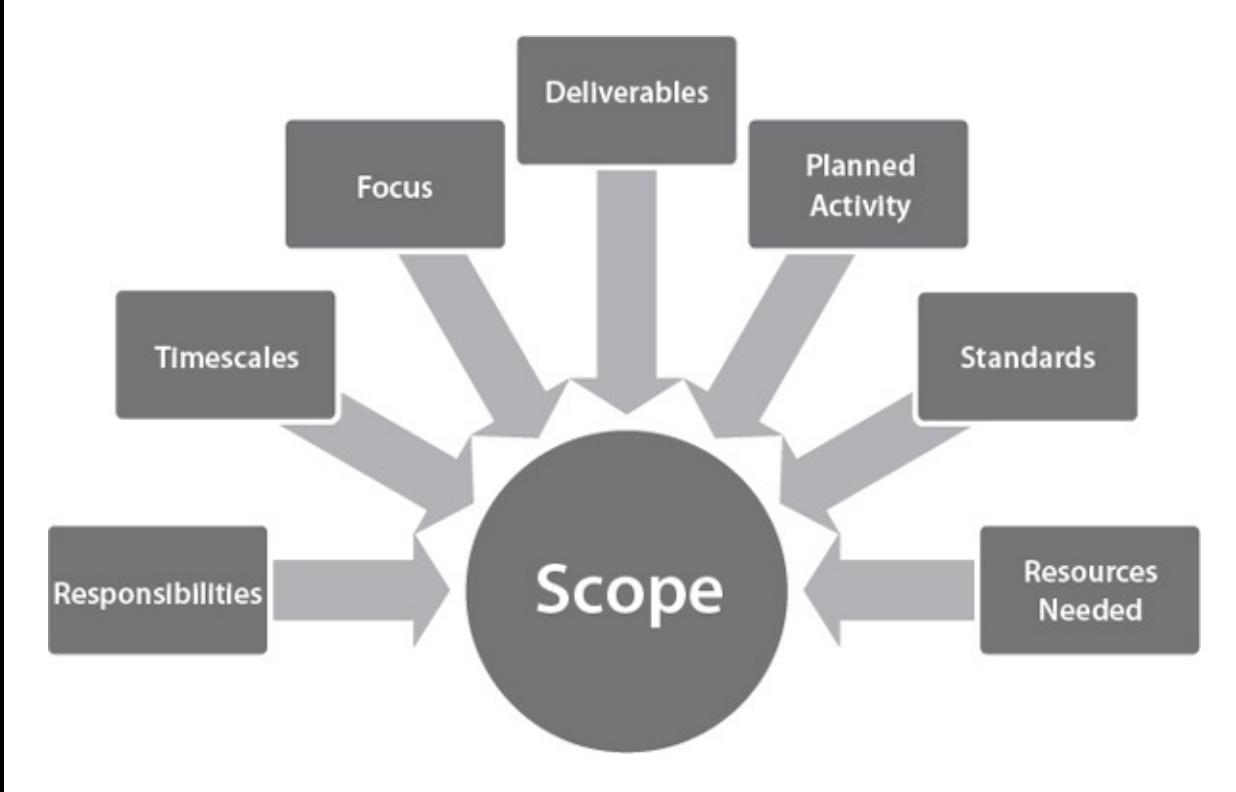
- Specific on the degree to which governance, risk management, and internal control issues are to be addressed, as agreed with the client.
- Consistent with the objectives of the organization.
- Sufficient to ensure the client receives what is intended from the engagement. Any reservations about this should be discussed at the outset and may result in the engagement not being undertaken.

Within the scope is an agreement about the areas of activity to be included in the risk identification and analysis. This may vary considerably, including (for example):

- All key or strategic risks for the organization.
- The risks associated with the implementation of a new IT system.
- Specific risks within an area of activity where controls have been found to be weak.

The agreed scope and expectations help determine who should attend the risk identification and evaluation sessions. The scope, therefore, sets boundaries for the engagement by expressing what is to be included (and perhaps—for the sake of clarity—also what is excluded). It delineates the respective roles and responsibilities and specifies what is planned in terms of activity and anticipated timescales. Finally, it defines engagement deliverables (the required outcomes) and their format. [Figure IV.4](#) illustrates the contents for a scope.

Figure IV.4. Consulting Engagement Scope



IV.A.3 Plan the Facilitation Exercise

The activities that are required for facilitation may take place in a single session or through a number of different events over a period of time. We described a range of risk identification activities in II.B.2. Activities involving groups of people need to be carefully facilitated to maximize the beneficial outcomes. Facilitated risk identification events commonly bring together representatives from key groups across the organization. The activity is often a structured combination of brainstorming and reflection. In planning the event, it is important to consult with the client and focus on the agreed scope and objectives. The internal auditor must think carefully about the structure of the activity—who will attend, the timing and location, resources needed, the initial information that needs to go to participants to help them prepare, and the best way to ensure that the desired outcome will be achieved.

One of the key elements that must be determined is the extent to which the facilitation and evaluation activity is structured. At the two extremes, the activity may be a wholly free-flowing, open discussion, or a rigid, facilitator-led

exercise. The choice should be based on the engagement objectives and scope, the needs and capabilities of the participants, the size of the group, the time available, and the level of risk management maturity.

IV.A.4 Facilitate the Activity

The content and structure of facilitation events vary considerably. Let's discuss some of the more common elements that an internal auditor may use.

KEY TERM

Icebreaker: Group activity designed to elicit cohesion and participation.

Many facilitators like to start a group session with an *icebreaker*. This is helpful, particularly when the members of the group are unfamiliar with each other or unaccustomed to working together. Icebreakers encourage participation through something that is usually informal and fun. When the ice is broken and people have relaxed with each other, they are usually more willing to contribute throughout the rest of the session.

Once members of the group are reasonably comfortable with each other, it may be useful to *set the context*. It is important that everyone understands the purpose of the event and has a realistic expectation of what is going to happen. The internal auditor also should clarify his or her own role as an independent facilitator helping the organization come to a conclusion about its risks and their relative severity. Included in this is the fact that, unlike an assurance engagement, the internal auditor is not going to deliver an opinion. Instead, he or she will provide recommendations that the client can either accept or decline. Participants must realize and value the fact that the resulting set of identified risks are to come from them, not the internal auditor.

KEY TERM

Groupthink: A group's adoption of a single viewpoint not reflecting individual opinions.

Brainstorming is a technique commonly used in risk identification. In its simplest form, the facilitator asks the group to come up with suggestions for risks that may exist to the area under review. Such activity should be spontaneous, fairly rapid, and widely participative. At this stage, there are no right or wrong answers. All suggestions are taken as valid. This may take place with the group as a whole or in smaller *breakout groups*, depending on the overall size. The outcomes of brainstorming or idea showers are usually captured quickly on flipcharts so that they can be seen by everyone and referred to later. The facilitator needs to use skill to keep the brainstorming focused and lively. Otherwise, it can wander off topic or lose momentum. Brainstorming is best done in short bursts, interspersed with other activities.

A common problem to watch for is known as *groupthink*. There is a tendency for groups to have a “herd instinct” and stick to a shared viewpoint, even when individuals might disagree. Peer pressure can act in a subtle fashion and persuade people to fall in line with the prevailing opinion, so as not to appear foolish. A skilled and vigilant facilitator challenges ideas as they are proposed and encourages participation in an environment in which people can say what they think without fear of being wrong. Brainstorming is a good technique that allows all opinions to be freely expressed.

To get things started, a useful technique to consider is a *survey or questionnaire* distributed and collected in advance. This ensures the facilitator can start the session with prior input that has been drawn from a broad cross-section of individuals. These findings may be presented before, after, or instead of a brainstorming session. They can be challenged and built upon in the risk identification process.

To give structure to the risk identification activity, the facilitator may decide to make use of *checklists* and *benchmarks*. These are another way of ensuring that the session does not start with a figurative or literal blank sheet of paper. Instead, the group can use the contents of the information provided as prompts for identifying the risks that exist within the given area under review.

Vulnerability assessments and *control risk self-assessments* are even more structured in their approach and particularly useful for guiding a group through a

comprehensive risk identification and evaluation exercise.

As ideas are generated, the facilitator will recap and summarize at regular intervals to keep the event on track. With risk identification, there is a tendency for individuals to suggest things that are actually only weaknesses or issues. The facilitator will need to bring to the group a deeper understanding of the evaluation process. Although the broad areas in which risk exists may have been identified, steps used in analysis are required to pinpoint what the risk actually is. (See II.B.3.) The facilitator can refer to key definitions (inherent risk, residual risk, relevant risk, root cause, etc.) to help with this process.

For example, a participant in a risk identification workshop may suggest that third-party contracts are a risk. With the assistance of the facilitator, the group can analyze where the risk lies. The facilitator could ask participants to determine which of the following processes is a source of risk with regard to third-party contracts:

- Deciding in which areas of activity to work with third parties.
- Selecting the parties with whom to work.
- Carrying out due diligence.
- Drafting the terms of the contract.
- Monitoring the delivery of the agreed service.
- Reviewing the context in which the relationship operates.

The facilitator also may ask more generally:

- What could go wrong?
- What are the root causes and the trigger events?
- How would such a risk materialize and what would the impact be?

In coming to an agreement about the likelihood, impact, and other criteria used to analyze the risks, subjective viewpoints can result in a great deal of

debate. Therefore, agreement on terms is essential. Words like high, medium, and low might be useful for an initial assessment. However, as greater levels of detail are considered, the terms soon will require definitions and possibly refinement. The more objective these measures are, the easier it will be to reach a consensus. This may require several steps. First, can we agree on what the risks are? Second, having identified the risks, can we agree about which one is the most and least important, relative to the others? Then, can we agree on a high, medium, and low classification? The further this type of analysis goes, the greater the necessity for well-defined terms.

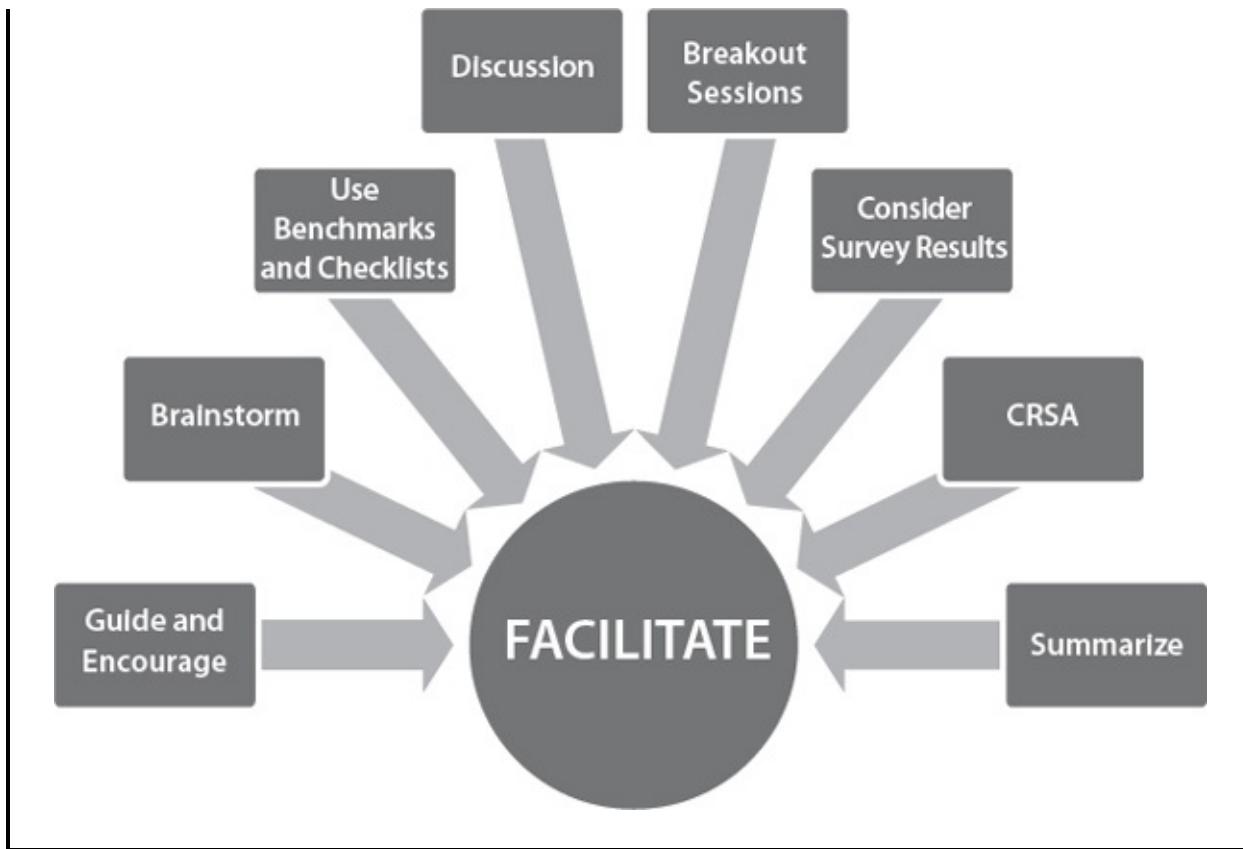
Measures of likelihood are a matter of frequency or number of occurrences expected over a given period of time. For impact, likelihood may be defined by financial value, volume of activity, scale of disruption, number of senior managers needed to address it, and similar factors. This moves the evaluation to questions of fact, rather than opinion. To help the group reach an evaluation, the facilitator can provide data from benchmarking, historical incidents, and professional projections, while recognizing that no two situations are identical and the past offers no guarantees for the future.

Given the potential for detailed and extensive discussions, the facilitator may decide that as much progress as possible has been made in a single session, but that further activity may be required at a later date. Returning to the matter after several days or weeks can reinvigorate the discussions and enable more rapid progress—as opposed to slogging away for many hours without a break.

The facilitator should end the session with a summary and concluding comments. The summary may include a review of what has been achieved, comparing the set and achieved objectives for the session, and agreeing action points. This helps reinforce what has been gained in terms of learning, clarifies what has been agreed, and secures buy-in for future activity.

The key elements that may form part of a facilitated risk identification and evaluation activity are shown in [Figure IV.5](#).

Figure IV.5. Facilitation Session Elements



For an alternative perspective on facilitation, Heron (1998) describes terms of different *dimensions*. These occur during the facilitation session itself. The facilitator may decide the sequence of dimensions when planning the activity, and often they will occur repeatedly in varying combinations in a single session. Each dimension is characterized by *facilitative questions* that are useful points for the facilitator to consider at the outset. The dimensions include:

1. The planning dimension: this is the goal-oriented, end-and-means aspect of facilitation that considers the goals of the group and the program it should undertake to fulfill them. The facilitative question: how will the group acquire its objectives and its program?
2. The meaning dimension: this is the cognitive aspect of facilitation, relating to the participants' understanding of what is going on, how they make sense of experiences, how they do things, and how they react to things. The facilitative question: how will experiences and actions of group members be meaningful?

3. The confronting dimension: this is the challenge aspect of facilitation, which involves raising consciousness about the group's resistance and avoidance of things it needs to face and deal with. The facilitative question: how will the group's consciousness be raised about these matters?
4. The feeling dimension: this is the affective aspect of facilitation, relating to managing feelings within the group. The facilitative question: how will group feelings be handled?
5. The structuring dimension: this is the formal aspect of facilitation, including the methods of learning, the form that is to be given to experiences within the group, and the structure of the process. The facilitative question: how should the group's learning experiences be structured?
6. The valuing dimension: this is the integrity aspect of facilitation, involving the creation of a supportive climate that honors and celebrates the personhood of group members—a climate in which participants can be genuine and disclose their reality as it is, while keeping in touch with their true needs and interests. The facilitative question: how can we create a climate of personal value, integrity, and respect?

The facilitator should be prepared to get the group to challenge anything that stops them from performing.

IV.A.5 Review the Effectiveness of the Activity

A review is always helpful to sharpen processes for the future, as well as to check whether something to be completed later has been overlooked. Such reviews are best conducted as close to the activity as possible. Feedback from participants will provide helpful commentary on how it felt from their perspective and what could have been done better. A comparison between what was planned and what actually occurred will help identify opportunities for improvement.

IV.A.6 Report Outcomes

The risk register records risk identification and evaluation. Even if the activity is not complete and further sessions are planned, it may be beneficial to the client to view the risk register on work in progress.

Also, a linked issue is which records should the internal auditor keep on a consulting project. This is similar to concerns about records on assurance engagements, as described in the *Standards*.

2330.C1 – The chief audit executive must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization’s guidelines and any pertinent regulatory or other requirements.

IV.A.7 Make Recommendations/Propose Further Actions

In the final part of the facilitation process, the internal auditor should discuss with the client any further actions that may be required, either to satisfy the original objectives of the engagement or to build upon the outcomes of the work completed. This may take the form of further facilitation exercises for risk identification in the same or other areas. In addition, the exercise may have identified the need for coaching on risk topics, coordination of risk activity, improvement to risk reporting, and developments in the organization’s approach to risk management. These types of advisory services are described in the following sections of this domain. Any assurance activities that may have been identified must be considered by the CAE for possible inclusion in the audit plan.

IV.B Coach Management in Responding to Risks

Coaching can be an extremely powerful tool and is a great way to empower other people. Coaches apply the benefit of their knowledge and skills to the service of developing an individual or a team for general or specific skills. A wealth of knowledge and expertise about risk is necessary for the internal auditors’ ability to deliver assurance on risk management processes. Although taking on the responsibility of responding to risks would impair their

independence, it is wholly acceptable (with the usual safeguards) for the internal auditors to coach others in doing so.

There are different models for coaching, but they all share a common focus on enabling someone else to learn, develop, or achieve. Unlike instruction (with the trainer explaining and demonstrating what needs to be done), coaching creates the opportunity for individuals to discover for themselves. A coach does not provide the answers to a problem but helps others to work out a solution that is appropriate for them and their circumstances. The intention is to equip an individual to continue to grow and develop—an ongoing benefit.

In this section, we will consider coaching specifically for the purpose of improving management's capability to respond effectively to risk. This is designed to yield long-term value by ensuring that management is better equipped to address risks and make informed decisions in planning and implementing responses. The coaching may focus on particular systems or controls when weaknesses have been identified or new activities are being introduced. Alternatively, it can be more general to build a broader understanding of the nature of risks and the options for responding to them. Coaching should not be seen as a way to fix a problem. Rather, it contributes toward a culture of continuous improvement and increasing risk management maturity.

KEY TERM

Coaching: A process of helping others develop through personal growth and discovery.

