MANAGEMENT

STRATEGY

MEASUREMENT

MANAGEMENT ACCOUNTING GUIDELINE

The Reporting of Organizational Risks for Internal and External Decision-Making

By

Marc J. Epstein

and

Adriana Rejc Buhovac

Published by:

CMA CANADA

AICPA®

NOTICE TO READERS

The material contained in the Management Accounting Guideline *Reporting of Organizational Risks for Internal and External Decision-Making* is designed to provide illustrative information with respect to the subject matter covered. It does not establish standards or preferred practices. This material has not been considered or acted upon by any senior technical committees or the board of directors of either the AICPA or the Society of Management Accountants of Canada and does not represent an official opinion or position of either the AICPA or the Society of Management Accountants of Canada.

MANAGEMENT

STRATEGY

MEASUREMENT

MANAGEMENT ACCOUNTING GUIDELINE

The Reporting of Organizational Risks for Internal and External Decision-Making

By

Marc J. Epstein
Rice University
and
Adriana Rejc Buhovac
University of Ljubljana

Published by The Society of Management Accountants of Canada
and The American Institute of Certified Public Accountants

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

ISBN 0-87051-655-8

THE REPORTING OF ORGANIZATIONAL RISKS FOR INTERNAL AND EXTERNAL DECISION-MAKING

INTRODUCTION

The regulatory pressures for improved risk assessment and reporting on internal control have increased around the world. The reason—corporate accounting failures, frauds, internal control breaches, and governance failures have been seen in companies and countries that thought they were immune to these events. In response, the requirements of the Sarbanes-Oxley Act of 2002 in the U.S. and similar new regulations in other countries are among the many prominent forces driving improved corporate governance and transparency. Risks that organizations face are larger and more varied, and have more global effect. These risks relate not only to reporting and compliance; they also include strategic and operations risks. Increased corporate strategic alliances and business partnerships also create growing risk interdependencies.

Although risk assessment processes generally have improved, inadequate risk reporting in some organizations has led to a failure to fully integrate identified risks into strategic and operational decisions. When planning a merger or an acquisition, for example, how confident can one be

CONTENTS

EXECUTIVE SUMMARY

A recent Management Accounting Guideline "Identifying, Measuring, and Managing Organizational Risk for Improved Performance", developed a model and measures for improving the identification and measurement of risks to improve management decisions. Clearly these risks are both larger and more varied than ever previously thought and, they are more global. Just as senior managers need more complete risk assessments for better management decision-making, external shareholders and other stakeholders are demanding increased reporting of these risks to better evaluate corporate performance.

Financial professionals want to provide a clear understanding of the risks and fair disclosure to both internal and external decision-makers without causing unnecessary alarm. This Guideline addresses these important issues and provides guidance for the reporting of risks for both internal and external decision-making.

about the expected gains without carefully considering all potential risks, including their assessed magnitude and probability of occurrence? Decision-makers need to understand the various organizational risks, to minimize mistaken investments that can cause significant organizational costs. Managers need good risk reporting systems to integrate risk evaluation into (a) their operational and capital investment decisions, (b) review of performance, and (c) compensation decisions. Improved organizational risk assessment and internal risk reporting is critical also for senior management and boards of directors, who are responsible for carefully establishing and reviewing corporate processes for identifying, assessing and managing risk.

The demand for disclosing risk externally is also growing. Investors, financial analysts, and other external stakeholders are increasingly aware of the critical role of proper risk management. They want better information on the various risks organizations confront, and how to address them, and are interested in organizational risks far beyond the traditional scope of financial risks. They want concrete assurance that a sound system and process is in place to identify, assess, and manage risks, so that they can better evaluate corporate performance and make more informed decisions.

Increased measurement and reporting of this broader set of risks is necessary, not only to meet the new regulatory requirements but also to improve managerial performance and stakeholder confidence. Senior corporate managers need to develop ways to effectively communicate organizational risks and risk management processes both internally and externally. They face decisions on what to report to each audience, and the form of risk reports, including how much detail to include. Senior management therefore needs to clearly understand the risks and promote disclosure to both internal and external decision-makers without causing unnecessary alarm or increasing reporting and compliance risks. A more effective organizational risk reporting system can provide internal and external stakeholders with information they need to (a) craft strategy, (b) make investment and other business and personal decisions and, at the same time, (c) inspire confidence in the organization's financial reporting and disclosure. This increased focus on risk can turn risk management and risk reporting into an opportunity and reward.

