

RISK ASSESSMENT FOR MID-SIZED ORGANISATIONS

COSO tools for a tailored approach, second edition

Scott McKay, CPA

Notice to Readers

Risk assessment for midsized organisations: COSO tools for a tailored approach, second edition, does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the author and the publisher are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Portions of this book have been adapted with permission from The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

© 2013 AICPA. All rights reserved.

American Institute of Certified Public Accountants, Inc.

New York, NY 10036-8775

Distribution of this material via the Internet does not constitute consent to the redistribution of it in any form. No part of this material may be otherwise reproduced, stored in third party platforms and databases, or transmitted in any form or by any printed, electronic, mechanical, digital or other means without the written permission of the owner of the copyright as set forth above. For information about the procedure for requesting permission to reuse this content, please email copyright@CGMA.org.

The information, and any opinions expressed in this material, do not represent official pronouncements of or on behalf of AICPA, CIMA, the CGMA designation or the Association of International Certified Professional Accountants. This material is offered with the understanding that it does not constitute legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The information contained herein is provided to assist the reader in developing a general understanding of the topics discussed, but no attempt has been made to cover the subjects or issues exhaustively. While every attempt to verify the timeliness and accuracy of the information herein as of the date of issuance has been made, no guarantee is or can be given regarding the applicability of the information found within to any given set of facts and circumstances.

1 2 3 4 5 6 7 8 9 0 PIP 1 9 8 7 6 5 4 3

ISBN: 978-1-94023-508-0

Publisher: Linda Prentice Cohen
Acquisitions Editor: Robert Fox
Developmental Editor: Suzanne Morgen
Project Manager: Amy Sykes

ABOUT THE AUTHOR

Scott McKay has joined Cherry, Bekaert & Holland, LLP as partner and has been named practice leader for the firm's risk advisory services group. In this role, McKay will work with other specialists across the firm to provide risk advisory services in enterprise risk management (ERM), internal audit outsourcing, Sarbanes-Oxley preparation, internal control design and implementation, IT audit and assurance services, as well as certain corporate forensic and anti-fraud control services. Scott M. McKay was formerly employed with Cree, Inc., headquartered in Durham, North Carolina. He was the company's corporate controller and was previously the director of internal audit responsible for internal assurance, risk advisory and forensic accounting services. Additionally, Scott worked as an Audit Manager with McGladrey & Pullen LLP where he performed audit, assurance and risk advisory services for both public and private companies in a variety of industries.

Scott is a Certified Public Accountant (CPA) in California and North Carolina and maintains several other professional credentials. He is frequently requested to speak on a variety of risk management topics for the institutions and organisations, including

- North Carolina State University;
- the Institute of Internal Auditors;
- the Association of Certified Fraud Examiners;
- the Information Systems Audit and Control Association;
- the North Carolina Chapter of Certified Public Accountants;
- and the American Institute of Certified Public Accountants (AICPA), where he also serves as a member in business and industry for the AICPA's Risk Management and Internal Control Advisory Panel.

Scott holds an undergraduate degree in business administration from the University of La Verne in Los Angeles, California, and a Masters in Accountancy from San Diego State University.

PREFACE

Companies often struggle with the concepts of risk and especially enterprise risk management (ERM). Embedded at the heart of ERM is the risk assessment process. This short book is designed to demystify risk identification at the enterprise or entity level, as opposed to risk identification at the activity or process level (which is also discussed), and will aid the user in developing a tailored approach to the organisation's risk management requirements. The approach is flexible and describes how to develop a top-down risk based self-assessment to create your organisation's entity-level risk taxonomy and corresponding risk assessments.

This second edition expands on the first with the addition of two COSO thought papers. 'Embracing Enterprise Risk Management: Practical Approaches for Getting Started' serves as an introduction and practical guide for how to start implementing an enterprise risk management programme. The final chapter, 'Understanding and Communicating Risk Appetite', offers an in-depth examination of how to develop, communicate, and monitor your organisation's risk appetite. Establishing an appropriate risk appetite is fundamental to the continued success of any ERM programme.

The rest of the book presents useful tools and approaches to assist with the challenge of implementing your organisation's ERM programme. Completing an entity-wide risk assessment is an essential step toward formalising and embedding ERM into a business culture. Once your organisation establishes the initial entity-level risk library (which we freely admit is the hardest part of ERM and requires the most thought leadership) and completes the initial risk assessments, it becomes clearer which risk areas may be underserved or overcontrolled and require further attention. This sets the stage for subsequent risk assessments that identify root causes, processes already in place, detailed risk management strategies, control gaps, and risk owners.

The purpose of the entity-wide risk assessment and ERM approach is multifold:

- To create a common language to identify, evaluate, and manage risk
- To identify and assess risks to achieving organisational objectives
- To establish and agree on risk tolerances and risk appetite and verify that residual risk levels align with management's expectations
- To identify risk management responses, current gaps, and risk owners
- To ensure that resource allocation aligns with organisational objectives and risk levels
- To leverage cross-functional expertise to manage risk to within acceptable levels

The primary goal of this book is to bring clarity to two areas: risk identification (this is the most important section) and risk assessment within your organisation's approach to risk management. Ideally you should be able to set up and facilitate a meaningful entity-level risk assessment with executives and managers in your organisation. With practice and perhaps a little technology you should be able to facilitate and complete the entity-level risk assessment with a group of managers in one hour or so.

CONTENTS

INTRODUCTION: EMBRACING ENTERPRISE RISK MANAGEMENT: PRACTICAL APPROACHES FOR GETTING STARTED	1
Overview and the Question of 'Where to Start?'	1
Keys to Success	2
Theme 1. Support From the Top Is a Necessity	2
Theme 2. Build ERM Using Incremental Steps	3
Theme 3. Focus Initially on a Small Number of Top Risks	4
Theme 4. Leverage Existing Resources	5
Theme 5. Build on Existing Risk Management Activities	5
Theme 6. Embed ERM Into the Business Fabric of the Organisation	5
Theme 7. Provide Ongoing ERM Updates and Continuing Education for Directors and Senior Management	6
Initial Action Steps and Objectives	6
Step 1. Seek Board and Senior Management Leadership, Involvement and Oversight	8
Step 2. Select a Strong Leader to Drive the ERM Initiative	8
Step 3. Establish a Management Risk Committee or Working Group	9
Step 4. Conduct the Initial Enterprise-wide Risk Assessment and Develop an Action Plan	10
Step 5. Inventory the Existing Risk Management Practices	11
Step 6. Develop Your Initial Risk Reporting	13
Step 7. Develop the Next Phase of Action Plans and Ongoing Communications	14
Continuing ERM Implementation	15
Chapter Summary	16
Where to Start: Draft Action Plan for an ERM Initiative	16

1	COMPELLING REASONS FOR ENTERPRISE RISK MANAGEMENT	21
	The Evolution of the COSO Internal Control: Integrated Framework to the COSO ERM Framework	23
2	ENTITY-WIDE RISK ASSESSMENT	25
	Risk Tolerance	26
	Materiality	27
	Objective Setting	31
3	IDENTIFYING RISK: ENTITY-LEVEL VERSUS ACTIVITY-LEVEL	33
	Risk Assessment	38
	Probability	39
	Potential Impact	41
4	RISK MANAGEMENT	45
	Control Maturity	47
	Residual Risk	48
5	ACTIVITY-LEVEL RISK ASSESSMENT	51
	Understanding the Approach: Financial Reporting	51
	Workshop Prerequisites	52
	Risk Factor Rating System	53
	Risk Factor Scale	54
	Weighting of Risk Factors	54
	Activity-Level Risk Factor Rating Table Guidelines	57
	Activity-Level Inherent and Fraud Risks	59
6	UNDERSTANDING AND COMMUNICATING RISK APPETITE	61
	Enterprise Risk Management and Decision Making	62
	Develop Risk Appetite	62
	Communicate Risk Appetite	62

Monitor and Update Risk Appetite	62
Can it Be Done?	63
Overview	64
Risk Appetite Is an Integral Part of Enterprise Risk Management	64
Considerations Affecting Risk Appetite	64
Steps in Adopting Risk Appetite	66
Risk Appetite Statements	66
Characteristics of Effective Risk Appetite Statements	67
Reluctance to Embrace Risk Appetite	68
Risk Appetites Are Not All the Same	68
Examples of Risk Appetite Statements	69
Risk Appetite and Risk Tolerance	71
Linking Risk Appetite and Risk Tolerance	72
Examples of Risk Tolerance Statements	74
Developing Risk Appetite	75
Facilitated Discussions	75
Discussions Related to Objectives and Strategies	76
Development of Performance Models	78
Communicating Risk Appetite	78
Broad Risk Appetite Statement	79
Risks Related to Organisational Objectives	79
Categories of Risk	80
Risk Appetite Cascades Through the Organisation	81
Monitoring and Updating Risk Appetite	82
Creating a Culture	82

Roles	83
Summary of Risk Appetite Considerations	86
EPILOGUE	89
REFERENCES	91
APPENDIX A: KEY TERMS	93
APPENDIX B: SAMPLE RISK LIBRARY	95
APPENDIX C: SAMPLE HEAT MAPS	97
APPENDIX D: SAMPLE CONTROL MATURITY MODELS	103
APPENDIX E: SAMPLE COMPANY MODEL MAPPED TO ENTITY-WIDE RISK LIBRARY	107
APPENDIX F: EXAMPLES OF RISK ASSESSMENT REPORTING	115
APPENDIX G: SAMPLE OF A FINANCIAL REPORTING RISK LIBRARY (INHERENT AND FRAUD RISKS)	125

INTRODUCTION: EMBRACING ENTERPRISE RISK MANAGEMENT: PRACTICAL APPROACHES FOR GETTING STARTED

OVERVIEW AND THE QUESTION OF 'WHERE TO START?'

The increased interest in and importance of enterprise risk management is being driven by many powerful forces. Most importantly, it is driven by the need for companies to manage risks effectively in order to sustain operations and achieve their business objectives. Other forces also come into play, including rating agency reviews, government regulations, expanded proxy disclosures and calls by shareholders and governance reform proponents for improving the way risks are managed by organisations.

Any entity that is currently operational has some form of risk management activities in place. However, these risk management activities are often ad hoc, informal and uncoordinated. And, they are often focused on operational or compliance-related risks and fail to focus systematically on strategic and emerging risks, which are most likely to affect an organisation's success. As a result, they fall short of constituting a complete, robust risk management process as defined by COSO (see the definition of ERM in box 1-1).

In addition, existing risk management activities often lack transparency. Transparency about how enterprise-wide risks are managed is increasingly being sought by directors and senior management, as well as various external parties seeking to understand an organisation's risk management activities. What's more, existing risk management processes often are not providing boards and senior management with an enterprise-wide view of risks, especially, emerging risks. Unfortunately, many organisational leaders are struggling with how to begin in their efforts to obtain strategic benefit from a more robust enterprise-wide approach to risk management.

Box 1-1: COSO Definition of Enterprise Risk Management

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

COSO's Enterprise Risk Management—Integrated Framework (2004)

This leads to the question 'Where do we start?' Answering this question can be a major challenge for organisations in which the perceived complexity of ERM and a lack of understanding of its strategic benefits may be barriers. At the same time, organisational pressures to reduce costs may prompt some decision makers

to look at risk management as something that can be deferred or viewed as a lower priority, thereby setting the stage for unmanaged risk exposures that could seriously threaten the viability of the organisation.

This introduction describes how an organisation can start to move from informal risk management to ERM. We discuss the increasing importance of and focus on ERM and the need for all types of organisations to understand and embrace ERM. And, we examine perceived barriers to starting ERM and working through those barriers.

The approaches described in this introduction are based on successful practices that organisations have used to develop an incremental, step-by-step methodology to start ERM. While this is not the only way to start an ERM initiative, this incremental approach is designed to be very adaptable and flexible. In the next three sections, we suggest specific, tangible actions that organisations can use to get started. The first section, 'Keys to Success', discusses overarching themes to provide management with a strong foundation for an effective ERM programme as they develop and tailor their specific approach to implementing ERM. The next section, 'Initial Action Steps and Objectives', lays out action-oriented 'how-to' steps to implement an initial ERM effort. These steps support development and implementation of a tailored ERM initiative. Finally, 'Continuing ERM implementation' talks about next steps to further develop and broaden the organisation's initial ERM effort.

KEYS TO SUCCESS

While specific action steps may vary, there are some consistent underlying themes that have proved valuable in successful ERM initiatives. These seven themes represent 'Keys to Success' for organisations that are now starting ERM initiatives and provide a useful foundation for specific actions detailed in the next section. These keys also help directors and management teams address some of the recognised barriers and resistance points to ERM adoption.

Theme 1. Support From the Top Is a Necessity

To successfully manage risk, an ERM initiative must be enterprise wide and viewed as an important and strategic effort. In the aftermath of the financial crisis of 2008, there has been a growing emphasis on the board's responsibilities for overseeing an organisation's risk management activities. For example, the corporate governance rules of the New York Stock Exchange require audit committees of listed corporations to discuss the risk assessment and risk management policies of their organisations. More recently, the US Securities and Exchange Commission (SEC) expanded proxy disclosures pertaining to the extent of the board's role in risk oversight. Moreover, credit rating agencies, such as Standard and Poor's (S&P) are also inquiring about enterprise risk management practices as part of their credit rating assessment processes.

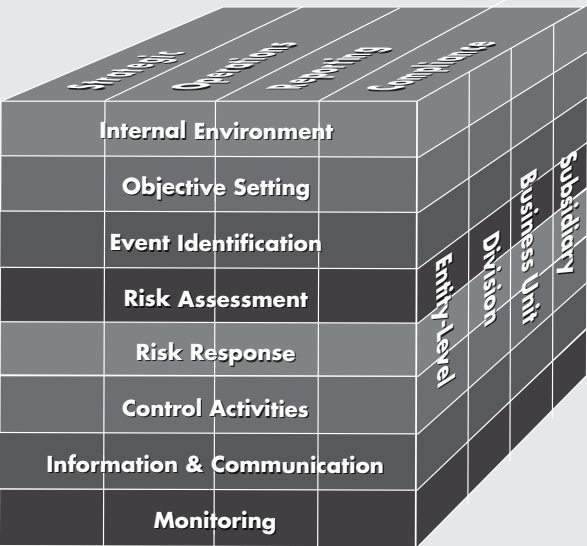
Support from the board of directors and senior management is needed to get the right focus, resources, and attention for ERM. Although it is not the job of the directors to manage the ERM activities, directors do need to demonstrate clear support for the ERM initiative as well as oversee what management has designed and implemented to manage top risk exposures. Thus, ERM must be enterprise wide, understood and embraced by its personnel, and driven from the top down through clear and consistent communication and messaging from the board and senior management. It is the board's responsibility to ensure that management is devoting the right attention and resources to ERM and is setting the right tone for ERM. What's more, the board should be comfortable that management has put in place an effective ERM leader who is widely respected across

the organisation and who has accepted responsibility for overall ERM leadership, resources, and support to accomplish the effort.

Top level support for ERM from the board and senior management is also important for establishing the desired ‘internal environment’ to foster ERM success (as described in Exhibit 1-1, the internal environment is one of the eight components of COSO’s ERM framework). This enterprise wide component is fundamental to setting the foundation for ERM and embedding it across the organisation. It also sets the stage for further development of other COSO ERM framework components including the establishment of the tone or the ‘risk culture’ of the organisation. S&P and other rating agencies have identified ‘risk culture’ as a key element of ERM and have stressed its importance in their releases.

Exhibit 1-1: COSO’s ERM Framework

The ERM framework consists of eight interrelated components. These components are derived from the way management runs a business and are integrated with the management process.



For more detailed information on enterprise risk management, the COSO ERM framework, and related practices and activities, see the following COSO publications, available through the COSO website at [COSO.org/guidance](https://www.coso.org/guidance):

- Enterprise Risk Management—Integrated Framework*
- Effective Enterprise Risk Oversight: The Role of the Board of Directors*
- Strengthening Enterprise Risk Management for Strategic Advantage*

Theme 2. Build ERM Using Incremental Steps

One perceived barrier to launching ERM is the perception that ERM is over complex and requires a major and costly effort to implement. Related to this perception is the belief that an organisation must implement all

of the components of ERM in one single effort for it to work and bring any tangible value to the organisation. Experience suggests otherwise.

In practice, some organisations, especially smaller organisations, have achieved ERM successes by taking an incremental, step-by-step approach to enhancing their risk management capabilities to provide a more enterprise-wide view over time rather than undertaking one massive launch effort. They start with a simple process and build from there using incremental steps rather than trying to make a quantum leap to fully implement a complete ERM process. By doing so, they are able to accomplish the following:

- **Identify and implement key practices to achieve immediate, tangible results.** For example, they may start by completing and sharing with their board for the first time a short list of enterprise-wide risks with certain action steps to address the risks identified. This initial step would be followed by a more detailed risk assessment delving deeper into other risks the organisation faces.
- **Provide an opportunity to change and further tailor ERM processes.** As the organisation and its executives and directors expand their knowledge of ERM, they have the opportunity to make additional requests to broaden or deepen the organisation's risk management activities.
- **Facilitate the identification and evaluation of benefits at each step.** This can be an effective way to respond to another possible barrier, which is evidenced in the question 'What value do we derive from ERM?' Here are two examples to illustrate this point:

EXAMPLE INCREMENTAL ACTION STEP	BENEFIT RECEIVED
Perform a risk assessment and prepare a short list of the organisation's most significant risks.	Board and senior management see and discuss, often for the first time, a consensus view of the organisation's most significant risks and how they are managed. This builds a common understanding and focus around these risks.
Identify opportunities to enhance risk management activities related to the significant risks identified.	Specific actions are identified to enhance the risk management activities on each significant risk. This results in a better understanding of the organisation's practices and how to enhance those practices and enables the identification of specific tangible benefits related to each action.

Theme 3. Focus Initially on a Small Number of Top Risks

For an organisation just starting out with ERM, it might make sense to first identify a small number of critical risks that can be managed, and then evolve from this starting point. For some organisations, such an approach might mean keeping the initial ERM focus on only those strategic risks that are deemed critical to the organisation achieving its strategic business objectives. Focusing initially on a smaller, manageable number of key risks would also be beneficial in developing related processes such as monitoring and reporting for those specific risks. This focused approach also keeps the developing ERM processes simple and lends itself to subsequent incremental steps to expand the risk universe and ERM processes.

Another way to keep ERM manageable is to focus initially on a few top risks in just one critical business unit. This limited focus could be used to develop initial risk management processes that can be expanded across the

enterprise to other business units. And when dealing with much smaller organisations, it can be useful to start things off by identifying just one critical risk or risk category and building ERM processes around that one risk.

Whichever specific risk approach is utilised, the critical success factor is to focus attention on a manageable number of key risks and then apply the lessons learned to identifying and managing additional critical risks across the enterprise.

Theme 4. Leverage Existing Resources

Another possible barrier to initiating an ERM process may be the view that significant resources including investments or outside expertise are needed to undertake an ERM project. For example, some directors or senior executives might think that they would need to hire an experienced chief risk officer or make significant investments in new technologies or automated tools. Such a viewpoint could prove to be a significant barrier to smaller organisations, in particular, which might have a strong desire to move ahead with ERM but have limited resources for making it happen.

Many organisations have successfully entered the ERM arena by leveraging their existing risk management resources. Organisations often discover that they have the personnel on their existing staffs, with the knowledge and capabilities relating to risks and risk management that can be effectively used to start. For example, some organisations have used their chief audit executive or their chief financial officer as the catalyst to begin an ERM initiative. In other instances, organisations have appointed a management committee, sometimes headed by their chief financial officer, to bring together a wide array of personnel from across the entity who collectively have sufficient knowledge of the organisation's core business model and related risks and risk management practices to get ERM moving. In addition, most organisations start their ERM effort without any specific enabling technology or automated tools other than basic spread sheets and word-processing capabilities.

Theme 5. Build on Existing Risk Management Activities

Any organisation with current operations has some form of risk management activities or risk related activities already in place. These might include activities such as risk assessments performed by the internal audit, insurance or compliance functions, fraud prevention or detection measures, or certain credit or treasury activities. By leveraging, aligning and subsequently enhancing these existing risk related activities, the organisation can achieve immediate and tangible benefits. For example, a company might implement a common set of risk definitions or a common risk framework across the organisation. Others have conformed their risk assessment methodologies so that all areas of the organisation performing a risk assessment do so using the same methodology.

Although it makes sense to build upon existing risk related activities, it must be done with the recognition that the existing activities probably do not constitute ERM. ERM requires risk management processes that ultimately are applied across the enterprise and represent an entity-wide portfolio view of risk, which is often missing from these existing functions.

Theme 6. Embed ERM Into the Business Fabric of the Organisation

As articulated in COSO's ERM definition in box 1-1, enterprise risk management is a process that is applied across the organisation. It is a management process, ultimately owned by the chief executive officer and involves people at every level of the organisation. The comprehensive nature of the ERM process and its pervasiveness across the organisation and its people provides the basis for its effectiveness.

ERM cannot be viewed or implemented as a stand-alone staff function or unit outside of the organisation's core business processes. In some companies and industries, such as large banks, it is common to see a dedicated enterprise risk management unit to support the overall ERM effort including establishing ERM policies and practices for their business units. However, because ERM is a process, organisations may or may not decide that they need dedicated, stand-alone support for their ERM activities.

Whether a risk management unit exists or not, a key to success is linking or embedding the ERM process into its core business processes and structures of the organisation. Some organisations, for example, have expanded their strategic plans and budgeting processes to include the identification and discussion of the risks related to their plans and budgets.

Theme 7. Provide Ongoing ERM Updates and Continuing Education for Directors and Senior Management

ERM practices, processes, and information continue to evolve. Thus, it is important for directors and senior executives to ensure that they are receiving appropriate updates, new releases, and continuing education on ERM, including information about regulatory requirements and best practices. This information provides the opportunity for directors and senior management to update their risk management processes as they become aware of new or developing practices. This ongoing improvement process is particularly important with the increased focus on ERM by regulators, rating agencies, and the SEC.

INITIAL ACTION STEPS AND OBJECTIVES

Building off the 'Keys to Success', this section details an initial action plan and steps to support development of a tailored ERM initiative. The plan reflects some simple, basic steps for implementing ERM, including the key step of performing an initial risk assessment. At the end of this chapter we include an example action plan, 'Where to Start: Draft Action Plan for an ERM Initiative', which can be further adapted for use by organisations. And in box 1-2 we have included responses to some common questions related to ERM that directors and senior management should find useful.

Box 1-2: Frequently Asked ERM Questions

• Do I need to appoint a chief risk officer?

No, COSO has observed that many organisations have started ERM using existing staff and appointing one of their key, senior-level personnel as the leader of the initiative. For example, some organisations have used their chief audit executive or their chief financial officer to begin the process. Regardless of title, the person selected to lead the ERM initiative must have the stature, authority and senior management leadership skills to be a true leader for ERM. Some organisations then develop their ERM processes to a point that they believe a dedicated chief risk officer is needed. However, organisations don't have to create a chief risk officer position in order to get started, nor does a more mature ERM process necessarily require a dedicated chief risk officer.

- **Do I need to form a functional ERM unit?**

No, many organisations have started ERM using management committees, working groups or existing personnel. Working groups or committees can take the lead in developing the organisation's initial approach to ERM or to conduct an initial risk assessment as part of their existing duties. For smaller organisations, in particular, a separate risk management unit may not be necessary. Again, ERM as defined by COSO is a process not a functional unit. Whether a functional risk unit is needed ultimately depends on the complexity of the organisation and the breadth and depth of its ERM processes.

- **What's wrong with just continuing my current, informal risk activities? Don't they constitute ERM?**

While you want to leverage existing, informal risk management activities, these activities often lack both transparency and an enterprise-wide view or application. Accordingly, they are unable to address risk in a portfolio manner, including aggregation of risk. In addition, existing, informal risk activities are more likely to be performed on an ad hoc basis and done separately; therefore, these informal risk activities lack the consistency of approach and communications required by ERM processes. Thus, an organisation's current, informal risk processes probably do not constitute true ERM. Increasingly, boards and other stakeholders, including rating agencies and regulators, are looking for ERM processes that are transparent, systematic, and repeatable and that produce an enterprise-wide view.

- **What role does the board play in ERM?**

The board is ultimately responsible for overseeing the ERM process, which is typically driven by management. The board's oversight responsibilities often involve using various board committees to oversee risks related to their areas of responsibility. In the end, effective engagement, involvement, and communications with the board are critical to ERM success. More specific guidance for boards is contained in the COSO thought paper, *Effective Enterprise Risk Oversight: The Role of the Board of Directors*.

- **Do I have to implement the complete COSO ERM framework to conduct ERM activities?**

COSO's *Enterprise Risk Management—Integrated Framework* notes that an entity may find it useful to discuss sub-sets of one or more of its objective categories to facilitate communications on a narrower topic. This approach can help an entity build its understanding of ERM and risk components on a step by step or incremental basis, staying within the context of the COSO ERM framework. As noted in an earlier section, many organisations are taking a step-by-step approach to ERM to facilitate building their understanding and experience with components of ERM. While this 'starting small' approach to ERM adoption has significant merit, care must be taken to maintain momentum.

If an organisation loses momentum and implements only a few initial ERM steps, it will fall short of having an adequate ERM process. See exhibit 1-1 for additional information about the COSO ERM framework.

Continued on p.8

Continued from p.7

• Do I need to use quantitative models and metrics in starting ERM?

The use of quantitative models and metrics may ultimately be useful in a more robust ERM environment, but they are not needed to launch an ERM effort. What's more, some types of risks—strategic or emerging risks, for example—may not lend themselves to quantification at all.

Many organisations start their ERM process by simply listing or identifying what management and the board believe to be their top risks and then reviewing how those risks are managed and monitored. Depending on the size and complexity of the organisation, quantitative modelling may, in the long run, prove helpful and even necessary to address certain types of risks, such as some financial and market risks. However, the quantification of all risks is not a goal. Management and the board need to first develop a solid understanding of ERM processes, approaches and tools and then ensure that the organisation's risk processes and tools are appropriate for the nature and scope of their specific risks and risk profile.

Step 1. Seek Board and Senior Management Leadership, Involvement, and Oversight

The board of directors and senior management set the tone for the organisation's risk culture. Their involvement, leadership, and oversight are essential for the success of any ERM effort.

A recent COSO thought paper, *Effective Enterprise Risk Management: The Role of the Board of Directors*, notes the following:

An entity's board of directors plays a critical role in overseeing an enterprise-wide approach to risk management. Because management is accountable to the board of directors, the board's focus on effective oversight is critical to setting the tone and culture towards effective risk management through strategy setting, formulating high level objectives, and approving broad-based resource allocations.¹

The board and senior management should agree on their initial objectives regarding ERM, its benefits and their expectations for successful ERM. At a high level, there should be clear agreement and alignment of the board's and senior management's expectations, timing and expected results. This should include agreement on the resources to be made available and targets dates for the effort. The board should also consider the timing and level of status reporting that will be required to effectively monitor and oversee the ERM effort.