Mentoring and coaching are similar approaches in that they are both about one individual (coach or mentor) helping another. In common language, we may even equate the two, but there are important differences. A mentor is usually someone who has a particular relevant experience, knowledge, or skill, and may be more senior than the person being mentored. The relationship is often specific to a period of transition as someone enters a new role or takes on new responsibilities that are within the mentor's own experience. The mentor helps that person step into the new position. A coach, on the other hand, may not have

specific prior knowledge or experience or be more senior than their client. The focus is not primarily on getting someone through a challenging period but on equipping them for continued success in the future. Coaching often tends to be for a shorter period than mentoring. Some of the potential benefits of coaching for individual managers and for the management team as a whole are illustrated in Figures IV.6 and IV.7.

Coaching works best as part of a strong relationship between the coach and those being coached. It is sometimes best understood as being a continuing dialogue through which the coach provides a combination of encouragement and challenge in a purposeful, constructive fashion. The coach needs to understand the present level of performance in the area to be developed (in this case, responding to risks) and focus attention on getting the client to explore alternative approaches that can yield improvements.

The Institute of Leadership and Management defines coaching as:

The process of enabling individuals to acquire the knowledge, skills, and techniques needed to perform effectively in their occupational role by motivating, inspiring, challenging, stimulating, and guiding them. The coach must be able to recognize the needs of individuals being coached, develop a coaching program appropriate to meet those needs, and help individuals achieve their full potential. (ILM, 2013)

In the case of coaching management on responding to risk, the internal auditors have many advantageous qualities:

- They are familiar with and understand the client's organization.
- They are experts in governance, risk, and control.
- Their skills in working with people are compatible with the skills of coaching.

Coaching may be used at any stage in an organization's risk management maturity, but it is most likely to have maximum appeal when:

- The organization recognizes that there is an opportunity or a need to improve its attitude to risk, embed risk management more extensively

into routine operations, and apply a greater awareness of risk to planning and decision-making.

- New managers join the organization or are promoted from other levels and must grow in their ability to manage risk.
- There is a wider organizational drive toward continuous improvement in all aspects of operations.
- There has been a program of training in risk-related matters and there is a need to ensure its full benefits are realized.
- Individuals have been identified or have identified themselves as requiring greater expertise in risk.
- The response management is making toward risk has been found (possibly through an assurance engagement) to be an area of *weakness within the risk management framework*.

Figure IV.6. Benefits to Individual Managers

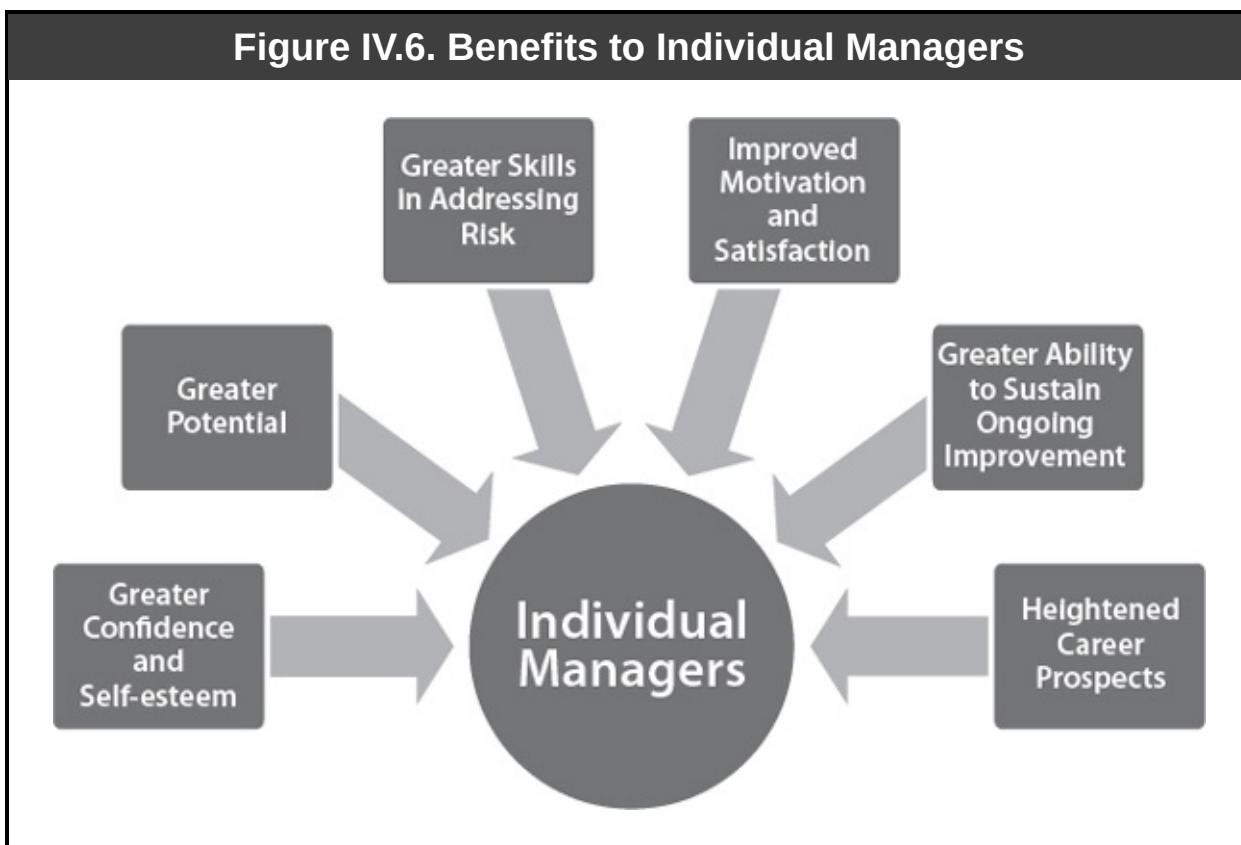
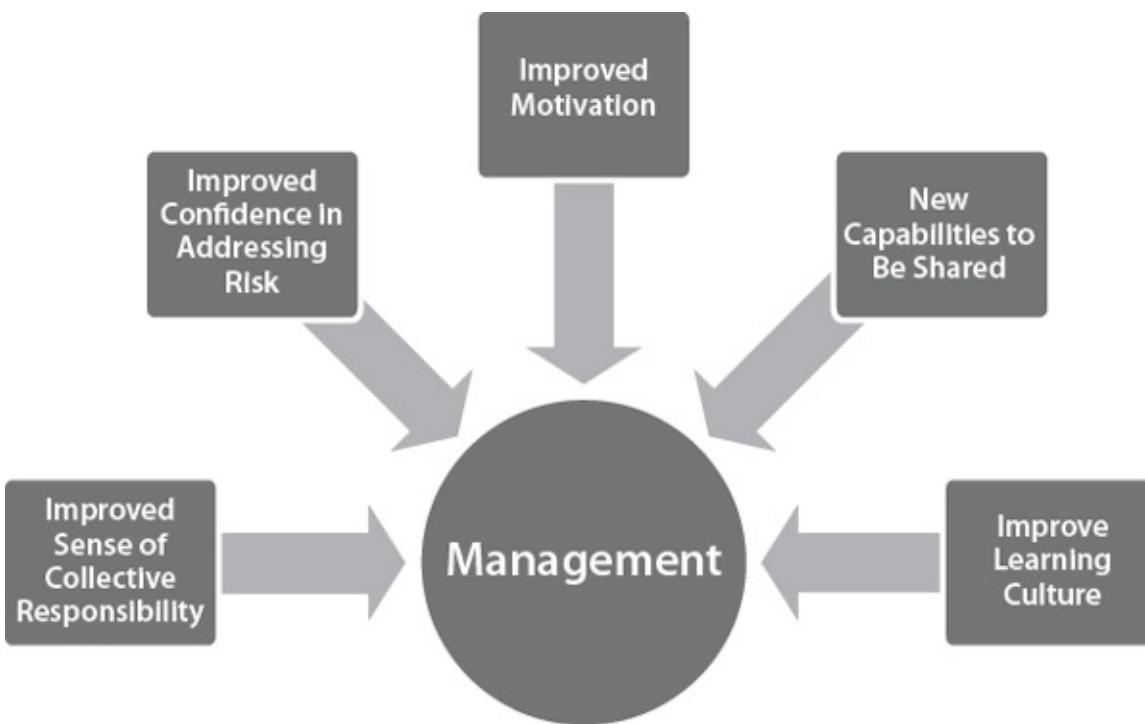
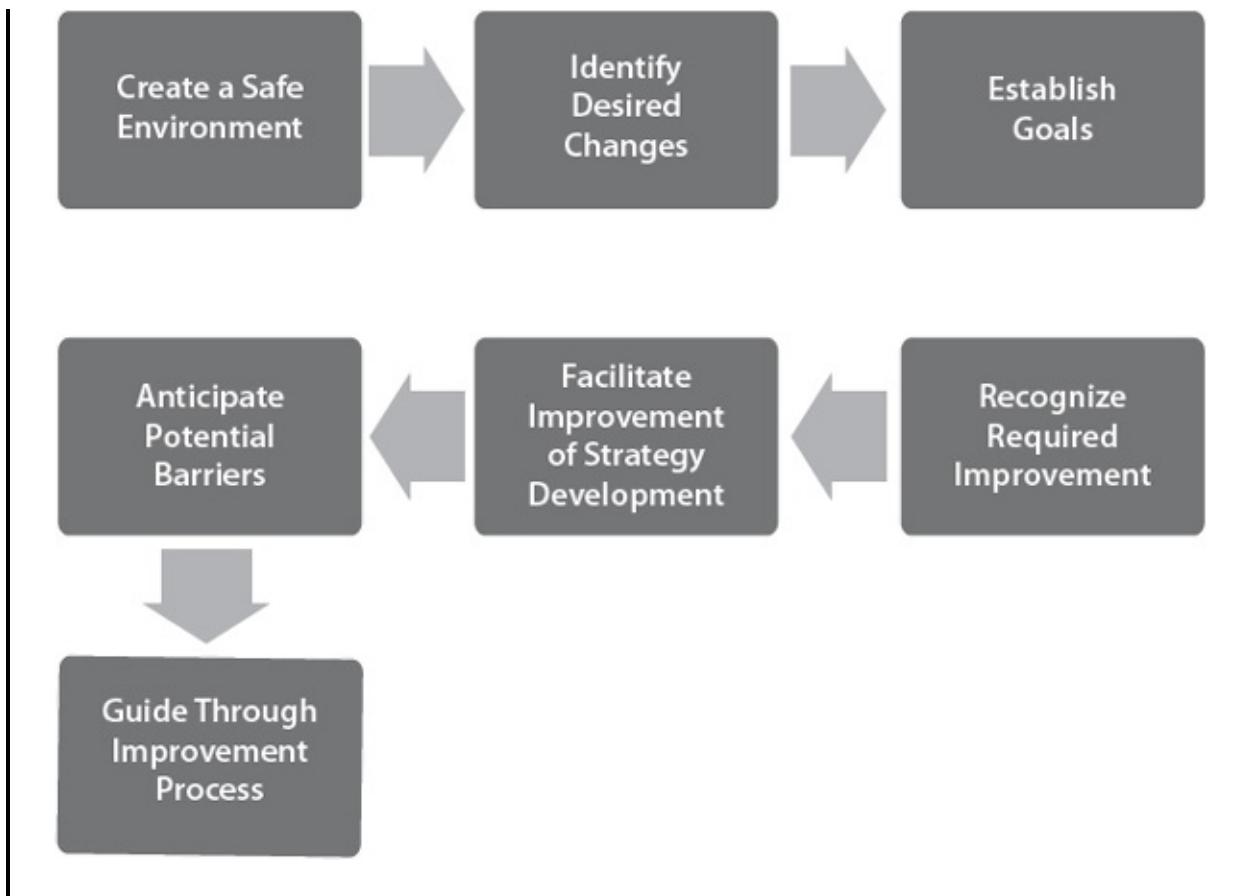


Figure IV.7. Benefits to Management as a Whole



When an internal auditor is asked to provide coaching to management in responding to risk, it is important to establish the scope and safeguards. In particular, the objectives and timescales of these activities must be agreed in advance. Expectations on both sides need to be clear and the independence of internal audit must be maintained. The internal auditor needs to ensure the client understands that management must accept responsibility for managing risk (in accord with Standard 2600). The coaching can take many forms, including both one-to-one and group sessions. Acting as coach, the internal auditor may adopt some of the steps shown in [Figure IV.8](#) and discussed below.

Figure IV.8. Coaching Steps



Those who are being coached need to have confidence in their coach, and that bond of trust is important to enable honest exchanges. The need for coaching does not mean that senior management or the board has concerns about an individual's ability, and the client should be able to talk freely with the internal auditor without worrying that conversations will be reported up the chain of command. Internal auditors are used to dealing with confidential matters. Unless significant control weaknesses or potential wrongdoing are identified, the internal auditor is able to treat topics discussed during coaching sessions as private.

It is necessary to identify the aspects of responding to risk that managers (individually) and management (collectively) hope to improve. Although the internal auditor will have an in-depth understanding of the strengths and weaknesses of the organization's risk management, it is essential that desired improvements are expressed and agreed. Because this is a coaching engagement rather than a training session, the internal auditors do not tell management what is wrong and what needs improving. Instead, they help management identify the

opportunities for improvement and set objectives. The changes needed will come in different forms—systems, processes, standards, monitoring, documentation, and reporting. Most significantly, however, is a required change in behavior and approach adopted by management and managers. The internal auditor as coach must allow managers to come to this conclusion and find an expression for the desired change.

The best approach to take is to support management in a self-assessment of the present effectiveness of responding to risk. Questions that may be asked to prompt this might include:

- What processes are working well—in accordance with expectation—and what others are less successful?
- Is the organization faced with regular surprises in the form of unexpected risks and opportunities?
- Are the actual frequency of occurrences and impacts of risk events in line with their assessed levels?
- Are controls in place working as intended?

The next stage is to help management set goals for improvements to these elements. In II.B.1, we explored the value in setting SMART objectives that are more likely to lead to real improvements. Feeling confident and empowered as a result of coaching, management will be well-equipped to set goals for itself.

Based on an understanding of the present position to a clear sense of intended future performance, the coach and management can work together to build a strategy that can move the organization toward its goals. The actions required may include training and development, investment in new or upgraded systems, and some form of business process reengineering to ensure alignment between risk management processes and operational activity. Such change-oriented projects require good communication with stakeholders and careful monitoring throughout the implementation process. Potential difficulties should be anticipated and remedial plans for mitigation should be made. The internal auditor can make valuable contributions to all of these steps while ensuring that management has the capabilities necessary to repeat similar steps in the future,

without the same level of coaching or with none at all.

IV.C Coordinate Risk Management Activities

Not all organizations have a fully mature risk management framework. As maturity evolves (see [Figure III.16](#)), it is likely that risk management activities were developed initially in silos (i.e., separately in different parts of the organization). This is part of a natural evolution of risk management brought about by the varying circumstances that prevail in operational areas, and has a lot to do with capabilities, opportunity, system complexity, leadership, and other similar factors. The internal auditors may be asked to assist in the coordination of these activities to improve consistency, efficiency, and effectiveness.

The move to ERM implies, among other things, that a greater degree of centralized control and coordination is required, and management often seeks advisory help from the internal auditors to assist with this transition. The CAE may temporarily take the place of a chief risk officer (CRO) but should exercise great caution. Again, unless stringent safeguards are in operation, this role can become very close to risk management.

Establishing effective enterprise-wide risk management is one of the principal responsibilities of management and the board, and this cannot be escaped by recruiting internal audit services to help with its coordination. The internal auditors will not subsequently be able to deliver assurance on any part of operations for which it has had responsibility, including aspects of the risk management framework. Assurance on this must be provided by other parties.

Maynard (1999) provides a list of roles the internal auditors can play in risk management activities:

1. Analyzing the audit universe through subjective and objective means to reveal audit priorities. This involves moving away from the audit cycle and using a range of quantitative and qualitative measures that evolve as circumstances change.
2. Analyzing management's ability to achieve its stated goals and

objectives in pre-audit narratives. This requires taking account of management's assessment of risk and risk tolerances.

3. Examining internal controls from the top downwards, using questionnaires and other similar means. This includes a consideration of the risk culture, tone at the top, organizational values, strategic planning, management information, and decision-making; and how these impact risk management.
4. Analyzing the processes for establishing and overseeing risk limits. These limits are determined by financial and operational resources, targets, and constraints.
5. Reviewing other risk management functions, such as treasury, compliance, and accounting control. It is important to get the big picture on risk exposures and determine how much reliance can be put on other sources of assurance.
6. Observing the strategic planning process and its results. This provides insights into emerging and changing risks.
7. Evaluating strategic initiatives. These may include strategic alliances and new projects.
8. Integrating audit activities. This may include pulling together IT and front-line auditing.
9. Basing the audit process on the net effect of risk exposures and compensating controls. Audit recommendations should be based on this equation, which also serves to determine the extent of substantive testing needed to confirm the position.
10. Partnering with management by providing consulting services and value-added information.
11. Reviewing ethics as a basic element of internal control.
12. Conducting a comprehensive audit of the entire risk management program.

The point about combined assurance is an important one. One of the key roles for the internal auditors to play is maintaining an overview of all internal and external sources of assurance to ensure that there are no significant gaps and no unnecessary overlaps and duplications. In addition to the assurance provided by the internal auditors, it also is given by management, the external auditors, health and safety inspectors, compliance officers, and many others.