This Guideline addresses these important issues and provides guidance on reporting risks to aid both internal and external decision-making. The Guideline's specific ***objectives*** are:

- To discuss the role and importance of risk management and reporting for improved strategic and operational decision-making by senior management and other managers (*The Risk Reporting Contribution Scheme*). This Guideline focuses first on internal risk reporting, then on external risk reporting.
- To address specific risk reporting questions, including the content of risk reports, their format, placement, distribution, and communication, and the intended impact of risk reporting (*The Risk Reporting Model*). Again, these questions will be addressed firstly to internal audiences' needs and requirements, then to those of external audiences.
- To provide templates for real-time and periodic internal and external risk reports;
- To discuss the challenges in risk reporting, including the potential for inappropriate decision-making or dysfunctional behavior of internal and external audiences.
- To discuss the importance of balancing the desire for a complete and fair presentation of organizational risks with avoidance of overreaction that could reduce appropriate risk-taking that is necessary for business success; and
- To provide guidance on organizational structure and responsibilities related to risk reporting.

The ***target audience*** of this Guideline is (a) CEOs and CFOs, (b) senior management teams, (c) boards of directors, (d) members of audit committees, and (e) accounting, internal audit, and finance professionals, all of whom confront challenges of risk assessment, risk analysis, risk control, and risk reporting. The Guideline may also be useful for external auditors, in particular those who attest to and report on management's assessment of the effectiveness of internal control over financial reporting.

RISK MANAGEMENT

In a recent Management Accounting Guideline, "*Identifying, Measuring, and Managing Organizational Risks for Improved Performance*", Marc J. Epstein and Adriana Rejc developed a model (the Risk Management Payoff Model) and

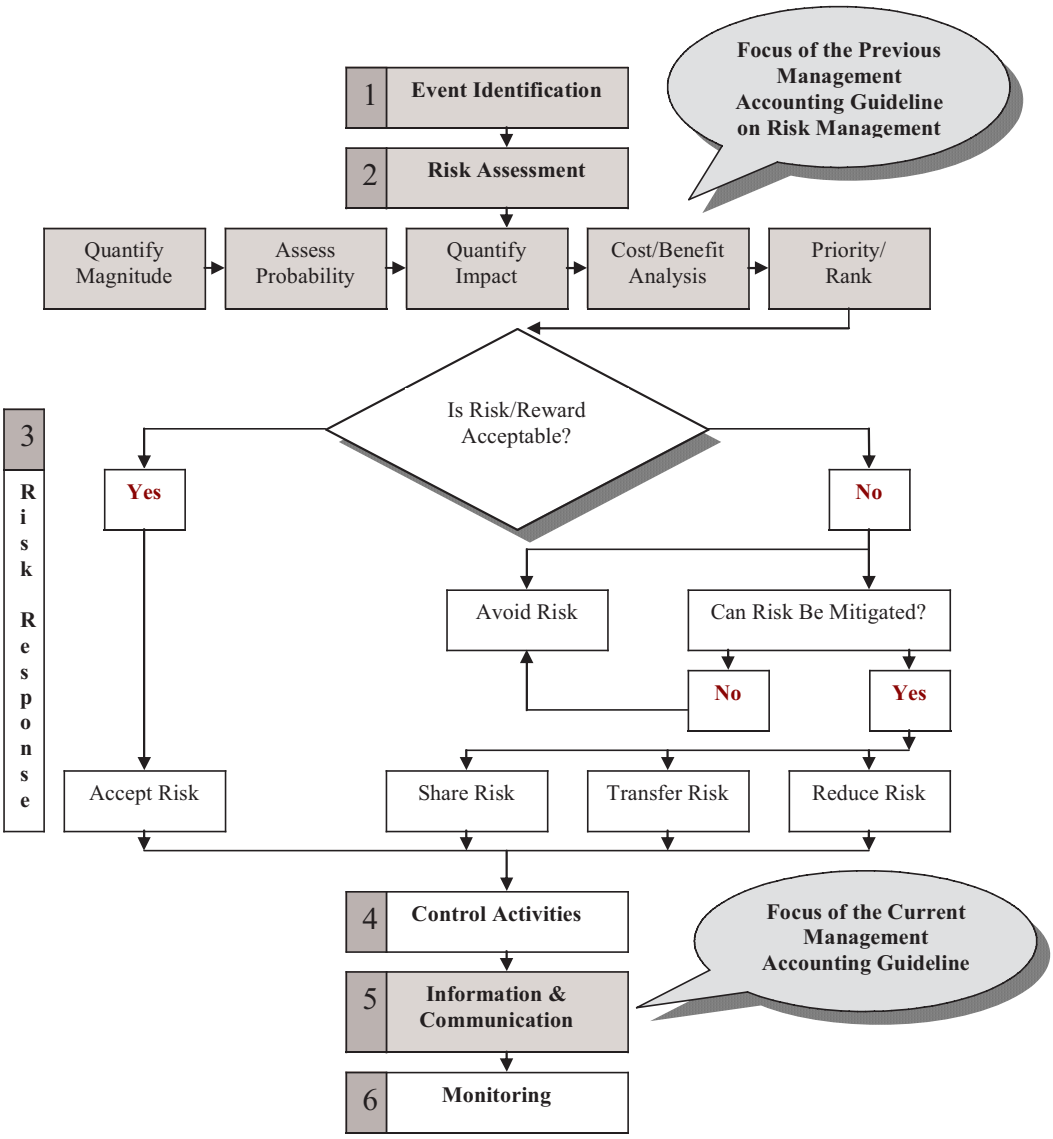
measures for improving the identification, measurement, and management of various organizational risks to improve management decisions. It built on newly created risk assessment requirements of the Sarbanes-Oxley Act of 2002 in the U.S., and similar new regulations in other countries. It also built on work by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the recently issued Enterprise Risk Management Framework, by further specifying the necessary tools for identifying and measuring a broad set of organizational risks.