This is also an appropriate time to lay the groundwork for the organisation's risk culture including how to best communicate a desire for more effective risk management. This initial communication may be focused at senior level executives to emphasise the importance of the initial ERM effort and the critical nature of these activities. Subsequent communications can be directed at describing the ERM effort in more general terms for a broader audience across the organisation.

Step 2. Select a Strong Leader to Drive the ERM Initiative

Finding a leader to head the initial ERM project is also critical for success. Management should identify a leader with the right attributes (see box 1-3 below) to head the ERM effort. This person does not need to be a chief risk

officer. Often, it is best to initially use existing resources, for example the chief audit executive or chief financial officer, for this role to get ERM started. This leader will not necessarily be the person to head ERM long term, but the person to get the initiative started and to take responsibility for moving the organisation's ERM activities to the next level.

It is critical that the risk leader have sufficient stature and be at an appropriate senior management level in the organisation to have a rich strategic perspective of the organisation and its risks and to be viewed as a peer by other members of senior management. Embedding ERM into the business fabric of the organisation is necessary. Having a risk leader who can be viewed as a peer by members of senior management is vital for the success of the ERM initiative.

Box 1-3: Attributes of Effective Leaders of Enterprise Risk Management

- Broad knowledge of the business and its core strategies
- Strong relationships with directors and executive management
- Strong communication and facilitation skills
- Knowledge of the organisation's risks
- Broad acceptance and credibility across the organisation

Step 3. Establish a Management Risk Committee or Working Group

To provide strong backing for its ERM effort, an organisation should consider creating a senior-level risk management committee or working group as the vehicle through which the designated risk leader can implement the ERM initiative.

While the use of a committee or working group in addition to the risk leader is optional, these committees have been used by risk leaders as an effective means to engage the right people across the organisation to ensure success of their ERM efforts.

Ideally, such committees or working groups would include 'C-suite' level executives as well as key business unit leaders to ensure that the organisation's ERM efforts are firmly embedded within the organisation's core business activities. Engaging senior executives at this level also ensures ERM receives appropriate attention and support and it can be very useful in building and communicating the risk culture across the organisation. And it provides top executives with the opportunity to share their insights about the types of risks that could impede the organisation's ability to achieve its business objectives, which will be important information during the initial risk assessment.

Typically, the organisation's ERM leader, as described previously in step 2, would head this committee and use it as a principle forum for implementation of ERM. Alternatively, an organisation could create a committee and use the committee solely for the purpose of implementing ERM. With this approach, a risk leader or chief risk officer could then be named at a later point as the organisation matures its ERM processes and decides it needs a dedicated leader.

Step 4. Conduct the Initial Enterprise-wide Risk Assessment and Develop an Action Plan

In many ways, this step is the heart of the initial ERM process. The focus here is to gain an understanding of and agreement on the organisation's top risks and how they are managed. The assessment is a top-down look at the risks that could potentially be most significant to the organisation and its ability to achieve its business objectives. While any organisation faces many risks, the starting point is to get a manageable list of what are collectively seen as the most significant risks. Here, members of the risk committee or working group can be most helpful by sharing their views or identifying people in the organisation who should be involved in the risk assessment.

While there is no one best way to conduct a risk assessment, many organisations start by obtaining a top-down view of the most important risk exposures from key executives across the organisation. This is typically accomplished by starting with a discussion of the organisation's business strategy and its components and then identifying the principal risks that would impede its ability to achieve its strategic objectives. An alternative is to discuss the strategies and risks of each of its major business units. To aid in these discussions, some organisations prepare a list of major risk categories, such as operational, financial, legal, market and then discuss exposures to that risk category for the business overall or each significant business unit.

It is often simplest and most effective for an organisation to conduct this initial, top-down risk assessment with a handful of key business-unit leaders and members of the C-suite. More individuals across and further within the organisation can be added later as the risk assessment process matures. This data gathering could be accomplished through interviews, surveys, facilitated discussion groups, or committee meetings. (See box 1-4 for some examples of questions to consider for this initial risk assessment.)

Box 1-4: Risk Assessment Questions

Outlined below are some sample questions that could be used in an interview with a senior executive or director during the risk assessment process. These questions are representative of the types of questions that could be asked to help identify the organisation's most significant strategic or emerging risks.

- What are your primary business objectives or strategies?
- What are the key components of enabling your business strategy or objectives?
- What internal factors or events could impede or derail each of these key components?
- What events external to the organisation could impede or derail each of the key components?
- What are the three most significant risk events that concern you regarding the organisation's ability to achieve business objectives?
- Where should the organisation enhance its risk management processes to have maximum benefit and impact on its ability to achieve business objectives?
- What types of catastrophic risks does the organisation face? How prepared is the organisation to handle them, if they occur?

- Can you identify any significant risks or exposures to third-parties (vendors, service providers, alliance partners, and the like) that concern you?
- What financial market risks do you believe are or will be significant?
- What current or developing legal, regulatory, and governmental events or risks might be significant to the success of the business?
- Are you concerned about any emerging risks or events? If so, what are they?
- What risks are competitors identifying in their regulatory reports that we have not been addressing in our risk analysis?

The organisation should then consider prioritising or ranking the risks identified. This step could be accomplished by a simple ranking of the perceived level of inherent risk or by a more detailed assessment of the probability and impact of each risk. Consider using a basic scale of high, medium and low for each inherent risk as a starting point rather than quantification or modelling. Again, during this initial assessment, many organisations find good discussion and simple classifications helpful.

As a result of some of the large and unexpected risks that have manifested themselves lately, some organisations are now expanding their impact and probability assessments to include other factors. Examples of these new factors include assessing the velocity of a risk or the level of preparedness of the organisation for that risk. For an example of an expanded risk assessment, see the Strategic Risk Profile following step 6.

Whatever specific approach is taken, the information gathered should be compiled into an initial list with a manageable number of risks or potential risk events. As the organisation matures its ERM processes, it can probe into finer levels of detail on other risks or, with enhanced knowledge of risk management activities, evolve its risk assessment from inherent risks to residual risks. Keep in mind, however, that focusing on too much detail or too many risks in the early stages of ERM adoption can impede progress on the broader ERM effort.

The organisation also needs to assess its risk responses related to identified risks and develop action plans to address any gaps that are beyond those acceptable. Typically, action plans stemming from the initial risk assessment would identify gaps in the existing risk management processes related to the risks identified and detail specific ways to address those gaps.

The initial risk assessment exercise is also a time to initiate discussions about the organisation's risk appetite relative to the risks identified. Some executives find it difficult to articulate, much less discuss, their organisation's risk appetite. To overcome this challenge, consider focusing initially on qualitative or narrative descriptions of the risk appetite, (for example, the organisation may have zero tolerance for anything related to customer or employee safety). Management can facilitate the discussion of the risk appetite by identifying types of activities or products that they will or will not undertake because of the perceived risks. Alternatively, they may discuss how risk aggressive or conservative they want to be compared to their peers or competitors.

Step 5. Inventory the Existing Risk Management Practices

During the risk assessment process, the organisation should also be taking an inventory of its current risk management practices to determine areas of strength to build upon and areas of weakness to address. This inventory becomes valuable information for management to assist in enhancing the risk management processes.

First, it enables the organisation to identify gaps in its current risk management processes relative to its most important and significant risks as they are identified. Oftentimes risk management activities are focused on existing operations and compliance risks, as opposed to significant external, emerging or strategic risks. As new risks are identified in the risk assessment process, the knowledge gained from a comprehensive inventory of existing risk management activities will help the organisation assess the connections between existing risk management processes and the most critical enterprise level risks so that management can determine if there are any gaps in how they are managing the most important risks. Further, it assists the organisation in mapping risks to underlying objectives.

Second, the inventory forms a baseline for the organisation as it continues to develop and enhance its ERM processes. It helps management demonstrate progress and the benefits of ERM by serving as a point of comparison as the processes mature.

A risk management alignment guide, such as the example depicted in box 1-5, can help facilitate compiling and documenting a high level inventory of the organisation's risk management activities. The guide can be developed in two steps. First, management would list the top risks in the risk category column, which would be identified during its initial risk assessment as described previously. Next, management would ensure that they have pinpointed an owner of the risk, articulated some form of risk appetite relevant to that risk and have considered what existing processes, if any, are in place to monitor the risk over time.

The last three columns would include information about any needed actions required to strengthen risk oversight and pinpoint management and board oversight related to the risk. In practice, organisations have found the completion of the risk owner column to be a useful exercise to ensure that they have a risk owner identified and acknowledged for each major risk. The risk management alignment guide, once completed, also serves as a concise and useful way to communicate the organisation's overall risk management practices at a high level for the board and senior management.

Box 1-5: Sample Risk Management Alignment Guide

RISK CATEGORY	RISK OWNER(S)	RISK APPETITE METRICS	MONITORING	ACTION PLANS	COMPANY OVERSIGHT	BOARD OVERSIGHT
REPUTATION RISK	CEO	Policy including specific metrics approved xx/xx/xx	Corporate Communications	Approved & Updated xx/xx/xx	Executive Committee	Full Board
OPERATIONS RISK	COO	Daily operations metrics in place in all operating divisions	Operations Management daily monitoring and reporting	Plans in place for each trigger point	Risk Management Internal Audit	Risk Committee

RISK CATEGORY	RISK OWNER(S)	RISK APPETITE METRICS	MONITORING	ACTION PLANS	COMPANY OVERSIGHT	BOARD OVERSIGHT
INFORMATION TECHNOLOGY RISK	CTO	Policies including daily performance metrics in place for security, back-up, and recovery	Daily monitoring against established performance standards	Contingency and back-up plans in place and periodically tested	Operating Committee Internal Audit	Audit Committee Full Board
RISK 4						






Step 6. Develop Your Initial Risk Reporting

The organisation next needs to develop its initial approach to risk reporting including its communication processes, target audiences and reporting formats. Organisations should start by keeping things simple, clear, and concise. Make it a point, however, that regardless of what specific reporting format employed, the reporting must reflect clearly the relative importance or significance of each risk. To this end, many organisations use simple lists, with their top risks listed in rank order. Others use colours or graphics along with their ranking to help focus attention on the most significant of the risks being reported. Also consider what status reporting and tracking you need to monitor progress on your action plans in order to address gaps in risk processes or risk responses identified during the ERM implementation.

The following sample strategic risk profile (box 1-6) includes three major strategic risk categories in the rows of the table (operations, reputation and information technology) and four possible risk factors in the columns of the table (likelihood, impact, velocity and readiness). The strategic risks are then listed in order of their overall priority and the red, yellow and green readiness symbols help readers easily prioritize risks (red being highest priority or most critical).

This example of a Strategic Risk Profile in box 1-6 is presented for illustrative purposes only. Organisations should test various risk-reporting formats, approaches and risk factors in addition to talking with directors and executives about the level of detail needed and formats they find most useful.

Box 1-6: Example Strategic Risk Profile

STRATEGIC RISK	DESCRIPTION OF RISK	LIKELIHOOD	IMPACT	VELOCITY	READINESS	PRIORITY
OPERATIONS RISK	Supply Chain Disruptions; Product Liability Events	Low	High	High		1
REPUTATION RISK	Damage to reputation caused by company actions and/or partner actions	Medium	High	High		2
INFORMATION TECHNOLOGY RISK	Liability to achieve objectives because of failures of enabling technology	Medium	High	High		3
RISK 4						4
RISK 5						5

Step 7. Develop the Next Phase of Action Plans and Ongoing Communications

The implementation of ERM is an evolutionary process that takes time to develop. In the spirit of continual improvement, once the initial ERM action plan has been completed, the working group or risk leader should conduct a critical assessment of the accomplishments to date and develop a series of action plans for the next stage of implementation. Following the incremental approach, the leader should identify next steps in the ERM roll-out that will foster additional enhancements and afford tangible benefits as a result.

The completion of the initial ERM action plan is also an opportune time for the risk leader and the ERM working group to convey the status and benefits achieved to the board of directors and senior management. The risk leader should also consider what types of ongoing education offerings and communications should be deployed across the organisation to continue to strengthen the organisation's risk culture and ERM capabilities.

CONTINUING ERM IMPLEMENTATION

The intent of this chapter is to provide a simple illustration of ways to launch ERM. It represents a beginning, not an end point. An organisation following this incremental approach to achieving ERM benefits will have taken a significant first step toward ERM and have a much better understanding of where it is headed and what needs to be accomplished next.

To lay the groundwork for ERM success, an organisation should first establish its initial ERM process as an ongoing and important element that will assist in achieving business objectives. Given the evolutionary nature of ERM and the dynamic nature of risk, the ERM process must be ongoing and not viewed as a one-time event. The initial risk assessment process will need periodic updating and the organisation will need to be attuned to the need to identify new and emerging risks. A solid foundation for risk management should be established and nurtured. Ongoing communications from directors and senior management will serve to reinforce and nurture the risk management culture.

Once ERM is off the ground, the organisation can look for additional ways to expand the implementation of ERM across the organisation. It should also be aware that, though tangible risk processes may have been implemented during this initial phase of ERM deployment, the processes may likely fall short of a complete ERM process and need to be enhanced. Accordingly, the organisation's risk management leaders need to continue to drive further development and maturity of the risk management processes. They need to pursue levels of risk management maturity that reflect the components of COSO's ERM framework.

As the organisation considers next steps, it should also evaluate the need for further developing and broadening the organisation's risk culture and practices. Here is a working list of activities to consider that will strengthen an organisation's risk culture and practices:

- A programme of continuing ERM education for directors and executives
- ERM education and training for business-unit management
- Policies and action plans to embed ERM processes into the organisation's functional units such as procurement, IT, or supply chain units
- Continuing communications across the organisation on risk and risk management processes and expectations
- Development and communication of a risk management philosophy for the organisation
- Identification of targeted benefits to be achieved by the next step of ERM deployment
- Development of board and corporate policies and practices for ERM
- Further discussion and articulation of a risk appetite for the organisation or significant business units, including quantification
- Establishment of clear linkage between strategic planning and risk management
- Integration of risk management processes into an organisation's annual planning and budgeting processes
- Expansion of the risk assessment process to include assessments of both inherent and residual levels of risk
- Exploration of the need for a dedicated chief risk officer or ERM functional unit

The specific next steps to be taken should be implemented by continuing the incremental approach, taking small, tangible steps rather than attempting to implement the complete ERM framework. The primary objective is to keep the momentum moving and to continue to evolve, expand, and deepen the organisation's ERM capabilities.

CHAPTER SUMMARY

Boards of directors and senior management need to challenge critically their organisations' risk management practices and take the opportunity to enhance their processes and improve their ability to meet their organisations' objectives.

The concepts, techniques and tools outlined here, coupled with COSO's *Enterprise Risk Management—Integrated Framework* and other COSO thought papers, are intended to provide a strong foundation and effective starting point for pursuit of ERM benefits. Collectively, these resources provide a robust source of information and knowledge of ERM practices and processes.

The ideas and recommendations presented in this introduction are neither intended to be, nor are they, the only way to enter the ERM arena. Ultimately, every organisation must develop its own approach to ERM, one that best suits its particular culture and circumstances.

Above all, keep in mind the benefits of taking small, incremental steps on the path toward full ERM rather than attempting to implement the complete ERM framework all at once. The goal is to keep the momentum for ERM that will continue to expand and deepen the organisation's ERM capabilities on a continual basis.

WHERE TO START: DRAFT ACTION PLAN FOR AN ERM INITIATIVE

Outlined here is an initial high-level draft of an action plan for ERM. This draft plan highlights key events and actions that organisations should consider in starting an ERM initiative. The draft is not intended to be viewed as a complete plan; furthermore, it requires careful tailoring and expansion prior to use. However, we believe it reflects useful information and is a practical draft plan as a basis to start.

1. Seek Board and Senior Management Involvement and Oversight

- a. Set an agenda item for the board and executive management to discuss ERM and its benefits
- b. Agree on high-level objectives and expectations regarding risk management
- c. Understand the process to communicate and set the tone and expectations of ERM for the organisation
- d. Agree on a high-level approach, resources, and target dates for the initial ERM effort

2. Identify and position a leader to drive the ERM Initiative

- a. Identify a person with the right attributes to serve as the risk management leader
 - i. Does not have to be a chief risk officer
 - ii. Use existing resources

- b.* Set objectives and expectations for the leader
- c.* Allocate appropriate resources to enable success

3. Establish a Management Working Group

- a.* Establish a management working group to support the risk leader and drive the effort across the organisation
- b.* Have the right key people in the group
 - i.* Sufficient stature
 - ii.* 'C-suite' representation
 - iii.* Business unit management
- c.* Look at using cross-functional teams
- d.* Agree on objectives for the working group
 - i.* Build ERM using incremental steps
 - ii.* Define some sought-after benefit to evaluate each step
 - iii.* Establish reporting process for management and the board

4. Conduct an Initial Enterprise-wide Risk Assessment and Action Plan

- a.* Focus on identifying the organisation's most significant risks
- b.* Look for risks at the strategic level
- c.* Consider risk factors beyond just probability and impact, for example
 - i.* Velocity of risk
 - ii.* Preparedness
 - iii.* Other factors
- d.* For the most significant risks
 - i.* Assess exposure to the risk
 - ii.* Assess adequacy of existing risk mitigation or monitoring
 - iii.* Identify opportunities to enhance mitigation or monitoring activities
- e.* Develop action plans to enhance risk management practices related to the risk identified
 - i.* Identify actions to implement the opportunities previously identified
 - ii.* Establish target dates and responsibilities
 - iii.* Develop process to monitor and track implementation

5. Inventory the Existing Risk Management Practices

- a.* Identify and inventory existing practices
- b.* Identify gaps and opportunities
 - i.* Consider initial completion of the risk management alignment guide

- c.* Develop specific action steps to close gaps
- d.* Produce and implement action plans to close gaps and manage risks

6. Develop Initial Risk Reporting

- a.* Assess adequacy and effectiveness of existing risk reporting
- b.* Develop new reporting formats
 - i. Consider extensive use of graphics and colours
 - ii. Consider developing a risk 'dashboard' for the board
- c.* Develop process for periodic reporting of emerging risks
- d.* Assess effectiveness of new reporting with stakeholders and revise as appropriate

7. Develop the Next Phase of Action Plans and Ongoing Communications

- a.* Conduct a critical assessment of the accomplishments of the working group
- b.* Revisit the risk process inventory and identify next processes for enhancement
- c.* Identify tangible steps for a new action plan including benefits sought and target dates
 - i. Review with executive management and the board
- d.* Implement with appropriate resources and support
- e.* Schedule sessions for updating or further educating directors and executive management
- f.* Assess progress and benefits of ERM initiative against objectives and communicate to target audiences
- g.* Continue organisation-wide communication process to build risk culture

Endnotes

- 1 Download COSO's thought paper *Effective Enterprise Risk Management: The Role of Board of Directors* from COSO's website (www.coso.org).

1

COMPELLING REASONS FOR ENTERPRISE RISK MANAGEMENT

Now that you have seen that implementing risk management processes can be easily achieved through the seven steps outlined in the introduction, let's examine the current regulatory climate and how it allows public companies to easily leverage their existing COSO framework into a successful ERM programme.

Though President Bush signed the Sarbanes-Oxley Act into law in 2002 in response to numerous financial and accounting frauds such as those at Enron and WorldCom, there is no explicit regulatory requirement to implement a comprehensive system of risk management. The Sarbanes-Oxley Act required large publicly traded companies (above a certain market capitalisation) to adopt an internal control framework, conduct risk assessments and tests of controls for reliable financial reporting, and disclose the results of the risk assessments of internal control over financial reporting in their public filings with the Securities and Exchange Commission (SEC). Yet, the scope of this legislation is narrow in that it focuses on risks associated with financial reporting and not on the much broader topic of enterprise risk.

In response to this legislation, most public companies adopted the COSO Internal Control—Integrated Framework¹ and spent millions upon millions of dollars to implement and report on their respective systems of internal control to the SEC. Unfortunately, many companies treated Sarbanes-Oxley as a compliance requirement instead of an opportunity to strengthen risk management over this facet of their enterprise risk portfolio.

Since that time, other public, private, non-profit, and governmental organisations have embarked on implementing more robust systems of internal control over financial reporting, either as a direct response to boards of directors and those charged with oversight or in anticipation of further regulation.

Hence, when business leaders hear *COSO* or *enterprise risk management* or *ERM*, they tend to think, 'Is this just an expensive compliance exercise?' and 'Why does my company need this?' We think these are very fair questions that deserve thoughtful responses.

Risk management and control maturity are often driven by regulatory compliance. However, being reactive to regulation provides the wrong motive to manage risk and leads to overcontrol; because people don't 'buy into' the effort, it's not sustainable. Long-term success is predicated on behavioural change. Time spent helping people clearly see the risk to achieving objectives leads to better-designed controls, management buy-in, and sustainable processes. When risk management makes sense, one of the de facto by-products is regulatory compliance.²

We don't suggest a company attempt to establish any system of risk management simply for the sake of compliance. If compliance becomes the motivator, you will fail to get long-term buy-in from employees and the effort will not be sustainable. Rather, if more time were spent focusing on identifying risks to objectives and assessing their likelihood and potential impact against the organisation's known risk management strategies, you would tend to get buy-in because the reason for implementing robust risk management make sense. Said differently, risk management is directed at risk, not at compliance.

The impact of the recent recession, which began in 2008, highlights the downstream consequences that materially affected and crippled several companies in multiple industries, such as investment banking, deposit banking, mortgage lending, construction, automobiles, insurance, and so on. No doubt we will see increased legislation forcing companies to implement systems of risk management and internal control that are more robust.

That said, on December 16, 2009, the SEC amended its proxy disclosure requirements.³

The amendments require registrants to make new or revised disclosures about

- compensation policies and practices that present material risks to the company;
- stock and option awards of executives and directors;
- director and nominee qualifications and legal proceedings;
- board leadership structure;
- the board's role in risk oversight; and
- potential conflicts of interest of compensation consultants that advise companies and their boards of directors.

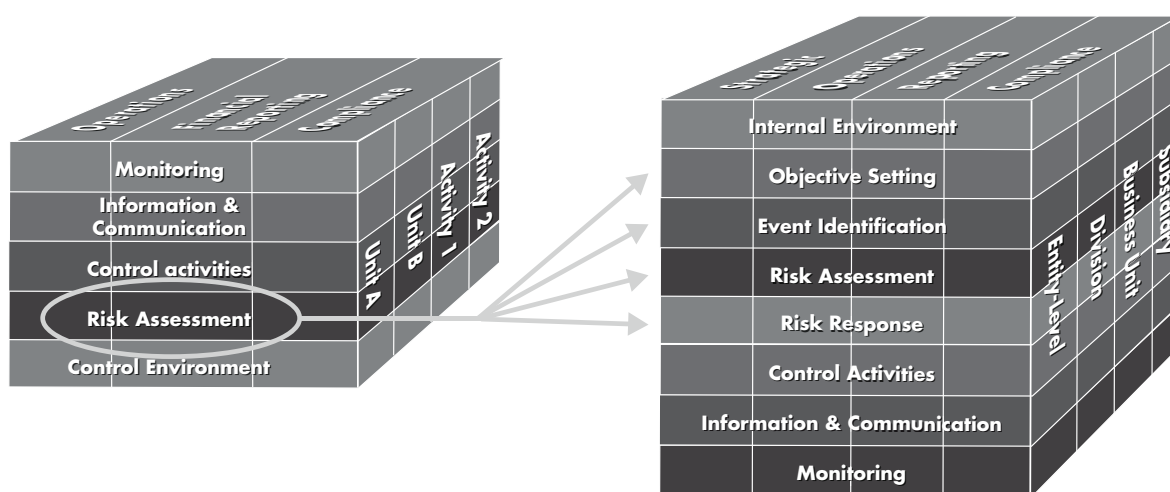
There have been numerous white papers and speeches from regulators, academics, and leaders in industry espousing greater risk management and risk oversight, several of which we reference in the appendixes. We believe it is only a matter of time before regulators, outside directors, and those charged with governance mandate that broader sections of industry implement ERM.

With that in mind, this publication demonstrates that you can implement a robust ERM system using the COSO ERM framework along with relatively straightforward risk concepts and simple desktop tools without spending millions of dollars.

Throughout this publication we expand on concepts contained in the COSO *Enterprise Risk Management—Integrated Framework* along with lots of practical application to assist you in developing your company's risk management system. An executive summary of COSO's *Enterprise Risk Management—Integrated Framework* that provides an overview of the key principles for effective ERM is available for free download at www.coso.org.

THE EVOLUTION OF THE COSO⁴ INTERNAL CONTROL: INTEGRATED FRAMEWORK TO THE COSO ERM FRAMEWORK⁵

Most public companies should be able to leverage their existing COSO Internal Control—Integrated Framework to use the COSO ERM framework pictured below and introduced previously in exhibit 1-1. The ERM framework essentially adds a ‘Strategic’ objective category and breaks out the COSO component ‘Risk Assessment’ into four separate components: (1) objective setting, (2) event identification, (3) risk assessment, and (4) risk response as depicted in the following figure.



Copyright 2011. COSO. All rights reserved. Used with permission.

Endnotes

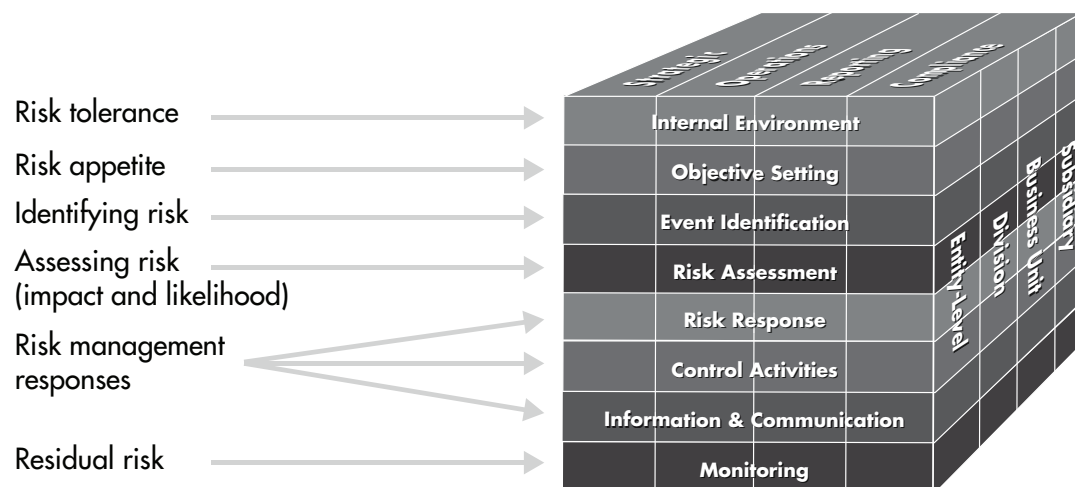
- 1 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the widely accepted COSO *Internal Control—Integrated Framework*.
- 2 Quoted in the white paper *Is Enterprise Risk Management at a Crossroads?* Jointly Commissioned by the AICPA and CIMA, August 2010; Scott M. McKay CPA, CFE, CIA, CCSA, Director Corporate Audit, Cree, Inc.
- 3 SEC Release No. 33-9089 *Proxy Disclosure Enhancements*, Final Rule.
- 4 COSO *Internal Control—Integrated Framework*, September 1992, www.coso.org, New York, NY.
- 5 COSO *Enterprise Risk Management—Integrated Framework*, September 2004, www.coso.org, New York, NY.