To drive consistency, the internal auditors are likely to be involved in the following areas of risk management coordination:

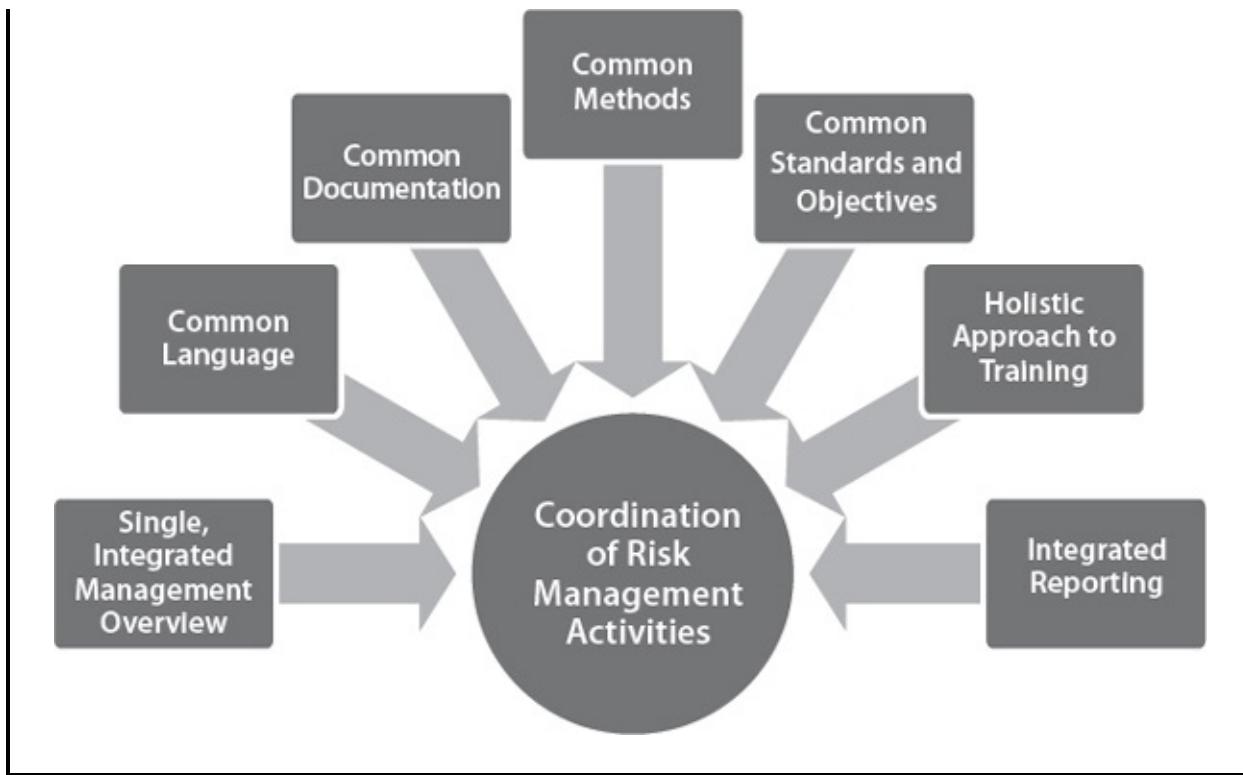
- Reviewing documentation and records related to risk management to identify whether the whole organization is using common terminology, definitions, and risk language.
- Holding meetings with managers to ensure they are aware of their responsibilities, know how to make proper use of risk management procedures, and understand the risk tolerances that impact their area of responsibility.
- Determining timetables and deadlines for risk reviews, risk register preparation, and updates.
- Organizing discussions with risk owners and other stakeholders to challenge risk identification and evaluation.
- Providing research and information to support ongoing improvement to risk management maturity.

These tasks identify where the focus of the coordination efforts should be applied and where the greatest benefits can be derived from the internal auditor's input. [Figure IV.9](#) provides an overview of risk management coordination and [Figure IV.10](#) depicts its goals.

Figure IV.9. Overview of Risk Management Coordination



Figure IV.10. Goals of Risk Management Coordination



What management requires from risk management is a clear and consistent picture of the exposure to risk and the degree of preparedness for materializing risks. Armed with this, management is able to make effective, informed decisions and plan activities accordingly. When risk management systems and processes are well-established with a strong second line of defense, the internal auditors are able to provide assurance on its effectiveness. However, if the current state of risk management falls short of an embedded ERM approach, the internal auditors can assist in strengthening the second line of defense. To secure a well-integrated view across the organization as a whole, common approaches among business units must be synchronized and interdependent.

A useful starting point for risk management coordination, the internal auditor acting in an advisory role (having already clearly established that management is responsible for risk management) must ensure that all those involved understand and are applying common terminology. Risk classifications, measurements, and definitions (risk, inherent risk, residual risk, ERM, impact, likelihood, etc.) need to be used consistently for the sake of effective communication. Through a review of documentation and reports, discussions with individuals and groups, and surveys and questionnaires, the internal auditor can establish the extent to which risk language is employed consistently. This review has to encompass all

levels of the organization, including members of the board. If there are inconsistencies, the internal auditor may recommend that management provide guidelines and training to reinforce uniform vocabulary.

Closely related to this is ensuring that teams use common tools for recording risks, risk incidents, and mitigation plans. To provide maximum support to management and the board in its governance responsibilities, a high-level report should capture the key risks, along with their relative inherent and residual severity, the controls in place, and any actions required for bringing levels back within appetite. From this master overview, it should be possible to drill down through progressive levels of detail to the specific operational risks and systems of control. This can be achieved only through standard templates, and using digital media and deploying either proprietary or tailor-made software makes it much easier.

When customs and practices have developed organically across an organization, it is unlikely that teams use the same approaches for identifying, evaluating, responding to, monitoring, and reporting on risks. Different objectives for risk management will have evolved and varying standards will be used. Business units may have, to a greater or lesser extent, adopted elements from the ISO Standards or COSO, or simply developed ad hoc arrangements. There needs to be a decision from the top about the single framework an organization will use. We stressed in domain I and elsewhere in this book that the choice of approach to risk management must be made to reflect the needs of the organization, taking into consideration key dimensions such as its size, culture, goals, and capabilities. In an advisory role, the internal auditor can provide information on available options to help determine the best fit. Once this has been agreed, the internal auditor can work with management to develop a plan of transition.

An important benefit arising from a coordinated approach to risk management is the opportunity to pool skills, provide peer-to-peer review, and deliver mentoring and coaching and other forms of training and development. It is likely that the internal auditor's review of current practice will identify training needs. Good practice can be shared and areas for development can receive the resources necessary for improvement. Acting in a coordination role, the internal auditor will be in a good position to make recommendations to management on training needs.

Standardized approaches to risk management will empower a holistic system for reporting, including coordinated deadlines, formats, and communication channels. When discussing risk reporting previously (II.B.7), we noted that a balance must be struck in the amount of detail provided. A coordinated system allows for the pooling and summarization of information as it is passed upward, so that each level of the organization receives the degree of detail it requires. Drawing reports together will reveal any common patterns—both good practice and weaknesses—and will allow management to address the findings in an efficient and cost-effective manner. A more detailed discussion of consolidated reporting on risks follows in the next section.

IV.D Consolidate Reporting on Risks

All those involved in an organization rely in some way on risk reporting. Those closest to the activity in which the risks may arise have direct access to how well controls are working, but even here, reports are needed for monitoring purposes and can provide clarity about underlying patterns over time. Senior management, the board, and other stakeholder groups are almost wholly reliant on reporting to stay abreast of risk exposure, the reliability of controls, emerging risks, and the overall effectiveness of risk management. This is vital to their responsibility for risk oversight.

KEY TERM

Consolidate: Strengthen and make more substantial by drawing together and adding to.

One of the key roles of a CRO is to bring together various pieces of risk reporting. In the absence of a CRO, the CAE may be asked to undertake this role. In developing the role of the CRO, the CAE must be careful not to become the risk manager, rather than risk coordinator. Otherwise, there may be a perception that the post-holder (and no one else) is responsible for managing risk.

The IIA Research Foundation's publication, *Corporate Governance and the Board: What Works Best*, suggests that the CRO "acts as the line managers' coach, helping them to implement a risk-management architecture and work with it on an ongoing basis. As a member of the senior management team, the CRO monitors the company's entire risk profile, ensuring major risks identified are reported upstream."

Within an ERM framework, risk reporting is provided internally and externally at various times for a range of audiences, from different levels and perspectives, and for a number of purposes. (See [Figure IV.11](#).) In mature risk management processes, reporting is fully embedded and integrated with business planning cycles and other forms of reporting.



Acting in an advisory role, internal auditing may be called upon by management to assist with the consolidation of reporting. Reporting needs to be planned, with a clear schedule of times, audiences, format, and content. In

fulfilling this role, the assigned internal auditor should consider both internal and external reporting needs as described below.

Internal Reporting: The Board

With ultimate responsibility for risk management, the board has specific requirements in terms of risk reporting. Having set the risk management framework and agreed to the appetite, the board needs to know whether risk management is operating as intended. It needs assurance that risk responses are enabling the organization to exploit opportunities and maintain risk exposures within appetite. It has an ongoing remit to monitor key risks and identify emerging ones. Where residual risk temporarily falls outside of appetite, the board requires an explanation of actions being taken to restore internal control and confirmation that the organization has the tolerance to endure the present situation. Finally, the board will request reports on monitoring and review to direct revisions and improvements as required.

Sobel and Reding (2012) analyze the reporting needs of the board under:

- Immediate communications.
- Periodic written communications.
- Periodic presentations.

Immediate communications relate to significant risk events that have the potential for major impact on strategy and need to be escalated to the highest level. In some instances, an emergency meeting of the board may be required to discuss and agree actions. *Periodic written communications* cover monthly or quarterly reports on key risk indicators, highlighting those that require attention. *Periodic presentations* are usually made to coincide with the timetable for board meetings to add commentary to written communications. They also provide information on changes to the risk profile, new or emerging risks, areas in which conditions have changed so that residual risk levels now exceed appetite, controls that have failed or require revisions, and important underlying trends in risk management performance.

In taking on a consulting engagement to consolidate risk reporting, the

internal auditor will need to review existing arrangements for communicating with the board. Because effective reporting aligns expectations with delivery, the internal auditor should confirm the information needs of the board, as well as review the current level of service provided.

Internal Reporting: Other

Other than the board, the key recipients for risk reports are staff and managers. Routine reporting provides status updates while ad hoc reporting addresses risk events (see Sobel and Reding, 2012). *Status reporting* tracks internal and external changes that may move risk management processes out of alignment with organizational needs. This includes prevailing conditions in the external environment (as characterized by the PESTEL model provided in I.C.1) and internal developments that alter the organization's capabilities (staff competencies, systems, processes, capacity, etc.). In addition, status reporting delivers regular updates on the state of risk management processes and notification of projected trends and conditions that require adjustments to ERM, such as risk events that have occurred and been managed. *Risk event escalation* is the reporting of risks that have materialized and threaten a disruption to operations. An effective system for such reporting includes tolerance levels that (when exceeded) require escalation to the next level of authority. The purpose of reporting is not only to provide information but also to seek authority and resources to initiate remedial action.

External Reporting

External risk reporting informs wider stakeholders (investors, customers, and the public at large) and satisfies regulatory requirements. There are disclosure requirements for a listed company's annual reports, as shareholders need to know how secure present value and future earnings are. Other requirements exist in the public sector.

In all aspects of risk reporting internal auditors have highly relevant expertise for evaluating the adequacy and effectiveness of arrangements. Based on their analysis, they are able to advise management on opportunities for revisions and improvement.

IV.E Maintain and Develop the Risk Management Framework

As discussed in previous sections, maintaining and developing the risk management framework is a role that internal auditors are sometimes asked to perform. Because this could come close to managing risk, very stringent safeguards are required. We have referred to the overriding safeguard several times throughout this manual—a common understanding and recognition that managing risk remains the responsibility of management. In addition, there should be agreement that the consulting role has a fixed time period during which the internal auditors will provide an interim solution to help management and the organization become better equipped to manage risks in the future.

However, having established the safeguards, it is clear that the internal auditors have a role to play in improving risk management. Standard 2100 states:

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

Improvements to the risk management framework can be achieved directly as a result of assurance engagements, as well. The 2050 Practice Guide states:

Internal audit's review of risk identification, risk evaluation, control identification and evaluation, and appropriate risk treatments challenges and enhances risk registers and the risk management framework.

The risk management framework refers to the overall approach to risk management, the risk strategy, and its objectives. If you asked a team of managers to show you their risk management framework, they might simply tell you what they do to identify, evaluate, and respond to risks. Alternatively, they might say that they use COSO's ERM framework. In many cases, what exists in practice is likely to be a customized approach with aspirations for moving closer to something akin to the COSO model.

In addition to the initial challenge of protecting independence (via a clearly documented scope and a report to the audit committee), the internal auditor must

ask:

- What is the current framework for risk management?
- In what ways does the organization wish to improve the framework?

A request for consulting (likely from management in response to perceived weaknesses and/or a desire for improvement) must only be for a specified period of time. The departure of a key player with responsibility for overseeing risk management activity also may precipitate a request for the internal auditors to temporarily step into this role.

Pickett (2005) describes five phases in the evolution of a risk management framework. Although this is not intended to be an accurate description of how frameworks actually develop over time—and certainly such an account could never hold true for all organizations—it does serve to highlight features that are key to risk management frameworks, and may be introduced and developed as the approach becomes more sophisticated. This also may assist the internal auditor in identifying opportunities for developing the framework when doing so at the request of management. A simple summary (with reference to Pickett, 2005) is provided in [Figure IV.12](#), and each phase is described below.

Figure IV.12. Risk Management Framework Evolution



Phase 1

A simplistic view of the organization prevails. The board sets the vision and mission and agrees to the strategy with the CEO and team of directors who, in turn, work with senior managers to implement it. The organization faces risk in its external environment through change and unpredictability, where risks are largely regarded as threats to achieving goals. Key performance indicators (KPIs) are set to help steer the organization to success, motivating managers to meet or exceed targets, in spite of the risks.

Phase 2

The organization starts to take account of risk in its outlook and planning. In part, this relates to a broader view that recognizes the multiple interests of stakeholders and the need to reflect these in the strategy. This increases the importance of strategic risk and the possibility of strategic solutions, rather than simply trying to achieve targets, despite the risks.

The foreword to the executive summary of COSO's ERM framework from 2004 suggests seven strategic solutions, quoted in Pickett (2005):

- Aligning risk appetite and strategy.
- Improving decision-making in response to risk.
- Reducing operational surprises (and losses).
- Being aware of and addressing cross-enterprise risks.
- Integrating responses to multiple risks across the organization.
- Identifying and taking advantage of upside risks (opportunities).
- Improving the deployment of resources informed by risk awareness.

In addition to strategic risks, the organization begins to take account of operational risks by identifying and monitoring them in a coordinated fashion. Such an approach requires the development of *risk maps*.

Phase 3

With a greater understanding of risk comes the possibility of defining the appetite for different types of risk. We discussed the determinants of risk appetite in I.A.3 and elsewhere. Pickett uses a list of 11 C's to describe this:

- Capability—how much risk the organization can tolerate.
- Commitment—the extent to which there is organizationwide buy-in to risk management.
- Choice—the attitude to risk as demonstrated in decision-making.
- Consistency—the degree of compatibility between risk management and the way the organization works.
- Context—the internal and external environments.
- Challenge—the empowering of managers by taking control of risk.

- Communication—the dissemination of risk appetite information to all stakeholders.
- Clarity—the degree of precision underlying the understanding of risk.
- Controls—the extent to which risks are mitigated.
- Core values—the organizationwide acceptability of a risk-based approach.
- Culture—the way the organization operates.

Phase 4

Risk management needs to become a well-defined and distinct (albeit, integrated) activity in its own right. This phase is something that the organization does as part of its operations. A risk is an event that may impact an objective and, therefore, risks are understood as being related to objectives. This captures the series of risk management processes that we described in detail in domain II (risk identification, assessment, response, monitoring, review, and reporting).

Phase 5

Finally, we may recognize and describe an enterprisewide risk management framework. Objectives, appetite, ownership, control, and reporting are embedded and integrated across the organization at all levels in a consistent, efficient, and cost-effective manner. There is a significant net contribution to the achievement of organizational objectives. Risk awareness is reflected in all important planning and decision-making. Such a framework facilitates a statement of internal control (if required), as it is possible to give an overall view on the current risk exposure and effectiveness of responses. There are robust systems in place for monitoring and improvement. The approach also can be validated by virtue of clear and auditable documentation from which assurance may be taken. Risk management processes are incorporated (without being lost) within routine operational activity.

In undertaking a consulting role to maintain and develop the risk management framework, the internal auditors need a full working knowledge of existing arrangements. This requirement is likely already met, considering their

responsibilities for providing assurance on risk management. To *maintain* the framework, the internal auditor can monitor activity, review the effectiveness of internal controls, and report to management any element that requires attention, because it is under-resourced, poorly configured, previously overlooked, or simply failing to operate as intended. This reporting makes it clear that management maintains responsibility for managing risk at all times. To *develop* the framework, the internal auditor can make recommendations to management regarding opportunities to strengthen internal controls, improve efficiency and/or effectiveness, add value to reporting arrangements, adopt more sophisticated tools for analysis and evaluation, and add to the maturity of risk management processes in any way. Once again, the internal auditors will not be empowered to deliver these improvements. They are, however, well-placed to make considered proposals that are sympathetic to the organization and that will move it closer to an embedded enterprise-wide risk management framework, akin to COSO's ERM framework.

IV.F Advocate for the Establishment of Risk Management

Risk management happens, even when it is not done consciously or formally. In an extreme case, an organization wholly ignorant of risk would carry on, with regular surprises and disappointments as a result. This is simply tolerating or accepting risk with an unlimited appetite but without any degree of forethought and planning. It is highly unlikely that any organization would take this approach (and less likely still that it would be successful). Risk management, therefore, will normally have a degree of structure to it but still may be a long way from being fully established with a comprehensive, integrated, enterprise-wide approach.

The internal auditors have a responsibility for promoting risk management as part of their assurance role. As the 2050 Practice Guide, Coordinating Risk Management and Assurance, states:

By independently reviewing the risk management process of an organization, internal audit can promote risk management throughout the organization and the audit process can be aligned with risk management frameworks. Consistent risk language used throughout the organization can be adopted by internal audit.

However, advocating risk management also may be a role that management specifically requests the internal auditors to take on as part of their advisory capacity. There are many ways of doing this, including:

- Education and training.
- Leading by example within the internal audit activity.
- Highlighting opportunities for improvements to risk management as part of all assurance engagements.
- Sharing good practice from within the organization and externally.
- Proposing and supporting risk management champions.
- Scenario planning that highlights hazards of poor risk management.
- Appealing to corporate governance codes that extol the virtues of risk management (e.g., King III).
- Getting involved at the point of risk incidents and escalation (being part of the solution).

These are all positive encouragements. Other approaches are possible but not recommended in the first instance. In jurisdictions where risk management is a legal requirement, the internal auditors can promote it from a compliance perspective. In an extreme situation, and as a last resort, an internal auditor could use whistleblowing as a means of encouraging management to address risk more robustly, although this is not a method to be taken lightly.

KEY TERM

Advocate: To inspire others to change behavior, attitude, or understanding.

It is in the best interests of the internal audit activity to promote risk management. If it is to adopt a risk-based approach, it needs to draw upon a risk

management framework—particularly, a comprehensive risk register. If these are not in place, the internal auditors will need to create them.

The internal auditor's goal in promoting risk management is to cultivate good practice and move the organization forward in the maturity of its risk management processes. This has to start with a thorough understanding of the present condition of risk management—something the internal auditor already has.