In that guideline, Epstein and Rejc provided a comprehensive overview of the risk management process (see Exhibit 1), specifically highlighting the role of risk identification and measurement (steps 1 and 2 in Exhibit 1). Risk identification and measurement represent the focus of that guideline, as indicated in Exhibit 1.

Risk management starts with 'Event Identification'. The Guideline suggested that, to minimize risk exposure, organizations should first make a comprehensive list of potential organization-wide risks. Within this step, Exhibit 2 presents a broader framework for identifying risk and listing potential risks organizations often face (see Exhibit 2).

Listing potential organizational risks could increase the attention managers and employees

Exhibit 1: Risk Management Process



Epstein and Rejc, 2005.

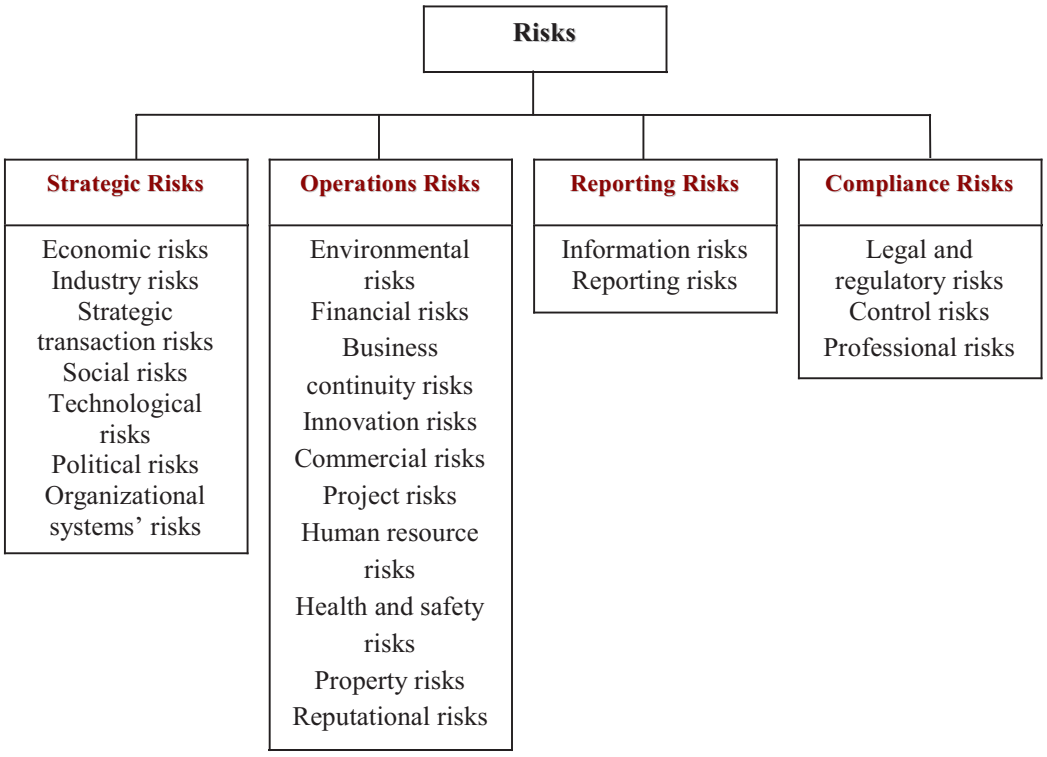
pay to events that might indicate risk. Each organization can develop a combination of techniques and supporting tools to identify risks, such as (a) internal analysis, (b) process flow analysis, (c) discovery of leading event indicators, and (d) facilitated, interactive group workshops and interviews, brainstorming sessions, etc. Developing these techniques and tools will likely ensure that all relevant risks are identified and their sources determined.