2

ENTITY-WIDE RISK ASSESSMENT

The entity-wide risk assessment approach to ERM should flow logically through the COSO ERM framework, starting from the top with the 'Internal Environment' component and proceeding to the 'Monitoring' component at the bottom (see figure 2-1).

Using the COSO ERM framework as a guide, the entity-wide risk assessment methodology is relatively straightforward. To help solidify risk management concepts, we have linked them to components of the framework and will use the following diagram throughout this publication.



Copyright 2011. COSO. All rights reserved. Used with permission.

Begin with defining risk in both positive and negative senses, and then establish corresponding materiality levels (ML) (both qualitative and quantitative) for use with the internal environment.

We recommend defining the word *risk* in the negative sense and substituting the word *opportunities* for risk in the positive sense. In other words, although allowing certain risks to occur (for example, misstating financial statements through errors or fraud) can be very damaging to the organisation, knowingly taking certain risks to increase the value of the organisation results in rewards (such as acquiring a complementary business at a good value, thereby increasing the company's stock price). Hence, we will use the following definitions with this approach to ERM.

Risk. The possibility of an event occurring that would negatively affect the achievement of objectives.

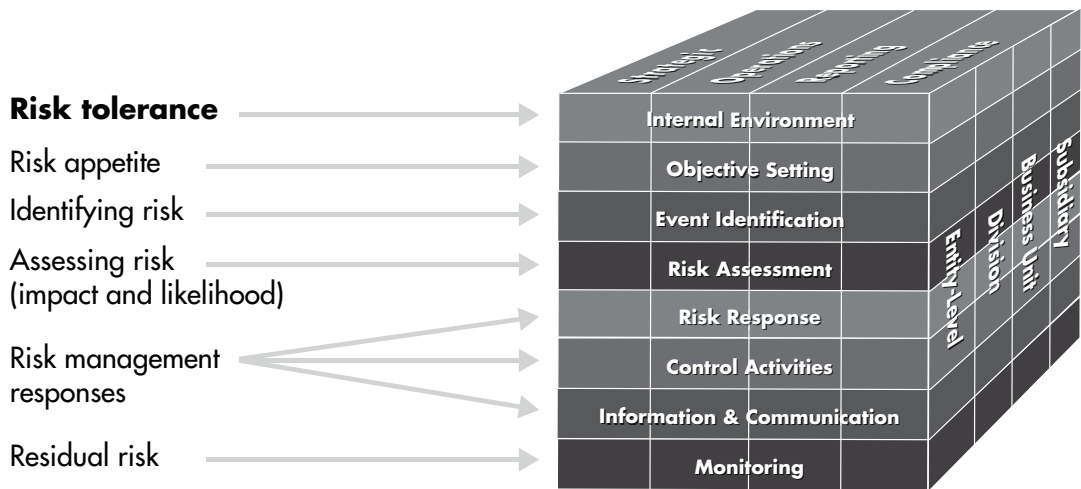
Risk Tolerance. Levels of risk clearly established in a company’s internal environment.

Opportunity. Attempting to increase the organisation’s value by taking on risk.

Risk Appetite. The level of risk that an organisation is willing to take on as part of its process to set objectives (that is, opportunities).

This chapter will briefly discuss some strategies for setting risk tolerance and risk appetite as the first step in your ERM assessment. For a more in-depth look at risk appetite, including sample risk tolerance statements and questions to facilitate the discussion of risk appetite, see chapter 6.

RISK TOLERANCE



Copyright 2011. COSO. All rights reserved. Used with permission.

Setting risk tolerance involves establishing and communicating company policies, guidelines, and general governance. Policies are the company’s formal ‘you shall’ and ‘you shall not’ statements that provide clarity to employees and establish the tone of the organisation’s governance structure. The following are a few examples of policies and guidelines common in many organisations and should help to clarify and establish your organisation’s own approach to risk tolerance levels:

- Annual operating plans that encompass operating and capital budgets
- Research and development spending limits
- Authorisation limits for construction in progress projects
- Authorisation limits for purchase orders
- Authorisation limits for cash disbursements
- Authorisation limits for travel and entertainment purchases
- Investment policies
- Banking policies

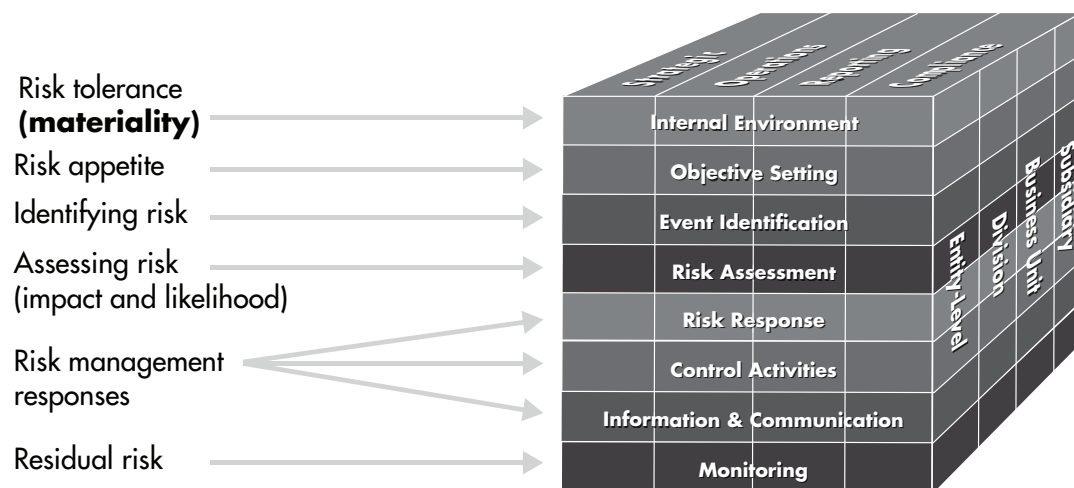
- Debt policies
- Merger and acquisition policies
- Procurement guidelines and policies
- Contract guidelines and authorisation policies

Unless governance is put in writing and widely disseminated, the organisation's tolerance for risk is often unclear and retained only in the local knowledge of peoples' minds, which will likely vary with the person and can result in unintended consequences. This scenario works fine for a while in small organisations in which a manager controls relatively few people, but in general it breaks down as a company grows and management's span of control broadens or at the point where change occurs within the organisation in the form of new managers, staff, or business systems.

Key Insight: Companies struggle to define the concept of risk tolerance. In other words, how much risk are we willing to accept? Establishing formal risk tolerances (that is, policies and guidelines) can be viewed as bureaucratic unless their purpose is clearly understood. Policies and guidelines, such as budgets and operating plans, may need to change frequently in times of business growth or business decline, and therefore they should be revisited and re-established regularly and be viewed not as bureaucratic one-time events but as opportunities to provide clarity and improve organisational effectiveness. The risk assessment process is a great opportunity to review and challenge current policies and guidelines because it helps companies identify emerging and declining risk areas, establish formal risk tolerances, and challenge the controls currently in place in order to avoid over controlling or undermanaging risk. See chapter 6 of this book for specific examples of risk tolerance statements.

Materiality

As briefly discussed earlier, the concept of materiality in both a qualitative and quantitative sense is part of the internal environment and quantitatively reflects an organisation's risk tolerances and risk appetites.



Copyright 2011. COSO. All rights reserved. Used with permission.

Executive-level managers tend to be concerned with matters that could be material to the enterprise as a whole. Said differently, they are concerned with entity-wide consolidated financial statements, where materiality can start to be quantified. So it makes sense to address materiality from a financial statement point of view. Once materiality is established at the enterprise level, it makes sense to work down to various ML at the business unit, shared service function, and individual employee strata.

To start, materiality should reflect certain levels of judgement that are influenced by management's perception of the needs of users of the organisation's financial statements, as well as other matters related to the achievement of the organisation's objectives and their own risk thresholds. We suggest using the term *materiality levels* (ML) because there will be many throughout an organisation.

To establish entity-wide materiality, we recommend beginning by using certain rules of thumb that have been developed over time by large auditing firms employing consolidated balance sheet and income statement metrics to derive some materiality baselines.

For example, on the balance sheet, consider initial materiality at 1.0 per cent of consolidated total assets (rule of thumb) and then apply judgement to arrive at upper and lower materiality limits. Potential errors affecting the balance sheet are misclassifications between current and long-term assets and liabilities and of course overstatements or understatements of assets and liabilities due to many factors. Note that this publication does not attempt to address potential errors affecting equity or net asset line items, which can be just as important, depending on the users of the financial statements.

For the income statement (or statement of operations), consider initial materiality using 5 per cent of annualised consolidated pre-tax income. Note that we believe the income tax expense line item should be considered separately because of its inherent complexity, high degree of subjectivity, exposure to changes in the business and to various tax authorities, and the possibility that external stakeholders may discount it altogether as just a cost of doing business. For example, Wall Street analysts and investors like to use EBIT¹ and EBITDA² and other metrics when assessing a company's value in terms of stock price. In addition, many companies report both generally accepted accounting principles (GAAP) and non-GAAP financial statements, excluding certain items such as the fair value of stock based compensation arrangements because of the estimated 'noncash' nature of the expense.

Next we recommend applying further judgment to the 5 per cent consolidated pre-tax income threshold to establish a materiality upper and lower limit. Note that for publically traded companies, defining limits to use with upper and lower materiality becomes somewhat easier because public companies can also consider the impact on diluted earnings per share a key investor metric.

The following table offers examples of how to apply these concepts.

Planning Materiality		
(Dollar) amounts in 000s	FY2XXX as of FOX Forecast Consolidated	
	Total Assets	Pretax Income
	\$1,347,002	\$44,032
Materiality calculations	1.00%	5.00%
	13,470	2,202
Management's judgement	30	(292)
ML upper limit	\$ 13,500	\$ 1,910
		A
		B
Management's judgement	(6,750)	(1,565)
ML lower limit	\$ 6,750	\$ 345
		C
EPS Considerations		
Potential impact of error (upper limit)		\$ 1,910
Diluted shares used		78,128
Effect per diluted share	A	\$ 0.024
Potential impact of error (lower limit)		\$ 345
Diluted shares used		78,128
Effect per diluted share	C	\$0.0044

Legend:

- A** Potential impact of error > ML upper limit considered strong indicator of a material weakness
- B** Considered more than inconsequential (potentially significant)
- C** Potential impact of error < ML lower limit considered inconsequential

Management's thresholds for materiality can work hand in hand with establishing and refining the organisation's risk tolerances discussed earlier. Certain materiality thresholds are most likely already established within your organisation. For example, the financial planning group may already be required to document variances between actual and budget when the variance exceeds a certain threshold amount. The operating performance of the organisation (also known as the 'run-rate' level of materiality) will help clarify and establish internal expectations for the level of precision needed when differences arise between management's expectations and actual results. Differences in budget to actual are then investigated based on how material they are and whether caused through error, fraud, control failure, unidentified risk, poor estimates, or unanticipated costs.

Key Insight: In determining the upper materiality limits, it is useful to ascertain answers to the following questions:

- What would cause management to restate previously published financial statements?
- What would cause the company to miss meeting loan covenants?
- What would cause the company to miss meeting surety bonding requirements?
- What would cause management to miss meeting more than one major corporate objective?
- What would cause donors or grantors (either public or private) to consider not funding certain organisational programmes?
- What would cause the company to lose an important business license, such as an import or export license?
- What would cause the company to incur a lawsuit?
- What would cause management to have to report a material control weakness to the audit committee and the public?

In determining the lower materiality limits, it is helpful to ascertain answers to the following questions:

- What would cause management to preannounce earnings ahead of an earnings call because of a difference in guidance and a failure to meet Wall Street expectations?
- What would cause management to have to report a significant control weakness to the company's audit committee?
- What would cause management to miss meeting a minor corporate objective?
- What would require further explanation and investigation in a budget to actual variance?

In determining impact thresholds that are considered nominal or less than inconsequential (below the lower materiality limit), consider when management requires explanations for budget to actual variances. Said differently, if the difference between the actual results and the expected results requires no explanation, then the difference must be within management's tolerance, the organisational goal was essentially achieved, and any errors or differences in expectations below this level must be nominal in nature and would not merit further consideration.

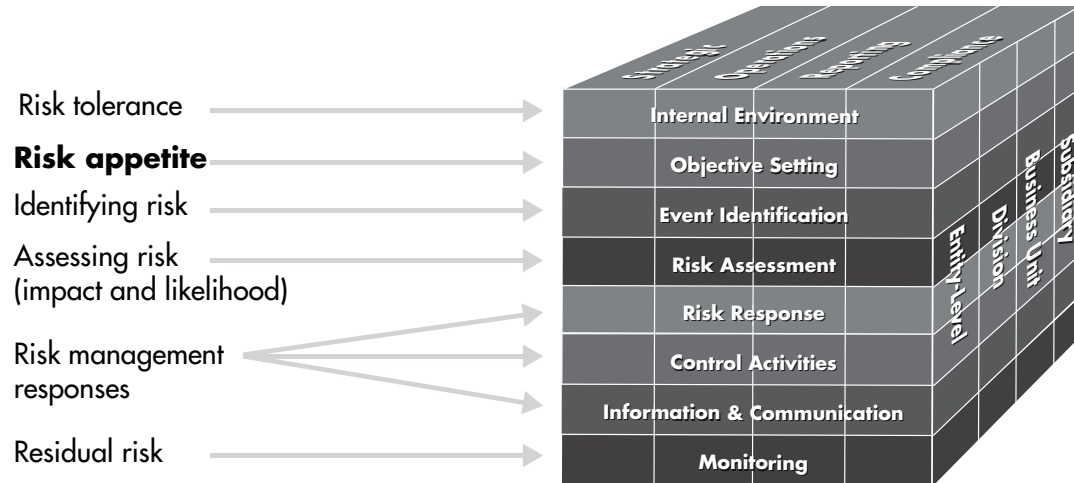
We recommend you define at least three to five levels of materiality in both qualitative and quantitative terms. Qualitative terms should be carefully selected, because once embedded in the business culture these terms will convey management's risk tolerance to a broad audience and help create an efficient and effective risk management culture within the organisation. The following are examples of qualitative terms:

1. Extreme or very material (affects the company's ability to continue business)
2. High or material
3. Medium or significant
4. Low or inconsequential
5. Negligible or trivial

We will revisit and incorporate these concepts and terms when we review the enterprise risk scale depicted later.

Objective Setting

As discussed earlier in this chapter, we defined the word *risk* in the negative sense and substituted the word *opportunities* for risk in the positive sense. Therefore, risk appetite is defined as the level of risk that an organisation is willing to take on as part of the 'objective setting' process (that is, opportunities to increase the organisation's value).



Copyright 2011. COSO. All rights reserved. Used with permission.

In most organisations, objective setting is performed at least annually, when the business sets operational goals typically tied to financial and nonfinancial metrics. Once enterprise-wide goals are established, there should be an iterative planning process to ensure that organisation resources are allocated sufficiently to meet the objectives. Unrealistic goal setting or even stretch goals are beyond the scope of this discussion. What is important is determining the range of acceptable performance against the objective and identifying risks that would prevent the achievement of the organisation's objectives.

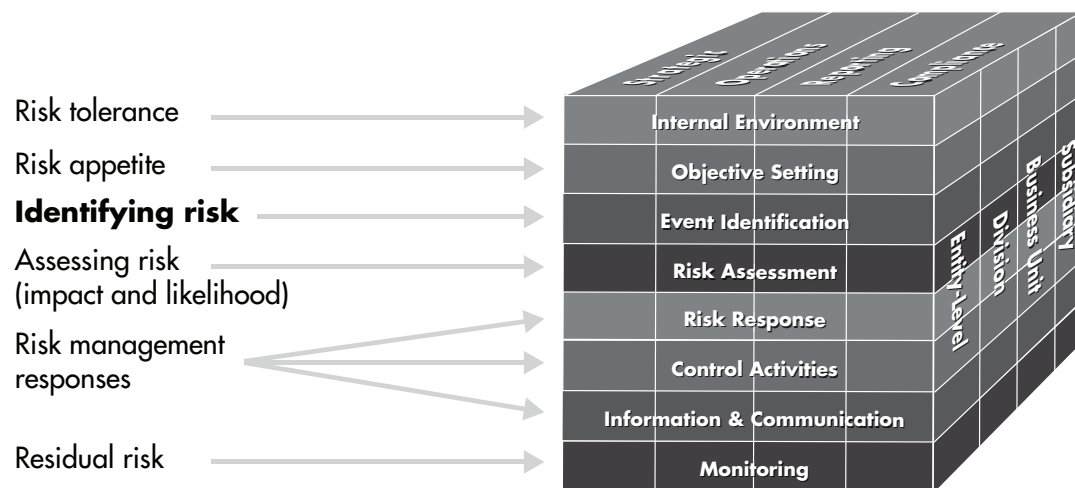
Endnotes

- 1 Earnings before income tax.
- 2 Earnings before income taxes, depreciation and amortisation.

3

IDENTIFYING RISK: ENTITY-LEVEL VERSUS ACTIVITY-LEVEL

Risk identification is the most important component in the ERM framework. It is known as the 'Event Identification' component.



Copyright 2011. COSO. All rights reserved. Used with permission.

In discussing the importance of risk management, participants generally agree that many companies fail to meet organisational objectives or that errors occur primarily because of the following three reasons:

1. Unidentified Risks—The organisation failed to identify a risk event.
2. Unmanaged Risks—The risk was known but undermanaged.
3. Control Failures—Controls that were thought to be working actually failed.

Highlighting these concepts at the beginning of a risk assessment workshop will help get management's buy-in and active participation in the risk identification, verification and risk assessment process.

To better understand entity-level risk identification, we must start with the process, or activity-level risk identification. A logical way to think about risk is to first distinguish between risks and root causes or, using a similar concept, risk and risk factors. Let's walk through the following risk model for what we define as an activity-level risk.

Process- or Activity-Level Risk Model

ROOT CAUSE	RISK	CONSEQUENCE	DOWNSTREAM EFFECT
Wet floor	Slip and fall	Sprained wrist	Medical bills

Key Insight: The takeaway in the preceding example is that there are many ways to 'slip and fall' (the risk event) and there can be many factors leading to this risk event. However, the most important point to remember when using this paradigm is not to get stuck in root cause analysis but to distinguish between the risk and the many potential root causes or risk factors that can lead to the risk event.

Let's use the model and apply the same principles with a commonly understood financial reporting risk known as revenue recognition.

ROOT CAUSE	RISK	CONSEQUENCE	DOWNSTREAM EFFECT
Side agreements	Revenue recognition	Revenue overstated	Incur time and cost to restate financial statements

In this example, the root cause driving revenue recognition risk was the existing side agreements that affected the company's normal revenue recognition process and that were unknown to finance managers responsible for revenue accounting. Side agreements that materially affected revenue recognition accounting and caused the company to restate its financial statements were detected by the company's auditors. In our hypothetical example, management will likely need to remediate control gaps that allowed side agreements to affect revenue recognition.

Using our same process-level risk model, let's expand it to capture the business processes where things may go wrong, such as the aforementioned side agreements that led to our revenue recognition risk, consequence, and downstream effect.

ROOT CAUSE	RISK	CONSEQUENCE	DOWNSTREAM EFFECT
<ul style="list-style-type: none"> • Customer credit and setup • Sales contracts • Customer purchase orders and sales order entry • Order fulfillment and shipping • Revenue accounting and accounts receivable • Returns, credit memos, and reserves • Collections, cash application, and reserves • Sales commissions • Distributor commissions 	<p>Revenue recognition</p> <ul style="list-style-type: none"> • Incomplete or inaccurate <p>Fraud risk factors</p> <ul style="list-style-type: none"> • Timing differences • Channel stuffing • Fictitious revenues <div style="border: 2px solid black; padding: 10px; margin-top: 10px;"> <p>Key Insight Root cause analysis starts at the process level.</p> </div>	<p>Due to inherent risk</p> <ul style="list-style-type: none"> • Miss shipments • Miss meeting quarterly or annual operating plans • Misstated earnings <p>Due to fraud risk</p> <ul style="list-style-type: none"> • Reputation damage 	<p>Due to inherent risk</p> <ul style="list-style-type: none"> • Loss of customer confidence • Loss of period revenue • Restate financial statements • Report material weakness to public • Stock price declines <p>Due to fraud risk</p> <ul style="list-style-type: none"> • SEC investigations • Class action lawsuits • Incur time and money to correct

Can you see that the lower-level risk events are actually most likely buried in the very processes that were initially designed and put in place to achieve certain information processing objectives? These risks, therefore, are also likely the result of poorly designed or inconsistently applied operating controls. Said differently, the root cause is most likely a control or controls failure.

Another way of thinking about root cause analysis is to ask the question ‘What could go wrong?’ This question should be directed at the processes and controls designed to ensure the achievement of the process objective.

A root cause analysis is not part of the initial entity-wide risk assessment because it uses a bottom-up (deep dive) approach directed at lower-level processes and controls. However, root cause analysis is considered a follow-up activity once risk areas that may be undermanaged or overcontrolled are identified (see chapter 5, *Activity-Level Risk Assessment*).

Most companies have functions in place that are intended to identify and address root causes of risk events, focused on the processes and activities designed to meet management’s objectives and reduce risk. Examples are quality control groups with quality standards like ISO/TS 16949 and process control methods like Failure Mode Effects Analysis or Environmental Health and Safety (EH&S) groups that were put in place to establish and monitor compliance with EH&S standards.

Process- or activity-level risk assessment key considerations would include addressing the following questions:

- What could go wrong?
- How can it go wrong?
- What is the potential harm?
- What can be done about it?

The root cause analysis identifies control gaps and can point to auditable activities, business systems, functions and people responsible for risk management at lower levels within the organisation.

Using a top-down risk based approach, it is initially more important to identify clearly the relevant high-level risk area or areas and high-level risk factors rather than to attempt a detailed activity-level root cause analysis, which will be discussed later. We have included a section on activity-level (process-level) risk assessment for use in later lower-level risk assessments.

Now that you have a good grasp of process- or activity-level risk, let's move on to explore our entity-level risk model that you can establish and use for the initial risk library with the entity-wide risk assessment workshop.

Entity-Level Risk Model

RISK NAME	RISK DESCRIPTION FACTORS	DOWNSTREAM EFFECT
Regulatory Reporting	Regulatory noncompliance <ul style="list-style-type: none"> • SEC • Generally accepted accounting principles reporting for banking, surety, and so forth • Tax (federal, state, local, foreign) • Department of Labor • Employee Retirement Income Security Act • Other similar factors 	Fines, penalties, loss of filing status, reputation tarnished, and so forth

In the preceding model, can you see SEC reporting is just one of the many risk factors affecting the organisation at the entity level? Further, not all risk factors will have the same weight during the risk assessment workshop. However, getting participant views on regulatory reporting risk in a broad sense helps bring to the surface the many critical risk factors important to risk management. One or more of those risk factors will drive the risk assessment results and identify underserved risk areas as well as areas that may be over controlled. Our experience indicates that compliance risk areas tend to be one of the primary factors that drive companies to greater levels of control maturity (see the section *Control Maturity* in chapter 4).

Now let's apply the entity-level risk model to an operational risk area.

RISK NAME	RISK DESCRIPTION FACTORS	DOWNSTREAM EFFECT
Manufacturing Risk	Poor yields, throughput, product quality, inability, to reduce production costs competitively, or inability to balance customer demand versus capacity	Higher costs, higher product returns, lost revenue, or loss of customers

This same risk model can be used to identify and capture entity-level risks across an organisation. Organisations can identify and categorise risks in one of four buckets using the COSO ERM framework's objective areas: (1) Strategic, (2) Operational, (3) Financial, and (4) Compliance.

Key Insight: Develop a succinct risk name along with a very brief risk description consisting of the key risk factors.

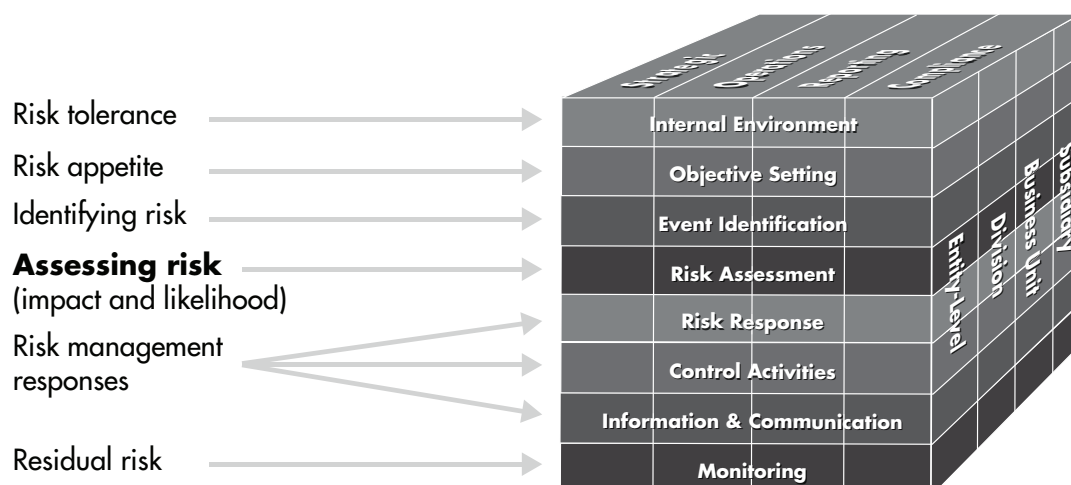
To distil a short list of entity-wide risk names and risk factors (we recommend no more than 20–30), consider starting with the risk factor section of your organisation's public filings or those of a competitor's public filings, analyst reports and industry information available through trade groups and other organisations.

Note that managers will often talk about 'reputation risk' and 'legal risk' and struggle in assessing these areas. We believe these risks are really the consequence or downstream effect of some other risk event and can be misleading if captured as part of the entity-wide risk library. (Refer to the expanded activity-level model.)

Risk can be viewed as either negative or positive (such as risking capital in an acquisition in order to reward stakeholders with increased returns on investment). We recommend making a clear distinction between the two sides of risk—that is, define *risk* in negative terms and *opportunities* as risk in positive terms.

RISK ASSESSMENT

The timing of the risk assessment should complement the organisation's objective setting process.



Copyright 2011. COSO. All rights reserved. Used with permission.