Advocating risk management is a continual process. To be in a position to promote best practice and drive continuous improvement, the internal audit activity must ensure that it remains conversant with trends and developments in the practice of risk management. As highlighted by Matthew Leitch (2004), in “Embedded Risk Management: The Auditors’ Contribution,” a basic level of knowledge about risk responses and internal controls is not sufficient to act as an advocate for risk management. Leitch argues that many internal auditors are inclined to rely on knowing about responses that typically can be integrated into routine activity and carried out by a junior individual or team with little or no understanding of risk. In contrast, best practices in risk management have gone a long way past this. It requires a considerable amount of management time and judgment to determine, design, and implement a risk response. Internal audit’s view of risk responses can operate at a more simplistic and almost mechanical level based on formal systems, such as finance, procurement, and IT. This tends to favor risk responses, such as:

- Segregation of duties.
- Signoffs and authorization.
- The use of standardized documentation.
- The use of risk-response tables.
- Testing.
- Insurance.
- Contingency planning.

Leitch may be speculating about what internal auditors know and understand. However, he makes a good argument that, if the internal auditors are serious about advocating risk management as a robust, agile, and valuable part of organizational activity, they need to promote risk responses that go beyond the obvious. His examples include:

- Keeping options open.
- Trying things to see what works.
- Incremental delivery of projects.
- The use of time buffers (which, as he explains, are part of critical path analysis used in project management).
- Decisions based on uncertainty, rather than on specific risks.
- Design of control systems from risk factors (instead of itemizing risks or control objectives).
- Statistical process control.
- Explicit representation of uncertainty in models (including rolling forecasts) used in decision-making.
- Conversational skills that probe for uncertainty and risk.

Advocacy is the art of inspiring others to take action. A rather inspired definition is offered by the Water Supply and Sanitation Collaborative Council (www.wsscc.org):

Advocacy involves looking outward to determine your objectives and audiences; looking inward to assess your resources; and looking ahead to monitor the effectiveness of your advocacy and adjust it to achieve your objectives.

In our context, it requires:

- Working with management to agree objectives for advocating the

establishment of risk management (although, as stated above, the internal audit activity has its own reasons for doing this).

- Identifying the target audiences for advocacy (which could conceivably include all stakeholders but should focus on the areas requiring the greatest impact).
- Reviewing the resources that can be applied to advocating risk management (time, mostly, although there may be financial costs if additional resources are required to cover the internal auditor engaged in advocacy).
- Setting and monitoring key performance indicators to assess the impact of advocacy. This, however, is not a simple task, as progress can be slow and almost intangible (but simple methods like polling the awareness of risk-related matters among target groups before and after advocacy can be effective).

Any advocacy is likely to be more successful when it is planned and the approach is based on research. There must be clarity about the action that the internal auditor is hoping to inspire in others through the advocacy. The short reason for advocacy is to improve the enterprisewide attitude toward risk. The longer reason involves deciding which elements need strengthening. This forms part of the initial conversation with management to determine the scope for the consulting engagement. The list of tasks for an advocacy project is very similar to the planning needed for any project, and may look something like the steps described in [Figure IV.13](#).

Figure IV.13. Advocacy Steps for Risk Management

Research and Preparation

What is the current state of the organization's risk management?

Agree Objectives

What is the desired impact and target audience(s)?

Set Targets and KPIs

How will success of the initiative be gauged?

Stakeholder Analysis

Who should be involved and what are their respective interests and needs?

Identify Resources Needed

How much staff time is required and is it included in the audit budget?

Develop Key Messages

What needs to be communicated and to whom?

Design Strategies

What activities (training, group discussions, risk assessment workshops, etc.) need to be delivered to transmit the messages?

Plan and Deliver Strategies

What are the practical steps required for implementation?

Monitor Delivery

Are the actions going according to plan?

Evaluate Outcomes

Have the desired impacts (changes in behavior, attitudes, awareness) been achieved?

Report to Management

What are the conclusions and recommendations for future action?

IV.G Develop Risk Management Strategy for Board Approval

One of the key responsibilities of the board with respect to risk management is to approve the strategy. For an organization without a formal risk management strategy or one that is underdeveloped or weak, it is common for management to seek support in creating a strategy or improving the existing one. Using their knowledge and skills, the internal auditors are in a position to fill this role.

There are different ways in which such a strategy can be put together and presented, but typically, it should include (in some form) the elements shown in [**Figure IV.14**](#). In developing this strategy, the internal auditor should consult with all key stakeholders, as well as determine how far the organization is willing and able to progress in the maturity of its risk management processes, based on organizational culture, capabilities, and strategic aims.

Figure IV.14. Risk Management Strategy



Role and Purpose

A strategy document should make clear the full extent of its role and purpose; in this case, the remit for risk management. This may be expressed as a vision or mission. Alternatively, it may be given as a simple statement defining the function of risk management and its intended impact. The words used should convey to everyone what risk management is all about in terms that are easy to understand and apply. This might be through a generic statement, such as the one provided by the Institute of Risk Management:

The purpose of risk management is to safeguard an organization, its customers, reputation, assets, and the interests of stakeholders by

identifying and managing all threats to the achievement of its business objectives.

In ISO 31000, the purpose of risk management is “to direct and control an organization with regard to risk” and in COSO’s ERM framework, “to identify potential events that may affect the entity, manage risk to be within the risk appetite, and provide reasonable assurance regarding the achievement of entity objectives.” These are very technical and rather dry. For a more meaningful statement, it is helpful to express the purpose in terms that are relevant to the organization. For PepsiCo, for example, it is simply “to ensure that risks are taken knowingly and purposefully,” although this is still fairly vague. A company called Electrobit (www.electrobit.com) describes risk management’s purpose as:

To secure positive development of earnings of the company and the continuation of the business by implementing risk management cost-effectively and systematically throughout the different businesses.

The description goes further to add:

Risk management is part of the company’s strategic and operative planning, daily decision-making process, and internal control system. Business objectives, risks, and risk management operations are combined through risk management as one chain of events.

The reason for trying to capture the purpose is to ensure that it is clear, not just to management and the board but to all concerned. It must be understood that risk management is an aid to organizational effectiveness, not something designed to eliminate risk or be an end in itself.

Objectives and KPIs

Closely allied with risk management’s role and purpose are its objectives. These provide greater details through a series of statements that collectively capture what the arrangements for risk management are aimed at achieving in the particular organization. Where these objectives are SMART, they can be used as KPIs and serve as a basis for the assessment of risk management effectiveness. A list of broad objectives for risk management is provided in

I.A.1. Again, a certain degree of contextualization, rather than using generic statements, renders the objectives more relevant and useful. Objectives may be framed by considering a series of questions, such as:

- How is risk management going to help the organization achieve its goals?
- In what aspects of activity is it designed to have the most impact?
- How is its value to be measured?

KPIs are important because they allow the organization to assess whether the strategy is successful or not. Possible KPIs (based on suggestions from the Institute of Risk Management) may relate to:

- Reduction in financial losses from fraud.
- Reduction in the number and time periods of project overruns.
- Improvements in cost management.
- Reduction in the number and frequency of risk incidents.
- Improvements to customer satisfaction ratings and perceived reputation.

Rationale and Principles

As a further refinement to the purpose of risk management, it is important to be clear how the strategy is aligned to the needs of the organization. Explicitly referring to the organization's vision, mission, values, and strategic aims will achieve this. The rationale may also explain why the proposed risk management strategy takes the form that it does, what shortcomings in the previous approach are being addressed, and how the revisions will benefit the organization. The principles underpinning a strategy are the guiding parameters that have been used to determine the approach and implementation.

Interdependencies

The revised risk management strategy will require adjustments in other areas of activity. There may be a need for training and development, additional

resources, or new operating processes. These are the interdependences that have to be in place for the new strategy to be implemented.

Standards, etc.

The risk management strategy should highlight the standards, templates, and frameworks relied upon when establishing the systems and processes and gauging their success. In II.A, we explored a range of recognized benchmarks that are available, as well as the relative merits of adopting them. The choice must be made on the basis of what is best for the organization and the extent to which it is ready to commit.

Definitions

Risk management depends on a substantial array of technical terms. Some of these have standard definitions, while others are ready for customization. In all cases, it is advisable to set these out clearly in the strategy. Definitions of key terms, such as risk, inherent and residual risk, trigger events, and risk response will help establish a common language and shared understanding. Other elements also need to be defined. For example, if the organization chooses to grade likelihood as being low, medium, or high, it should be clear on the meaning of these terms to reduce subjectivity as much as possible. Because there are no standard definitions, the organization must make a choice on the basis of practicality and clarity. Low likelihood, for instance, may be defined as an event with less than a 25 percent chance of occurring in the next 12 months. Alternatively, it may be an event that, on average, will occur once every three months.

Risk Policies

Some organizations have a single risk management policy included in the strategy or as a separate document. Others choose to have separate policies for each significant area of activity or type of risk, such as health and safety, data protection, and human resources. The risk management strategy needs to reference these policies so that the whole approach is unified and can be readily comprehended.

Processes

The processes to be used for risk management may be included either in the strategy or a separate policy document. Regardless, important principles that relate to the way the organization is actually going to undertake risk management need to be established, agreed, and included in the strategy. The processes are used for:

- Risk identification.
- Risk analysis and evaluation.
- Risk response.
- Response implementation and monitoring.
- Review.
- Reporting.

Administration

Risk management delivery requires that decisions be made about documentation and the use of IT. Standard templates should be agreed upon for items such as the risk register and a risk reporting schedule.

Gap Analysis

Having set out the blueprint for a new risk management strategy, a gap analysis will show the difference between the present position and the desired one. This is a precursor to implementing an action plan.

Action Plan

Finally, the action plan should describe the required steps needed to deliver the strategy and fill the gaps. The plan should include assigned responsibilities, timescales, budget and other resources, measurable outcomes, and monitoring and reporting arrangements.

The development of a risk management strategy draws upon all the internal auditors' knowledge and understanding on risk. It is an opportunity to leverage

all of this coherently and set out a vision that will help the organization on its journey toward embedded ERM. By involving key individuals from all parts of the organization, the internal auditors will enhance their own expertise.

Summary

This concludes our consideration of the various consulting (or advisory) roles the internal auditors can play to support risk management. In all of the different approaches, we have stressed the need for these two lines of defense to remain distinct through the proper application of stringent safeguards. As long as these are in place, there is a great deal that the internal auditors can offer to management through their expertise in governance, risk, and control. It is also important to understand the benefits to both sides. The internal audit activity gathers useful additional insights through its consulting work that can be applied to future assurance engagements. In addition, there is much to be gained by all stakeholders—including the internal auditors—from robust, well-coordinated, and embedded enterprise-wide risk management. Acting in a capacity to promote risk management requires the internal auditors to be well-versed in leading practices relating to the associated standards and processes. They also must possess a thorough understanding of the client organization and its provisions for addressing risk.

Internal auditors, therefore, should welcome the challenge of providing management with advisory services, in addition to their assurance function. The two roles are complementary and jointly serve to ensure that the internal audit activity delivers a uniquely valuable contribution to the organization.

APPENDIX A

Sample CRMA Exam Questions

1. Which one of the following is an objective of risk management?
 - A. To increase the likelihood of maximizing profits.
 - B. To facilitate greater operational effectiveness and efficiency.
 - C. To identify employees who are inclined to commit fraud.
 - D. To limit ambitions and risk-taking across the organization.

2. Which of these statements BEST describes risk culture?
 - A. The system of values and behaviors present throughout an organization that shape risk decisions.
 - B. The leadership and commitment to risk management from the highest levels of the organization.
 - C. The level of authority and trust awarded to managers to determine the risks they are prepared to take.
 - D. The policies and processes that define risk ownership, risk responsibilities, and risk reporting requirements.

3. When is an organization risk-enabled?
 - A. When a risk strategy and policies are in place and communicated.
 - B. When risk management and internal control are fully embedded into operations.
 - C. When the organization establishes a risk committee, a risk management team, and risk processes.
 - D. When risk appetite has been defined.

4. The IIA's definition of risk, taken from the glossary of the International Professional Practices Framework, is as follows: "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.” Which one of the following is NOT a risk?

- A. Fluctuations in currency exchange rates will reduce sales in some markets.
 - B. Power failure to the engine room for a prolonged period will reduce production.
 - C. A shortage of qualified and well-trained employees will prevent expansion.
 - D. Failure to achieve profit targets will reduce shareholder dividends.
5. Residual risk is BEST defined as:
- A. The risk that a material error exists in the financial statements after the audit.
 - B. The portion of inherent risk that remains after management executes its risk responses.
 - C. The risk that audit procedures will fail to detect the error.
 - D. The internal and external risks that exist if there are no internal controls in place.
6. What is the primary purpose of a code of ethical behavior and statement of values in an organization?
- A. To prevent people in the organization from breaking the law.
 - B. To clarify the expectations the organization has of its staff and what external stakeholders can expect.
 - C. To minimize reputational damage to the organization.
 - D. To increase profits.
7. There are a number of internal and external stakeholders who have an interest in successful enterprise-wide risk management, but who has the primary responsibility for identifying and managing risks?
- A. Owners and shareholders.
 - B. The board of directors.

- C. Management.
 - D. Risk managers.
8. According to COSO's framework, there are two types of controls: hard and soft. Which of the following are soft controls?
- A. Controls that rely on behavior and attitude.
 - B. Controls that are relatively easy to introduce, monitor, and manage.
 - C. Policies, processes, and specific measures, such as password protection.
 - D. Controls (such as inspections and reviews) performed by people.
9. In January 2013, The IIA published a Position Paper, The Three Lines of Defense in Effective Risk Management and Control. Which one of the following operates as a second line of defense?
- A. External auditors.
 - B. Senior management.
 - C. Risk management.
 - D. Operational management.
10. During monthly management meetings, the team leader always asks for feedback on progress and ideas for new ways of working. What sort of management style is the team leader using?
- A. Democratic.
 - B. Autocratic.
 - C. Laissez-faire (from the French meaning to let happen).
 - D. Impoverished.
11. There are a number of simple techniques commonly used to assist decision-making. Which of the following is NOT one of those techniques?
- A. Cause and effect (or fish) diagrams.
 - B. Cost-benefit analysis.
 - C. Six thinking hats.
 - D. Delegation.

12. A purchasing manager has subcontracted repairs and maintenance to a facilities management company. This is a new relationship and has been entered into quickly. Which one of the following is NOT a control measure that will help to mitigate the risks?
- A. A schedule of regular communication and reporting.
 - B. Financial penalties for missed targets and performance failures.
 - C. Stated objectives and itemized responsibilities for each party.
 - D. Identifying an alternative subcontractor.
13. An organization's chief risk officer (CRO) is most effective when the CRO:
- A. Manages risk as a member of senior management.
 - B. Shares the management of risk with line management.
 - C. Shares the management of risk with the CEO.
 - D. Monitors risk as part of the enterprise risk management team.
14. The ISO 31000 and COSO ERM models have been thoroughly tested and developed over many years and are widely regarded. The ISO framework helps organizations with three activities. Which of the following is NOT one of the three activities?
- A. Increase the likelihood of achieving objectives.
 - B. Improve the identification of opportunities and threats.
 - C. Help managers better deal with the wide range of risks that threaten an entity's objectives.
 - D. Effectively allocate and use resources for risk treatment.
15. You are the chief audit executive (CAE) for a defense contractor in the aerospace sector. Senior management and the board are very concerned about information security risks. They have asked you to recommend a risk management framework for the organization. Which ONE of the following would you recommend?
- A. COSO's ERM framework.
 - B. ISO 31000.
 - C. IIA GAIT for Business and IT Risk.

- D. The National Institute of Standards and Technology (NIST 800-37).
16. ISO 31000 provides a framework with five components for managing risks and the way in which they interrelate in an iterative manner. Which of the following is one of the five components?
- A. Internal environment.
 - B. Mandate and commitment.
 - C. Categorization of information and information systems.
 - D. Control activities.
17. The COSO thought leadership paper, Understanding and Communicating Risk Appetite, identifies four considerations affecting risk appetite. “The amount of risk that the entity is able to support in pursuit of its objectives” is which of the four?
- A. Existing risk profile.
 - B. Risk capacity.
 - C. Risk tolerance.
 - D. Attitudes toward risk.
18. Which of the following is the best approach to use when benchmarking the risk management process?
- A. Meet with a competitor in your industry and exchange risk management process information.
 - B. Ask your regulator which framework to use.
 - C. Meet with company operational management to establish a set of criteria and objectives.
 - D. Research several frameworks and select the guidance from some or all of the frameworks that work well with your company’s industry, culture, and objectives.
19. According to COSO’s internal control framework, a precondition to risk assessment is:
- A. Establishing control procedures or activities.
 - B. Establishing a monitoring mechanism.

- C. Establishing objectives or goals.
 - D. Establishing performance measures.
20. An organization has calculated that for every day its call center is not available, it loses \$250,000. The director of telecommunications has identified external threats as the most serious risks to the call center and has asked a consultancy firm to set up a duplicate offsite call center with backup hardware and software. What has the director done?
- A. Recognized that external threats cannot be reduced and ACCEPTS the risks.
 - B. Established a contingency plan to REDUCE the risks.
 - C. Entered into a contractual agreement to SHARE the risks.
 - D. Taken action to limit the potential impact of external threats to AVOID the risks.
21. According to Robert S. Kaplan and Annette Mikes, establishing rules to define *what to do* and *what not to do* will only be successful in controlling one specific category of risk. Which of the following is the specific risk category?
- A. Strategic risks.
 - B. External risks.
 - C. Internal risks.
 - D. Theoretical risks.
22. Which phrase BEST describes a control risk self-assessment exercise?
- A. Examining how well controls are working in managing key risks.
 - B. Using standardized checklists to assist risk identification.
 - C. Reviewing processes systematically to identify vulnerabilities and threats.
 - D. Determining the cost-effectiveness of controls.
23. Which of the following procedures form part of risk reporting?
- I. Changes to the risk profile or the level of severity of risks.

- II. Systematic checking of risk mitigation plans.
 - III. Weaknesses identified in the system for internal control.
 - IV. Updates on actions that have been taken with respect to risk treatments.
- A. 1, 2, and 4 only.
- B. 1, 3, and 4 only.
- C. 1, 2, and 3 only
- D. 2, 3, and 4 only.
24. Which activity does the following statement from the Project Management Institute describe? “... the process of developing options and actions to enhance opportunities and reduce threats to project objectives.”
- A. Risk analysis.
- B. Risk mitigation planning.
- C. Risk prioritization.
- D. Risk mitigation implementation.
25. According to Sobel and Reding, a review of risk management processes has three goals. Which one of the following is NOT one of those goals?
- A. To determine the effectiveness of the risk management team.
- B. To determine that the organization is achieving its goals because risk management is working.
- C. To identify and repair weaknesses and faults in risk management processes.
- D. To identify changes in the organization’s objectives and environments and ensure risk management processes remain in alignment.
26. What type of indicator is a fall in sales on the previous period measured by value and volume of goods and services?
- A. Lag indicator.
- B. Lead indicator.
- C. Challenge indicator.
- D. RAG (red, amber, green) indicator.