Within the 'Risk Assessment' step, all risks identified as potentially important should be assessed for magnitude and probability of occurrence. Various quantitative techniques are available. In addition to assessing the potential cost of a risk materializing, benefits accruing from an appropriate response to the risk should also be assessed. Quantification of both costs and benefits then makes it possible to determine the payoff of a risk management initiative. This Guideline argues that organizations need a framework of key factors (antecedents and consequences) that can enable decision-makers to assess (a) the impacts of risks on costs, but also and more importantly, (b) the benefits offered by successful risk management initiatives.

Exhibit 3 describes the key elements of a measurement model (*Risk Management Payoff Model*) that includes factors for organizational success in dealing with risks, strategically and operationally. The model includes the critical *inputs* and *processes* that lead to risk-related outputs and, ultimately, to overall organizational success (*outcomes*). It also includes specific drivers related to risk-related inputs, processes, outputs, and outcomes. By identifying the causal relationships between these drivers, managers can better understand how risk management strategies, structures, and systems affect organizational performance. The *Risk Management Payoff Model* demonstrates how improved risk measurement and management provides benefits throughout the organization. Benefits extend to (a) enhanced working environment, (b) improved allocation of resources to the risks that really matter, (c) sustained or improved corporate reputation, and (d) other gains, all of which lead to prevention of loss, better performance and profitability, and increased shareholder value.

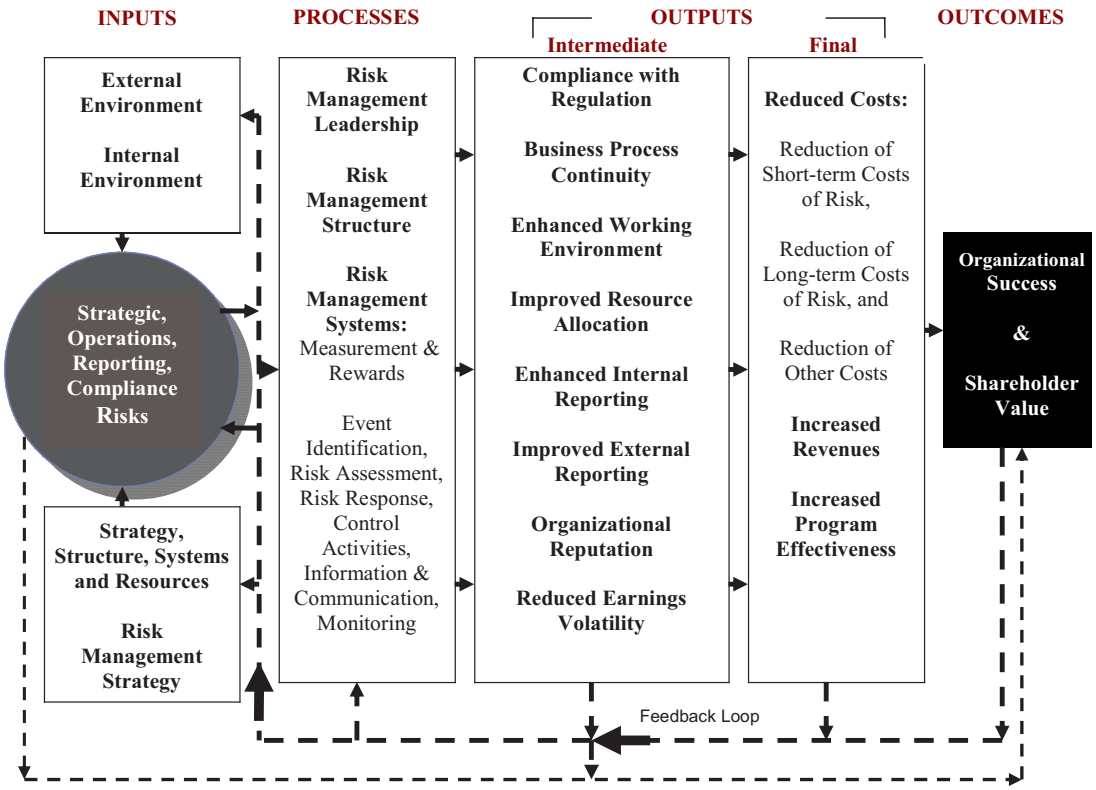
In addition to the *Risk Management Payoff Model*, step 2 in Exhibit 1 includes specific performance

Exhibit 2: Organizational Risks



Epstein and Rejc, 2005.