We strongly recommend using self-assessment workshops instead of surveys to capture the participants' initial inputs. Workshop leaders can be highly effective by capturing and vetting participants' thoughts on any given risk area. Before scheduling a risk assessment workshop, be sure to have the initial risk library (risk names and factors) fairly well defined and laid out to show their interdependence. Otherwise, avoid holding a risk identification workshop until all the preparatory work is complete. Beginning a workshop with a blank piece of paper is a sure-fire way to lose participant interest and derail your ERM initiative.

Ideally, having a well prepared self-assessment workshop coupled with the use of some form of electronic voting technology can yield quick and meaningful results that go a long way to satisfy the information needs of busy managers.

We recommend using a short slide deck presentation for the initial workshop to clarify the purpose and approach to this facet of risk management, with greater emphasis applied to (1) risk identification, (2) risk assessment, including developing the concepts of likelihood and potential impact incorporating qualitative and quantitative materiality, and (3) introducing the concepts of control maturity (discussed later) in order to estimate the amount of residual risk associated with a given risk event.

Ask participants to evaluate risk names, risk descriptions (brief descriptions should include all relevant risk factors), and risk areas based on their knowledge or perception of risk management currently in place within the organisation.

Establish the time horizon for assessing risks as one quarter, one year, or longer.

Key Insight: Risk assessment time horizons should be established corresponding to either annual operating plans or longer-term strategic organisational objectives. We recommend using a one-year time period, which is common with most organisations' annual operating planning horizons and will serve to capture a sense of risk velocity (that is, how quickly a risk event could emerge).

Solicit what participants know about risk tolerances (organisational policies) already established within the organisation.

Key Insight: The facilitator can help participants establish risk tolerances by encouraging managers to express their thoughts about acceptable levels of missing objectives such as budgets, production goals, and other standards that they may already be held accountable for internally to senior management.

Evaluate whether participants' assessments of risk should be given equal weighting. For example, you may agree to give more weight to line managers responsible for risk management activities than to corporate executives who may be less knowledgeable about control maturity in a given area, or vice versa.

Key Insight: The results of the initial risk assessment reflect participants' views of residual risk after taking into account their knowledge or perception of control maturity already in place.

The vast majority of corporate risk assessment tools suffer from two major shortcomings:

- A failure to quantify risks in terms of potential impact on the organisation, such as in terms of cash or earnings
- Integrating a control maturity model (CMM) so that participants can assess various risks based on their knowledge or perception of the current risk management practices in place at their organisations

We have included information depicting a reasonably comprehensive risk assessment scale (heat map) and integrated a CMM in an Excel workbook that is available for download from www.cpa2biz.com/RiskAssessmentDownload. Please see the following discussion of probability (likelihood) and potential impact. Your organisation may desire to use tools with more or less precision.

PROBABILITY

Many organisations are familiar with certain probability terms—such as *remote*, *reasonably possible*, and *probable*—because they are commonly used by auditors, accountants, and lawyers helping companies make decisions about how much disclosure is required in a company's financial statements regarding contingencies.¹

Therefore let's use these well-known qualitative terms to establish a three point probability scale:

- Remote
- Reasonably possible (or possible)
- Probable

Leveraging these terms, we need to add two more terms to develop a five point probability scale. Adding another lesser known term and its reciprocal, we can then attempt to enhance the qualitative level of precision used when expressing the likelihood of a given risk event:

- More likely than not (or likely)
- More unlikely than not (or unlikely)

To bring more precision to the probability assessment in terms of a percentage, let's put a stake in the ground using the term *more likely than not* (MLTN).

In the field of professional taxation, US tax rules define the term *more likely than not* as a given taxpayer's ability to take a defensible tax position. For the taxpayer to recognise the tax position in its tax return, it must meet the MLTN threshold or have a greater than 50 per cent chance that the tax position will be sustainable on examination by the taxing authority. In other words, the tax position must be sustained if challenged under audit. Further, it is assumed that in taking the tax position, the tax authority is aware of all relevant facts related to the tax position. In other words, the taxpayer taking the tax position cannot assume that the tax authority will not discover all the relevant facts associated with the position, bringing into question whether the tax position meets the recognition threshold of MLTN. Said differently, the taxpayer cannot assume any level of detection risk.

That said, let's build on the MLTN as a precise percentage stake in the ground and create its reciprocal—that is, *more unlikely than not* (MULTN), thereby splitting our current qualitative view of probability into two distinct hemispheres.



It's a fairly simple matter to insert the previously discussed terms *remote* and *probable* as reciprocals on either side of MULTN and MLTN metrics, thus leaving the qualitative probability of *possible* to insert nicely in the middle of our five point probability scale.

- Remote
- More likely than not (or likely)
- Reasonably possible (or possible)
- More unlikely than not (or unlikely)
- Probable

Remote is commonly used by meteorologists (weather forecasters) to express the chance of rain. A remote chance of rain is commonly expressed as less than 10 per cent, which leaves *probable* at the other end of the scale, or greater than 90 per cent. Now all we need to complete our scale is to squeeze out the percentage range for the term *reasonably possible*.

Reasonably possible is commonly used by accountants and lawyers to express a range of possible outcomes in estimating a contingent liability anywhere from 25 per cent to 60 per cent, with about 40 per cent being a comfortable midpoint in the range. So now we can reasonably construct a more precise table reflecting our qualitative terms and the corresponding ranges of probability for use later with our risk assessment scale, as shown in the following table.

Probability (Likelihood) Table

QUALITATIVE TERM	SHORT NAME	PROBABILITY RANGE
Remote	Remote	< 10%
More unlikely than not	Unlikely	≥ 10% < 25%
Reasonably possible	Possible	≥ 25% ≤ 50%
More likely than not	Likely	> 50% ≤ 90%
Probable	Probable	> 90%

POTENTIAL IMPACT

In planning the risk assessment workshop, helping managers quantify the potential impact of risk events is one of the most important exercises in the risk management process. Operational managers often struggle with the concept of materiality and how to define it in both qualitative and quantitative terms. Therefore, finance and risk management professionals should spend considerable time in helping managers define the different levels of materiality for use with assessing the impact of potential risk events.

This risk assessment scale uses increasing qualitative and quantitative expressions to help participants apply more precision to the assessment process. The risk rankings (1–25) were chosen instead of a simple five by five scale to clearly differentiate the likelihood and potential impact of entity-level risk. Further, when assessing risk, participants should use a well-defined CMM (note that the CMM is integrated with the Risk Assessment Model) to rate risks on the basis of their knowledge or perception of the maturity of internal controls employed to manage a given risk area. (See the section *Control Maturity* in chapter 4.)

Enterprise Risk Assessment Scale (1 to 25)

> \$75 million(m)	■	Very material: May affect company's ongoing existence
> \$1.9m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$230k - \$1.9m	■	Significant: More challenging to achieve some objectives
> \$20k - \$230k	■	Inconsequential: May have some undesirable outcomes
< \$20k	■	Trivial: No noticeable impact on objectives

High ≥ \$0.000 EPS* or cash and equivalents
 Low ≥ \$0.000 EPS or cash and equivalents
 * EPS = Earnings per share

Potential Impact	Extreme	15	19	22	24	25
	High	10	14	18	21	23
	Medium	6	9	13	17	20
	Low	3	5	8	12	16
	Negligible	1	2	4	7	11
	Remote	Unlikely	Possible	Likely	Probable	
Likelihood						
% ranges	0-10%	>10-25%	>25-50%	>50-90%	>90-100%	

Endnotes

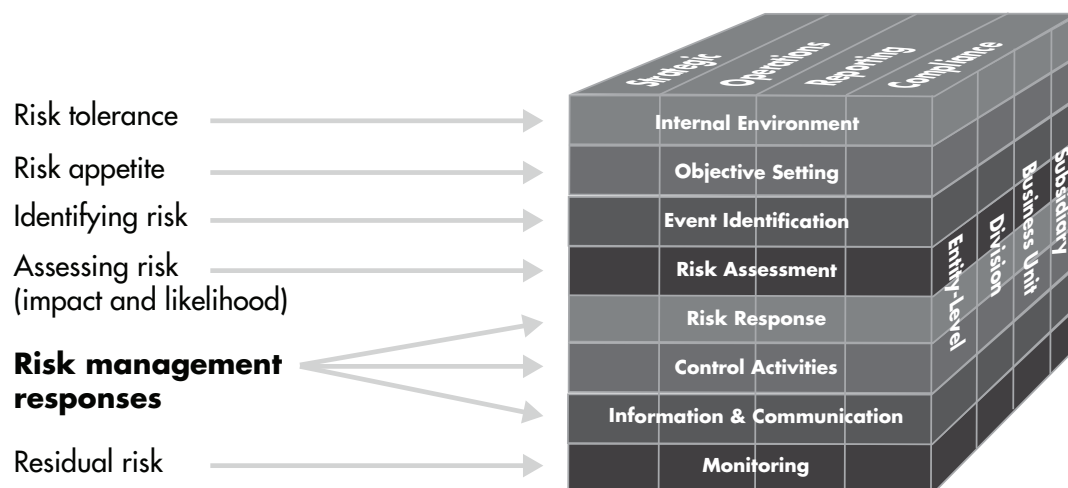
- 1 See Financial Accounting Standards Board *Accounting Standards Codification*[®] (ASC) 450, *Contingencies* (formerly known as FAS 5).

4

RISK MANAGEMENT

Risk management response concepts are simple when you understand that you are limited to only four options:

1. Internal controls
2. Risk avoidance strategies
3. Risk transfer (risk sharing) strategies
4. Risk acceptance



Copyright 2011. COSO. All rights reserved. Used with permission.

Note that our experience indicates that when conducting risk assessment workshops and asking participants when they evaluate a given risk area to consider how it is managed, the number one response provided by participants is that the risk area is managed using internal controls. Because internal controls can be evaluated and tested in terms of design and operating effectiveness, the concept of control maturity can be incorporated into the risk assessment workshop using a control maturity model (CMM) (see the section *Control Maturity* in this chapter).

In selecting risk management responses, a company defaults to risk acceptance when all other risk management strategies are exhausted or no other risk management strategy is employed. ERM guides a company to ensure that risk acceptance aligns with management's risk tolerance, risk appetite, or both.

Key Insight: When facilitating the entity-wide risk assessment and asking participants to assess a given risk area, make sure to elicit whether they think controls are 'well defined' (see the control maturity scale in this chapter) or 'soft' (see 'repeatable' in the control maturity scale) or 'more informal' (see 'immature' in the CMM discussed later).

Internal controls that contain defined or more mature attributes can be more easily measured for design and operating effectiveness either through audit or self-assessment and hence provide positive assurance to stakeholders that residual risk is within management's acceptance levels.

After you establish participants' views on formal or informal controls, ask them which risk management strategies they believe the company employs. Often there can be lack of clarity regarding the level within the organisation at which individual risks will be managed—that is, whether individual risks are to be mitigated by the corporate shared service centres or left to business units to manage. Using CMMs will help draw out the collective wisdom of the organisation and get managers to agree on which functions are primarily responsible for managing risk and how shared services can best support the business units in achieving their goals. This will help break down silos and embed risk management into the business culture.

CONTROL MATURITY

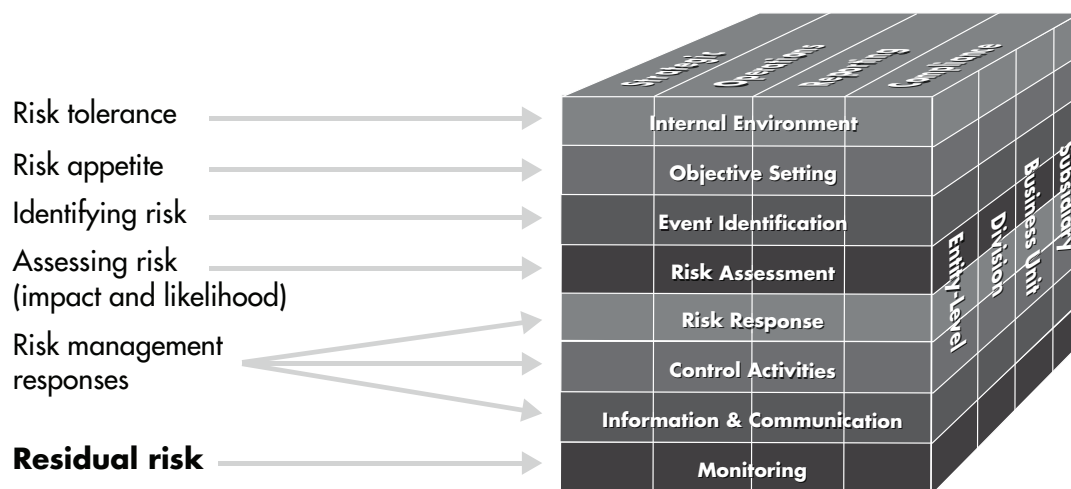
Maturity Evolution	Scale	Model Levels	Control Capability Attributes
	5	World Class	Controls are considered 'world-class', based on benchmarking and continuous improvement; the controls infrastructure is highly automated and self-updating, thus creating a competitive advantage; there is extensive use of real-time monitoring and executive dashboards.
	4	Mature	Key performance indicators and monitoring techniques are employed to measure success; there is greater reliance on prevention versus detection controls; strong self-assessment of operating effectiveness by process owners occurs; change of accountability exists and is well understood.
	3	Defined	Controls are well defined and documented, thus there is consistency even in times of change; overall control awareness exists; control gaps are detected and remediated timely; performance monitoring is informal, placing great reliance on the diligence of people and independent audits.
	2	Repeatable	Controls are established with some policy structure; formal process documentation is still lacking; there is some clarity on roles, responsibilities and authorities, but not accountability; increased discipline and guidelines support repeatability; high reliance on existing personnel creates exposure to change.
	1	Immature	Controls are fragmented and ad hoc; they are generally managed in silos and reactive; formal policies and procedures are lacking; efforts are dependent on the 'heroics' of individuals to get things done; there is a higher potential for errors; costs are higher because of inefficiencies; effort is not sustainable.

Key Insight: During the risk assessment workshop, take the time to read out loud the CMM descriptions for *immature*, *repeatable*, *defined*, and *mature*. Invariably you will see managers unconsciously nodding in agreement with the description of these attributes and get further buy-in in how to mitigate risk—that is, to mature the controls.

Do you remember what tends to drive a company's control maturity? The answer is some form of regulatory requirement. For example, to achieve a level 3 or 'defined' level of control maturity, the internal controls must be well defined and documented. Regulators inspect documented policies and procedures and consider undocumented policies and procedures as ad hoc or immature. Note that hard policies without documented procedures and control descriptions can also be referred to as 'soft controls' (see the 'repeatable' attributes previously described in the CMM).

Note that internal control is the number one risk management response that participants provide when asked how the company manages a given risk area.

RESIDUAL RISK



Copyright 2011. COSO. All rights reserved. Used with permission.

As noted earlier, the organisation can often lack clarity as to where and how individual risks will be managed—that is, whether individual risks are to be mitigated by the corporate shared service centre or left to business units to manage.

When participants consider control maturity during the risk assessment workshop, the results of the initial risk assessment provide the participants' view of residual risk. However, any risk assessment will not provide comfort over the effectiveness of internal control or other risk management activities apart from some form of independent assurance.

Therefore, it makes sense to have some form of residual risk evaluation. Typically, this requires either an independent audit or some other form of self-assessment of the risk management activities. Once complete, risk management gaps—whether in design or operation—will be identified and the risk management programme will continue to mature and provide comfort regarding the achievement of objectives and will afford managers better insight for decisions about taking on risk.

5

ACTIVITY-LEVEL RISK ASSESSMENT

As discussed in chapter 3, key considerations for process—or activity-level risk assessment—would include addressing the following questions at the process level:

- What could go wrong?
- How can it go wrong?
- What is the potential harm?
- What can be done about it?

A logical way to think about risk is to first distinguish between risks and root causes or, using a similar concept, risk and risk factors. Let's revisit the following risk model for what we define as an activity-level risk.

Process or Activity-Level Risk Model

ROOT CAUSE	RISK	CONSEQUENCE	DOWNSTREAM EFFECT
Wet floor	Slip and fall	Sprained wrist	Medical bills

UNDERSTANDING THE APPROACH: FINANCIAL REPORTING

The following list will help you adapt an activity-level approach to conducting risk assessment workshops with business process owners and other key stakeholders.

- Activity-level risk assessment workshop prerequisites
- Understanding the activity-level approach (financial reporting)
- Activity-level risk factors
- Activity-level risk factor rating system (guidelines)
- Inherent risk (unintentional errors)
- Fraud risk (intentional errors)

We recommend adopting a brainstorming approach to assessing risks against the significant accounts, processes, and related assertions.

Determining risks is inherently subjective and requires judgement. Risks are defined as the possibility of acts or events occurring that would have an adverse effect on the organisation's business processes or cycles and associated information processing objectives. Furthermore, if a risk affects the business process, then logically it may affect the significant account and the relevant COSO financial statement assertions as follows:

- Completeness (C)
- Existence/Occurrence (E/O)
- Valuation/M Measurement (V/M)
- Rights and Obligations (R/O)
- Presentation/Disclosure (PD)

WORKSHOP PREREQUISITES

Before conducting an activity-level risk assessment with business management and process owners, ensure you have prepared the following:

- An account mapping to the significant business processes and sub-processes (we recommend using the financial reporting line item—for example, 'Accounts receivable, net'). In addition, include the relevant financial statement assertions, information processing objectives, and other COSO objectives that should be determined for the significant account and the related business processes or sub-processes. Note that significant accounts and disclosures should be determined, beginning with accounts and disclosures presented in the organisation's audited financial statements and footnotes. The organisation should consider the following in determining significant accounts:
 - Whether the item is separately disclosed in the consolidated financial statements
 - Qualitative and quantitative factors
 - Materiality at the consolidated financial statement level
- Prepare the activity-level risk assessment template, including the specific inherent (unintentional errors) and fraud risks (intentional errors) associated with the significant account and its hierarchy of processes and sub-processes. In addition, list all documented relevant control activities associated with the process either directly or indirectly that would mitigate the risk to the relevant financial statement assertions.
- Determine the business process owner or owners and the appropriate level of management participation—for example, controller, CFO, CIO, product marketing manager, and so forth—to involve in the process.
- Schedule a meeting to perform the risk assessment to include all company personnel identified in the step above.
- Provide participants with copies of the risk assessment documents.
- Note that the estimated time to complete the risk assessment varies with the business process but generally is estimated to be approximately one to one and a half hours (allow for two hours if it is a first time risk assessment).

Because there are a myriad of risks both known and unknown, we recommend that your organisation make use of risk factors (see the table that follows for an example). When identifying and capturing specific risks to process objectives (discussed later), end user computing tools like spread sheets are sufficient to house the risk management system initially.¹

RISK FACTORS	DEFINITION
1. Complexity	Complexity as a function of financial statement data compilation <ul style="list-style-type: none"> • Routine • Nonroutine • Estimation process involved in determining financial statement amount. This includes the level of management competence required and the degree of experience, subjectivity, knowledge, and judgement used to determine the amount or disclosure reported in the published financial statements.
2. Centralisation	Centralisation of the process—that is, how many people are involved in the process, especially as it relates to upper management
3. Change	Change in business systems, personnel involved, or new classes of transactions
4. Distance	Distance from corporate headquarters and the degree of senior management oversight
5. History	Time and results of the last audit—for example, the number of exceptions and types of deficiencies noted
6. Volume	The number of transactions, activities, or both subject to a potential risk of error
7. Inherent risk	Unintentional errors (specific risk)
8. Fraud risk	Intentional errors: (1) corruption, (2) asset misappropriation, or (3) fraudulent statements (specific risk)
9. Impact	The potential magnitude of an error or loss to the auditable unit (as revealed in financial reporting account or disclosure)

Once the specific risks to the objective, account, or process are identified, they are assessed using knowledge of the process in order to determine the potential impact to the relevant financial statement process, the account and its related assertions, or both.

RISK FACTOR RATING SYSTEM

The assessed level of risk and impact is expressed numerically in this example using the following terms: *high* = 3, *medium* = 2, and *low* = 1.

Guidance for ratings (high, medium, and low) varies with the risk factor category. We use suggested interpretations and guidelines that are contained within the risk factor table that appears later in this chapter.

RISK FACTOR SCALE

This risk factor scale uses a table of guidelines associated with each factor so that users of the system can express judgement in initially rating the risk factors with a three point scale.

- Very important (high = 3)
- Average importance (medium = 2)
- Somewhat important (low = 1)

WEIGHTING OF RISK FACTORS

Once risk factors have been determined and scaled, weights must be assigned to each of these risk factors to indicate their relative importance to the business unit, process, account, or class of transactions.

Methods for weighting risk factors include judgmentally assigning a weight to each risk factor to express its importance to the process or direction of the risk trend—for example, a new accounting pronouncement is required under the equity process. Complexity as a risk factor for the equity process is already considered ‘high’. The new accounting pronouncement will significantly increase the complexity factor and therefore it should be weighted as ‘high’. Hence, complexity as a risk factor of the equity process would be a ‘high x high’ or, as expressed numerically, a $9 = (3 \times 3)$. Other considerations when weighting risk factors, such as ‘change’ or ‘history,’ can be made by considering the risk factor trend as follows:

- Decreasing. A low weight (1).
- Constant. A medium weight (2).
- Increasing. A high weight (3).

Examples of risk scale times risk weighting are as follows:

- (High x high) = $9 (3 \times 3)$.
- (High x medium) = $6 (3 \times 2)$.
- (High x low) = $3 (3 \times 1)$.

Note that we use the numerical risk number in both the risk factor scale and weighting in determining the overall risk for each account, cycle, process, and so on.

Generally, with the exception of the ‘complexity’ factor, we recommend assigning the lowest weight to each given risk factor. Because of the range of elements included in the complexity factor—for instance, the degree of subjectivity, technical knowledge, and judgement—we recommend weighting this factor as ‘high’ across all processes to allow for a greater range in assessing the degrees of complexity in a given financial element.

The following is an example employing the activity-level risk assessment methodology applied at the account level.

Account	In Scope	Code	Balance	%	OVERALL RISK	1—COMPLEXITY	7—INHERENT RISK	8—FRAUD RISK
Cash and cash equivalents	Yes	A [101XX-108XX]	350,307	16	1	L	L	M
Short-term investments: Held to maturity	Yes	B [109XX]	340,000	30	1	L	L	L
Short-term investments: Available for sale	Yes	C [191XX]	328,974	—	1	L	L	L
Accounts receivable, net	Yes	D [111XX]	17,175	1	3	H	H	M
Income tax receivable	Yes	E [141XX]	—	—	n/a	n/a	n/a	n/a
Inventories, net	Yes	F [12XXX]	55,058	3	3	H	M	M
Deferred income taxes – current	Yes	G [142XX]	18,255	1	3	H	H	M
Prepaid expenses and other current assets	Yes	H [13XXX-14XXX]	18,961	1	1	L	L	L
Assets of discontinued operations	Yes	I [11110 & 14400]	—	—	n/a	n/a	n/a	n/a
Property and equipment, net	Yes	J [16XXX-17XXX]	292,947	13	1	L	L	L
Long-term investments: Held to maturity	Yes	K [151XX]	411,560	19	1	L	L	L
Long-term investments: Available for sale	Yes	L [191XX]	—	—	n/a	n/a	n/a	n/a
Intangible assets, net	Yes	M [17XXX & 191XX]	84,616	4	2	M	L	L
Goodwill	Yes	N [1912X]	88,204	4	2	M	L	L
Deferred income taxes	Yes	O [1912X]	—	—	n/a	n/a	n/a	n/a
Other long-term assets	Yes	P [19XXX]	4,343	0	1	L	L	L
Accounts payable, trade	Yes	Q [201XX]	(33,169)	–19	1	L	L	M
Accrued salaries and wages	Yes	R [21XXX]	(23,539)	–14	1	L	L	M
Income tax payable	Yes	S [245XX]	(4,370)	–3	2	H	M	L
Deferred income taxes	Yes	T [246XX]	(2,011)	–1	3	H	H	M
Other current liabilities	Yes	U [24XXX]	(6,594)	–4	1	L	L	L
Liabilities of discontinued operations	Yes	V [20115]	—	—	n/a	n/a	n/a	n/a
Deferred income taxes and contingent tax reserves	Yes	W [281XX]	(41,089)	–24	3	H	H	M
Other long-term liabilities	Yes	X [2817X]	(7,010)	–4	1	L	L	L
Long-term liabilities of discontinued operations	Yes	Y [28175]	—	—	n/a	n/a	n/a	n/a
Contingencies	Yes	ZZ	—	—	2	M	H	H
Preferred stock	Yes	Z	—	—	n/a	n/a	n/a	n/a
Common stock	Yes	ZA [31111]	(135)	0	1	L	L	L
Additional paid-in-capital	Yes	ZB [3112X]	(1,490,590)	–73	3	H	H	L
Accumulated other comprehensive income, net of taxes	Yes	ZC [7157X]	(3,418)	0	2	M	M	H

Continued on p.56

Continued from p.55

Account	In Scope	Code	Balance	%	OVERALL RISK	1—COMPLEXITY	7—INHERENT RISK	8—FRAUD RISK
Retained earnings	Yes	ZD [321XX]	(489,402)	−24	1	L	L	L
Product revenue, net	Yes	ZE [4100X]	(333,346)	−38	2	M	M	H
Contract revenue, net	Yes	ZF [4101X]	(15,992)	−2	2	M	M	M
Cost of product revenue, net	Yes	ZG [5100X]	27,671	4	3	H	H	H
Cost of contract revenue, net	Yes	ZH [5101X]	12,118	2	2	M	M	L
Research and development	Yes	ZI [5107X & 6141X]	76,681	12	1	L	L	H
Sales, general and administrative	Yes	ZJ [5XXXX-6XXXX]	94,131	15	1	L	L	L
Amortisation of acquisition related intangibles	Yes	ZK [1911X]	3,890	1	2	M	L	L
Loss on disposal or impairment of long-lived assets	Yes	ZL [7152X]	3,914	1	1	L	M	L
Gain on sale of investments, net	Yes	ZM [7154X]	(1)	0	1	L	L	L
Other nonoperating income	Yes	ZN [715XX]	(15,606)	−2	1	L	L	L
Interest income, net	Yes	ZO [7112X]	(7,263)	−1	1	L	L	L
Income tax expense	Yes	郑 [7211X]	52,558	8	3	H	H	M
Income (loss) from discontinued operations, net of related taxes	No	ZQ [6XXXX-7XXXX]	—	—	2	M	M	L
Nature of business	Yes	FN-01			1	L	L	L
Recent accounting pronouncements	Yes	FN-02			1	L	L	L
Significant accounting policies	Yes	FN-02			1	L	L	L

The following is an example employing the activity-level risk assessment methodology applied at the process level.