27. If key risks are the most important risks, what is a *key risk indicator*?
- A. A measure that indicates a risk that has already materialized.
 - B. A measure that indicates a risk incident is about to occur.
 - C. A measure that indicates the root cause of a risk incident.
 - D. A measure that indicates the organization is performing to expectations.
28. Which of the following BEST describes the internal auditors' role when providing assurance on management risk reporting?
- A. Creating a report of the company's key risks.
 - B. Reviewing the accuracy and timeliness of key risk reports.
 - C. Providing key risk reports to the audit committee.
 - D. Providing key risk reports to the external auditors.
29. When establishing a risk reporting plan, management should:
- A. Consider the types of events that could occur and determine the frequency of reporting based on severity.
 - B. Create a plan based on management's needs.
 - C. Report all events to the board of directors.
 - D. Consider the needs of the board of directors.
30. When conducting a review of the management of key risks, an internal auditor will need to specify the scope and objectives of the audit and then gather evidence. Which of the following criteria is specified by the *Standards* for gathering information as evidence?
- I. Sufficient information.
 - II. Reliable information.
 - III. Relevant information.
 - IV. Useful information.
- A. 1 only.
 - B. 1 and 2 only.
 - C. 1, 2, and 3 only.
 - D. 1, 2, 3, and 4.

31. What should an internal auditor do when reviewing a risk associated with an activity?
- A. Determine how the risk should best be managed.
 - B. Provide assurance on the management of the risk.
 - C. Update the risk management process based on risk exposures.
 - D. Design controls to mitigate the identified risks.
32. Who has primary responsibility for providing information to the audit committee on the professional and organizational benefits of coordinating internal audit assurance and consulting activities with other assurance and consulting activities?
- A. The external auditor.
 - B. The CEO.
 - C. The CAE.
 - D. Each assurance and consulting function.
33. Which risk indicator reveals the root cause of a risk event and prompts an organization to take action?
- A. Challenge indicator.
 - B. Risk indicator.
 - C. Action indicator.
 - D. Health indicator.
34. Who is MOST responsible for providing assurance to the board of directors regarding risk management adequacy and effectiveness?
- A. Management.
 - B. External auditors.
 - C. Audit committee.
 - D. Internal auditors.
35. Management implements a new process for which the correct processing may be interpreted differently by a regulator. On what should the internal auditors' assurance to the board of directors focus?

- A. Whether management's decision-making process had a risk assessment, relevant information, and appropriate approvals before implementation.
 - B. Whether the information management used in making the decision was accurate.
 - C. Whether management has consulted with the regulator before implementation.
 - D. Whether the risk assessment process performed by management used the appropriate criteria.
36. When it comes to risk management, which of the following activities should the internal auditors NOT carry out?
- A. Make decisions on mitigation of risk.
 - B. Consolidate reporting on risk.
 - C. Facilitate the identification of risk.
 - D. Monitor risk.
37. Who is responsible for identifying the risk universe in a fully mature ERM environment?
- A. Management.
 - B. The internal auditors.
 - C. Management and the internal auditors working together.
 - D. The board of directors.
38. An internal audit activity is performing an integrated audit of a critical system. Working with management, the internal auditors have determined that loss of the system for more than three hours is unacceptable. Which of the following is the BEST way to manage this risk?
- A. Share the risk by purchasing insurance products.
 - B. Reduce the impact via business continuity planning.
 - C. Share the risk by outsourcing to an internal audit activity willing to accept the risk.
 - D. Reduce the risk by investing in technology with enhanced failure self-detecting and backup capabilities.

39. An internal audit activity is using a process elements approach to assess its organization's risk management process. One of the key process elements requires structured and ongoing communication. Which of the following techniques could provide the MOST relevant and useful evidence?
- A. Documented review of board and audit committee meetings.
 - B. Interviews with those impacted by organizational operations.
 - C. Interviews with individuals involved in risk management.
 - D. Results from previous audits.
40. An internal audit activity is using a key principles approach to assess its organization's risk management process. One of the key principles is that "risk management is transparent and inclusive." In their review, the internal auditors are focusing on the risk counsel activities. Which of the following techniques could provide the MOST relevant and useful evidence?
- A. Ongoing CAE observation via ex officio participation at risk counsel meetings.
 - B. Review the risk management literature for best practices.
 - C. Process mapping the organization's risk identification activities.
 - D. Results from previous audits.
41. An auditor becomes aware of a new regulation. To the best of the auditor's knowledge, management has not assessed the risks. What should the auditor do?
- A. Notify the audit committee/board that management has not addressed the risk.
 - B. Perform a risk assessment and determine the appropriate risk treatment.
 - C. Notify management of the regulatory/compliance risk and provide advice.
 - D. Perform an audit of the compliance activity.
42. When leading the risk management implementation, which activity should the CAE NOT perform?
- A. Obtain support and approval from management.

- B. Develop a plan for responsibility transition to management.
 - C. Perform an audit of the ERM process.
 - D. Allow management to make risk decisions.
43. When looking at risk criteria, which of the following activities can the internal auditors perform as part of their consulting role?
- A. Determine possible risk events and outcomes.
 - B. Challenge management's risk criteria.
 - C. Align decisions with risk tolerance.
 - D. Communicate risk criteria to the business.
44. Which is NOT a safeguard when the internal auditors provide ERM consulting?
- A. Documenting internal audit's consulting role in the internal audit charter.
 - B. Making risk management decisions.
 - C. Advising management on risk.
 - D. Following The IIA's *Standards* regarding consulting engagements.
45. Management has asked internal audit to (as part of its consulting role) help decide how best to mitigate a compliance risk. How should the internal auditors respond?
- A. Refuse to be involved in that decision.
 - B. Advise management to avoid the risk by obtaining insurance.
 - C. Perform an audit in the area and report it to management.
 - D. Perform research on the options and provide analysis.
46. The chief information security officer asks the CAE to offer risk advice regarding the implementation of a new security application. The only IT auditor left the internal audit activity last week and a replacement has not been hired. What should the CAE do?
- A. Accept the consulting engagement
 - B. Decline the consulting engagement.
 - C. Accept the consulting engagement, but have the external auditor review

- the CAE's advice.
- D. Accept the consulting engagement and hire a consulting agency.
47. The chief compliance officer accepts a CAE position for a newly created internal audit activity. Three months later, the new chief compliance officer asks the CAE to provide advice regarding an update of the compliance policy. What should the CAE do?
- A. Decline the consulting engagement.
- B. Accept the consulting engagement, but remind the new chief compliance officer that the CAE has worked in the area.
- C. Accept the consulting engagement, but have the external auditor review the CAE's advice.
- D. Decline the consulting engagement, but have lunch with the chief compliance officer to offer advice off the record.
48. Which of the following is the LEAST likely benefit an organization can expect in implementing combined assurance?
- A. Makes the oversight role of the board more effective.
- B. Leads to improved efficiency in assurance activities.
- C. Leads to reduction in external auditor fees for the annual audit of financial statements.
- D. Reduces assurance fatigue for managers and operations personnel.
49. In coordinating the implementation of a combined assurance approach to risk management, the internal audit activity receives assurance on various risks from a number of assurance providers in the organization. To evaluate the reliability of the assurance from each particular provider, the internal auditor would do which of the following?
- I. Review the policies and procedures of every assurance provider to ensure they prevent personnel from giving assurance in any area where they had operating responsibilities.
- II. Re-perform a sample of every assurance provider's work.
- III. Assess the extent to which the assurance provider's objectives and responsibilities are clearly articulated.

- IV. Determine whether assurance providers have sufficient expertise regarding organizational processes and risk.
- A. 2 only.
 - B. 4 only.
 - C. 1, 3, and 4 only.
 - D. 1, 2, 3, and 4.
50. An organization is introducing a new product that is essential to retaining market share in a highly competitive industry. The internal audit activity has provided consulting services to the product development team. The auditors on this project believe several significant risks that could result in a “train wreck” have not been identified and assessed. The CAE is invited to the CRO’s risk council meeting. At the meeting, the CAE presents the risks and coaches management on possible responses. At the end of the discussion, the risk council elects to go forward with the product launch because none of the risks presented were catastrophic. Which of the following is the BEST way for the CAE to respond to the risk council’s decision?
- A. No action is needed. It is a management decision and the risks are within the organization’s risk appetite.
 - B. No action is needed. The CRO has primary responsibility for coaching management on responses and internal audit cannot be involved because it would impair independence and objectivity.
 - C. Discuss the matter with senior management after the meeting and communicate the matter to the board.
 - D. Discuss the matter with the external auditors and communicate the matter to appropriate external parties.

APPENDIX B

Suggested Solutions to Sample CRMA Questions

Question 1

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: B

- A. Incorrect. Among many others, this is an organizational objective that an ERM system will help to achieve.
- B. Correct. The aim of ERM is to increase the likelihood that the organization will be well run and achieve multiple objectives.
- C. Incorrect. Preventive and detective controls are risk response designed for this purpose.
- D. Incorrect. ERM should encourage measured risk-taking, not prevent it.

Question 2

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: A

- A. Correct. Risk management will be embedded in an organization when risk identification, analysis, and treatment are a routine part of decision-making.
- B. Incorrect. Leadership and commitment are important factors in developing a risk culture, but they require buy-in and application from everyone.
- C. Incorrect. The primary purpose of a risk culture is not to limit or control what people can or cannot do.
- D. Incorrect. Policies and procedures alone do not guarantee risk management will be effective.

Question 3

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: B

- A. Incorrect. These are important parts of establishing ERM, but they need to be applied before the organization is risk-enabled.
- B. Correct. ERM is enabled when it is working effectively throughout the organization.
- C. Incorrect. These are structural elements within the ERM framework.
- D. Incorrect. Risk appetite sets limits and tolerances, but it is only one element of the ERM process and needs to be applied effectively in a risk-enabled organization.

Question 4

(From The IIA's Definition of Internal Auditing, Code of Ethics, and Standards) Solution: D

- A. Incorrect. This is a risk with significant impact that could be mitigated through a response.
- B. Incorrect. This is a risk with significant impact that could be mitigated through a response.
- C. Incorrect. This is a risk with significant impact that could be mitigated through a response.
- D. Correct. This is not a risk but the converse of an objective resulting from the failure to apply sufficient control.

Question 5

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: B

- A. Incorrect. This is “audit risk” from the external auditor’s perspective.
- B. Correct. A management response will reduce a residual risk to an inherent level within the risk appetite.
- C. Incorrect. This is “detection risk” in the external audit risk model.

D. Incorrect. This is inherent risk.

Question 6

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: B

- A. Incorrect. Although it is part of ethical behavior, an ethical code goes beyond this.
- B. Correct. An ethical code and statement of values define expected behavior for everyone in the organization.
- C. Incorrect. A code is not a risk response.
- D. Incorrect. Increased profits result from doing the right thing, but that is not the primary objective of an ethical code.

Question 7

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: C

- A. Incorrect. Owners and shareholders are detached from operations and are not in a position to manage risks.
- B. Incorrect. While the board provides challenge to the risk management process, it does not manage risks.
- C. Correct. Managers at all levels of the organization have a responsibility to identify and manage risks.
- D. Incorrect. Risk managers help devise risk systems and procedures and facilitate risk workshops, reporting, and monitoring, they do not identify and manage risks.

Question 8

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: A

- A. Correct.

- B. Incorrect. These are hard controls.
- C. Incorrect. These are hard controls.
- D. Incorrect. These are hard controls.

Question 9

(From IIA Position Paper, The Three Lines of Defense in Effective Risk Management and Control)

Solution: C

- A. Incorrect. These are external to the organization.
- B. Incorrect. These are stakeholders.
- C. Correct.
- D. Incorrect. These are the first line.

Question 10

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: A

- A. Correct. This is an inclusion style.
- B. Incorrect. Autocratic has little or no consultation.
- C. Incorrect. Laissez-faire is a hands-off style.
- D. Incorrect. Impoverished style is task-focused rather than people-focused.

Question 11

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: D

- A. Incorrect. These diagrams provide the basis for decisions on preventative controls.
- B. Incorrect. This is financial cost versus value decision tool.
- C. Incorrect. These are thinking modes to assist in decision-making.
- D. Correct. Delegation is a management style, not a decision-making tool.

Question 12

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: D

- A. Incorrect. This is a detective control.
- B. Incorrect. This is a corrective control.
- C. Incorrect. This is a preventative control.
- D. Correct. This will only avoid risks for a short time.

Question 13

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: D

- A. Incorrect. Senior management has an oversight role in risk management.
- B. Incorrect. The risk knowledge at the line level is specific only to that area of the organization.
- C. Incorrect. The chief audit executive (CAE) is not responsible for managing risk.
- D. Correct. The chief risk officer (CRO) is most effective when supported by a specific team with the necessary expertise and experience related to organizational risk.

Question 14

(From the CRMA Study Guide, Domain I: Organizational Governance Related to Risk Management)

Solution: C

- A. Incorrect. ISO focuses on this activity (per CRMA Study Guide, Domain II).
- B. Incorrect. ISO also focuses on this activity.
- C. Correct. This is COSO's (not ISO's) key objective (per CRMA Study Guide, Domain II).
- D. Incorrect. ISO also focuses on this activity.

Question 15

(From the CRMA Study Guide, Domain I: Organizational Governance

Related to Risk Management)

Solution: D

- A. Incorrect. Both A and B are widely accepted frameworks, but D was designed for this sector.
- B. Incorrect. Both A and B are widely accepted frameworks, but D was designed for this sector.
- C. Incorrect. GAIT provides a top-down approach to identifying IT general controls, but D was designed to focus on information security risks.
- D. Correct. NIST was specifically designed for information systems and this sector.

Question 16

(From ISO 31000, Section 4.2)

Solution: B

- A. Incorrect. Both A and C are components of COSO's ERM framework.
- B. Correct. This is the first component in the ISO framework. The other components are 1) design of framework for managing risk, 2) implementing risk management, 3) monitoring and review of the framework, and 4) continual improvement of the framework.
- C. Incorrect. Both A and C are components of COSO's ERM framework.
- D. Incorrect. This is one of the principle steps in NIST 800-37.

Question 17

(From COSO's thought leadership paper, Understanding and Communicating Risk Appetite)

Solution: B

- A. Incorrect. This is the “current level and distribution of risks across the entity and across various risk categories.”
- B. Correct. Risk capacity is the amount of risk the entity can support.
- C. Incorrect. This is “acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives.”
- D. Incorrect. This is “the attitudes toward growth, risk, and return.”

Question 18

(From the CRMA Study Guide, Domain II: Principles of Risk Management Processes)

Solution: D

- A. Incorrect. Sharing trade secrets would not be ethical.
- B. Incorrect. Although such a framework may have value, it may not meet all the needs of your company.
- C. Incorrect. While meeting with operational management would incorporate management's expertise, it may not provide a complete view of your industry or regulations.
- D. Correct. Reviewing multiple frameworks (and other sources) would allow you to determine what would work best for your company.

Question 19

(From COSO's *Internal Control – Integrated Framework*)

Solution: C

- A. Incorrect. Risks must be identified prior to controls because control activities are designed to address specific risks.
- B. Incorrect. Monitoring occurs after risks are identified and controls are implemented.
- C. Correct. In the COSO framework, risks are only relevant with respect to objectives.
- D. Incorrect. Performance measures are not an explicit part of the COSO model.

Question 20

(From the CRMA Study Guide, Domain II: Principles of Risk Management Processes)

Solution: B

- A. Incorrect. The manager has taken action.
- B. Correct. This is a controlled response to reduce a risk.
- C. Incorrect. While there is a third party involved, management still owns and takes full responsibility for managing the risk.
- D. Incorrect. There is a response, not avoidance.

Question 21

(From Robert S. Kaplan and Annette Mikes, *Managing Risk: A New Framework*)

Solution: C

- A. Incorrect. Strategic risks cannot be fully controlled, as it may be inherently risky to increase rewards.
- B. Incorrect. The organization does not have the ability to prevent external risks.
- C. Correct. Internal risks can be controlled, eliminated, reduced, or avoided.
- D. Incorrect. The risk is not avoided because there is a response.

Question 22

(From the CRMA Study Guide, Domain II: Principles of Risk Management Processes)

Solution: A

- A. Correct. CRSA is about matching controls to mitigate risks, usually through facilitated group sessions.
- B. Incorrect. This is one way to aid risk identification, but it does not incorporate group discussion of risks or consideration of appropriate controls.
- C. Incorrect. This describes assessments.
- D. Incorrect. This could be discussed, but it is not the primary purpose of CRSA.

Question 23

(From the CRMA Study Guide, Domain II: Principles of Risk Management Processes)

Solution: B

- A. Incorrect.
- B. Correct. Item 2 is part of control and assurance with the risk management process and does not form part of reporting. Only option B excludes item 2.
- C. Incorrect.
- D. Incorrect.

Question 24

(From the CRMA Study Guide, Domain II: Principles of Risk

Management Processes)

Solution: B

- A. Incorrect. Risk analysis considers the origins and nature of risks and precedes assessment and prioritization.
- B. Correct. The mitigation plan is a record of what is required to implement the intended response or make amendments to existing responses.
- C. Incorrect. Prioritization comes before mitigation planning and is about ranking the severity of risks.
- D. Incorrect. Implementation is about taking action.

Question 25

(From the CRMA Study Guide, Domain II: Principles of Risk Management Processes)

Solution: A

- A. Correct. A review is designed to continuously improve the effectiveness of the risk process, not a specific department or team.
- B. Incorrect. Achieving goals is a key objective of risk management.
- C. Incorrect. Risk processes need to evolve as the organization develops.
- D. Incorrect. Risk processes need to evolve as the organization develops.

Question 26

(From Key Term and Figure III.4: Lead and Lag Indicators)

Solution: A

- A. Correct. A lag indicator is a measure of something that has already impacted the organization.
- B. Incorrect. A lead indicator is a measure of something that will impact the organization.
- C. Incorrect. This is a measure that indicates the root cause of a risk incident.
- D. Incorrect. This is an indicator of current risk status—red, amber, and green.

Question 27

(From Figure III.6: Types of Key Risk Indicators [Mainelli, 2007])

Solution: B

- A. Incorrect. This is historical and describes a lag indicator.
- B. Correct. A KRI is a measure that suggests a risk is about to materialize.
- C. Incorrect. This describes a challenge indicator.
- D. Incorrect: This describes a health indicator.

Question 28

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: B

- A. Incorrect. Management should create reports of key risks.
- B. Correct. Internal audit's key role is providing assurance on the accuracy and timeliness of risk reporting.
- C. Incorrect. Management should provide reports on key risks.
- D. Incorrect. Management should provide reports on key risks.