Exhibit 3: Risk Management Payoff Model



Epstein and Rejc, 2005.

measures for inputs, processes, outputs, and outcomes. Such metrics will of course vary from one organization to the next. This Management Accounting Guideline offers many measures from which managers can select or adapt metrics that are more closely aligned with their organization's risk management strategy. Finally, step 2 in Exhibit 1 includes a formula to calculate the ROI of risk management initiatives, so that managers can better (a) monitor and manage risks, (b) evaluate the profitability of risk management initiatives, and (c) evaluate the tradeoffs between different risk responses.

Having identified the various risks and measured their potential impact, the organization must decide how to respond. This Guideline suggests various approaches and techniques for preventing, mitigating, transferring, and sharing organizational risks. Using the quantification process outlined in the *Risk Management Payoff Model*, management can more knowledgeably determine an appropriate risk response, as well as assess the effectiveness of existing risk management processes and controls. By creating formal internal control systems, detailing how they will identify, measure, and respond to significant risks to their businesses, and then communicating the risks to the appropriate parties, managers can improve organizational operating efficiency and overall organizational success.

THE IMPORTANCE OF ORGANIZATIONAL RISK REPORTING

The focus of this Guideline, *The Reporting of Organizational Risks for Internal and External Decision-Making*, is on risk information and communication (step 5 in Exhibit 1). Along with more rigorous identification and measurement of broad organizational risks, improved reporting (disclosure) of organizational risks is needed so that managers and other stakeholders can more effectively consider those risks and make more informed decisions.

Improved internal decision-making is facilitated when managers apply various analytical approaches to their decisions, and also incorporate numerous variables into capital investment and operating decisions. ROI is calculated, using projections of revenues and costs based on the best available data. Unfortunately, the decision models of many

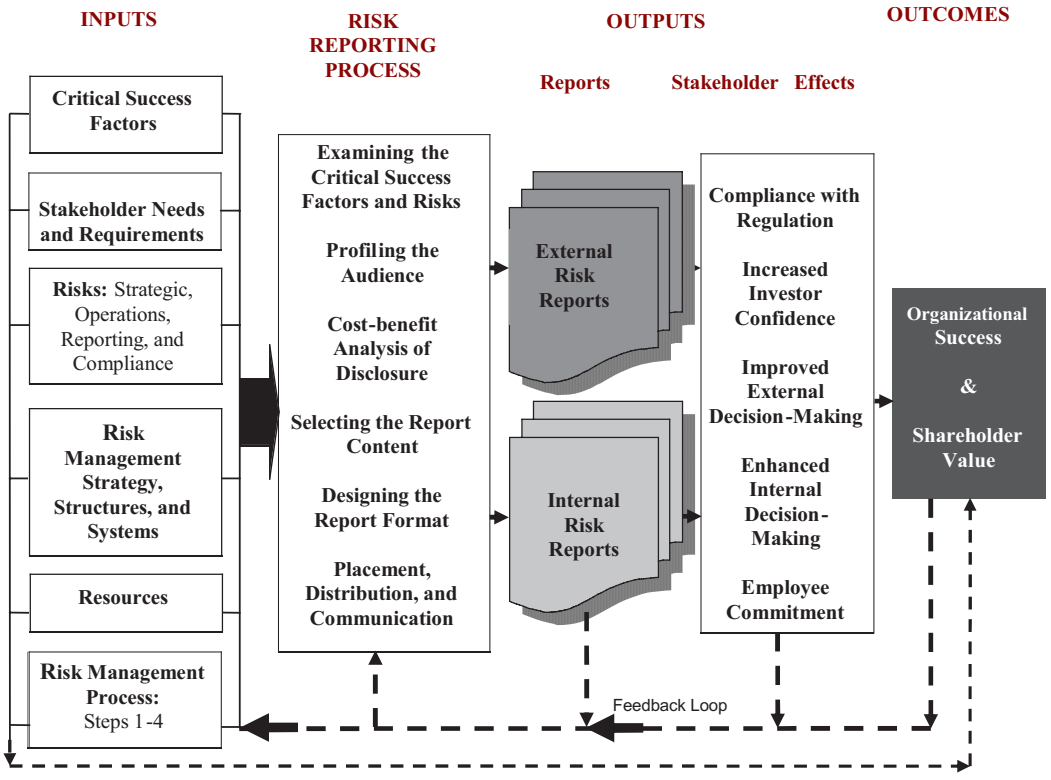
organizations are incomplete, since they do not explicitly incorporate evaluations of potential risks, which has often led to poor decision-making. Organizations can improve decision-making by attempting to formally integrate estimates of a broader set of organizational risk-related costs and benefits into their decisions. These risks include the risks of (a) technological obsolescence of product assembly (or the product or service itself), (b) financial risks, (c) potential breakdowns in the supply chain, (d) risks inherent in new product or service development (and in R&D investments generally), and (e) other risks. As a reliable and timely risk reporting process provides credible information on organizational risks, employees also can make better decisions and accelerate continuous and breakthrough organizational improvements.