Cycle	Process	In scope	Overall Risk	1—Complexity	2—Centralisation	3—Change	4—Distance	5—History	6—Volume	7—Inherent risk	8—Fraud risk	9—Impact
Accounts Receivable	Customer master file maintenance and customer credit	Yes	1	L	L	L	L	L	M	L	M	L
Accounts Receivable	Revenue recognition controls—monitoring terms	Yes	2	L	M	L	L	L	H	L	H	H
Accounts Receivable	Manuel credit memos	Yes	1	L	M	L	L	L	L	L	M	L
Accounts Receivable	Collections	Yes	1	L	L	L	L	L	H	L	M	L
Accounts Receivable	Cash application	Yes	1	L	L	L	L	L	H	M	M	L
Accounts Receivable	Sales reserves	Yes	3	H	M	H	L	H	M	H	H	H
Accounts Receivable	Allowance for doubtful accounts	Yes	2	M	M	L	L	L	M	M	M	M
Accounts Receivable	Distributor commissions	Yes	1	M	L	L	L	L	L	L	M	L
Accounts Receivable	Accounts receivable period end	Yes	2	M	L	L	L	L	M	L	M	H

The following is an example employing the activity-level risk assessment methodology applied at the specific inherent and fraud risk levels.

Type	Risk	Overall risk	7—Inherent risk	8—Fraud risk
ICFR risks and root causes	AR risk 1—AR transactions not properly processed (C, E/O)	1	L	n/a
ICFR risks and root causes	AR risk 2—AR balances not properly recorded (C, E/O)	1	L	n/a
ICFR risks and root causes	AR risk 3—AR reserves estimates not accurate/incorrect assumptions (V/A)	3	H	n/a
ICFR risks and root causes	AR risk 4—AR period end cutoff is incomplete/inaccurate (C)	1	L	n/a
ICFR risks and root causes	AR risk 5 (Fraud)—Accounts receivable (including reserves) fraud schemes occur	2	n/a	M

ACTIVITY-LEVEL RISK FACTOR RATING TABLE GUIDELINES

RISK FACTOR	SUGGESTED GUIDELINES FOR RATING RISK FACTORS	RELEVANT WEIGHT
COMPLEXITY	<p>Complexity as a function of financial statement data compilation or technical knowledge involved in determination of financial statement amount.</p> <ul style="list-style-type: none"> • Low = Routine, complex systems based processing • Medium = Routine, complex process involving significant judgement, experience, or knowledge • High = Nonroutine or estimation, complex processing involving significant judgement, subjectivity, experience, or knowledge 	High
CENTRAL	<p>Centralisation and direct control of processes by upper management (CEO, CFO, Corporate Controller, and so forth)</p> <ul style="list-style-type: none"> • Low = Decentralised process • Medium = Centralised process in which few members of upper management are involved but monitoring is performed (by an oversight committee) • High = Centralised process in which one member or a few members of management are involved and exclusive control over a significant portion of the process exists that affects one or more key accounts or disclosure 	Low

Continued on p.58

Continued from p.57

RISK FACTOR	SUGGESTED GUIDELINES FOR RATING RISK FACTORS	RELEVANT WEIGHT
CHANGE	<p>Change in business systems, personnel involved or new class of transactions</p> <ul style="list-style-type: none"> • Low = Change in single non-management process owner personnel • Med = Change in multiple personnel, affecting low and medium risk areas • High = Change in business systems or a new class of transactions or key process owner—for example, cost accounting manager 	Low
DISTANCE	<p>Distance from corporate headquarters and the degree of senior management oversight</p> <ul style="list-style-type: none"> • Low = Primary location of process is at HQ • Med = A significant amount of the process or class of transactions is affected overseas • High = A material amount of the process or class of transactions is affected overseas 	Low
HISTORY	<p>Time and results of last audit</p> <ul style="list-style-type: none"> • Low = Few exceptions or minor control deficiencies are identified in PY audits • Med = Several exceptions or control deficiencies are identified in PY audits • High = Significant findings are noted in PY audits 	Low
VOLUME	<p>Number of transactions in a given period</p> <ul style="list-style-type: none"> • Low = Annually • Medium = Quarterly or monthly • High = Weekly or daily 	Low
INHERENT RISK	<p>Inherent risk of errors (unintentional errors)</p> <ul style="list-style-type: none"> • Low = History of acceptable performance and unexpected symptoms are rare • Medium = History of occasional occurrence and occasional symptoms exist • High = History of regular occurrence and ongoing symptoms exist 	Low

RISK FACTOR	SUGGESTED GUIDELINES FOR RATING RISK FACTORS	RELEVANT WEIGHT
FRAUD RISK	<p>Fraud risk of errors (intentional errors)</p> <ul style="list-style-type: none"> • Low = Few fraud indicators, history of acceptable performance, symptoms are rare • Medium = Multiple fraud indicators and occasional symptoms exist • High = Multiple fraud indicators, history of occurrence and ongoing symptoms exist 	Low
IMPACT	<p>Misstatement due to risk and ineffective controls could result in material misstatement in financial reporting</p> <ul style="list-style-type: none"> • Low = Impact is not considered to be material • Medium = Impact is considered less than material but an error would warrant further investigation • High = Impact is considered material to the account 	Low

ACTIVITY-LEVEL INHERENT AND FRAUD RISKS

Inherent risks should be stated in terms of the process objective being adversely affected. That is, the assessed likelihood of the risk and impact to the process would result in the business process objective not being achieved and would affect the related financial statement assertion or assertions. For example, '*INV Risk 2***—Inventory estimates not accurate/incorrect assumptions (V/M).*'

Fraud risks are expressed using the Uniform Occupational Fraud Classifications.² For example, '*INV Risk 4 (FR)—Improper inventory reserve valuation (V/M).*' Please note that we have included a library of common risks to financial reporting using a simple naming convention and risk descriptions including the related financial statement assertion to help you with this facet of activity-level risk assessment.

Inherent and fraud risks should be assessed in terms of the likelihood of occurrence based on knowledge of the process and controls.

Many professionals will recommend that you assess the likelihood of the risk or risks assuming that controls do not operate effectively and then reassess the risk assuming that controls are effective. We do not believe this adds value to the risk assessment process. We recommend you assess the likelihood of the risk or risks assuming that controls do operate effectively. Finally, assess the impact to the financial statements based on the likelihood of the risk occurring. Note there may be a residual risk even though controls operate effectively.

Endnotes

- 1 There are several software models available that are designed to support these types of risk management and control systems. Care should be exercised in selecting software, because prices vary widely, implementation can be complex, and embedded methodologies can work against your company's approach.
- 2 Note that specific risks of fraud can be identified using an acceptable framework such as the *Uniform Occupational Fraud Classification System* published by the Association of Certified Fraud Examiners, which can serve to limit the assessment and fraud risk definitions to well defined categories of fraud.

6

UNDERSTANDING AND COMMUNICATING RISK APPETITE

Organisations encounter risk every day as they pursue their objectives. In conducting appropriate oversight, management and the board must deal with a fundamental question: How much risk is acceptable in pursuing these objectives? Added to this, regulators and other oversight bodies are calling for better descriptions of organisations' risk management processes, including oversight by the board. This chapter expands upon the overview of and risk tolerance, materiality, and risk appetite in chapter 2.

The COSO publication *Enterprise Risk Management—Integrated Framework* explicitly states that organisations must embrace risk in pursuing their goals. The key is to understand how much risk they are willing to accept. Further, how should an organisation decide how much risk it is willing to accept? To what extent should the risks accepted mirror stakeholders' objectives and attitudes towards risk? How does an organisation ensure that its units are operating within bounds that represent the organisation's appetite for specific kinds of risk? These questions are embodied in the notion of an entity's 'risk appetite'. The objective of this chapter is to help an organisation—its senior management, board, and key operating personnel—develop and communicate a clear understanding of its risk appetite, both to determine which objectives to pursue and to manage those objectives within the organisation's appetite for risk.

Risk appetite is the amount of risk, on a broad level, an organisation is willing to accept in pursuit of value. Each organisation pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.

Many organisations view risk appetite as the subject of interesting theoretical discussions about risk and risk management, but do not effectively integrate the concept into their strategic planning or day-to-day decision making. We believe that discussions about applying risk appetite go well beyond theory, and that when properly communicated, risk appetite provides a boundary around the amount of risk an organisation might pursue. An organisation with an aggressive appetite for risk might set aggressive goals, while an organisation that is risk-averse, with a low appetite for risk, might set conservative goals.

Similarly, when a board considers a strategy, it should determine whether that strategy aligns with the organisation's risk appetite. When properly communicated, risk appetite guides management in setting goals and making decisions so that the organisation is more likely to achieve its goals and sustain its operations.

ENTERPRISE RISK MANAGEMENT AND DECISION MAKING

ERM is not isolated from strategy, planning, or day-to-day decision making. Nor is it about compliance. ERM is part of an organisation's culture, just as making decisions to attain objectives is part of an organisation's culture.

To fully embed ERM in an organisation, decision makers must know how much risk is acceptable as they consider ways of accomplishing objectives, both for their organisation and for their individual operations (division, department). For example, one CEO recently reported that his organisation needed to increase its risk appetite amid expectations that key measures of its profitability would fall or stagnate. A financial organisation with a lower risk appetite might choose to avoid opportunities that are more risky but offer greater returns. Finally, another organisation with a high risk appetite might decide to procure natural resources from a volatile country where the total investment could be wiped out at the whim of the political leader. The rewards may be high, but so too may the risks. Organisations make decisions like these all the time. Only if they clearly think about their risk appetite can they balance risks and opportunities.

An organisation must consider its risk appetite at the same time it decides which goals or operational tactics to pursue. To determine risk appetite, management, with board review and concurrence, should take three steps:

1. Develop risk appetite
2. Communicate risk appetite
3. Monitor and update risk appetite

These three steps are discussed briefly in the next three paragraphs, and in detail in the rest of this chapter.

Develop Risk Appetite

Developing risk appetite does not mean the organisation shuns risk as part of its strategic initiatives. Quite the opposite. Just as organisations set different objectives, they will develop different risk appetites. There is no standard or universal risk appetite statement that applies to all organisations, nor is there a 'right' risk appetite. Rather, management and the board must make choices in setting risk appetite, understanding the trade-offs involved in having higher or lower risk appetites.

Communicate Risk Appetite

Several common approaches are used to communicate risk appetite. The first is to create an overall risk appetite statement that is broad enough yet descriptive enough for organisational units to manage their risks consistently within it. The second is to communicate risk appetite for each major class of organisational objectives. The third is to communicate risk appetite for different categories of risk.

Monitor and Update Risk Appetite

Once risk appetite is communicated, management, with board support, needs to revisit and reinforce it. Risk appetite cannot be set once and then left alone. Rather, it should be reviewed in relation to how the organisation

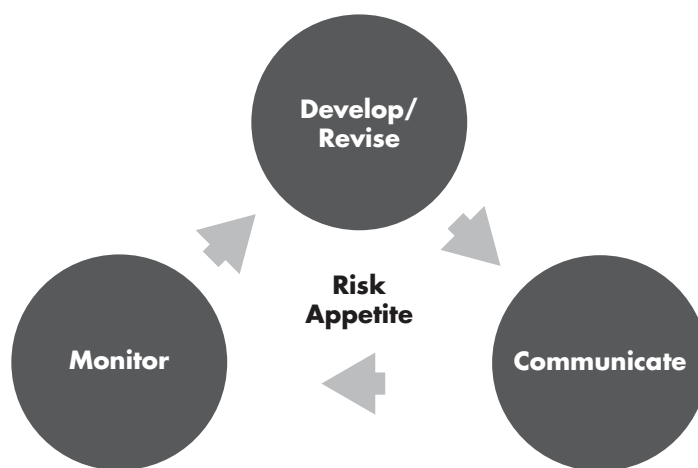
operates, especially if the entity's business model changes. Management should monitor activities for consistency with risk appetite through a combination of ongoing monitoring and separate evaluations. Internal auditing can support management in this monitoring. In addition, organisations, when monitoring risk appetite, should focus on creating a culture that is risk-aware and that has organisational goals consistent with the board's.

CAN IT BE DONE?

This is a common question. Its tone implies two things: (1) articulating risk appetite is too difficult, and (2) risk is considered when management sets strategies, and to further communicate risk appetite is an exercise that simply adds overhead and does not contribute to organisational growth.

Recent world events—involving governments, businesses, not-for-profit organisations, and the recent financial crisis—clearly show that having a communicated risk appetite built into organisational activities could have preserved a considerable amount of capital. We all know the costs of failing to manage risk. Examples include the cost to companies and travellers when air travel closed down after a volcanic eruption in 2010 in Iceland; the cost of the financial crisis to US taxpayers, stockholders, and debt holders; and the social cost of government budgets in Greece, Spain, Ireland, and Portugal.

Perhaps organisations are still tied to the old-school thinking that 'It will not happen here.' The easy rebuttal is that it has happened somewhere, so all organisations should work to manage their risks within their risk appetite. Rather than asking 'Can it be done?' let's say 'Let's get it done.' Determining risk appetite is an element of good governance that managements and boards owe to stakeholders.



OVERVIEW

Risk Appetite Is an Integral Part of Enterprise Risk Management

COSO's Enterprise *Risk Management—Integrated Framework* defines risk appetite as follows:

The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. ... Risk appetite guides resource allocation. ... Risk appetite [assists the organisation] in aligning the organisation, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks.¹

This definition raises some important points. Risk appetite

- is strategic and is related to the pursuit of organisational objectives;
- forms an integral part of corporate governance;
- guides the allocation of resources;
- guides an organisation's infrastructure, supporting its activities related to recognising, assessing, responding to and monitoring risks in pursuit of organisational objectives;
- influences the organisation's attitudes towards risk;
- is multi-dimensional, including when applied to the pursuit of value in the short term and the longer term of the strategic planning cycle; and
- requires effective monitoring of the risk itself and of the organisation's continuing risk appetite.

As an organisation decides on its objectives and its approach to achieving strategic goals, it should consider the risks involved, and its appetite for such risks, as a basis for making those important decisions. Those in governance roles should explicitly understand risk appetite when defining and pursuing objectives, formulating strategy, and allocating resources. The board should also consider risk appetite when it approves management actions—especially budgets—strategic plans, and new products, services, or markets (in other words, a business case).

In working towards their objectives, organisations choose strategies and develop metrics to show them how close they are to meeting those objectives. Managers are motivated to achieve the objectives through reward and compensation programmes. The strategy is then operationalised by decisions made throughout the organisation. Decisions are made to achieve the objectives (increase market share, profitability, and the like). But achieving objectives also depends on identifying risk and determining whether the risks are within the organisation's risk appetite.

Considerations Affecting Risk Appetite

Risk appetite is not developed in isolation from other factors. An organisation should consider its capacity to take on extra risk in seeking its objectives. It should also consider its existing risk profile, not as a determinant of risk appetite but as an indication of the risks it currently addresses. An overview of the considerations affecting risk appetite is shown in figure 6-1.

Figure 6-1: Overview of Considerations Affecting Risk Appetite



There may be other factors to consider as well. Some organisations may gauge how quickly their competitive environment is changing. A telecommunications company, for example, must anticipate how technology and user preferences will affect product development, making a relevant time frame important.

As an example of high risk appetite, a defence contractor dealing in trucks decided that the risk of being behind in technology was so large that it essentially ‘bet the company’ on developing a vehicle appropriate for the types of wars occurring around the world. If the contractor had been unsuccessful in procuring a new government order, it would have been out of business. The risk appetite was high, but it was understood by all involved in the process.

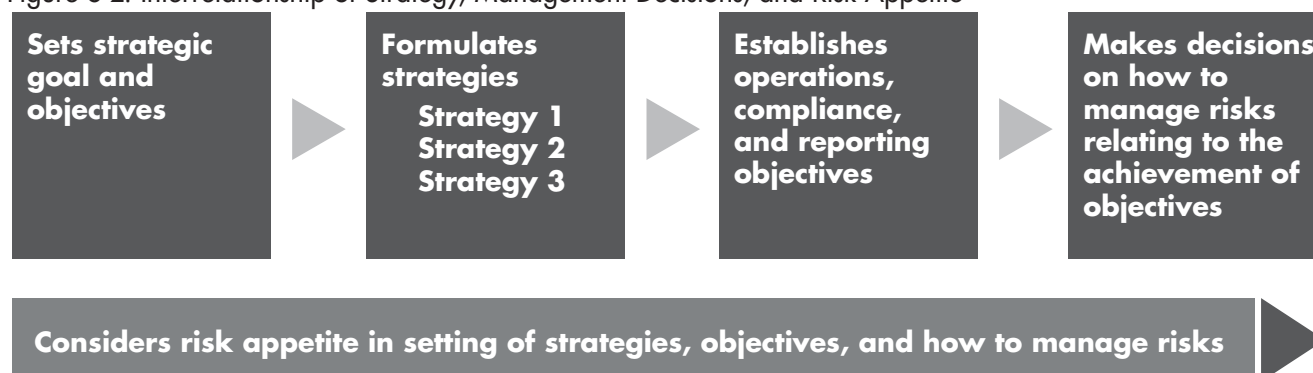
However, the board was well aware of the risks, having debated the issue extensively in board meetings, and it concurred with management’s decision (an acknowledgement of risk appetite and the linkage of risk appetite and strategy). The investing public was also aware because the nature of the risks had been communicated (and the stock dropped to historic lows). What is notable is that the risk was carefully debated and the company was going to succeed or die—as opposed to almost certainly dying (slowly)—if it did not take on risk through an aggressive strategy.

The point is that risk and strategy are intertwined. One does not exist without the other, and they must be considered together. That consideration takes place throughout the execution of the strategy, and it is most important when strategy is being formulated with due regard for risk appetite.

An organisation has a number of goals and objectives it can pursue. Ultimately, it will decide on those that best meet stakeholder preferences for growth, return, safety, sustainability, and its willingness to accept risk. The objectives, in turn, may be pursued using a number of alternative strategies. As shown in figure 6-2, the articulation of a risk appetite provides bounds on the choice of strategies and the operational decisions that are made to pursue those objectives.

One major problem that led to the financial crisis of 2008 was that although organisations had created objectives, there was no articulation of risk appetite or identification of those responsible for the consequences when risks were incurred.

Figure 6-2: Interrelationship of Strategy, Management Decisions, and Risk Appetite



Steps in Adopting Risk Appetite

Each organisation must determine its own risk appetite; there is no single universal risk appetite. But how does an organisation get to the point of having a risk appetite statement that can be communicated through the organisation? And how does risk appetite stay relevant over time?

To effectively adopt risk appetite, an organisation must take three key steps:

1. Management develops, with board review and concurrence, a view of the organisation's overall risk appetite.
2. This view of risk appetite is translated into a written or oral form that can be shared across the organisation.
3. Management monitors the risk appetite over time, adjusting how it is expressed as business and operational conditions warrant.

These three steps are discussed in detail in subsequent sections.

In a recent survey, less than half of the respondents said they had a formal process for developing and communicating risk appetite.²

Risk Appetite Statements

An organisation's risk appetite should be articulated and communicated so that personnel understand that they need to pursue objectives within acceptable limits.

Without some articulation and communication, it is difficult for management to introduce operational policies that assure the board and themselves that they are pursuing objectives within reasonable risk limits. A risk appetite statement effectively sets the tone for risk management. The organisation is also more likely to meet its strategic goals when its appetite for risk is linked to operational, compliance, and reporting objectives.

The length of a risk appetite statement will vary by organisation. Some statements require several sentences to express how much risk is acceptable, while others may be more succinct and still clearly communicate management's appetite for risk. The aim is to balance brevity with the need for clarity.

Characteristics of Effective Risk Appetite Statements

A risk appetite statement is useful only if it is clear and can be implemented across the organisation. As we noted earlier, risk appetite must relate to the pursuit of organisational objectives and must start at the top. In developing and evaluating a statement, the organisation should ensure that risk appetite (see figure 6-3)

- directly links to the organisation's objectives;
- is stated precisely enough that it can be communicated throughout the organisation, effectively monitored, and adjusted over time;
- helps with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risks (discussed in the next section);
- facilitates alignment of people, processes, and infrastructure in pursuing organisational objectives within acceptable ranges of risk;
- facilitates monitoring of the competitive environment and considers shareholders' views in identifying the need to reassess or more fully communicate the risk appetite;
- recognises that risk is temporal and relates to the time frame of the objectives being pursued; and
- recognises that the organisation has a portfolio of projects and objectives, as well as a portfolio of risks to manage, implying that risk appetite has meaning at the individual objective level and at the portfolio level.

Figure 6-3: Using Risk Appetite to Develop a Risk Appetite Statement



Risk appetite should be descriptive enough to guide actions across the organisation. Management and the board should determine whether compensation incentives are aligned with risk appetite, not only for top management but throughout the organisation.

Reluctance to Embrace Risk Appetite

Some organisations are reluctant to develop and communicate risk appetite. Others might argue that risk management did not prevent the financial crisis of 2008 and thus question the usefulness of ERM in general. Others believe that they have expressed their organisation's risk appetite in the normal course of business, and that developing further risk appetite statements will not result in any new approach to managing risk.

Such arguments can be misleading to management and the board. To forgo discussion of an organisation's risk appetite is to assume that everyone will understand vague comments. History shows that when risk appetite is not considered (especially in compensation schemes), the organisation often suffers from greater risks than anticipated. For example, had financial institutions clearly communicated a risk appetite for unsecured mortgage-backed financial instruments, their management and boards would have likely asked questions that would have led to better risk identification, such as the following:

- What if housing failures differ from the historical model?
- What if mortgages fail systematically and are highly correlated to an area we are investing in?
- Could decisions made by some of our operational personnel be creating risks that go beyond our risk appetite?

Risk Appetites Are Not All the Same

Regulators and investors are calling for greater disclosure of risk management processes so that shareholders can better understand not only the risks an organisation faces, but the organisation's appetite for risk and how it manages (or accepts) that risk. For example, a mining company we are aware of clearly identified its risk appetite and risk mitigation procedures for operational risks. At the same time, it decided it could not manage commodity price risk, leaving stakeholders to decide how to consider that risk in developing their portfolios.

To earn an 'adequate' score for overall ERM from some rating agencies, management must be able to articulate risk appetite and assess and reconcile the appropriateness of individual risk limits given to operational management.

Some companies embrace a high appetite for regulatory risk believing that it will lead to greater profitability because regulator fines were significantly lower than the cost of mitigating the compliance risks. One company ignored many health and safety regulations and fines when incurred, but it did not fully understand the magnitude of risks, such as the government shutting down its operations. While the company had a high risk appetite for fines, its lack of appreciation for the risk of shutdown led to a poorly articulated and implemented risk appetite. Organisations can choose to have high or low risk appetites, but those appetites need to consider shareholder interests and the type and magnitude of risks that the organisation needs to manage. We have no preference for a particular level of appetite. Whatever the risk appetite is, it should be stated clearly enough that it can be managed throughout the organisation, and reviewed by the board of directors.

Examples of Risk Appetite Statements

Risk appetite statements often start out broad and become more precise as they cascade into departments and operations across the organisation. Some organisations find that broad statements crafted around terms such as ‘low’, ‘medium’, or ‘high’ appetite meet the characteristics of risk appetite statements listed above. Others are more precise, making statements like ‘We are not comfortable accepting more than a ten per cent probability that we will incur losses of more than a set dollar amount in pursuit of a specific objective.’

Which type of statement is best for a particular entity is a management decision. Some organisations may find terms like ‘low appetite’ clear enough to be communicated and monitored effectively within the organisation. However, such statements are vague and can be difficult to communicate and implement. Often, as organisations become more experienced in risk management, their risk appetite statements will become more precise.

The following examples of risk appetite statements illustrate the characteristics we identified above.

Health Care Organisation: The following represents one part of the health care organisation’s risk appetite statement. The organisation has specific objectives related to (1) quality of customer care, (2) attracting and retaining high-quality physicians and health researchers, and (3) building sustainable levels of profit to provide access to needed capital and to fund existing activities. The statement starts as follows:

The Organisation operates within a low overall risk range. The Organisation’s lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.

This risk appetite statement does three things effectively:

- Communicates, with sufficient precision, that the organisation wants to sustain its business over a long period of time
- Expresses a low risk appetite in pursuing all the organisation’s objectives
- Expresses a very low appetite for risks associated with employee safety and compliance

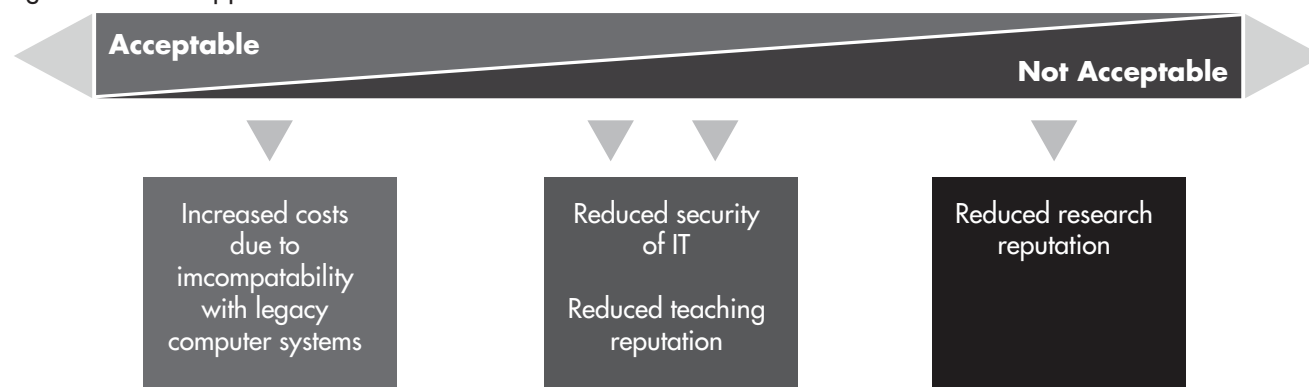
‘Business performance can be increased if capital and resources are allocated more effectively, reflecting the balance of risks and rewards in a more integrated and dynamic fashion. In that respect, risk appetite can be considered the cornerstone of modern approaches to bank management, such as value-based management (VBM) and its various implementations.’³

University: The university’s main objective is to continue as a preeminent teaching and research university that attracts outstanding students and is a desired place of work for top faculty.

The university’s risk appetite statement acknowledges that risk is present in almost every activity. The critical question in establishing the risk appetite was ‘How willing is the university to accept risk related to each area?’ In thinking through the process, members of management used a continuum (figure 6-4) to express risk

appetite for the university's major objectives (teaching, research, service, and operational efficiency). They placed various risks along the continuum as a basis for discussion at the highest levels.

Figure 6-4: Risk Appetite Continuum



From an operational viewpoint, for example, management assigned a high risk appetite to the cost of computer incompatibility, a more moderate risk appetite to issues of teaching excellence, a low risk appetite to information system security, and a very low risk appetite to its reputation as a leading research organisation.

The university found that ordering its risk appetites across the continuum helped it shape a risk statement. Putting this into practice, the university

- exhibited a higher risk appetite when approving a new computer system that offered greater processing capacity but also had potential compatibility issues with legacy systems;
- exhibited a low risk appetite for significant breaches of security or unauthorised access to classified records (the new system was viewed as better controlled than the legacy system, thus supporting the decision to approve the new system);
- expressed a moderate risk appetite for teaching quality; and
- expressed a very low risk appetite for risks that would significantly reduce its research reputation.