Question 29

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: D

- A. Incorrect. The board should have input on the type of information reported and frequency.
- B. Incorrect. The board should have input on the type of information reported and frequency.
- C. Incorrect. The board should have input on the type of information reported and frequency.
- D. Correct. The board should set the type of information reported and the frequency.

Question 30

(From the CRMA Study Guide, Domain III: Assurance Role of the Internal Auditor)

Solution: D

- A. Incorrect. This is appropriate but not the only criteria.
- B. Incorrect. This is appropriate but not the only criteria.

- C. Incorrect. This is appropriate but not the only criteria.
- D. Correct. All four items are required by the *Standards*.

Question 31

(From III.C and [Figure III.9: Steps to Assurance](#))

Solution: B

- A. Incorrect. Determining how unacceptable risk should be managed is the role of management.
- B. Correct. The internal auditor's role is to provide assurance on the management of risk.
- C. Incorrect. Designing and updating the risk management process is the role of management.
- D. Incorrect. Designing controls would impair the internal auditor's independence.

Question 32

(From III.C, Provide Assurance that Risks Are Adequately Evaluated)

Solution: C

- A. Incorrect. External audit's focus is on the financial statements.
- B. Incorrect. The CEO would not normally be responsible for planning.
- C. Correct. The CAE should provide the audit committee with information on coordination.
- D. Incorrect. Not all other assurance and consulting activities are organizationally responsible to the audit committee for their work.

Question 33

(From the CRMA Study Guide, Domain III: Assurance Role of the Internal Auditor)

Solution: A

- A. Correct. The challenge indicator prompts action.
- B. Incorrect. The risk indicator records the final impact.
- C. Incorrect. The action indicator provides feedback on action.

D. Incorrect. The health indicator shows whether the action worked.

Question 34

(From the CRMA Study Guide, Domain III: Assurance Role of the Internal Auditor)

Solution: A

- A. Correct. As the owner of risk management, management is most responsible for providing assurances.
- B. Incorrect. External auditors typically do not provide assurance on risk management.
- C. Incorrect. The audit committee does not get involved in the day-to-day dealings of risk management.
- D. Incorrect. While the internal auditors provide assurance, they are not responsible for risk management.

Question 35

(From the CRMA Study Guide, Domain III: Assurance Role of the Internal Auditor)

Solution: A

- A. Correct. The internal auditors should provide assurance on the decision-making.
- B. Incorrect. Internal audit may not be able to provide assurance on the information used.
- C. Incorrect. Consulting with a regulator may not be possible. Also, deciding who to consult is a management decision.
- D. Incorrect. The internal auditors may not be able to assess whether the criteria were used.

Question 36

(From the CRMA Study Guide, Domain III: Assurance Role of the Internal Auditor)

Solution: A

- A. Correct. Management is responsible for mitigating risk.

- B. Incorrect. The internal auditors may report on risk to the audit committee.
- C. Incorrect. The internal auditors may identify risk for audit or consulting purposes.
- D. Incorrect. The internal auditors should monitor risk for purposes of identifying their internal audit plan.

Question 37

(From the CRMA Study Guide, Domain III: Assurance Role of the Internal Auditor)

Solution: A

- A. Correct. In a fully mature ERM environment, management has the capability to identify the risk universe.
- B. Incorrect. The internal auditors identify the risk universe in earlier stages of ERM maturity.
- C. Incorrect. In a fully mature ERM environment, management identifies the risk universe and the internal auditors use that universe.
- D. Incorrect. The board typically does not have enough involvement in day-to-day operations to identify the universe.

Question 38

(From COSO's ERM Framework)

Solution: D

- A. Incorrect. This is reactive and there are better responses.
- B. Incorrect. Although many organizations use this, D is more proactive.
- C. Incorrect. This does not address the damage to the organization's reputation.
- D. Correct. This provides early warning and promotes timely action.

Question 39

(From IIA Practice Guide, Assessing Risk Management Using ISO 31000)

Solution: C

- A. Incorrect. C provides the most relevant and useful evidence.
- B. Incorrect. C provides the most relevant and useful evidence.

- C. Correct. Interviews with individuals directly involved in risk management activities could produce the most relevant and useful information.
- D. Incorrect. These results may no longer be relevant or useful.

Question 40

(From IIA Practice Guide, Assessing Risk Management Using ISO 31000)

Solution: A

- A. Correct. Ongoing observation could provide “real time” assurance. It also could “shut down” discussions in some risk cultures.
- B. Incorrect. Best practices literature will not provide relevant and useful information on the transparency and inclusiveness of the organization’s risk counsel discussions.
- C. Incorrect. Although C is a good technique, it is not as valuable as A in providing the most relevant and useful information on the transparency and inclusiveness of the organization’s risk counsel discussions.
- D. Incorrect. These results may no longer be relevant or useful.

Question 41

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: C

- A. Incorrect. Management should be notified first.
- B. Incorrect. The internal auditors should not determine risk treatment.
- C. Correct. The internal auditors should notify management and provide advice.
- D. Incorrect. Identifying a risk would not by itself necessitate an audit.

Question 42

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: C

- A. Incorrect. Management support and approval should be obtained.
- B. Incorrect. The CAE should not permanently be responsible so as not to impair objectivity.
- C. Correct. This would be auditing one’s own work, which impairs objectivity

- and is not in accordance with IIA *Standards*.
- D. Incorrect. Management should make risk decisions.

Question 43

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: B

- A. Incorrect. The internal auditors may provide advice, but management should make the determination.
- B. Correct. If it is a consulting role, the internal auditors should challenge management criteria with risk appetite.
- C. Incorrect. Management should align its decisions with risk tolerance.
- D. Incorrect. Management should communicate risk criteria.

Question 44

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: B

- A. Incorrect. This is a safeguard.
- B. Correct. Internal auditors should not make risk decisions.
- C. Incorrect. This is a safeguard.
- D. Incorrect. This is a safeguard.

Question 45

(From *Enterprise Risk Management* [Sobel and Reding, 2012])

Solution: D

- A. Incorrect. The internal auditors may provide their advice as long as management makes the decision.
- B. Incorrect. The internal auditors should not make the decision.
- C. Incorrect. An audit may not be necessary to obtain information.
- D. Correct. If it is a consulting engagement, the internal audit function may perform research and analysis.

Question 46

(From the CRMA Study Guide, Domain IV: Consulting Role of the

Internal Auditor)

Solution: B

- A. Incorrect. The internal audit function should decline consulting engagements for which it lacks the required experience.
- B. Correct. A consulting engagement should be declined if the internal audit function lacks the required experience.
- C. Incorrect. A consulting engagement should be declined if internal audit lacks the required experience.
- D. Incorrect. Management should decide whether to hire an external consultant.

Question 47

(From the CRMA Study Guide, Domain IV: Consulting Role of the Internal Auditor)

Solution: A

- A. Incorrect. The CAE should not accept the engagement because he/she held responsibility for the function less than 12 months ago.
- B. Correct. The CAE should not accept the engagement because he/she held responsibility for the function less than 12 months ago.
- C. Incorrect. The CAE should not accept the engagement because he/she held responsibility for the function less than 12 months ago.
- D. Incorrect. The CAE should not provide advice, even off the record, because he/she held responsibility for the function less than 12 months ago.

Question 48

(From Sarens et al., *Combined Assurance: Case Studies on a Holistic Approach to Organizational Governance*, IIA Research Foundation, 2012)

Solution: C

- A. Incorrect. This is one of the major benefits of the combined assurance approach.
- B. Incorrect. This is one of the major benefits of the combined assurance approach.
- C. Correct. Implementation of combined assurance is not likely to reduce fees

- for the external financial audit.
- D. Incorrect. This is one of the major benefits of the combined assurance approach.

Question 49

(From the CRMA Study Guide, Domain IV: Consulting Role of the Internal Auditor)

Solution: C

- A. Incorrect. Re-performance of work for each provider is not practical, and in cases where technical expertise is required, it is not possible. It would only be done in selective cases.
- B. Incorrect. Assessment of competency alone is not sufficient.
- C. Correct. Consideration of 1, 3, and 4 are necessary, in addition to the assurance provider's impact in terms of getting results.
- D. Incorrect. Re-performance of work for each provider is not practical, and in cases where technical expertise is required, it is not possible.

Question 50

(From IIA Position Paper, The Role of Internal Auditing in Enterprise-wide Risk Management; Standard 2600; and the Code of Ethics [Integrity])

Solution: C

- A. Incorrect. This is primarily because the internal auditors are responsible for reviewing the management of key risks.
- B. Incorrect. This is primarily because the internal auditors are responsible for reviewing the management of key risks.
- C. Correct. Collectively the risks could result in a “train wreck.” The response conforms to mandatory guidance.
- D. Incorrect. C is a better response.

APPENDIX C

CRMA Exam Syllabus

NOTE: Exam topics and/or format are subject to change as approved by The IIA's Professional Certification Board (PCB).

The CRMA exam includes two sections: Part 1 of the Certified Internal Auditor (CIA) exam and a separate CRMA exam, which consists of 100 multiple-choice questions covering four domains. The CRMA exam requires a completion time of two hours. Candidates can take the exams in any order; however, they must complete both the CIA Part 1 and the CRMA exam before the certification is granted.

All content covered in the four domains of the CRMA exam will be tested at the proficiency level (P). This means that candidates must exhibit proficiency (thorough understanding and the ability to apply concepts) in these topic areas.

Standards Tested On the CRMA Exam

- CIA exam Part 1 topics tested include aspects of The IIA's International Professional Practices Framework (IPPF), responsibilities of the internal audit activity, independence and objectivity, governance concepts, risk identification and management, management controls, and audit planning.
- The CRMA exam topics tested include governance aspects and principles of risk management assurance in addition to appropriate assurance and consulting roles for internal audit professionals.

CRMA Exam Domains

The CRMA exam core content is divided among four domains according to the following percentages:

Domain I: Organizational Governance Related to Risk Management (25–30%)

Domain II: Principles of Risk Management Processes (25–30%)

Domain III: Assurance Role of the Internal Auditor (IA) (20–25%)

Domain IV: Consulting Role of the Internal Auditor (IA) (20–25%)

See below for a more detailed breakdown of the contents of each domain.

Domain I: Organizational Governance Related to Risk Management (25–30%)

I.A Assess Risk Management Processes in the Context of Alignment with Strategic Imperatives

I.A.1 Objectives of Risk Management Processes I.A.2 Organization's Risk Culture

I.A.3 Risk Capacity, Appetite, and Tolerance of Organization

I.B Assess the Processes Related to the Elements of the Internal Environment in Which Organizations Seek to Manage Risks and Achieve Objectives

I.B.1 Integrity, Ethical Values, and Other Soft Controls

I.B.2 Role, Authority, Responsibility, etc., for Risk Management

I.B.3 Management's Philosophy and Operating Style

I.B.4 Legal/Organizational Structure

I.B.5 Documentation of Governance-related Decision-making

I.B.6 Capabilities, in Terms of People and Other Resources (e.g., Capital, Time, Processes, Systems, and Technologies)

I.B.7 Management of Third-party Business Relationships I.B.8 Needs and Expectations of Key Internal Stakeholders I.B.9 Internal Policies

I.C Assess the Processes Related to the Elements of the External Environment in Which Organizations Seek to Manage Risks and Achieve Objectives

- I.C.1 Key External Factors (Drivers and Trends) That May Impact the Objectives of the Organization I.C.2 Needs and Expectations of Key External Stakeholders (e.g., Involved, Interested, Influenced)

Domain II: Principles of Risk Management Processes (25–30%)

II.A Benchmark Risk Management Processes Using Authoritative Guidance

II.B Evaluate Risk Management Processes

- II.B.1 Setting Objectives at All Levels to Achieve Strategic Initiatives
II.B.2 Identifying Risks
II.B.3 Risk Analysis and Evaluation, Including Correlation, Interdependencies, and Prioritization
II.B.4 Risk Response (e.g., Avoid, Transfer, Mitigate, Accept), Including Cost/Benefit Analysis
II.B.5 Developing and Implementing Risk Mitigation Plans
II.B.6 Monitoring Risk Mitigation Plans and Emerging Risks
II.B.7 Reporting Risk Management Processes and Risks, Including Risk Mitigation Plans and Emerging Risks
II.B.8 Periodic Review of Risk Management Processes to Aid in Continuous Improvement

Domain III: Assurance Role of the Internal Auditor (IA) (20–25%)

III.A Review the Management of Key Risks

III.B Evaluate the Reporting of key Risks

III.C Provide Assurance that Risks Are Adequately Evaluated

III.D Provide Assurance on Risk Management Processes

Domain IV: Consulting Role of the Internal Auditor (IA) (20–25%)

IV.A Facilitate Identification and Evaluation of Risks

IV.B Coach Management in Responding to Risks

IV.C Coordinate Risk Management Activities

IV.D Consolidate Reporting on Risks

IV.E Maintain and Develop the Risk Management Framework

IV.F Advocate for the Establishment of Risk Management

IV.G Develop Risk Management Strategy for Board Approval

Exam Nondisclosure

The CRMA exam is a nondisclosed examination, which means that current exam questions and answers will not be published or divulged.

CRMA® Exam Administration Information

Note: This document reflects CRMA examination information as of date of publication. Visit The IIA's website for current information at (<https://global.theiia.org/certification/crma-certification/pages/crma-certification.aspx>).

The CRMA is designed for internal auditors and risk management professionals with responsibility for and experience in providing risk assurance, governance processes, quality assurance, or control self-assessment (CSA). It

demonstrates an individual's ability to evaluate the dynamic components that comprise an organization's governance and enterprise risk management program and provide advice and assurance around these issues.

**Candidates from the Following Countries Must Contact Their Local
IIA Institute for More Information about Local Certification
Processes**

Argentina	Germany	New Zealand
Australia	Greece	Norway
Austria	Indonesia	Philippines
Belgium	Italy	Singapore
Brazil	Japan	South Africa
Bulgaria	Korea	Spain
China	Malaysia	Sweden
Chinese Taiwan	Mexico	Switzerland
Czech Republic	Morocco	Thailand
France	Netherlands	Turkey

The information presented in this book regarding CRMA pertains only to those countries that are not listed above.

Computer-based Testing

The CRMA exam will begin registration May 1, 2013, and testing will begin July 1, 2013, in English only. Before scheduling an exam, you must apply and register in The IIA's Certification Candidate Management System (CCMS) (<https://i7lp.integral7.com/durango/do/login?ownername=iiia&channel=iiia&>

basechannel=integral7).

The CRMA exam is available through computer-based testing, allowing you to test year-round at more than 500 locations worldwide. Candidates are able to sit for exams at any IIA-authorized Pearson VUE testing center worldwide, regardless of whether the testing center is located in your hometown or country. To locate the testing centers nearest you, visit the Pearson VUE website (<http://pearsonvue.com/ia/>).

Eligibility Requirements

By applying to become a candidate in the CRMA program, an individual agrees to accept the conditions of the program. These include eligibility requirements, exam confidentiality, Code of Ethics, Continuing Professional Education (CPE), and any other conditions enacted by The IIA's Professional Certification Board (PCB).

CRMA candidates must meet the following eligibility requirements:

CIA Part 1

The candidate must have successfully completed the requirements and passed Part 1 of the CIA exam. This can be done before, during, or after completion of the CRMA exam, but must be completed before the certification is appointed. Candidates should review the requirements for the CIA exam Part 1 at (<https://global.theiia.org/certification/CIA-Certification/Pages/Exam-Syllabus-Part-1.aspx>).

Education

The candidate must have a post-secondary (four-year) or equivalent degree from an accredited college or university. A two-year degree plus three years of general business experience may be substituted. For further details, please refer to The IIA Certification Candidate Handbook (<https://global.theiia.org/certification/cia-certification/pages/eligibility-requirements.aspx>).

Character Reference

The candidate must exhibit high moral and professional character and submit a completed Character Reference Form signed by a CIA, CCSA, CFSAs, CRMA, or the candidate's supervisor. This one-page form is included in The IIA Certification Candidate Handbook (<https://global.theiia.org/certification/cia-certification/pages/eligibility-requirements.aspx>).

Work Experience

The candidate must acquire two years of auditing experience or controls-related business experience such as risk management, quality assurance, or CSA. A completed Experience Verification Form is required. Candidates may apply to the program and sit for the exam before satisfying the professional experience requirement but will not be certified until all program requirements have been met. This one-page form is included in The IIA Certification Candidate Handbook (<https://global.theiia.org/certification/cia-certification/pages/eligibility-requirements.aspx>).

Eligibility Period

Effective November 2010, the certification program's eligibility requires candidates to complete the program certification process within four years of application approval. If a candidate has not completed the certification process within four years, all fees and exam parts will be forfeited.

Confidentiality

The CRMA certification exam is a nondisclosed exam. Candidates agree to keep the contents of the CRMA exam confidential and therefore may not discuss the specific exam contents with anyone except The IIA's Certification Department. Unauthorized disclosure of exam material will be considered a breach of the Code of Ethics and could result in disqualification of the candidate or other appropriate censure.

Code of Ethics

CRMA candidates agree to abide by the Code of Ethics established by The IIA.

Continuing Professional Education

Upon certification, CRMAs are required to maintain their knowledge and skills and stay abreast of improvements and current developments by satisfying CPE requirements.

IIA Membership

In most cases, you do not have to be a member of The IIA to take the CRMA exam or become a CRMA, but we encourage you to consider its advantages. There are some countries, however, that do require candidates to be IIA members to take the CRMA exam. See the section above with the heading “Countries with Additional CRMA Certification Requirements” for more details.

IIA members receive discounts on CRMA review materials and courses and have access to the latest exam preparation resources, networking opportunities, and current CRMA news and information.

APPENDIX D

References

INTRODUCTION

1. Kaplan, Robert, and Anette Mikes. 2012. Managing Risks: A New Framework. *Harvard Business Review*.

DOMAIN I

ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

1. AS/NZS. 1999. *Risk management 4360:1999*. Standards Association of Australia. Available at http://www.schleupen.de/content/schleupen/schleupen013223/A.4.1.4_Australia_ (retrieved February 13, 2013).
2. AIRMIC, Alarm, IRM. 2002. *A Risk Management Standard*. Available at http://www.theirm.org/publications/documents/Risk_Management_Standard_030 (retrieved February 8, 2013).
3. AIRMIC, Alarm, IRM. 2010. *A Structured Approach to Enterprise Risk Management (ERM)*. Available at <http://theirm.org/ISO31000guide.htm> (retrieved February 8, 2013).
4. The Institute of Risk Management – IRM publications, including 2002 Risk Standard. Available at <http://www.theirm.org/publications/PUpublications.html>.
5. ISACA. Certified in Risk and Information Systems Control (CRISC). Available at www.ISACA.org and <http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx>.
6. Barfield, R. 2013. Risk Appetite – How hungry are you?