Appropriate external disclosure of organizational risks and risk management initiatives allows shareholders and financial analysts to more properly value company shares. Improved disclosures make capital allocation more efficient, and reduce the average cost of capital. Voluntary disclosure also decreases price volatility and narrows bid-ask spreads, enhancing securities liquidity. Customer loyalty may also increase, and fair and favorable media publicity may result.

Exhibit 4 represents a framework for monitoring the contribution of risk reporting. *The Risk Reporting Contribution Scheme* describes the key factors (inputs, processes, outputs, and outcomes) for organizational success in risk reporting.

As Exhibit 4 shows, the quality and success of risk reporting is dependent on various factors; of these, inputs and processes are most critical. ***Inputs*** relate to the *stakeholder risk reporting requirements and expectations*, such as regulatory requirements, investors' and customers' expectations, etc. These requirements and expectations, along with the various *risks* the organization is facing, such as strategic, operational, reporting, and compliance risks, represent the most important inputs to the risk reporting process. Other inputs include the organization's existing *risk management strategy*, and *governance and risk management structures and systems* that provide the context for establishing risk reporting processes. Existing systems, including incentive pressures, may either instill risk awareness in the organizational culture, or inhibit risk management and risk reporting efforts. Therefore, to establish a proper

Exhibit 4: The Risk Reporting Contribution Scheme



basis for effective risk management and reporting, an organization must continuously examine the various internal and external audiences' (stakeholder) requirements, and establish appropriate risk management structures, systems, strategies, and risk culture. Critical inputs to risk reporting also include available organizational resources, such as individuals with the necessary skills and experience, financial resources, and access to required information.

Smooth ***processes*** require committed corporate leaders and focused efforts of risk management leaders. Processes include (a) examining the critical success factors and risks that may endanger achieving business objectives, (b) evaluating the costs and benefits of informed voluntary disclosure to both internal and external audiences, and (c) determining the target audiences for risk reports, the reports' content and format, and their appropriate placement, distribution, and communication.

These processes will ensure various risk reporting ***outputs***, starting with the internal and external reports themselves. High quality and timely risk reports provided to selected internal and external audiences should have specific stakeholder effects, such as (a) improved internal decision-making (managers), (b) full regulatory compliance (government and regulatory institutions), (c) increased investor confidence in capital markets (shareholders), and (d) more general improved external decision-making (customers, suppliers, other business partners, employees, etc.). Effective risk reporting should then ultimately lead to greater overall organizational success and increased shareholder value (***outcomes***). Providing a cause-and-effect format of the various risk reporting activities helps managers understand the value they are receiving from the organization's risk reporting efforts.

Risk reporting also provides critical feedback to the risk management process and constitutes an important element in strategic planning. Although risk management continues throughout the year to accomplish strategic and tactical objectives and allow modification of plans as factors change, strategic planning uses risk reports to develop strategic objectives and strategies. As critical inputs to strategic planning, risk management in general, and risk reporting in particular, reach beyond compliance with increasing regulation. High-performing organizations will leverage their investments in compliance efforts (such as those imposed by the Sarbanes-Oxley Act or other requirements) to build a comprehensive risk management and reporting system that will drive value from a complex, expensive, and mandatory process. Risk reporting will shift from compliance-based to strategy-based, and then further to business-based organizational risk disclosure. This Guideline builds on this, and discusses the critical risk reporting questions in the light of risk reporting's strategic and business role.

The *Risk Reporting Contribution Scheme* can be adapted into any management system. It is compatible with strategic measurement and management frameworks, such as the balanced scorecard and shareholder value analysis, which focus on a better understanding of the causal relationships and linkages within organizations, and the actions managers can take to improve customer and corporate profitability and drive increased value. It is also consistent with other proposed business reporting models, such as the *Model of Business Reporting* (AICPA, 2004).