This example illustrates how risk appetite and strategy interact at the highest levels of an organisation. The discussion of risk appetite guided the university's strategies for dealing with issues such as budget cuts and their effect on teaching, research, service, and operations.

Financial Services Organisation: This company considers quantitative measures to be part of setting risk appetite, and it focuses on economic capital as a primary measure. The company manages its financial operations to attain a reasoned relationship between risk and return, which serves as a guideline for acceptable credit risks, market risks, and liquidity risks. The company's business operations also involve risks related to strategic, reporting, compliance, and operations objectives.

This organisation's view of risk appetite specifies not only risk appetite but also acceptable tolerances around that risk appetite that require action to be taken. For example, the company communicates its risk appetite for loan impairment losses by stating that such losses should not exceed 0.25 per cent of the loan portfolio. The company has a low tolerance for exceeding this level, and significant remediation is expected should losses go beyond 0.28 per cent. The same company has a low risk appetite related to its insurance business, stating that claims incurred should be no more than 70 per cent of insurance premium revenue.

This organisation reviews its risk appetite annually, adjusting it by type of risk and setting target values for risk-specific indicators in light of the economic cycle and market prospects. The board reviews the risk appetite and associated policies whenever the economic outlook changes significantly.

RISK APPETITE AND RISK TOLERANCE

Risk tolerance relates to risk appetite but differs in one fundamental way: risk tolerance represents the application of risk appetite to specific objectives. Risk tolerance is defined as

The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.⁴

While risk appetite is broad, risk tolerance is tactical and operational. Risk tolerance must be expressed in such a way that it can be

- mapped into the same metrics the organisation uses to measure success;
- applied to all four categories of objectives (strategic, operations, reporting, and compliance); and
- implemented by operational personnel throughout the organisation.

Because risk tolerance is defined within the context of objectives and risk appetite, it should be communicated using the metrics in place to measure performance. In that way, risk tolerance sets the boundaries of acceptable performance variability. A simple example in the financial industry would be to state an appetite for risks associated with collateralised debt obligations (CDO) where the CDOs are divided into tranches reflecting the estimated credit worthiness of the underlying debt. An entity buying these CDOs may set minimum risk rating levels for these tranches and then set a tolerance reflecting the maximum downside risk that is acceptable.

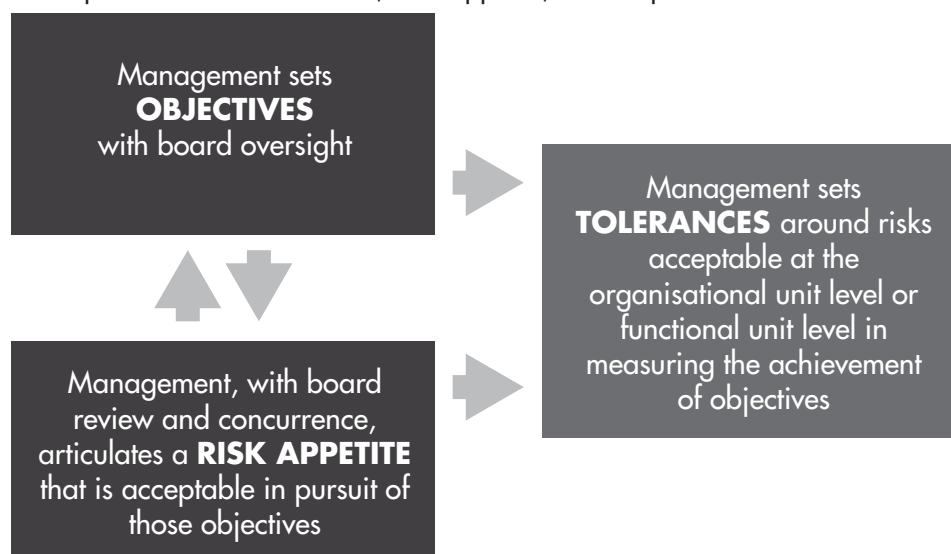
Risk tolerances guide operating units as they implement risk appetite within their sphere of operation. Risk tolerances communicate a degree of flexibility, while risk appetite sets a limit beyond which additional risk should not be taken.

Some tolerances are easy to express in qualitative terms. For example, an organisation may have a low risk appetite for non-compliance with laws and regulations and may communicate a similarly low tolerance for violations—for example, a zero tolerance for some types of violations and slightly higher tolerances for other types of violations.

Or tolerance may be stated in quantitative terms. A company could say that it requires backup on its computer systems so that the likelihood of computer failure is less than 0.01 per cent.

Risk tolerances are always related to risk appetite and objectives (figure 6-5). Tolerances can apply to detailed areas such as compliance, computer security, product quality, or interest rate variability. Risk appetite and risk tolerances, together with objectives, guide the organisation's actions.

Figure 6-5: Relationship Between Risk Tolerance, Risk Appetite, and Objectives



Most organisations have multiple operational objectives related to profitability, some of which might create additional or complementary risks. For example, the managers of an aerospace company might want to improve a product's profitability but know the company has a low risk appetite for not meeting client expectations. They know they cannot reduce product costs if such changes would decrease performance. For example, the company might use new technology, but it cannot use inferior components.

To further illustrate, assume management and the board have set specific profit objectives by product line—for example, maintain a specific gross margin or return on capital for the product line. But they have communicated a low risk appetite for product failure, for loss of customers because of product quality or delivery, and for potential lawsuits related to product design or performance. The articulation of risk tolerances helps guide the company's operational development.

Linking Risk Appetite and Risk Tolerance

The following examples illustrate the relationship between risk appetite and related risk tolerances.

Aerospace Supplier: This company translates its risk appetite statement into tolerances for operational implementation. A high-level objective is to grow by 8 per cent a year (revenue and operating earnings) by working with customers to improve products and market share. Because of the long-term nature of its supply arrangements and product development, the company has communicated the broad parameters of its risk appetite, which then cascade into risk tolerances relating to operations, reporting, and compliance, as shown below. While the company seeks to grow at this rate, acquisitions should not put the company's capital structure at risk. There is a low risk appetite for allowing the capital structure to be so leveraged that it hinders the company's future flexibility or ability to make strategic acquisitions.

Operations Tolerances

- Near zero risk tolerance for product defects
- Low risk tolerance for sourcing products that fail to meet the company's quality standards

- Low, but not zero, risk tolerance for meeting customer orders on time, and a very low tolerance for failing to meet demands within a defined number of days
- High risk tolerance for potential failure in pursuing research that will enable the company's product to better control, and increase the efficiency of, energy use

Reporting Tolerances

- Low risk tolerance concerning the quality, timing, and accessibility of data needed to run the business
- Very low risk tolerance concerning the possibility of significant or material deficiencies in internal control
- A low risk tolerance related to financial reporting quality (timeliness, transparency, GAAP, and so forth)

Compliance Tolerances

- Near zero risk tolerance for violations of regulatory requirements or the company's code of ethics

Company management has been comfortable communicating risk appetite through its actions and performance reviews. However, as the company has grown, it has found that the risk appetite is not fully understood, especially among new operational units. Nor is it understood that policies relate to objectives and are often designed to minimise the risks involved in pursuing those objectives. One division, for instance, failed to follow a company policy because it did not fully understand that the policy was in place to mitigate a significant risk, thus leading to losses. Linking the policy to the risk and risk appetite would have led to better mitigation of the underlying risks.

University: The university in our earlier example has a very low appetite for risk associated with its research reputation. However, given budget shortages, the university also knows it cannot make the same commitment to research and teaching as in the past. The organisation has expressed a higher risk appetite for actions resulting in lower-quality teaching. In other words, research that leads to better understanding and innovation is extremely important, but the quality of teaching, though important, is an area where the university can accept more risk for potential decreases.

The university communicated its risk appetite in broad terms, both through the university and, as a public institution, within the state. However, to operationalise the risk appetite within each of its schools, the university had to express risk tolerances for the two key objectives of excellence in research and teaching—while dealing with a 10 per cent budget decrease. The risk tolerances were expressed as follows.

Research: Tolerance Statements Consistent With Low Risk Appetite

- The university does not expect any decrease in the nature, quality, or number of publications related to its research mission.
- The university does not expect any decrease in the number or dollar value of outside research grants generated by faculty.

Teaching: Tolerance Statements Consistent With Moderate Risk Appetite

- Student teaching evaluations should not decline by more than 5 per cent.
- Where individual schools within the university are ranked by outside evaluators on student preparedness and quality of students, there should be no more than a 5 per cent decline.

- The calibre of students wanting to attend the university should not decline by more than 2 per cent, as measured by standard university admissions data such as test scores, percentile ranking in high school graduating class, or extent of community service before attending university.

The idea behind the risk tolerances is that if the university falls below any of the measures, corrective action will take place. Corrections will come not from adjusting the risk appetite but from reassessing the risk appetite and the strategies the university has implemented in the context of the risk appetite.

Examples of Risk Tolerance Statements

The following examples from organisations show how risk tolerance might be stated and aligned with broader risk appetite.

RISK APPETITE	RISK TOLERANCE
The organisation has a higher risk appetite related to strategic objectives and is willing to accept higher losses in the pursuit of higher returns.	While we expect a return of 18 per cent on this investment, we are not willing to take more than a 25 per cent chance that the investment leads to a loss of more than 50 per cent of our existing capital.
The organisation has a low risk appetite related to risky ventures and, therefore, is willing to invest in new business but with a low appetite for potential losses.	We will not accept more than a 5 per cent risk that a new line of business will reduce our operating earnings by more than 5 per cent over the next ten years.
A health services organisation places patient safety amongst its highest priorities. The organisation also understands the need to balance the level of immediate response to all patient needs with the cost of providing such service. The organisation has a low risk appetite related to patient safety but a higher appetite related to response to all patient needs.	We strive to treat all emergency room patients within 2 hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (5 per cent of the time) patients in need of non-life-threatening attention may not receive that attention for up to four hours.
A retail company has a low risk appetite related to the social and economic costs for sourced products from foreign locations that could be accused of being child sweatshops or having unhealthy working conditions.	For purchasing agents, the risk tolerance is set at near zero for procuring products that do not meet the organisation's quality and sourcing requirements.
A manufacturer of engineered wood products operates in a highly competitive market. To compete, the company has adopted a higher risk appetite relating to product defects in accepting the cost savings from lower-quality raw materials.	The company has set a target for production defects of 1 flaw per 1,000 board feet. Production staff may accept defect rates up to 50 per cent above this target (ie, 1.5 flaws per 1,000 board feet) if cost savings from using lower-cost materials is at least 10 per cent.

DEVELOPING RISK APPETITE

We have identified the characteristics of an effective risk appetite statement and noted how those characteristics are useful in managing risk. We have also examined the relationship between risk appetite and risk tolerances. Now we will discuss how an organisation can bring out the many ‘implicit feelings’ that management and the board may have about what they believe is the organisation’s risk appetite and how discussion of those feelings leads to development of risk appetite.

Developing a risk appetite is not an end in itself and should not require an inordinate amount of time. Remember the purposes of risk appetite are

- to provide effective communication throughout the organisation in order to drive the implementation of enterprise risk management;
- to change discussions about risk so that they involve questioning of whether risks are properly identified and managed within the risk appetite; and
- to provide a basis for further discussion of risk appetite as strategies and objectives change.

Also, keep in mind that any expression of risk appetite must be preceded by a discussion of strategies and objectives. The risk appetite must be linked to those objectives.

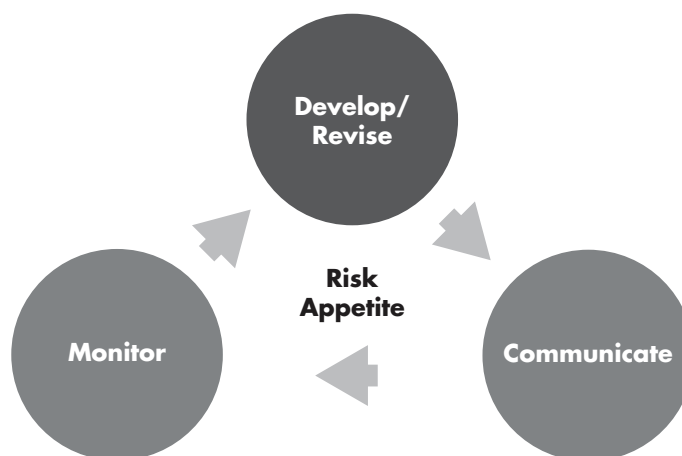
Management and boards often use one of three approaches to discuss and develop their risk appetite:

(1) facilitated discussions, (2) discussions related to objectives and strategies, or (3) development of performance models.

Facilitated Discussions

Facilitated discussions can be very effective for a variety of organisations. After several iterations, management and the board can develop a risk appetite statement that reflects the combined views of the organisation’s leadership and governance bodies.

The major advantage of this approach is that the facilitators encourage management and the board to clearly prioritise their objectives and their risk appetite. In addition, various scenarios can be discussed to see how the risk appetite would influence decision making throughout the organisation. When discussing risk appetite, those involved should keep the organisation’s strategic plan, including goals and mission, at the forefront.



Developing risk appetite is about managing the organisation. It is not about developing a statement to be filed in a report. There are many ways to create a clear statement of risk appetite. Organisations should identify the parameters of their risk appetite along key strategic, operational, reporting and compliance objectives.

A questionnaire can help capture views on risk appetite and business scenarios. Exhibit 6-1 shows an example. Note that the questions are broad and should be tailored to the unique factors that drive an organisation's success.

Discussions Related to Objectives and Strategies

Often the risk appetite an organisation is willing to accept becomes more evident when management considers major issues facing the organisation, such as new product lines, acquisitions or joint ventures. Management of organisations with a lower risk appetite will usually react differently to acquisition, expansion, competition, and market volatility than will peers with a higher risk appetite. Reviewing and assessing these reactions can provide insight into the organisation's current risk appetite.

This approach allows management to go the extra step in discussing major strategies because it asks what the perceived risks are in pursuing objectives. The board then reviews and supports management's identification and communication of risk appetite as it relates to specific objectives.

Exhibit 6-1: Questions to Facilitate Discussion of Risk Appetite at Management and Board Level

1. On a scale of 1 to 10, with 1 being the lowest, describe what you believe the organisation's overall risk appetite has been and what you think it should be. Explain any differences between what you perceive it has been and what you believe it should be. Relate this to your number 1 strategic goal.
2. Various operations help an organisation achieve its objectives. Using the categories below, or other categories consistent with the organisation's operations, rate the desired risk appetite related to the following (rating can be broad, such as high, medium, or low, or precise, such as specific metrics that should not be exceeded):
 - a. Meeting customer requirements
 - b. Employee health and safety
 - c. Environmental responsibility
 - d. Financial reporting
 - e. Operational performance
 - f. Regulatory compliance
 - g. Shareholder expectations
 - h. Strategic initiatives/growth targets

As you rate each category, indicate areas where you believe the organisation is taking either too much or too little risk in pursuing its objectives.

3. How would you rate the effectiveness of the organisation's process for identifying, assessing, managing, and reporting risks in relation to the overall risk appetite? What are the major areas for improvement?
4. Are management's strategies communicated sufficiently for there to be meaningful discussion of risk appetite in pursuit of those strategies, both at the broad organisational level and at the operational level, and for consistency to be analysed?
5. How satisfied are you that the board is providing effective oversight of the risk appetite through its governance process? This includes board committees and/or the board itself to help set the appetite and to monitor over time that management is adhering to the overall risk appetite in pursuit of value.
6. Whom do you see as more accepting of risk, or more willing to take risks to meet the goals of the organisation?
 - a. Management
 - b. Board
 - c. Management and board have similar levels of acceptable risk
7. Does the organisation motivate management (senior management and operational management) to take higher than desired risks because of the compensation plans in place? If yes, how do you believe the compensation plans should be modified to bring approaches for generating high performance within the risk appetite?
8. What do you believe the organisation should do?
 - a. Reduce its risk appetite
 - b. Increase its risk appetite
 - c. Make no change
9. Do you believe there are risks considered to be above the organisation's existing risk appetite that need to be reduced? In other words, are there areas where the risk appetite, as currently used, is too low?
10. What risks over the past five years were, in your view, above the organisation's risk appetite? Were the risks understood when a strategy was developed? How could management have communicated its risk appetite so that the board could both (a) evaluate the risk appetite and (b) provide proper oversight? How could management have communicated its risk appetite so as to hold operational units to actions consistent with the risk appetite?

One advantage to this approach is that the board can be seen as supporting or challenging management's risk appetite. Another is that management gains a sense of the board's risk appetite for specific strategies and can incorporate that knowledge into a risk management process. The major disadvantage of this approach is that it can be less comprehensive. It often does not generate the specificity needed for the organisation's day-to-day activities.

Development of Performance Models

Some organisations, particularly financial institutions, use quantitative measures to express their overall risk appetite. They often arrive at these measures through performance modelling.

A company could, for instance, use economic capital to express risk appetite. Economic capital is the amount of capital a financial institution needs to remain solvent. This determination is based both on regulatory requirements and on management's assessment of how much economic capital the institution needs to retain.

As an example, management might set its economic capital at 6 per cent of total assets. As the organisation models different scenarios of economic activity, economic situations and its asset portfolio, it needs to set some probability around the ability to maintain economic capital. A management and board with a low risk appetite might want to be 99.9 per cent confident (999 out of 1,000 model results) that economic activities will not place the institution below its desired level of economic capital. A company with a higher risk appetite might start with the same dollar amount but require a confidence level of only 95 per cent (950 out of 1,000 model results). Thus, risk appetite can be composed of both dollar elements and probability elements.

As part of developing (and monitoring) risk appetite, a company may model its overall risk profile. This involves taking 'bottom-up' risk information and developing models that consider company-specific risks, including industry factors and broad economic factors, to create a calculated risk profile. The profile can then be compared to the overall risk appetite, helping management and the board to discuss how much risk the organisation is prepared to accept. Some organisations also review key ratios from peer companies and industries to gain more input into the risk level suitable for their organisation.

Modelling is typically only one part of the process of setting risk appetite. For one thing, an organisation needs considerable data to prepare these calculations. For another, there are usually certain risks that are difficult to quantify and model with precision. Management and the board still need to debate and discuss the levels above which capital at risk is seen to be too high and in excess of appetite.

COMMUNICATING RISK APPETITE

Once an overall risk appetite is developed, management must then choose the right mechanism for communicating it. As we noted earlier, risk appetite statements will vary, and organisations may communicate risk appetite at various levels of detail or precision. The point is that each organisation should determine the best way to communicate risk appetite to operational leaders in a specific enough manner that the organisation can monitor whether risks are being managed within that appetite.

To be effective, risk appetite must be

- operationalised through appropriate risk tolerances;
- stated in a way that assists management in decision making; and
- specific enough to be monitored by management and others responsible for risk management.

We have encountered three main approaches for communicating risk appetite: (1) expressing overall risk appetite using broad statements, (2) expressing risk appetite for each major class of organisational objectives, and (3) expressing risk appetite for different categories of risk.

Broad Risk Appetite Statement

Organisations that communicate overall risk appetite in broad terms may develop high-level statements that reflect acceptable risk levels in pursuing their objectives.

Some organisations use graphics, like those in figure 6-6, in discussing risk appetite. A common approach is to apply some form of colour banding within a heat map that indicates acceptable versus unacceptable risk levels. With this approach, risks are grouped by objective, summarised and then plotted on the risk map. The organisation sets either the assessment criteria or the location of the colour banding to express higher versus lower risk appetites. For instance, the heat maps on the right show that risks related to objectives 1 and 2 would exceed the appetite of a company with a low risk appetite, but not necessarily that of a company with a high risk appetite. Risks related to objective 3 would exceed the appetite of both companies. (See appendix C for more sample heat maps.)

The advantage of this approach is that it is simple to convey the level above which risks are seen as unacceptable. We also find that discussions with management and the board on the relative positioning of the bands can draw out important differences between management's and the board's views on desired risk appetite.

The broad descriptions are effective when they are partitioned to show that not all objectives have the same risk appetite.

Risks Related to Organisational Objectives

Organisations that communicate risk appetite for each major class of organisational objectives are likely to communicate risk appetite in some form of statement. Consider the risk appetite statement from the health care organisation we referred to earlier:

The Organisation operates within a low overall risk range. The Organisation's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.

Figure 6-6: Colour Banding in Heat Maps

Low Risk Appetite

Catastrophic					3
Major					
Moderate			1		
Minor					2
Insignificant	4				
	Almost never	Unlikely	Possible	Likely	Almost certain

High Risk Appetite

Catastrophic					3
Major					
Moderate			1		
Minor					2
Insignificant	4				
	Almost never	Unlikely	Possible	Likely	Almost certain

The advantage of this approach is that it allows for more delineation between the levels of acceptable risk for each class of objectives. It does not, for instance, treat risks related to legal compliance the same way as risks related to operations. This approach may also help with decision making, especially if resources are limited and need to be allocated across a company's organisational units. Another advantage is that viewing risks in relation to classes of objectives requires less effort than, say, the third approach below. The challenge is to develop a statement that accommodates specific risk types that should be viewed differently in terms of acceptable level of risk.

Categories of Risk

The third option is to communicate appetite for categories of risk. Some organisations use broad, generic risk categories, such as economic, environmental, political, personnel, or technology, in their risk appetite statements. Others use more tailored risk categories that apply to their field. For example, a company in information processing may group risks related to system availability, data security and privacy, system scalability, system design, and release management.

A mining company we are aware of has specific objectives for cash flow and capital structure that include maintaining low volatility of cash flow. There are many causes of cash flow volatility, ranging from operations to uncertain commodity prices. Management believes that investors understand commodity price risk, and it has pursued objectives that enable the company to benefit from price increases while being exposed to losses from price decreases. Management believes that this price risk—even though it can result in volatile earnings—is within the appetite of the organisation (and its stakeholders). Therefore, the company has not attempted to mitigate this exposure through a commodity price hedge programme. Conversely, the same company is unwilling to accept a similar level of cash flow volatility caused by production delays, and it has adopted rigorous processes to maintain steady production.

The advantage of communicating risk appetite according to categories of risk is that management can exercise judgement about acceptable levels given the unique considerations of each group of risks. By allowing for greater judgement, this approach reduces the perception that risk management is overly prescriptive.

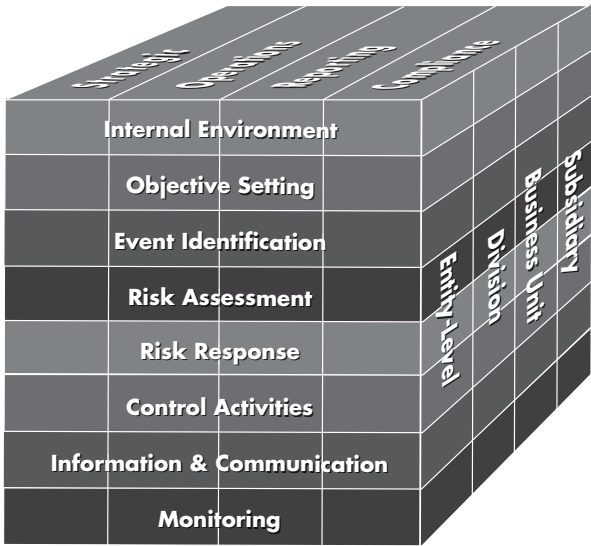
Risk Appetite Cascades Through the Organisation

The method of communicating a risk appetite statement is important, but so is the ability to communicate that statement across the organisation in a way that ensures operations are consistent with the risk appetite. It is especially important for those who pursue the operational tactics related to organisational objectives—local sales forces, country managers, strategic business units—to clearly understand and be aligned with risk appetite.

All too often, the risk appetite and tolerances set by the organisation are not adhered to or understood in context by those managing the day-to-day business and facing customers and potential risks every day.

Risk appetite needs to be communicated by management, embraced by the board and then integrated across the organisation. The ERM framework is often depicted as a cube (see figure 6-3). It is important not to overlook the side of the cube, which shows that all units must understand the organisation's risk appetite and related risk tolerances.

Risk appetite and risk tolerances are set across the organisation. Risk appetite is set at the highest level of the organisation in conjunction with goals and objectives. As risk appetite and objectives are communicated throughout the organisation (subsidiary, division, or business unit level) the strategic goals and risk appetite are expressed in more specific performance terms. Strategies are reflected in performance objectives, and risk appetite is expressed in terms of risk tolerance. The more precise articulation of performance objectives and risk tolerances helps management to identify situations where corrective actions are needed. Performance metrics and risk tolerances that are more specific lend themselves to better monitoring.



MONITORING AND UPDATING RISK APPETITE

Once an organisation’s risk appetite is developed and communicated, management, with board support, must revisit and reinforce it. Risk appetite cannot be set once and then left alone for extended periods. Rather, it should be reviewed and incorporated into decisions about how the organisation operates. This is especially important if the organisation’s business model begins to change.

Management cannot just assume that responsible individuals will implement risk management within the appropriate risk appetite. Therefore, some organisations will review the application of risk appetite through a series of monitoring activities. Management should monitor the organisation’s activities for consistency with risk appetite through the specifics identified with risk tolerances. Most organisations have key performance risk metrics that they use to measure performance. It is easy to integrate risk tolerances into the monitoring process used to evaluate performance. Internal auditing can provide independent insight on the effectiveness of such processes.

Creating a Culture

For many organisations, monitoring risk tolerances requires a culture that is aware of risk and risk appetite. Management, by revisiting and reinforcing risk appetite, is in a position to create a culture whose organisational goals are consistent with the board’s, and to hold those responsible for implementing risk management within the risk appetite parameters.

Many organisations are effective at creating a risk-aware culture: a culture that emanates from senior management, cascades through the organisation and is supported by the board. In an effective culture, each member of the organisation has a clear idea of what is acceptable, whether in relation to behaving ethically, pursuing the wrong objectives, or encountering too much risk in pursuing the right objectives.



Creating a culture is one way of reinforcing overall risk appetite. The approach is best used when the organisation has a well-communicated risk appetite and associated risk tolerances, to the point at which the following outcomes exist:

- Consistent implementation across units
- Effective monitoring and communication of risk and changes in risk appetite
- Consistent understanding of risk appetite and related tolerances for each organisational unit
- Consistency between risk appetite, objectives, and relevant reward systems

This approach draws on ongoing and separate evaluations conducted as part of the organisation's monitoring. The individuals doing the monitoring consider whether the objectives being set and the risk response decisions being made are consistent with the organisation's stated risk appetite. Any variation from the stated (or desired) risk appetite is then reported to management and the board as part of the normal internal reporting process.