PricewaterhouseCoopers. Available at http://www.pwc.com/en_GX/gx/banking-capital-markets/pdf/risk_appetite.pdf (retrieved February 7, 2013).

7. Boddy, D. 2011. *Management: An Introduction*, 5th Edition. London: Prentice Hall Europe.

8. Carroll, A. B., and A. K. Buchholtz. 2008. *Business and Society: Ethics and Stakeholder Management*. Andover: Cengage Learning.

9. Centre for Ethical Leadership. 2013. *Ethical Leadership*. Available at <http://ethicalleadership.org/about-us/philosophies-definitions/ethical-leadership> (retrieved February 3, 2013).

10. COSO. 2004. *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

11. Department for Business Innovation and Skills. 2013. *Corporate Governance*. Available at <http://www.berr.gov.uk/whatwedo/businesslaw/corp-governance/page15267.html> (retrieved February 16, 2013).

12. Drummond, G., J. Ensor, and R. Ashford. 2001. *Strategic Marketing: Planning and Control*. Oxford: Butterworth-Heinemann.

13. Farrell, Michael, and Angela Hoon. 2009. What's your company's risk culture? Published online by *Business Week* at www.business.com (retrieved February 5, 2013).

14. Hatch, M. J. 2006. *Organization Theory*, 2nd Edition. Oxford: Oxford University Press.

15. Henry, A. 2007. *Understanding Strategic Management*. Oxford: Open University Press.

16. Hooley, G. H., J. A. Saunders, and N. F. Piercy. 1998. *Marketing Strategy and Competitive Positioning*, 2nd Edition. Harlow: Prentice Hall.

17. Institute of Business Ethics. 2013. What is business ethics? Available at www.IBE.org.uk (retrieved February 3, 2013).

18. IIA. 2005. *An Approach to Implementing Risk Based Internal Auditing*. London: Chartered Institute of Internal Auditors.
19. IIA. 2009. *Risk Management Processes – the Fundamentals*. London: Chartered Institute of Internal Auditors.
20. IIA. 2012. International Professional Practices Framework. The Institute of Internal Auditors.
21. IIA. 2013. Position Paper, The Three Lines of Defense in Effective Risk Management and Control. The Institute of Internal Auditors.
22. IOD. 2012. *Business Risk: A Practical Guide for Board Members*. Director Publications Ltd.
23. IRM. 2012. *Risk Culture: Under the Microscope Guidance for Boards*. The Institute of Risk Management. Available at www.irm.co.uk (retrieved February 5, 2013).
24. ISO 31000:2009. *Risk management – Principles and guidelines*.
25. Jensen, Michael C., and William H. Meckling. 1976. Theory of the Firm, Managerial Behavior, Agency Costs, and Ownership Structure. *Journal of Financial Economics* 3: 305–360.
26. Nicholson, Francis, and Daphne Turner. 2010. *Strategic Management*. London: Chartered Institute of Internal Auditors.
27. Peale, N. V., and K. Blanchard. 1988. *The Power of Ethical Management*. New York: William Morrow and Company.
28. Porter, M. 1980. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. New York: Free Press.
29. Porter, M. 1983. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: Free Press.
30. Schwartz, M. 2004. Effective Corporate Codes of Ethics: Perceptions of Code Users. *Journal of Business Ethics*, vol. 55, no. 4.

31. Turner, Daphne, and Francis Nicholson. 2012. *The Internal Audit Environment*. London: Chartered Institute of Internal Auditors.
32. VolResource. 2012. *Policies and Procedures Checklist*. Available at <http://www.volresource.org.uk/samples/checklst.htm> (retrieved February 10, 2013).
33. Walker, David. 2009. *A Review of Corporate Governance in UK Banks and Other Financial Industry Entities: Final Recommendations 26 November 2009*. Available at http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/d/walker_review_261109.pdf (retrieved February 9, 2013).

DOMAIN II **PRINCIPLES OF RISK MANAGEMENT PROCESSES**

1. 1st Secure IT. 2013. *Sarbanes Oxley Compliance*. Available online at www.1stsecureit.com (retrieved March 5, 2013).
2. AIRMIC, Alarm, IRM. 2002. *A Risk Management Standard*. Available online at
http://www.theirm.org/publications/documents/Risk_Management_Standard_030
3. AIRMIC, Alarm, IRM. 2010. *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*. Available at http://www.theirm.org/documents/SARM_FINAL.pdf.
4. AS/NZS. 1999. *Risk management 4360:1999*. Standards Association of Australia. Available at
http://www.schleupen.de/content/schleupen/schleupen013223/A.4.1.4_Australia_
5. Cheshire, John. 2010. *Risk Assurance and Audit Management*. London: Chartered Institute of Internal Auditors.
6. COSO. 2012. *Risk Assessment in Practice*. Committee of Sponsoring Organizations of the Treadway Commission.
7. de Flander, Jeroen. 2010. *Strategy Execution Heroes: Business Strategy Implementation and Strategic Management Demystified, a Practical*

Performance Management Guidebook for the Successful Leader. The Performance Factory.

8. Deloitte. 2005. *Risky business? Managing Risk and Creating Value in a Volatile World.* London: Deloitte Research.
9. Gall, John. 1978. *Systemantics; How Systems Work ... and Especially How They Fail.* New York: Pocket Books. Reviewed in *Why do systems fail and problems sprout anew?* www.laetusinpaesens.org (retrieved March 3, 2013).
10. IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors.
11. IIA. 2013. *International Standards for the Professional Practice of Internal Auditing.* The Institute of Internal Auditors.
12. IIA. 2013. Position Paper, The Three Lines of Defense in Effective Risk Management and Control. The Institute of Internal Auditors.
13. Leitch, Matthew. 2008. *Intelligent Internal Control and Risk Management.* Gower Publishing Company.
14. Nicholson, Francis, and Daphne Turner. 2010. *Strategic Management.* London: Chartered Institute of Internal Auditors.
15. Pickett, KH Spencer. 2005. *Auditing the Risk Management Process.* John Wiley & Sons Inc.
16. PMI. 2013. *A Guide to the Project Management Body of Knowledge (PMBOK Guide),* Fifth Edition. Project Management Institute.
17. PricewaterhouseCoopers. 2009. *Exploring Emerging Risks: Extending Enterprise Risk Management (ERM) to Address Emerging Risks.* Available online at <http://www.pwc.com/gx/en/research-publications/pdf/pwcglobalriskserm.pdf>.
18. Sadgrove, Kit. *The Complete Guide to Business Risk Management,* Second Edition. Gower Publishing Ltd.

19. Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation.
20. TBS. 2013. *Risk Management Guide*. Treasury Board Secretariat of Canada. Available online at <http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir01-eng.asp>.

DOMAIN III ASSURANCE ROLE OF THE INTERNAL AUDITOR

1. Adamec, B., L. Leinicke, J. Ostrosky, and W. Rexroad. 2005. Getting A Leg Up. *Internal Auditor*: 40–45.
2. Balanced Scorecard Institute. 2012. *What is the Balanced Scorecard?* Available at www.balancedscorecard.org (retrieved March 9, 2013).
3. Beasley, M., B. Branson, and B. Hancock. 2010. *Developing key risk indicators to strengthen enterprise risk management: how key risk indicators can sharpen focus on emerging risks*. Committee of Sponsoring Organizations of the Treadway Commission.
4. Cheshire, John. 2010. *Risk Assurance and Audit Management*. London: Chartered Institute of Internal Auditors.
5. Collins, Nina. 2012. *Internal Audit Practice*. London: Chartered Institute of Internal Auditors.
6. IIA. 2009a. Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures. The Institute of Internal Auditors.
7. IIA. 2009b. Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning. The Institute of Internal Auditors.
8. IIA. 2009c. Practice Guide, Formulating and Expressing Internal Audit Opinions. The Institute of Internal Auditors.
9. IIA. 2009d. Position Paper, The Role of Internal Auditing in Enterprise Risk

Management. The Institute of Internal Auditors.

10. IIA. 2009e. Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes. The Institute of Internal Auditors.

11. IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors.

12. IIA. 2012. International Professional Practices Framework. The Institute of Internal Auditors.

13. IIA and RIMS. 2012. *Risk Management and Internal Audit: Forging a Collaborative Alliance*. The Institute of Internal Auditors and the Risk and Insurance Management Society. Available online at
<https://na.theiia.org/standards-guidance/Public%20Documents/RIMS%20and%20The%20IIA%20Executive%20Framework.pdf> (retrieved March 7, 2013).

14. ISO 31000:2009. *Risk management – Principles and guidelines*.

15. ISO/IEC 15504. *Information technology – Process assessment*, Parts 1 to 9, 2004–2011.

16. Kaplan, R., and D. Norton. 1996. *The Balanced Scorecard – translating strategy into action*. Massachusetts: Harvard Business School.

17. Mainelli, M. 2007. Correlation causes questions: environmental consistency confidence in wholesale financial institutions. Included in Cox, D. (ed). 2007. *Frontiers of Risk Management: Key Issues and Solutions*. Euromoney Institutional Investor Plc.

18. Pickett, KH Spencer. 2005. *Auditing the risk management process*. John Wiley & Sons Inc.

19. Protiviti. 2010. *Board Risk Oversight: A Progress Report*, Committee of Sponsoring Organizations of the Treadway Commission. Available online at http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf.

20. Sobel, Paul J. 2011. *Internal Auditing's Role in Risk Management*. The Institute of Internal Auditors Research Foundation. Available online <http://www.theiia.org/bookstore/product/internal-auditings-role-in-risk-management-1561.cfm>.
21. Walker, P., W. Shenkir, and T. Barton. 2011. *Improving Board Risk Oversight through Best Practices*. The Institute of Internal Auditors Research Foundation.

DOMAIN IV CONSULTING ROLE OF THE INTERNAL AUDITOR

1. IIARF. 2012. *Sawyer's Guide for Internal Auditors*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.
2. ILM. 2013. What is coaching? Available on the Institute of Leadership and Management's website www.i-l-m.com (retrieved March 29, 2013).
3. Leitch, Matthew. 2004. Embedded Risk Management: The Auditors' Contribution. Available at www.irmi.com/expert/articles/2004/leitch04.aspx (retrieved April 1, 2013).
4. Maynard, Gregg R. 1999. Embracing Risk. *Internal Auditor*.
5. Pickett, KH Spencer. 2005. *Auditing the Risk Management Process*. John Wiley & Sons Inc.
6. Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation.

APPENDIX E

Suggested Reading

DOMAIN I

ORGANIZATIONAL GOVERNANCE RELATED TO RISK MANAGEMENT

AIRMIC, Alarm, IRM. 2010. *A Structured Approach to Enterprise Risk Management (ERM)*. Available at <http://theirm.org/ISO31000guide.htm> (retrieved February 8, 2013).

Centre for Ethical Leadership. 2013. *Ethical Leadership*. Available at <http://ethicalleadership.org/about-us/philosophies-definitions/ethical-leadership> (retrieved February 3, 2013).

COSO. 2004. *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

Institute of Business Ethics. 2013. What is business ethics? Available at www.IBE.org.uk (retrieved February 3, 2013).

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors.

IIA. 2013. Position Paper, The Three Lines of Defense in Effective Risk Management and Control. The Institute of Internal Auditors.

Sobel, Paul J. 2011. *Auditor's Risk Management Guide: Integrating Auditing and ERM*. CCH Inc.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Especially chapters 1 and 2.)

DOMAIN II

PRINCIPLES OF RISK MANAGEMENT PROCESSES

COSO. 2004. *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organization; of the Treadway Commission.

COSO. 2012. *Risk Assessment in Practice*. Committee of Sponsoring Organizations of the Treadway Commission.

ISO 31000:2009 Risk Management – Principles and Guidelines.

Deloitte. 2005. *Risky business? Managing Risk and Creating Value in a Volatile World*. London: Deloitte Research.

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors.

Leitch, Matthew. 2008. *Intelligent Internal Control and Risk Management*. Gower Publishing Company. (Especially chapters 2 and 3.)

PwC. 2009. *Exploring Emerging Risks: Extending Enterprise Risk Management (ERM) to Address Emerging Risks*. PricewaterhouseCoopers. Available online at <http://www.pwc.com/gx/en/research-publications/pdf/pwcglobalriskserm.pdf>.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Especially Section 2, chapters 3–8.)

Kaplan, Robert S., and Anette Mikes. 2012. Managing Risks: A New Framework. *Harvard Business Review*, Vol. 90 Issue 6: 48–60.

DOMAIN III

ASSURANCE ROLE OF THE INTERNAL AUDITOR

Beasley, M., B. Branson, and B. Hancock. 2010. *Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risks*. Committee of Sponsoring Organizations of the Treadway Commission.

IIA. 2009d. Position Paper, The Role of Internal Auditing in Enterprise Risk Management. The Institute of Internal Auditors. Available online at <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Audit> (retrieved March 7, 2013).

IIA. 2009e. Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes. The Institute of Internal Auditors.

IIA. 2011. Practice Guide, Reliance by Internal Audit on Other Assurance Providers. The Institute of Internal Auditors. Available online at <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Reliance-by-Internal-Audit-on-Other-Assurance-Providers-Practice%20Guide.aspx>.

IIA. 2010. Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. The Institute of Internal Auditors. Available online at <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Assessing-the-Adequacy-of-Risk-Management-Practice-Guide.aspx> (retrieved March 7, 2013).

IIA and RIMS. 2012. *Risk Management and Internal Audit: Forging a Collaborative Alliance*. The Institute of Internal Auditors and the Risk and Insurance Management Society. Available online at <https://na.theiia.org/standards-guidance/Public%20Documents/RIMS%20and%20The%20IIA%20Executive%20Report%20on%20Risk%20Management%20and%20Internal%20Auditing>

Protiviti. 2010. *Board Risk Oversight: A Progress Report*. Committee of Sponsoring Organizations of the Treadway Commission. Available online at http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf.

Sobel, Paul J., 2011. *Internal Auditing's Role in Risk Management*. The Institute of Internal Auditors Research Foundation. Available online at <http://www.theiia.org/bookstore/product/internal-auditing-s-role-in-risk-management-1561.cfm>.

Walker, P., W. Shenkir, and T. Barton. 2011. *Improving Board Risk Oversight*

Through Best Practices. The Institute of Internal Auditors Research Foundation. (Especially chapter 9.)

DOMAIN IV CONSULTING ROLE OF THE INTERNAL AUDITOR

IIA. 2009. Position Paper, The Role of Internal Auditing in Enterprise Risk Management. The Institute of Internal Auditors. Available online at <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditor> (retrieved March 7, 2013).

IIA. 2012. Standard 2050: Coordination. The Institute of Internal Auditors.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. The Institute of Internal Auditors Research Foundation. (Especially chapter 8, “Risk Management Reporting.”)

GLOSSARY

NOTE: Many of the definitions in this glossary are taken from the glossary in The IIA's International Professional Practices Framework, or have been modified as appropriate to conform to the discussions in this textbook.

Add Value

Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement, and/or reducing risk exposure through both assurance and consulting services.

Adequately Designed — See Controls Are Adequately Designed.

Advocate

Inspire others to change their understanding, attitude, or behavior by promoting a particular viewpoint or position.

Appropriate Evidence

Any piece or collection of evidence gained during an engagement that provides relevant and reliable support for the judgments and conclusions reached during the engagement.

Assurance Layering

A technique of coordinating multiple assurance activities designed to mitigate a known risk to a needed or desired level within an established risk tolerance.

Assurance Map

A visual depiction of the different assurance activities and assurance functions within an organization. Such a depiction can help identify gaps or overlaps in

assurance activities and help assess that risk is managed consistent with the board's and management's expectations.

Assurance Mapping

The process of coordinating and reviewing all assurance activities to identify and fill gaps and eliminate overlaps.

Assurance Services

An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Audit Engagement — See Assurance Services.

Audit Observation

Any identified and validated gap between the current and desired state arising from an assurance engagement.

Audit Opinion

Internal audit's statement of the effectiveness of internal controls based on an independent and objective evaluation.

Audit Risk

The risk of reaching invalid audit conclusions and/or providing faulty advice based on the audit work conducted.

Audit Scope

The agreed span of an audit as defined by the purpose, planned activities, objectives, risks, and controls under review as well as any areas expressly excluded.

Audit Universe

A compilation of the subsidiaries, business units, departments, groups, processes, or other established subdivisions of an organization that exist to manage one or more business risks.

Autocratic

A highly centralized style of management or decision-making with little or no consultation.

Benchmarking

Systematic comparison of actual activity or performance with given standards of excellence or best practice.

Big Data

A term used to refer to the large amount of constantly streaming digital information, massive increase in the capacity to store large amounts of data, and the amount of data processing power required to manage, interpret, and analyze the large volumes of digital information.

Board

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.

Bottom-up Approach

To begin by looking at all processes directly at the activity level, and then aggregating the identified processes across the organization.

Business Ethics

The moral principles and values used to inform organizational activities and decision-making.

Business Process

The set of connected activities linked with each other for the purpose of achieving one or more business objectives.

Business Process Outsourcing (BPO)

The act of transferring some of an organization's business processes to an outside provider to achieve cost reductions, operating effectiveness, or operating efficiency while improving service quality.

Capabilities

Activities an organization is equipped to undertake given its resources (including staff expertise, technical knowhow, patents, reputation, equipment, facilities, customer base, and capital).

Cause

The reason for the difference between the expected and actual conditions (why the difference exists).

Checklist (for Risk Identification)

A prepared set of common risks, usually classified under broad headings, used as a prompt or suggestions to help identify the actual risks that exist in a given activity or entity.

Chief Audit Executive

A senior position within the organization responsible for internal audit activities. When internal audit activities are obtained from external service providers, the chief audit executive is the person responsible for overseeing the service contract and the overall quality assurance of these activities, and follow-up of engagement results. The term also includes titles such as general auditor, head of internal audit, chief internal auditor, internal audit director, and inspector general.

Coaching

A process for helping others develop by enabling them to discover and grow.

Code of Ethics

The Code of Ethics of The Institute of Internal Auditors contains principles relevant to the profession and practice of internal auditing and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing. A code of ethics more generally is any set of guidelines designed to direct behavior.

Combined Assurance

Aligning various assurance activities within an organization to ensure assurance gaps do not exist and assurance activities minimize duplication and overlap but still manage risk consistent with the board's and management's expectations.

Compensating Control

An activity that, if key controls do not fully operate effectively, may help to reduce the related risk. Such controls also can back up or duplicate multiple controls and may operate across multiple processes and risks. A compensating control will not, by itself, reduce risk to an acceptable level.