CURRENT REGULATIONS AND GUIDANCE ON REPORTING OF ORGANIZATIONAL RISKS

Reporting regulations vary greatly around the world. However, there is a clear trend toward requiring greater transparency in financial reporting and more accountability to investors that comes from various sources, including the Sarbanes-Oxley Act in the U.S., the European Union's Company Law Directives, and comparable initiatives in other jurisdictions (for example, the Canadian Securities Administrators rules (2002) or the Companies (Auditing & Accounting) Bill 2003 in Ireland—see Appendix 1 for more detail). CEOs, CFOs, directors, and especially audit committee members of listed companies are being held more accountable for the integrity of their financial statements and the effectiveness of internal controls. Directors and audit committee members are also taking on greater responsibility for oversight of corporate management and the organization's relationship with the external auditor. Investors around the world are thus receiving new reports from management and auditors on the adequacy of internal control over financial reporting.

Although reports on internal control over financial reporting may be instrumental in restoring confidence in the integrity of financial reporting, the reporting of organizational risks must satisfy needs for improved internal and external decision-making. Reports on internal control over financial reporting issued by management and the independent auditor do not provide any assurance

on the viability of, for example, an organization's businesses, or its ability to achieve financial goals. Internal and external audiences need more complete information on the risks organizations face and how they intend to manage those risks. Yet, reporting regulation in highly regulated countries tends to focus on a narrow set of risks, primarily market and credit risks, and risks connected with the use of financial instruments. Currently, regulatory bodies do not explicitly require any integrated framework for broader corporate risk disclosure.

In the absence of specific regulations, managers considering broader disclosure of risk information externally can refer to the **guidance on effective voluntary disclosure** provided by company experiences, professional associations, and academia. The term voluntary disclosure describes disclosures, primarily outside the financial statements, that are not explicitly required by generally accepted accounting principles or regulation. The following frameworks propose to enrich financial reporting by including a section devoted to communicating forward-looking information and describing the risk profile of the company (for more detail on the frameworks see Appendix 2):

- A framework for voluntary disclosure proposed by The American Institute of Certified Public Accountants (AICPA, 1994, 2004).
- A reporting framework published by The Canadian Institute of Chartered Accountants' reporting guidelines (CICA, 2001).
- The COSO Enterprise Risk Management—Integrated Framework (2004a, 2004b).
- A specific model to calculate a risk management initiative ROI proposed by Epstein and Rejc (2005).
- Finally, the SEC's encouragement of disclosure by companies of *forward-looking information* in their annual reports.

Generally, though, an integrated approach to a broader voluntary disclosure of organizational risk and internal reporting of risks is still lacking.

THE RISK REPORTING MODEL

The focus on risk reporting for regulatory compliance is likely to continue. In addition, improved voluntary disclosure will remain a prominent element of greater accountability. Nevertheless, organizations should leverage the knowledge gained by the regulatory-driven compliance efforts to improve overall risk management, its process and reporting, for improved corporate governance and decision-making.