ROLES

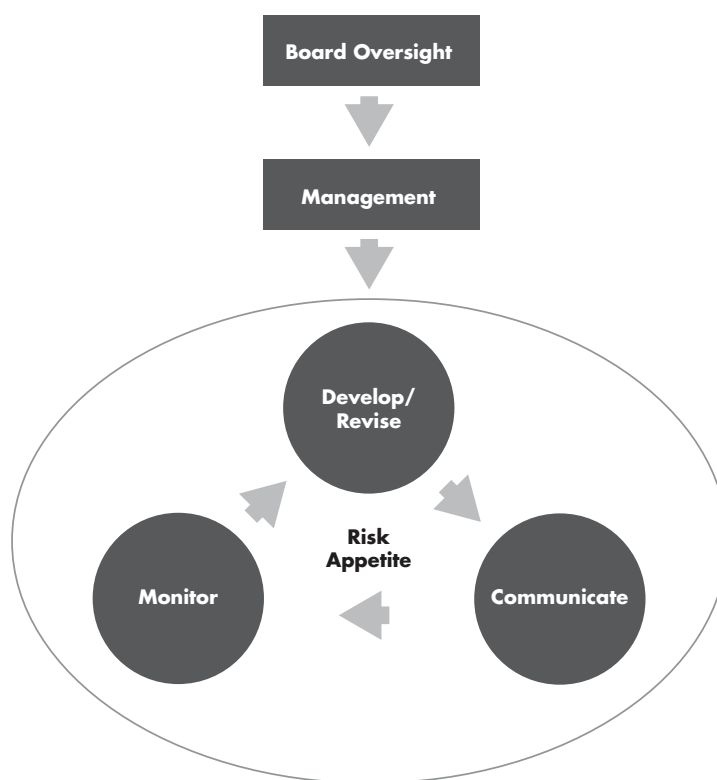
It is management's role to develop the risk appetite and to obtain the board's agreement that the risk appetite is suitable for the organisation. We believe that the board is in place to oversee management and to monitor the broader risk management process, including whether the organisation is adhering to its stated risk appetite. Any board, serving any organisation of any size or structure (for-profit, not-for-profit, private), has a fiduciary responsibility to question management's development and implementation of a risk appetite and to require changes if it believes the risk appetite is either badly communicated or inconsistent with shareholder values.

Effective board oversight of an organisation's risk appetite should include

- clear discussion of the organisation's objectives and risk appetite;
- oversight of the organisation's compensation plan for consistency with risk appetite;
- oversight of management's risk identification when pursuing strategies to determine whether the risks exceed the risk appetite;

- oversight of strategies and objectives to determine whether the pursuit of some objectives may create unintended consequences or organisational risks in other areas; and
- a governance structure that requires regular conversations on risk appetite, through the board and board committees, concerning matters such as strategy formulation and execution, M&A activity and business cases to pursue major new initiatives.

Governance does not stop with board oversight. It includes management's development of the infrastructure for risk management and the allocation of resources across the organisation. Exhibit 6-2 is a summary of matters for the board and management to consider in evaluating how effective their processes are for developing, communicating and monitoring risk appetite.



Boards are very good at questioning strategies. They are only a step away from addressing meaningful questions that can help with setting the organisation's risk appetite. For example, when the board asks how much an organisation should pay for an acquisition, it is an expression of risk appetite.

Exhibit 6-2: Board and Management Responsibilities

1. **Management establishes risk appetite:** An organisation cannot know how well it is managing risk unless it establishes ranges of acceptable risk it can take in pursuit of its objectives. In doing so, management must effectively and clearly communicate:
 - a. Goals and objectives
 - b. Strategies
 - c. Metrics (to know whether objectives are being achieved)
 - d. Relevant time periods for pursuing the objectives
 - e. Ranges of risk the organisation is willing to take in pursuing the objectives
2. **Board oversees risk appetite:** Oversight of the risk appetite (or acceptable ranges of acceptable risk) should be considered at the board level in conjunction with the senior management team.
3. **Applies throughout organisation:** Risk appetite needs to be applied regularly throughout all functional units of the organisation. Culture is important: the organisation must work to build the board's view of risk appetite into the organisational culture.
4. **Aligns with stakeholders and managers:** Because individuals are accountable for their results, every organisation needs a robust governance process to ensure that compensation and incentive systems are aligned with the organisation's objectives and are managed to fall within the organisation's risk appetite.
5. **Manages risks and risk appetite over time:** Organisations need to understand that risk appetites may change over time. Boards must be proactive on two levels:
 - a. Communicating their articulation of risk appetite
 - b. Monitoring organisational actions, processes, and the like to determine whether organisational activity has strayed outside the organisation's risk appetite
6. **Monitors to ensure adherence to risk appetite:** Adherence to an organisation's risk appetite, as well as to its risk management processes, should be monitored regularly. The results of the monitoring should be reported to the audit committee or board, or both, and to the relevant members of executive management.
7. **Supports culture:** The tone at the top influences the culture of the organisation. The tone can be either positive or negative in ensuring that risks are managed within acceptable limits. Ideally, prudent risk taking is built into the organisation's culture in its public statement of core values.
8. **Considers resources:** It takes effort to operate within the organisation's risk appetite. Resources must be available and dedicated to operating within this appetite.
9. **Communicates through strategies and objectives:** Risk appetite is communicated effectively only if the organisation can clearly communicate its major strategies and objectives at both the global level and the functional/operational level.
10. **Clearly communicates how much risk the organisation is willing to accept at all levels:** Risk appetite and risk tolerance are complementary concepts. They can be combined to determine acceptable ranges of risk for the organisation.

Risk appetite is developed by management and reviewed by the board. The COSO ERM framework emphasises the board's important role in overseeing risk management. Oversight should begin with a studied discussion and review of management's articulation of risk appetite relative to the organisation's strategies.

SUMMARY OF RISK APPETITE CONSIDERATIONS

The COSO ERM framework sets out five principles related to risk appetite:

1. It is a guidepost in strategy setting.
2. It guides resource allocation.
3. It aligns organisation, people, processes, and infrastructure.
4. It reflects the entity's risk management philosophy and influences the culture and operating style.
5. It is considered in strategy setting so that strategy aligns with risk appetite.

Risk appetite does not exist in a vacuum; rather, it is an integral part of an organisation's strategies for achieving objectives. The concept of risk appetite permeates all organisations, from charities and governments to small businesses and publicly traded corporations.

Endnotes

- 1 COSO, *Enterprise Risk Management—Integrated Framework*, p. 19.
- 2 Towers Watson, *2011 Risk and Finance Manager Survey*.
- 3 IBM, *Risk Appetite: A Multi-faceted Approach to Risk Management*, April 2008.
- 4 COSO, *Enterprise Risk Management—Integrated Framework*, p. 20.

EPILOGUE

Establishing an effective ERM programme requires careful thought and selection of the organisation's ERM concepts and tools and how they are presented and used in a risk assessment workshop. This includes considering the importance of identifying a credible risk management champion to facilitate the risk assessment workshops and draw out the collective wisdom of the management team.

To facilitate the risk assessment workshop a short PowerPoint presentation is available to accompany this book. It explains the key concepts of entity-level versus process-level risk assessment. An Excel workbook is also available. It contains examples of the tools needed to conduct the risk assessment workshop, such as heat maps and how the company determined materiality and incorporated the concepts of control maturity. Visit www.cpa2biz.com/RiskAssessmentDownload to download these resources.

The appendices at the end of this book contain examples of an entity-level risk library, risk assessment tools (heat maps and control maturity models), and guidelines on how to report entity-level risk assessments in the aggregate. In addition, we included an example of how to map the entity-level risk library to operations and support services functions and identify risk owners and risk management gaps.

As discussed earlier, once you complete the initial entity-level risk assessment, detailed follow-up on activity-level risk assessments become a logical extension of your risk management programme. See the discussion in chapter 5, *Activity-Level Risk Assessment*.

REFERENCES

COSO. 'Strengthening Enterprise Risk Management for Strategic Advantage', < www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL.pdf > , accessed 12 Sept. 2013

Federal Reserve Bank of New York. 'Observations on Risk Management Practices During the Recent Market Turbulence', < www.ny.frb.org/newsevents/news/banking/2008/SSG_Risk_Mgt_doc_final.pdf > , accessed 12 Sept. 2013

SEC. 'Risk Management Lessons from the Global Banking Crisis of 2008', < www.sec.gov/news/press/2009/report102109.pdf > , accessed 12 Sept. 2013

Commissioner Luis A. Aguilar, SEC Speech: 'Regulatory Reform That Optimizes the Regulation of Systemic Risk', speech, New York City, NY, 16 Apr. 2010, < <http://www.sec.gov/news/speech/2010/spch041610laa.htm> > , accessed 12 Sept. 2013

Erik Sirri, '*Testimony Concerning Lessons Learned in Risk Management Oversight at Federal Financial Regulators*' before US Congress, Senate, Committee on Banking, Housing, and Urban Affairs; 18 Mar. 2009 < <http://www.sec.gov/news/testimony/2009/ts031809es.htm> > , accessed 12 Sept. 2013

Chairman Mary L. Schapiro, '*Testimony Concerning Regulation of Systemic Risk*', before US Congress, Senate, Committee on Banking, Housing, and Urban Affairs; 23 Jul. 2009, < <http://www.sec.gov/news/testimony/2009/ts072309mls.htm> > , accessed 12 Sept. 2013.

SEC. 'Notice of Filing of Proposed Rules on Auditing Standards Related to the Auditor's Assessment of and Response to Risk and Related Amendments to PCAOB Standards' < <http://www.sec.gov/rules/pcaob/2010/34-62919.pdf> > , accessed 12 Sept. 2013

APPENDIX A: KEY TERMS

compliance. Adherence to policies, plans, procedures, laws, regulations, contracts, or other regulations.

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.

control activity. Policies, procedures, and processes designed to serve as measurable checks to ensure the desired outcome of an objective, whether a corporate objective or information processing objective.

control objective. An explicit statement that defines the purpose of the process such that it is designed to ensure the achievement of an objective.

control deficiency. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.¹

control self-assessment. A technique that allows managers and work teams directly involved in business units, functions, or processes to participate in assessing the organisation's risk management and control processes

fraud. Any illegal act characterised by deceit, concealment, or violation of trust perpetrated to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.

opportunity. Attempting to increase the organisation's value by taking on risk.

risk. The possibility of an event occurring that would negatively affect the achievement of objectives. Can be thought of as the converse of a control objective.

risk appetite. The level of risk that an organisation is willing to take on as part of the objective setting process (that is, opportunities).

risk tolerance. Levels of risk clearly established in a company's internal environment.

Endnotes

- 1 “Public Company Accounting Oversight Board Auditing Standard No. 2.” <http://pcaobus.org/Standards/Auditing/Pages/default.aspx>.

APPENDIX B: SAMPLE RISK LIBRARY

No.	Risk Name	Risk Description (Primary Risk Factors)
1	Business Interruption	Natural disasters, fire, utility supply, infrastructure failure, IT failure, labour, terrorism, industrial sabotage, or counterparty risk
2	Mergers and Acquisitions or Postintegration Risk	Insufficient due diligence, planning, valuation or post-integration
3	Market	Unfavourable market dynamics—for example, customers' inability to produce marketable products or increased competition
4	Geopolitical	Unstable political environment creating unfavourable property rights, labour risks, and so on
5	Attracting Talent	Inability to attract qualified personnel
5.1	Retaining Talent	Inability to retain qualified personnel—for example, employees perceive few career advancement opportunities, or the corporate culture creates exposure to high employee turnover
6	Import and Export Compliance	Compliance risk with various global regulatory departments—In the United States these departments include Office of Foreign Assets Control (OFAC), Export Administration Regulations (EAR), or International Traffic in Arms Regulations (ITAR)
7	Government Contract Compliance	Government contractor compliance violations—for example, charging unallowable costs to contracts
8	Information Security	Compromise of information assets (via internal or external treats) <ul style="list-style-type: none"> • Trade secrets • Employee privacy data • Key financial data
9	Intellectual Property (IP) Infringement	Company sued for IP or patent infringement
10	Obsolescence	Product technological obsolescence
11	Customer Concentration and Distribution	Inability to expand product distribution channels effectively, or existence of high customer concentration
12	Manufacturing	Poor yields, throughput, or quality, or inability to reduce production costs or to balance customer demand versus capacity
13	New Product Introduction	Inability to timely complete or commercialise new product designs or make commercially viable devices
14	Supply Chain	Supply chain interruptions (both internal and external) due to fulfilment challenges and limited source suppliers or overstocking
15	Environmental Health and Safety	Regulatory compliance violations and personal health and safety exposure
16	Physical Assets	Assets not maintained, damaged, or otherwise compromised so that production or physical assets are impaired
17	Regulatory Reporting	Security and Exchange Commission financial reporting, tax compliance reporting, labour reporting, Employee Retirement Income Security Act, statutory reporting, and so on
18	Cash Management	Credit risk (default, concentration, settlement, collateral); liquidity risk (cash flow, opportunity cost, concentration) and price risk (currency, commodity, and so forth)
19	Contractual	Compromised legal or contractual relations—for example, vendors or subcontractors don't comply with contract commitments, or there are sales or distribution contract violations
20	Corruption	Conflicts of interest, bribery, illegal gratuities, or economic extortion
21	Asset Misappropriation	Loss of cash, inventory or other assets
22	Financial Statement Fraud	Intentional asset or liability overstatement or understatement, or improper expense or revenue recognition
23	Information Systems	Inability to capture or retain access or to disseminate critical information needed to effectively and efficiently run the business and create competitive advantage

APPENDIX C: SAMPLE HEAT MAPS

Enterprise Risk Assessment Scale (1 to 25)

> \$_____ million(m)	■	Very material: May affect company's ongoing existence
> \$_____ m - \$_____ m	■	Material: Difficult to achieve multiple objectives
> \$_____ k - \$_____ m	■	Significant: More challenging to achieve some objectives
> \$_____ k - \$_____ k	■	Inconsequential: May have some undesirable outcomes
< \$_____ k	■	Trivial: No noticeable impact on objectives

High ≥ \$0.000 EPS* or cash and equivalents

Low ≥ \$0.000 EPS or cash and equivalents

* EPS = Earnings per share

Potential Impact	Extreme	15	19	22	24	25
	High	10	14	18	21	23
	Medium	6	9	13	17	20
	Low	3	5	8	12	16
	Negligible	1	2	4	7	11
		Remote	Unlikely	Possible	Likely	Probable
Likelihood						
% ranges	0-10%	>10-25%	>25-50%	>50-90%	>90-100%	

Enterprise Risk Assessment Scale (5 x 5)

> \$_____ million(m)	■	Very material: May affect company's ongoing existence
> \$_____ m - \$_____m	■	Material: Difficult to achieve multiple objectives
> \$_____ k - \$_____m	■	Significant: More challenging to achieve some objectives
> \$_____ k - \$_____k	■	Inconsequential: May have some undesirable outcomes
< \$_____ k	■	Trivial: No noticeable impact on objectives

High ≥ \$0.000 EPS or cash and equivalents
 Low ≥ \$0.000 EPS or cash and equivalents

Potential Impact	Extreme	5	10	15	20	25
	High	4	8	12	16	20
	Medium	3	6	9	12	15
	Low	2	4	6	8	10
	Negligible	1	2	3	4	5
		Remote	Unlikely	Possible	Likely	Probable
Likelihood						
% ranges	0-10%	>10-25%	>25-50%	>50-90%	>90-100%	

Enterprise Risk Assessment Scale (4 x 4)

> \$_____ m - \$_____ m	■	Material: Difficult to achieve multiple objectives
> \$_____ k - \$_____ m	■	Significant: More challenging to achieve some objectives
> \$_____ k - \$_____ k	■	Inconsequential: May have some undesirable outcomes
< \$_____ k	■	Trivial: No noticeable impact on objectives

High ≥ \$0.000 EPS or cash and equivalents
 Low ≥ \$0.000 EPS or cash and equivalents

Potential Impact	High	4	8	12	16
	Medium	3	6	9	12
	Low	2	4	6	8
	Negligible	1	2	3	4
		Remote	Unlikely	Possible	Probable
Likelihood					
% ranges	0-20%	>20-40%	>40-60%	>60-100%	

Enterprise Risk Assessment Scale (3 x 3)

> \$_____ m - \$_____ m ■ Material: Difficult to achieve multiple objectives

> \$_____ k - \$_____ m ■ Significant: More challenging to achieve some objectives

> \$_____ k - \$_____ k ■ Inconsequential: May have some undesirable outcomes

High ≥ \$0.000 EPS or cash and equivalents

Low ≥ \$0.000 EPS or cash and equivalents

Potential Impact	High	3	6	9
	Medium	2	4	6
	Low	1	2	3
		Remote	Possible	Probable
Likelihood				
% ranges	0-20%	>20-60%	>60-100%	

Enterprise Risk Assessment Scale (Qualitative Only)

Potential Impact	Severe					
	High					
	Medium					
	Low					
	Negligible					
		Remote	Unlikely	Possible	Likely	Probable

APPENDIX D: SAMPLE CONTROL MATURITY MODELS

Maturity Evolution	Scale	Model Levels	Capability Attributes
	5	World Class	Controls are considered 'world-class', based on benchmarking and continuous improvement; the controls infrastructure is highly automated and self-updating, thus creating a competitive advantage; there is extensive use of real-time monitoring and executive dashboards.
	4	Mature	Key performance indicators and monitoring techniques are employed to measure success; there is greater reliance on prevention versus detection controls; strong self-assessment of operating effectiveness by process owners occurs; change of accountability exists and is well understood.
	3	Defined	Controls are well defined and documented, thus there is consistency even in times of change; overall control awareness exists; control gaps are detected and remediated in a timely manner; performance monitoring is informal, placing great reliance on the diligence of people and independent audits.
	2	Repeatable	Controls are established with some policy structure; formal process documentation is still lacking; there is some clarity on roles, responsibilities and authorities, but not accountability; increased discipline and guidelines support repeatability; high reliance on existing personnel creates exposure to change.
	1	Immature	Controls are fragmented and ad hoc; they are generally managed in silos and reactive; formal policies and procedures are lacking; efforts are dependent on the 'heroics' of individuals to get things done; there is a higher potential for errors; costs are higher because of inefficiencies; effort is not sustainable.

Maturity Evolution	Scale	Model Levels	Control Maturity Model
	5	Optimal	Integrated Systems or processes Low error rate Continuously self-improving controls and processes
	4	Managed	Management or committee oversight Predictable results Self-improving process
	3	Formal	Formal written policy and procedures Clear accountability Qualitative assessment of results
	2	Recurring	Repeatable processes Significant human interaction or input required Strategic plan based on past performance
	1	Informal	Ad hoc actions or processes Manually intensive processes or controls No formal policy or desk procedures

Maturity Evolution	Scale	Model Levels	Control Maturity Model
	3	Mature	Self-improving controls and processes
	2	Formal	Formal written policy and procedures
	1	Informal	No formal policy or desk procedures

APPENDIX E: SAMPLE COMPANY MODEL MAPPED TO ENTITY-WIDE RISK LIBRARY

<div>Manufacturing company</div> <div>P1 = Primary risk owner</div> <div>P2 = Secondary risk owner</div> <div>Risk management gap =</div> <table><tr><td>10</td><td>15</td><td>20</td><td>25</td></tr><tr><td>8</td><td>12</td><td>16</td><td>20</td></tr><tr><td>6</td><td>9</td><td>12</td><td>15</td></tr></table>																	10	15	20	25	8	12	16	20	6	9	12	15	<div>Objective area</div> <div>Strategic</div> <div>Operations</div> <div>Reporting</div> <div>Compliance</div>				<div>Risk Mgmt Strategy</div> <div>Control</div> <div>Avoidance</div> <div>Share</div> <div>Accept</div>	<div>Corp comm., branding, and business development</div> <div>Sales (worldwide)</div> <div>Sales (China)</div> <div>Sales (product specific)</div> <div>R&D</div> <div>Product marketing</div> <div>Product line 1</div> <div>Product line 2</div> <div>Product line 3</div> <div>Product line 4</div> <div>Product line 5</div> <div>MFG (US)</div> <div>MFG (Malaysia)</div> <div>MFG (China)</div> <div>Customer service & shipping</div> <div>Procurement</div>	<div>Operations</div> <div>Business Units</div> <div>Sales</div> <div>Marketing</div> <div>C/A/S/A</div> <div>S</div> <div>O</div> <div>R</div> <div>C</div> <div>Share Control</div> <div>Share Control</div> <div>Share Control</div> <div>Share Control</div> <div>Control Accept</div> <div>Avoidance Share</div> <div>Control</div> <div>Control</div> <div>Control</div> <div>Control</div> <div>Avoidance transfer control</div> <div>Purchasing</div> <div>Customer service</div> <div>Manufacturing</div>																	<div>Procure materials and services</div> <div>Manage orders, logistics, and provide customer support</div>
10	15	20	25																																																	
8	12	16	20																																																	
6	9	12	15																																																	
<div>Insert corporate objectives (top 5)</div>																																																				
<div>Risk universe</div>																																																				
<div>Risk name</div>	<div>GEO</div>	<div>Risk description</div>					<div>S</div>	<div>O</div>	<div>R</div>	<div>C</div>	<div>C/A/S/A</div>	<div>Marketing</div>	<div>Sales</div>			<div>Business Units</div>			<div>Manufacturing</div>	<div>Customer service</div>	<div>Purchasing</div>																															
<div>Business interruption</div>	<div>US</div>	<div>Natural disasters, fire, utility supply, infrastructure failure, IT failure, labour, terrorism or industrial sabotage, and/or counter party risk</div>					<div>X</div>	<div>X</div>			<div>Share Control</div>							<div>P1</div>																																		
	<div>MAL</div>						<div>X</div>	<div>X</div>			<div>Share Control</div>						<div>P1</div>																																			
	<div>PRC</div>						<div>X</div>	<div>X</div>			<div>Share Control</div>						<div>P1</div>																																			
<div>M&A/post integration</div>		<div>Insufficient due diligence, planning, valuation or post integration</div>					<div>X</div>	<div>X</div>			<div>P2</div>						<div>P1</div>																																			
<div>Market risk</div>		<div>Unfavourable market dynamics, for example, customers' inability to produce marketable products and/or increased competition</div>					<div>X</div>				<div>P2</div>	<div>P2</div>	<div>P2</div>	<div>P1</div>																																						
<div>Geo/political risk</div>		<div>Unstable political environment creates potential for nationalisation of facilities, property rights, labour risks, security threats, and so forth</div>					<div>X</div>				<div>P2</div>					<div>P1</div>																																				
<div>Human capital</div>	<div>Attracting talent</div>		<div>Inability to attract qualified personnel</div>						<div>X</div>		<div>Control</div>	<div>P1</div>	<div>P1</div>	<div>P1</div>	<div>P2</div>	<div>P2</div>	<div>P2</div>	<div>P2</div>	<div>P1</div>	<div>P1</div>																																
	<div>Retaining talent</div>		<div>Inability to retain qualified personnel</div>						<div>X</div>		<div>Control</div>	<div>P1</div>	<div>P1</div>	<div>P1</div>		<div>P1</div>	<div>P1</div>	<div>P1</div>																																		
	<div>Import/export compliance risk</div>		<div>EAR/ITAR compliance risk</div>							<div>X</div>	<div>Control</div>	<div>P2</div>	<div>P2</div>						<div>P1</div>																																	
<div>Government contract compliance risk</div>		<div>Ability to avoid government contractor compliance violations, for example charging unallowable costs to contracts</div>								<div>X</div>	<div>Control</div>																																									
<div>Information security risk</div>		<div>Unauthorised disclosure of proprietary information, for example, trade secrets, or data privacy</div>					<div>X</div>	<div>X</div>			<div>Avoidance transfer control</div>																																									

<div>Manufacturing company</div> <div>P1 = Primary risk owner</div> <div>P2 = Secondary risk owner</div> <div>Risk management gap =</div> <table><tr><td>10</td><td>15</td><td>20</td><td>25</td></tr><tr><td>8</td><td>12</td><td>16</td><td>20</td></tr><tr><td>6</td><td>9</td><td>12</td><td>15</td></tr></table>														10	15	20	25	8	12	16	20	6	9	12	15	<div>Objective area</div> <div>Strategic</div> <div>Operations</div> <div>Reporting</div> <div>Compliance</div>				Risk Mgmt Strategy	Corp comm., branding, and business development	Sales (worldwide)	Sales (China)	Sales (product specific)	R&D	Product marketing	Product line 1	Product line 2	Product line 3	Product line 4	Product line 5	MFG (US)	MFG (Malaysia)	MFG (China)	Customer service & shipping	Procurement
10	15	20	25																																											
8	12	16	20																																											
6	9	12	15																																											
Insert corporate objectives (top 5)																																														
Risk universe																																														
Risk name	GEO	Risk description	S	O	R	C	C/A/S/A																																							
IP infringement risk		Company sued for IP and/or patent infringement	X				Avoidance transfer control																																							
Obsolescence risk		Product technological obsolescence	X				Transfer control																																							
Customer concentration/distribution risk		Inability to effectively expand product distribution channels and/or high customer concentration risk	X				Transfer control																																							
Manufacturing risk		Manufacturing risk—poor yields, throughput, quality, or cannot reduce costs, and/or inability to balance customer demand vs. capacity		X			Transfer control																																							
NPI Risk		Inability to timely complete/commercialise new product designs and achieve technology breakthroughs required to make commercially viable devices eg. _____ and/or technologies developed may not have ready commercial value		X			Control																																							
Supply chain risk		Supply chain interruptions (both internal and external) due to fulfillment challenges and limited source suppliers		X			Control																																							
EH&S risk		Compliance violations and personal health and safety exposure				X	Transfer control																																							
Physical asset risk		Assets not maintained, damaged, or otherwise compromised so that production is impaired		X			Control																																							

Continued on p.110

Continued from p.109

<div>Manufacturing company</div> <div>P1 = Primary risk owner</div> <div>P2 = Secondary risk owner</div> <div>Risk management gap =</div> <table><tr><td>10</td><td>15</td><td>20</td><td>25</td></tr><tr><td>8</td><td>12</td><td>16</td><td>20</td></tr><tr><td>6</td><td>9</td><td>12</td><td>15</td></tr></table>				10	15	20	25	8	12	16	20	6	9	12	15	<div>Objective area</div> <table><tr><td>Strategic</td><td>Operations</td><td>Reporting</td><td>Compliance</td></tr></table>				Strategic	Operations	Reporting	Compliance	Risk Mgmt Strategy	Corp comm., branding, and business development	Sales (worldwide)	Sales (China)	Sales (product specific)	R&D	Product marketing	Product line 1	Product line 2	Product line 3	Product line 4	Product line 5	MFG (US)	MFG (Malaysia)	MFG (China)	Customer service & shipping	Procurement
				10	15	20	25																																	
				8	12	16	20																																	
				6	9	12	15																																	
Strategic	Operations	Reporting	Compliance																																					
Insert corporate objectives (top 5)																																								
Risk universe																																								
Risk name	GEO	Risk description	S	O	R	C	C/A/S/A																																	
Regulatory reporting		SEC financial reporting, tax compliance reporting, labor reporting, ERISA, statutory reporting, and so forth			X	X	Control																																	
Cash Management		Credit Risk—(default, concentration, settlement, collateral) Liquidity Risk—(cash flow, opportunity cost, concentration) Price Risk—(currency, commodity, etc) cash Taxes		X			Control																																	
Contractual risk		Legal or contractual relations are compromised, for example, vendors/subcontractors don't comply with contract commitments and/or sales/distribution contract violations		X			Transfer control																																	
Fraud risk	Corruption	Conflicts of interest, bribery, illegal gratuities, and economic extortion				X	Control																																	
	Asset misappropriation	Loss of cash, inventory, or other assets		X			Control																																	
	Financial state-ment fraud	Intentional asset or liability over/understatement or improper revenue recognition			X		Control																																	
Information knowledge management risk		Inability to capture, retain, access, and/or disseminate critical information and/or data privacy compromise affects ability to effectively and efficiently run the business and create competitive advantage	X		X		Control																																	