Compliance

Conformity and adherence to applicable laws and regulations (COSO definition). May also include conformity and adherence to policies, plans, procedures, contracts, or other requirements.

Condition

The factual evidence that the internal auditor found in the course of the examination (what does exist).

Conflict of Interest

Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

Consolidate

Strengthen and make more substantial by drawing disparate strands together.

Consulting Services

Advisory and related services, the nature and scope of which are agreed to with the customer, are intended to improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Contingency plan

A provisional plan prepared in advance for the purposes of recovering the

situation if risks materialize or other things go wrong.

Continuous Auditing

Using computerized techniques to perpetually audit the processing of business transactions.

Control

Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. See also Internal Control and System of Internal Controls.

Control Environment

The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal controls. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

Control Risk

The potential that controls will fail to reduce controllable risk to an acceptable level.

Control Risk Self-assessment (CRSA)

A structured process for identifying and analyzing risks, usually within a given

framework, carried out by the risk owners, often with support from a facilitator.

Controllable Risk

The portion of inherent risk that management can reduce through day-to-day operations and management activities.

Controls Are Adequately Designed

Present if management has planned and organized (designed) the controls or the system of internal controls in a manner that provides reasonable assurance that the organization's entity-level and process-level risks can be managed to an acceptable level.

Controls Are Operating Effectively

Present if management has executed (operated) the controls or the system of internal controls in a manner that provides reasonable assurance that the organization's entity-level and process-level risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

Corruption

Acts in which individuals wrongfully use their influence in a business transaction to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another (for example, kickbacks, self-dealing, or conflicts of interest).

Criteria

The standards, measures, or expectations used in making an evaluation and/or verification of an observation (what should exist).

Customer

The subsidiary, business unit, department, group, individual, or other established subdivision of an organization that is the subject of a consulting engagement.

Data Analytics

A process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting

decision-making.

Database

A large repository of data, typically contained in many linked files, and stored in a manner that allows the data to be easily accessed, retrieved, and manipulated.

Delegation

The passing of authority to a subordinate for certain tasks or roles while retaining the ultimate responsibility for their undertaking.

Democratic

A style of management or decision-making that is highly decentralized and widely participative.

Detective Control

An activity that is designed to discover undesirable events that have already occurred. A detective control must occur on a timely basis (before the undesirable event has had a negative impact on the organization) to be considered effective.

Downside Risk — See Pure Risk.

Effect

The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the consequence of the difference).

Emerging Risk

A previously unknown risk that may not yet be fully understood that has arisen due to changes in the internal or external environments or changes to the organization's objectives and activities.

Engagement

A specific internal audit assignment or project that includes multiple tasks or activities designed to accomplish a specific set of objectives. See also Assurance Services and Consulting Services.

Engagement Work Program

A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

Enterprise Risk Management — See Risk Management.

Entity-level Control

A control that operates across an entire entity and, as such, is not bound by, or associated with, individual processes.

External Auditor — See Independent Outside Auditor.

Facilitate

To help make something happen.

Framework

A body of guiding principles that form a template against which organizations can evaluate a multitude of business practices. These principles are comprised of various concepts, values, assumptions, and practices intended to provide a yardstick against which an organization can assess or evaluate a particular structure, process, or environment or a group of practices or procedures.

Fraud

Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

Fraudulent Financial Reporting

Acts that involve falsification of an organization's financial statements (for example, overstating revenues or understating liabilities and expenses).

General Information Technology Controls

Controls that operate across all IT systems and are in place to ensure the integrity, reliability, and accuracy of the application systems. Also represents a specific example of an "entity-level control."

Governance

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

Groupthink

A tendency among groups to adopt a common position even where differences of opinion exist arising through peer pressure and an unwillingness to appear to be different or wrong.

Hard Controls

Controls that are effected by policies, processes, and structure.

Icebreaker

A group activity designed to familiarize individuals with each other and encourage greater collaboration.

Illegal Acts

Activities that violate laws and regulations of particular jurisdictions where an organization is operating.

Impairment to Independence or Objectivity

The introduction of threats that may result in a substantial limitation, or the appearance of a substantial limitation, to the internal auditor's ability to perform an engagement without bias or interference.

Independence

The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels. See also Organizational Independence.

Independent Outside Auditor

A registered public accounting firm, hired by the organization's board or executive management, to perform a financial statement audit providing assurance for which the firm issues a written attestation report that expresses an opinion about whether the financial statements are fairly presented in accordance

with applicable Generally Accepted Accounting Principles.

Individual Objectivity

An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires internal auditors not to subordinate their judgment on audit matters to that of others.

Information Technology Governance

The leadership, structure, and oversight processes that ensure the organization's IT supports the objectives and strategies of the organization.

Information Technology Operations

The department or area in an organization (people, processes, and equipment) that performs the function of running the computer systems and various devices that support the business objectives and activities.

Inherent Limitations of Internal Control

The confines that relate to the limits of human judgment, resource constraints and the need to consider the cost of controls in relation to expected benefits, the reality that breakdowns can occur, and the possibility of collusion or management override.

Inherent Risk

The combination of internal and external risk factors in their pure, uncontrolled state, or, the gross risk that exists, assuming there are no internal controls in place.

Insight

An end product or result from the internal audit function's assurance and consulting work designed to provide valued input or information to a client or customer. Examples include identifying entity-level root causes of control deficiencies, emerging risks, and suggestions to improve the organization's governance process.

Internal Audit Charter

A formal, written document that defines the internal audit function's purpose, authority, and responsibility. The charter should (a) establish the internal audit function's position within the organization, (b) authorize access to records, personnel, and physical properties relevant to the performance of engagements, and (c) define the scope of the internal audit function.

Internal Audit Function

A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations.

Internal Control

A process, effected 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.

Key Control

An activity designed to reduce risk associated with a critical business objective.

Key Performance Indicator

A metric or other form of measuring whether a process or individual tasks are operating within prescribed tolerances.

Key Principles Approach

This approach to providing risk management assurance compares what is present within the entity under review with a given set of principles (from ISO, COSO, or other similar source), thus identifying areas that confirm and others that require further improvement.

Key Risk

A significant risk on account of its ability to cause serious disruption to the

organization's objectives or core activities.

Key Risk Indicator (KRI)

A measure used to indicate that certain trigger events or conditions likely to precipitate a risk event have occurred or arisen.

Lag Indicator

A signal of something (such as a risk incident) that has already occurred.

Laissez-faire

A style of management characterized by a lack of intervention and a tendency to allow things to happen.

Lead Indicator

A signal that something (such as a risk incident) is likely to occur in the near future.

Limited Assurance — See Negative Assurance.

Material Observation

An individual observation, or a group of observations, is considered “material” if the control in question has a reasonable possibility of failing and the impact of its failure is not only significant, but also exceeds management’s materiality threshold.

Maturity Model

The principle underpinning the risk management maturity model is that over time, one would expect (and internal audit should encourage) a steady evolution in the maturity of risk management processes. Providing assurance on risk management processes on this basis involves identifying the current level of risk maturity and exploring with management the opportunities that exist for advancing maturity further.

Mission

Statement of an organization's purpose.

Monitoring

A process that assesses the presence and functioning of governance, risk management, and control over time.

Negative Assurance

Assurance based on the absence of any evidence to the contrary.

Network

A configuration that enables computers and devices to communicate and be linked together to efficiently process data and share information.

Objectives

What an entity desires to achieve. When referring to what an organization wants to achieve, these are called business objectives, and may be classified as strategic, operations, reporting, and compliance. When referring to what an audit wants to achieve, these are called audit objectives or engagement objectives.

Objectivity — See Individual Objectivity.

Observation

A finding, determination, or judgment derived from the internal auditor's test results from an assurance or consulting engagement.

Ongoing Assessments

Risk mitigation may be monitored routinely as part of the risk management processes themselves as a regular and systematic feedback in the cycle to check that actions are being taken as planned and controls are operating as expected. See also Separate Assessments.

Operating Effectively — See Controls Are Operating Effectively.

Operating System

Software programs that run the computer and perform basic tasks, such as recognizing input from the keyboard, sending output to the printer, keeping track of files and directories on the hard drive, and controlling various computer peripheral devices.

Operational Objective

A goal that is usually short- to mid-term (within a year or two) that is activity-focused and designed to enable the achievement of strategic objectives.

Opportunity

The possibility that an event will occur and positively affect the achievement of objectives.

Organizational Independence

The chief audit executive's line of reporting within the organization that allows the internal audit function to fulfill its responsibilities free from interference. See also Independence.

Oversight

High-level continuous monitoring.

Policy

A statement of the attitude and/or approach taken by an entity toward a given area of activity. **Positive Assurance**

Assurance based on a statement noting confirmed evidence of effective or ineffective controls.

Preventive Control

An activity that is designed to deter unintended events from occurring.

Private Sector

Those organizations and enterprises owned by private individuals, usually operated primarily for financial gain.

Procedure

The steps taken by an organization to undertake a given activity in accordance with its policy.

Probability-Proportional-to-Size (PPS) Sampling

A modified form of attribute sampling that is used to reach a conclusion regarding monetary amounts rather than rates of occurrence.

Process Elements Approach

This approach to providing assurance on risk management processes involves a validation of each of the key processes, looking for evidence that they are working according to expectation and that as a whole the risk management framework is effective.

Process-level Control

An activity that operates within a specific process for the purpose of achieving process-level objectives.

Professional Skepticism

The state of mind in which internal auditors take nothing for granted; they continuously question what they hear and see and critically assess audit evidence.

Psychology of Risk — See Risk Psychology.

Public Sector

Those organizations and enterprises undertaken by the state on behalf of the public to provide a service to targeted groups and individuals that is not readily available from other means.

Pure Risk

A risk that is wholly negative with the potential to damage or constrain objectives without the possibility of creating positive opportunity.

RAG Rating

A system of colored indicators (red, amber, and green like traffic lights) to signify criticality. Red is used when the most urgent attention is needed, amber when caution is required, and green when conditions are as expected.

Reasonable Assurance

A level of assurance that is supported by generally accepted auditing procedures and judgments. Reasonable assurance can apply to judgments surrounding the effectiveness of internal controls, the mitigation of risks, the achievement of objectives, or other engagement-related conclusions.

Residual Risk

The portion of inherent risk that remains after management executes its risk responses (sometimes referred to as net risk).

Risk

The possibility that an event will occur and impact objectives, whether positively or negatively.

Risk Appetite

The amount of risk, on a broad level, an organization is willing to accept in pursuit of its business objectives. Risk appetite takes into consideration the amount of risk that management consciously accepts after balancing the cost and benefits of implementing controls.

Risk Assessment

The identification and analysis (typically in terms of impact and likelihood) of relevant risks to the achievement of an organization's objectives, forming a basis for determining how the risks should be managed.

Risk Attitude

The aggregated risk appetite for an entity being the overall tendency to accept or avoid risk.

Risk Aware

A level of risk maturity where there is a scattered, silo-based approach to risk management across an entity.

Risk Capacity

The amount of risk an entity or activity is able to tolerate as a consequence of its capabilities.

Risk Capture

The ability to record and document a risk event when a risk materializes.

Risk Correlation

The association of two or more risks such that their likelihoods and impacts vary

together in a direct relationship, being an example of a particular kind of interdependency.

Risk Criteria

Factors that may be used to analyze risk, the most common being likelihood (or probability) and impact (consequence), with other criteria including volatility, velocity, and vulnerability.

Risk Culture

An organization's overall attitude and approach toward risk and risk management.

Risk-defined

A middle-tier level of risk maturity in which risk appetite is defined and where there are defined risk management policies and strategies in place.

Risk-enabled

The highest level of risk maturity where risk management processes and internal controls are enterprisewide and fully embedded.

Risk Escalation

The process of reporting a risk event upwards in the management structure for the purposes of sharing the information and authorizing remedial action (including the implementation of contingency plans).

Risk Event (or Risk Incident)

The occurrence or materialization of a risk.

Risk Identification

The process of finding, recognizing, and describing risks.

Risk Incident — See Risk Event.

Risk Interdependency

The relationships between two or more risks that, when combined, may precipitate a greater impact or additional consequences than when the risks arise on their own.

Risk Level (or Risk Severity)

The overall threshold of a risk, usually measured as the simple product of likelihood and impact, although organizations may choose to weight these factors and may take other factors such as vulnerability and velocity into account.

Risk Managed

A high level of risk maturity in which there is an enterprisewide approach that is well communicated.

Risk Management

The process conducted by management to understand and deal with uncertainties (that is, risks and opportunities) that could affect the organization's ability to achieve its objectives. More generally, risk management can refer to any efforts made to address risk within a given endeavor.

Risk Management Framework

The overall arrangements for addressing risk within an organization.

Risk Map

A graphical depiction of risks, usually based on the two axes of likelihood and impact.

Risk Maturity

The degree to which an organization, its culture, and/or its risk management processes are robust, where robustness is a function of how embedded risk management processes are within the organization, and the extent to which a consideration of risk impacts decision-making, planning, resource allocation, and other key activities.

Risk Mitigation

An action, or set of actions, taken by management to reduce the impact and/or likelihood of a risk to a lower, more acceptable level.

Risk Naive

A low level of risk maturity with very limited appreciation of the existence of risk in which risks are not addressed systematically.

Risk Prioritization

The ranking of risk according to severity to target attention and resources to the most significant risks.

Risk Profile

The overall picture of risk across a range of categories, showing the sum total exposures.

Risk Psychology

The subjective elements inherent in the identification and assessment of and attitude toward risk.

Risk Register

A structured record of all of the key risks within an organization or defined area of activity together with the analysis.

Risk Response

An action, or set of actions, taken by management to achieve a desired risk management strategy. Risk responses can be categorized as risk avoidance, reduction, sharing, or acceptance. Exploiting opportunities that, in turn, enable the achievement of objectives, is also a risk response. ISO 31000 refers to this step in risk management as risk treatment.

Risk Severity — See Risk Level.

Risk Tolerance

The acceptable levels of risk size and variation relative to the achievement of objectives, which must align with the organization's risk appetite. It is also described as being the acceptable variation from risk appetite, (i.e., by how much and for how long the entity can accept residual risk levels above appetite).

Risk Treatment — See Risk Response.

Risk Universe

The sum total of all the relevant risks impacting a given entity or organization.

Sampling Risk

The risk that the internal auditor's conclusion based on sample testing may be different than the conclusion reached if the audit procedure was applied to all items in the population.

Secondary Control

An activity designed to either reduce risk associated with business objectives that are not critical to the organization's survival or success or serve as a backup to a key control.

Scope — See Audit Scope.

Separate Assessments

Risk management mitigation may be monitored by separate assessments, which are those that are not part of risk management processes themselves but are initiated and administered as required to gain assurance on their effectiveness. See also Ongoing Assessments.

Significant Observation

An individual observation, or a group of observations, is considered "significant" if the control activity in question has a reasonable possibility of failing and the impact of its failure is significant.

Soft Controls

Controls that rely on the behavior and attitude of individuals.

Stakeholder

Individuals or parties with an interest (or stake) in a given project, enterprise, or organization.

Standard

A professional pronouncement promulgated by the International Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities and evaluating internal audit performance.

Strategic Objectives

What an entity desires to achieve through the value creation choices management makes on behalf of the organization's stakeholders.

Strategy

Refers to how management plans to achieve the organization's objectives.

Sufficient Evidence

A collection of evidence gained during an engagement that, in its totality, is enough to support the judgments and conclusions made in the engagement.

Sweet Spot

The optimal position used to refer to a number of different situations, including the optimal balance between risk and benefits.

System of Internal Controls

Comprises the five components of internal control: the control environment, risk assessment, control activities, information and communication, and monitoring that are in place to manage risks related to the financial reporting, compliance, and operational objectives of an organization. See also Internal Control.

Third-party Service Provider

A person or firm, outside the organization, that provides assurance and/or consulting services to an organization.

Three Lines of Defense

A model of assurance whereby management control is the first line of defense in risk management, the various risk, control, and compliance oversight functions established by management serve as the second line of defense, and independent assurance is the third line of defense.

Tone at the Top

The entitywide attitude of integrity and control consciousness, as exhibited by the most senior executives of an organization. See also Control Environment.

Top-down Approach

To begin at the entity level with the organization's objectives, and then identify the key processes critical to the success of each of the organization's objectives.

Transparency

Communicating in a manner that a prudent individual would consider to be fair and sufficiently clear and comprehensive to meet the needs of the recipient(s) of such communication.

Upside Risk

Risk with the potential for positive opportunity or gain.

Values

Statements of what an organization stands for and the moral principles that guide its activities, often included with its vision, mission, and strategic objectives as part of its strategic plan.

Vulnerability Assessment

The process of identifying and evaluating risks for a given venture or organization by examining the propensity for failure.

Walk-through

A method of testing controls by following the control processes in operation from start to finish.

Work Program — See Engagement Work Program.

CRMA

EXAM STUDY GUIDE
1st Edition

10841

EARN YOUR CRMA CERTIFICATION AND TAKE THE NEXT STEP IN YOUR CAREER

The *CRMA® Exam Study Guide*, 1st Edition, compiles the comprehensive review material you need to prepare for the Certification in Risk Management Assurance™ (CRMA®) exam. Crucial information is presented in this one-of-a-kind study guide for each of the four official exam domains:

- I: Organizational governance related to risk management
- II: Principles of risk management processes
- III: Assurance role of the internal auditor
- IV: Consulting role of the internal auditor

Written and reviewed by an international team of practitioners and academics, the study materials are designed for a global audience. Included are sample CRMA exam practice questions with suggested solutions, the exam syllabus, and a list of supplementary study materials.

With current information and trends, explanatory examples, and useful figures and tables, the *CRMA® Exam Study Guide* will not only serve as an aid to taking the exam but will also enhance your knowledge of risk management assurance for audit-related activity.

ABOUT THE AUTHORS

Francis Nicholson, CIA, CRMA, has served as the education director for the Chartered Institute of Internal Auditors for more than six years, responsible for membership and professional development services for both individuals and employers. His background is predominantly in education, having delivered, developed, and managed adult and professional training programs for colleges and universities. Nicholson's primary field is business studies, spanning accounting, finance, economics, and management studies. He works with practitioners, chief audit executives, and academics to ensure that the guidance, support, and resources provided raise the skills and status of the individual and the standards of professional practice.

Chris Baker, CMIIA, CRMA, has served as the technical manager for the Chartered Institute of Internal Auditors since 2007, promoting and developing the professional practice of internal auditing by building the body of knowledge available in the UK and Ireland. Since 2011, he has developed and coordinated the Institute's External Quality Assessment (EQA) service. Baker has more than 30 years of practical experience in governance, risk management, control, and internal auditing.



ISBN 978-0-89413-736-5



9 780894 137365