<div>Manufacturing company</div> <div>P1 = Primary risk owner</div> <div>P2 = Secondary risk owner</div> <div>Risk management gap =</div> <table><tr><td>10</td><td>15</td><td>20</td><td>25</td></tr><tr><td>8</td><td>12</td><td>16</td><td>20</td></tr><tr><td>6</td><td>9</td><td>12</td><td>15</td></tr></table>										10	15	20	25	8	12	16	20	6	9	12	15	Objective area				Risk Mgmt Strategy	Corp finance and accounting	Treasury and risk management	Corp tax	Corp financial planning	Legal and stock plan admin	Information technology (IT) systems	Administration and human resources	Compensation and benefits	Facilities	Security	EH&S	Executive management team	Internal audit	Corp governance (Board of Directors)																																																																																																																																																																																																																		
10	15	20	25																																																																																																																																																																																																																																																							
8	12	16	20																																																																																																																																																																																																																																																							
6	9	12	15																																																																																																																																																																																																																																																							
Insert corporate objectives (top 5)										Strategic	Reporting	Operations	Compliance	Control Avoidance Share Accept	Manage accounting and control data	Manage capital and risk	Manage accounting and control data	Manage accounting and control data	Provide decision support	Provide decision support	Manage information technology	Manage human resources; manage employee services	Manage plant equipment and facilities	Plan and manage the business	Provide assurance and risk advisory	Governance and risk oversight																																																																																																																																																																																																																																
Risk universe										S	O	R	C	C/A/S/A	Finance			Legal	IT	HR and administration	Facilities			Executive	Internal audit	Governance																																																																																																																																																																																																																																
Risk name	GEO	Risk description	US	MAL	PRC	Insufficient due diligence, planning, valuation or post integration	Unfavourable market dynamics, for example, customers' inability to produce marketable products and/or increased competition	Unstable political environment creates potential for nationalisation of facilities, property rights, labour risks, security threats, and so forth	Inability to attract qualified personnel						Inability to retain qualified personnel	EAR/ITAR compliance risk	Ability to avoid government contractor compliance violations, for example charging unallowable costs to contracts				Unauthorised disclosure of proprietary information, for example, trade secrets, or data privacy	P2	P2				P2	P2	P2	P2	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1

Continued from p.111

[illegible]

<div>Manufacturing company</div> <div>P1 = Primary risk owner</div> <div>P2 = Secondary risk owner</div> <div>Risk management gap =</div> <table><tr><td>10</td><td>15</td><td>20</td><td>25</td></tr><tr><td>8</td><td>12</td><td>16</td><td>20</td></tr><tr><td>6</td><td>9</td><td>12</td><td>15</td></tr></table>		10	15	20	25	8	12	16	20	6	9	12	15	Objective area				Risk Mgmt Strategy	Corp finance and accounting	Treasury and risk management	Corp tax	Corp financial planning	Legal and stock plan admin	Information technology (IT) systems	Administration and human resources	Compensation and benefits	Facilities	Security	EH&S	Executive management team	Internal audit	Corp governance (Board of Directors)
		10	15	20	25																											
		8	12	16	20																											
		6	9	12	15																											
Strategic	Operations	Reporting	Compliance	Control Avoidance Share Accept	Manage accounting and control data	Manage capital and risk	Manage accounting and control data	Provide decision support	Provide decision support	Manage accounting and control data	Manage information technology	Manage human resources; manage employee services	Manage plant, equipment and facilities	Plan and manage the business	Provide assurance and risk advisory	Governance and risk oversight																
	ERM					Support Services																										
	S	O	R	C	C/A/S/A	Finance				Legal	IT	HR and administration	Facilities		Executive	Internal audit	Governance															
Regulatory reporting	GEO	Risk description																														
Cash Management		SEC financial reporting, tax compliance reporting, labor reporting, ERISA, statutory reporting, and so forth																														
		Credit Risk—(default, concentration, settlement, collateral)																														
		Liquidity Risk—(cash flow, opportunity cost, concentration)																														
		Price Risk—(currency, commodity, etc) cash Taxes																														
Contractual risk		Legal or contractual relations are compromised, for example, vendors/subcontractors don't comply with contract commitments and/or sales/distribution contract violations																														
Fraud risk	Corruption	Conflicts of interest, bribery, illegal gratuities, and economic extortion																														
	Asset misappropriation	Loss of cash, inventory, or other assets																														
	Financial state-ment fraud	Intentional asset or liability over/understatement or improper revenue recognition																														
Information knowledge management risk		Inability to capture, retain, access, and/or disseminate critical information and/or data privacy compromise affects ability to effectively and efficiently run the business and create competitive advantage																														

APPENDIX F: EXAMPLES OF RISK ASSESSMENT REPORTING

A—This series of risks was grouped largely according to the external nature of their risk factors.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

- (1) Business interruption United States
- (1.1) Business interruption Indonesia
- (1.2) Business interruption China
- (2) Mergers and acquisitions (M&A) or postintegration risk
- (3) Market risk
- (4) Geopolitical risk

Potential Impact	Extreme					
	High	1		1.1		
	Medium			1.2	3	
	Low			2		
	Negligible			4		
		Remote	Unlikely	Possible	Likely	Probable
		Likelihood				
% ranges		0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

- The company does not have a comprehensive business continuity plan or primary risk owner. However, components of the BCP clearly exist and are managed by various functions—for example, the facilities,

environmental health and safety, and IT departments. These functions are considered more mature in the United States, but less so in Asia Pacific operating areas. The risk of factory fire was considered the most likely and highest risk factor by operations participants and IT failure the most prominent risk factor affecting support service functions.

- The company does not have a dedicated internal business development or mergers and acquisitions (M&A) function or post-integration teams. Several participants indicated the company tends to overleverage existing resources for M&A and post-integration activities.
- Opportunities appear to exist in how the company assesses and manages market risk—that is, whether individual risks are to be mitigated by the corporate centre or left to business units to manage. Increased competition tended to be higher than customer design risk factors.

B—Risks associated with human capital were reduced into two primary categories: (1) attracting talent and (2) retaining talent. Qualitative factors considered by participants varied by classes of employees. For example, certain participants indicated that potential turnover costs in attracting and retaining key scientists and engineers were more significant in the short term (FY09) because of the loss of local corporate knowledge and the high learning curve associated with new hires.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

- (5) Attracting talent
(5.1) Retaining talent

Potential Impact	Extreme					
	High					
	Medium			5.1		
	Low			5		
	Negligible					
		Remote	Unlikely	Possible	Likely	Probable
Likelihood						
% ranges		0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

- An assessment of annual recruiting fees and a time lag analysis of how long existing position gaps remain open may be useful key performance indicators in assessing hard and soft costs associated with attracting and retaining talent.
- Opportunities may exist in developing key performance indicators by employee categories or department function.
- Current economic conditions (the lagging recession) present opportunities to attract high calibre talent in all professional disciplines and should be exploited.

C—These risks were identified as specific compliance risks affecting material classes of transaction. Participants largely considered these risks to be well managed.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High ≥ \$0.025 EPS or cash and equivalents		
Low ≥ \$0.005 EPS or cash and equivalents		

Risk Legend

- (6) Import/export compliance risk
(7) Government contract compliance risk

Potential Impact	Extreme					
	High					
	Medium					
	Low					
	Negligible					
		7	6			
		Remote	Unlikely	Possible	Likely	Probable
Likelihood						
% ranges		0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

- Custom, duties, and value added tax compliance was specifically identified as reasonably possible and potentially significant.
- Other potential risk factors associated with import or export compliance were identified—for example, Restriction of Hazardous Substances Directive (RoHS); Registration, Evaluation and Authorisation of Chemicals (REACH); and Toxic Substances Control Act (TSCA) compliance standards—and may warrant further investigation and assessment for potential impact to the company and for gaps in risk management.

D—The risk of compromised trade secrets and intellectual property not covered by patents was contrasted with the probability of lawsuits alleging infringement claims. Most participants indicated that the potential impact associated with compromised trade secrets was medium in the short term (FY09) but could be more significant, even material, over a longer time horizon. Infringement claims against the company, however, are likely to probable, and the potential impact could exceed budgeted spending in the company's annual operating plan because of the current mix of lawsuits and uncertainties involving potential outcomes.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

- (8) Trade secret or intellectual property (IP) compromise risk
 (9) IP infringement risk

Potential Impact	Extreme					
	High				8	
	Medium				9	
	Low					
	Negligible					
		Remote	Unlikely	Possible	Likely	Probable
Likelihood						
% ranges		0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

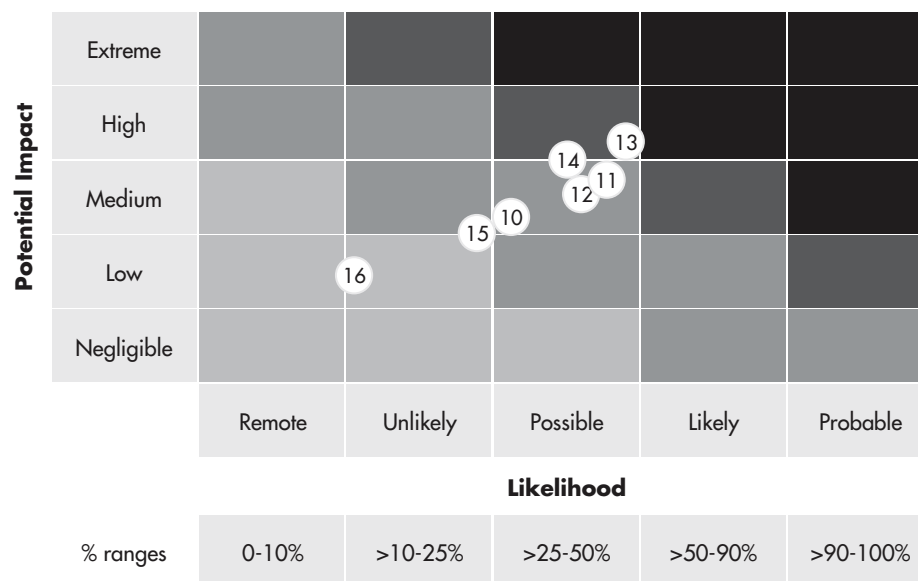
- Primary risk owners, functions, policies, procedures, processes, and controls could be more clearly linked to managing these risks. Once this has been completed, stakeholders should review risk management strategies and reassess risks in these areas.
- Internal control, risk transfer, and avoidance strategies are all used to manage the potential impact of both of these risks.
- Some participants indicated that the company has greater exposure to trade secret or intellectual property compromise from internal threats and potential bribery schemes from foreign competitors seeking to enter the market. Previously assessed inherent mitigating factors, such as capital investment that was considered a significant barrier to entry, may no longer be relevant. The company should reassess and consider implementing a more robust data leakage programme.

E—These risks were grouped together primarily according to their interrelated nature and effect on operations.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

- (10) Obsolescence risk
 (11) Customer concentration or distribution risk
 (12) Manufacturing risk
 (13) NPI risk
 (14) Supply chain risk
 (15) EH&S risk
 (16) Physical asset risk



Potential risk management gaps and follow-up:

- A more accurate sales forecasting function was a recurring theme thought to be a key risk indicator associated with several of these interrelated risks.
- The perception of supply chain risk increased with the vertical supply chain as viewed by downstream business units.
- The likelihood and potential impact of risk events appeared highest with the new product introduction process, indicating that opportunities may exist in how the company is structured and manages new product introduction.
- Environmental health and safety and physical asset risk have robust dedicated functions responsible for risk management and were considered fairly well managed in the United States. However, some uncertainty exists among participants as to risk ownership and how mature these functions are in Asia Pacific locations.

F—Regulatory reporting and cash management were considered reasonably well managed based on participants' perceptions of control maturity. However, contractual risks associated with vendors and certain outsourcing functions may merit closer scrutiny of vendors' performance against contract expectations.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

- (17) Regulatory reporting
 (18) Cash management
 (19) Contractual risk

Potential Impact	Extreme					
	High					
	Medium		17	18		
	Low			19		
	Negligible					
		Remote	Unlikely	Possible	Likely	Probable
		Likelihood				
	% ranges	0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

- Regulatory reporting was considered managed in the areas of Securities and Exchange Commission and tax compliance reporting. However, certain participants identified a possible likelihood of compliance risk factors affecting the employee benefits area that could be potentially significant.
- Some participants indicated cash management opportunities that exist in hedging foreign currency and commodity risk. For invested cash, capital preservation was considered more important than interest income given the current finance and credit market uncertainties. Therefore, the company recently amended its investment policies to be more conservative.
- It was somewhat unclear if contract performance reviews were routinely conducted and who was primarily responsible—that is, whether individual risks are to be mitigated by the corporate centre or left to business units to manage.
- A potential opportunity exists to conduct vendor contract audits to ensure compliance with contract commitments. Audit findings of noncompliance could result in vendor credits and reduced costs on future purchases of materials and outsourcing services.

G—Fraud risk was defined using the Association of Certified Fraud Examiners' Uniform Occupational Fraud Classification System.¹ Overall the risk of fraud is considered well managed. The potential impacts of financial statement fraud were assessed as medium to high, with a remote to unlikely probability of occurrence given the current maturity of internal control over financial reporting.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

- (20) Corruption
(21) Asset misappropriation
(22) Financial statement fraud

Potential Impact	Extreme					
	High					
	Medium		22			
	Low			20		
	Negligible		21			
		Remote	Unlikely	Possible	Likely	Probable
		Likelihood				
	% ranges	0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

- Risk of Foreign Corrupt Practices Act (FCPA) violations was considered reasonably possible given a rapidly expanding sales force. The company plans to conduct more frequent compliance awareness training and implement quarterly control self-assessments, including representations covering FCPA and general corruption risks.
- Risk of financial statement fraud was considered remote based on the control maturity. However, a single event was considered potentially material.

H—Although several participants (six) did not see this risk as critically affecting their function areas, the vast majority of participants (more than 25) assessed risks associated with how the company manages information using its IT business systems as being between possible and probable and that the potential impact (opportunity cost) to the organisation tended toward the high end of the potential impact range.

> \$75m	■	Very material: May affect company's ongoing existence
> \$1.95m - \$75m	■	Material: Difficult to achieve multiple objectives
> \$340k - \$1.95m	■	Significant: More challenging to achieve some objectives
> \$25k - \$340k	■	Inconsequential: May have some undesirable outcomes
< \$25k	■	Trivial: No noticeable impact on objectives
High	≥	\$0.025 EPS or cash and equivalents
Low	≥	\$0.005 EPS or cash and equivalents

Risk Legend

(23) Information systems risk

Potential Impact	Extreme					
	High				23	
	Medium					
	Low					
	Negligible					
		Remote	Unlikely	Possible	Likely	Probable
Likelihood						
% ranges		0-10%	>10-25%	>25-50%	>50-90%	>90-100%

Potential risk management gaps and follow-up:

- Participants believed that the company was not achieving efficiencies or gaining competitive advantage managing information through core business systems and that substantial opportunity exists to do so. The company is investing heavily in IT infrastructure and in cost and planning business systems. In addition, the company has hired a CIO and formed an IT steering committee to ensure IT capital projects are appropriately prioritised, managed, and transitioned to functional user groups tied to performance.
- The company does not routinely supply in-house or outsourced user training on core business systems like its enterprise resource planning and manufacturing execution system, which creates exposure to change and limits the company's ability to automate transactions and gain operational efficiencies by leveraging the information technology of its business systems.

Endnotes

- 1 The Association of Certified Fraud Examiners (ACFE) has developed the Uniform Occupational Fraud Classification System, which the company has incorporated into its risk assessment process both at the entity and activity levels. The ACFE periodically issues a 'Report to the Nation' on fraud risk metrics by industry that is widely accepted as the leading authority on fraud risk and its impact on governments and industry.

APPENDIX G: SAMPLE OF A FINANCIAL REPORTING RISK LIBRARY (INHERENT AND FRAUD RISKS)

Type	Risk
ICFR Risks & Root Causes	ACQ Risk 1—Acquired intangibles are not timely impaired (V)
ICFR Risks & Root Causes	ACQ Risk 2—Purchase accounting is not accurate or properly recorded (C, V/A)
ICFR Risks & Root Causes	ACQ Risk 3—Goodwill is not timely impaired (V)
ICFR Risks & Root Causes	ACQ Risk 4 (Fraud)—Improper valuations are performed for acquired intangibles (V)
ICFR Risks & Root Causes	AP Risk 1—AP transactions are not properly processed (C, E/O)
ICFR Risks & Root Causes	AP Risk 2—AP balances are not properly recorded (C)
ICFR Risks & Root Causes	AP Risk 3—AP period end cut-off is incomplete or inaccurate (C)
ICFR Risks & Root Causes	AP Risk 4 (Fraud)—Disbursement fraud schemes occur
ICFR Risks & Root Causes	AR Risk 1—AR transactions are not properly processed (C, E/O)
ICFR Risks & Root Causes	AR Risk 2—AR balances are not properly recorded (C, E/O)
ICFR Risks & Root Causes	AR Risk 3—AR reserves estimates are not accurate or assumptions are incorrect (V/A)
ICFR Risks & Root Causes	AR Risk 4—AR period end cut-off is incomplete or inaccurate (C)
ICFR Risks & Root Causes	AR Risk 5 (Fraud)—Accounts receivable (including reserves) fraud schemes occur
ICFR Risks & Root Causes	CS Risk 1—Customer contracts or purchase orders are not properly authorised or communicated (E/O, R/O)
ICFR Risks & Root Causes	CS Risk 2—Sales orders are not accurately processed (E/O)
ICFR Risks & Root Causes	CS Risk 3—Product physical shipments occur but are transacted in the wrong period (C)
ICFR Risks & Root Causes	CS Risk 4—RMA or RMA credit memo is not properly processed (C, V/A)
ICFR Risks & Root Causes	EL Risk 1—Ineffective corporate governance and control environment exist
ICFR Risks & Root Causes	EL Risk 2—Inadequate risk assessment occurs
ICFR Risks & Root Causes	EL Risk 3—Inadequate information and communication exist
ICFR Risks & Root Causes	EL Risk 4—Monitoring is ineffective
ICFR Risks & Root Causes	EQU Risk 1—Equity transactions are not properly processed or recorded (C, E/O, P/D)
ICFR Risks & Root Causes	EQU Risk 2—Stock based compensation is not properly valued and expensed (V/A)
ICFR Risks & Root Causes	EQU Risk 3—Equity period end cutoff is incomplete or inaccurate (C, P/D)
ICFR Risks & Root Causes	EQU Risk 4 (Fraud)—Stock option schemes occur
ICFR Risks & Root Causes	FN Risk 1—Required financial statement presentation disclosures are omitted (P/D)
ICFR Risks & Root Causes	FN Risk 2—Required financial statement disclosures are not in accordance with GAAP (P/D)
ICFR Risks & Root Causes	FN Risk 3—Footnotes disclose incorrect, incomplete, or improper (V/A, P/D)
ICFR Risks & Root Causes	FN Risk 4—Contingencies are omitted or not properly disclosed (P/D)
ICFR Risks & Root Causes	FN Risk 5—Related parties are omitted or not properly disclosed (P/D)
ICFR Risks & Root Causes	FN Risk 6—Income tax disclosures are omitted or not properly disclosed (P/D)
ICFR Risks & Root Causes	FS Risk 1—Consolidated financial statements are not completely or accurately prepared (P/D)

Continued on p.126

Continued from p.125

Type	Risk
ICFR Risks & Root Causes	FS Risk 2—Financial statements are not presented in accordance with GAAP (P/D)
ICFR Risks & Root Causes	FS Risk 3 (Fraud)—Financial statements contain improper disclosures
ICFR Risks & Root Causes	GL Risk 1—Journal entries are not properly authorised or processed (C, E/O, R/O, V/A, P/D)
ICFR Risks & Root Causes	GL Risk 2—Journal entries are not properly recorded (C, E/O, R/O, V/A, P/D)
ICFR Risks & Root Causes	GL Risk 3—GL trial balance or financial report is inaccurate or incomplete (P/D)
ICFR Risks & Root Causes	GL Risk 4 (Fraud)—Improper journal entries are recorded (P/D)
ICFR Risks & Root Causes	GOV Risk 1—Unallowable costs are processed and recorded to government contracts (C, P/D)
ICFR Risks & Root Causes	GOV Risk 2—Overhead rates or incurred costs estimate are not accurate or assumptions are incorrect (C, V/A)
ICFR Risks & Root Causes	GOV Risk 3 (Fraud)—Contract revenue timing differences occur (C)
ICFR Risks & Root Causes	INV Risk 1—Inventory is not properly processed or recorded (C, E/O, P/D)
ICFR Risks & Root Causes	INV Risk 2—Inventory estimates are not accurate or assumptions are incorrect (V/A)
ICFR Risks & Root Causes	INV Risk 3—Inventory period end cut-off is incomplete or inaccurate (C)
ICFR Risks & Root Causes	INV Risk 4 (Fraud)—There is improper inventory reserve or asset valuation (V/A, P/D)
ICFR Risks & Root Causes	INV Risk 5 (Fraud)—Improper classification of production and research and development costs occur
ICFR Risks & Root Causes	INV Risk 6 (Fraud)—Misappropriation of inventory occurs
ICFR Risks & Root Causes	INV Risk 7 (Fraud)—Improper use of production factors to manipulate recognition of expense occurs
ICFR Risks & Root Causes	IT Risk 1—Ineffective IT control environment exists
ICFR Risks & Root Causes	IT Risk 2—Unapproved, inappropriate, erroneous, or fraudulent modification of system functionality occurs
ICFR Risks & Root Causes	IT Risk 3—Application software acquisition and development are not controlled or appropriately managed
ICFR Risks & Root Causes	IT Risk 4—Inappropriate access to systems results in erroneous, inappropriate, or fraudulent modification of data
ICFR Risks & Root Causes	IT Risk 5—Key financial reporting information is inaccessible, lost, or destroyed
ICFR Risks & Root Causes	LLA Risk 1—LLA balances are not properly processed or recorded (C, E/O)
ICFR Risks & Root Causes	LLA Risk 2—Depreciation or amortisation is not accurately processed or recorded (V/A)
ICFR Risks & Root Causes	LLA Risk 3—Expenses are not properly capitalised or expensed (V/A, P/D)
ICFR Risks & Root Causes	LLA Risk 4—LLA impairments are not timely, accurate, processed, or recorded (V/A)
ICFR Risks & Root Causes	LLA Risk 5 (Fraud)—Improper asset valuations are performed and recorded (V/A)
ICFR Risks & Root Causes	LLA Risk 6 (Fraud)—Misappropriation of physical assets occurs
ICFR Risks & Root Causes	OMA Risk 1—Other assets transactions are not authorised or are incorrectly processed or recorded (E/O, V/A)
ICFR Risks & Root Causes	OMA Risk 2—Other liabilities and related estimates are not accurate (C, V/A)
ICFR Risks & Root Causes	OMA Risk 3 (Fraud)—Other assets or liabilities are intentionally overstated or understated (C, E/O, V/A)
ICFR Risks & Root Causes	PAY Risk 1—Payroll is not properly processed (C, E/O)
ICFR Risks & Root Causes	PAY Risk 2—Payroll is not properly recorded (C, E/O)
ICFR Risks & Root Causes	PAY Risk 3 (Fraud)—Payroll schemes occur (R/O)
ICFR Risks & Root Causes	PUR Risk 1—Receipt of goods period end cut-off is incomplete or inaccurate (C)
ICFR Risks & Root Causes	PUR Risk 2 (Fraud)—Purchasing schemes occur
ICFR Risks & Root Causes	SALES Risk 1—Sales terms are incomplete or not accurately processed (E/O)
ICFR Risks & Root Causes	SALES Risk 2—Revenue recognition per customer terms is improper according to GAAP (V/A, P/D)
ICFR Risks & Root Causes	SALES Risk 3—Revenue period end cut-off is incomplete or inaccurate (C, P/D)
ICFR Risks & Root Causes	SALES Risk 4 (Fraud)—Fictitious revenue schemes occur (E/O)
ICFR Risks & Root Causes	SALES Risk 5 (Fraud)—Revenue timing differences occur (C)

Type	Risk
ICFR Risks & Root Causes	SALES Risk 6 (Fraud)—Improper side agreements exist and are unknown to management (E/O, P/D)
ICFR Risks & Root Causes	SALES Risk 7 (Fraud)—Sales channel stuffing occurs (E/O, P/D)
ICFR Risks & Root Causes	SALES Risk 8 (Fraud)—Bribery schemes occur to gain business—for example, kickbacks or bid rigging (R/O)
ICFR Risks & Root Causes	TAX Risk 1—Income tax attributes are not identified or properly treated (C, P/D)
ICFR Risks & Root Causes	TAX Risk 2—Income tax expense is not accurately processed (R/O)
ICFR Risks & Root Causes	TAX Risk 3—Income tax expense is not properly recorded (R/O, P/D)
ICFR Risks & Root Causes	TAX Risk 4—Deferred tax balances are not properly reconciled or recorded (C, P/D)
ICFR Risks & Root Causes	TAX Risk 5—Tax contingencies are not identified or properly valued (E/O, R/O, V/M, P/D)
ICFR Risks & Root Causes	TAX Risk 6—Tax positions are not identified or recognised (C)
ICFR Risks & Root Causes	TAX Risk 7—Tax positions do not meet recognition requirements according to GAAP (E/O)
ICFR Risks & Root Causes	TAX Risk 8—Tax positions are not properly measured according to GAAP (V/M)
ICFR Risks & Root Causes	TAX Risk 9 (Fraud)—Income taxes are intentionally understated (C, E/O, P/D)
ICFR Risks & Root Causes	TAX Risk 10 (Fraud)—Deferred income taxes are improperly valued (V/M, P/D)
ICFR Risks & Root Causes	TR Risk 1—Cash balances are not properly processed and recorded (E/O, P/D)
ICFR Risks & Root Causes	TR Risk 2—Investments are not properly processed or recorded (C, E, V/A)
ICFR Risks & Root Causes	TR Risk 3—Investments are not properly valued (V/A, P/D)
ICFR Risks & Root Causes	TR Risk 4 (Fraud)—Cash larceny schemes occur (E/O, R/O)