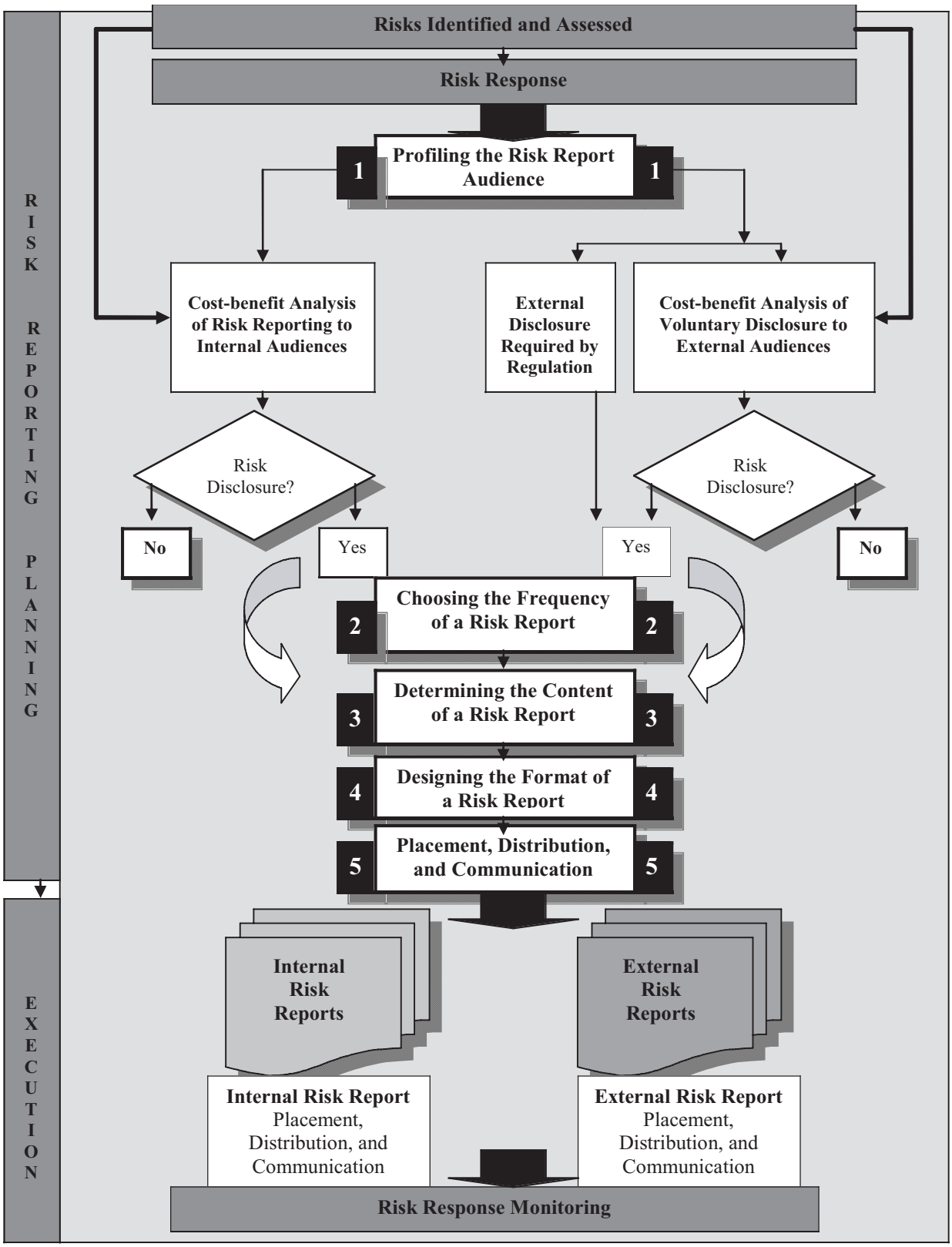
Exhibit 5 provides *The Risk Reporting Model* that is developed to help organizations decide on critical questions related to reporting organizational risks to internal and external audiences, and to carry out risk reporting. These questions relate to (a) the target audience for risk reports, internal or external, each with its various subgroups of stakeholders, (b) the frequency of a risk report, which can be both real-time and periodic, and (c) its content, format, and finally its placement, distribution, and communication.

As seen in Exhibit 5, some information about organizational risks comes directly from the 'Risk Identification' and 'Risk Assessment' steps, while other information comes from the 'Risk Responses' step. They typically differ in informational accuracy and completeness. Information from risk identification is important for on-time risk reporting and completeness of risk reports, while information arising from risk assessment and risk response add more accuracy to the disclosure on risk management. Both types of risk information are important for credible and on-time reporting of organizational risks.

Organizations must decide on each of the risks identified, assessed, or responded to, whether they should be reported to any of the audiences, and if so, what level of detail to provide. Determining the target audience, an important starting point, affects other risk reporting decisions. Whenever a disclosure is required by a regulatory requirement, as may be the case in external risk reporting, the organization must comply and provide appropriate disclosure. On the other hand, voluntary disclosures should be subject to careful cost-benefit analysis of audiences' needs and the disclosure. Organizations should compare (a) the benefits of a specific disclosure (type and detail of risk) to improved internal and external stakeholder decision-making and the organizations' businesses with (b) the costs of disclosing.

The next section describes in detail the first step in the *Risk Reporting Model*, profiling the risk report audience. Discussion on the audiences for risk reports will include who they are and their specific organizational risk-related interests. The remaining critical risk reporting issues—frequency, content, format, and placement—will be addressed separately under the 'Guidance on

Exhibit 5: The Risk Reporting Model



the Reporting of Organizational Risks for *Internal Decision-Making*' and the 'Guidance on the Reporting of Organizational Risks for *External Decision-Making*', respectively. The section numbers correlate with Exhibit 5.

1 Profiling the Risk Report Audience 1

Profiling The Risk Report Audience

Reporting organizational risks should operate on multiple levels to address the needs of diverse audiences, each with their own specific needs, requirements, expectations, agendas, and levels of expertise. Exhibit 6 presents the most important internal and external audiences for internal and external risk reports.

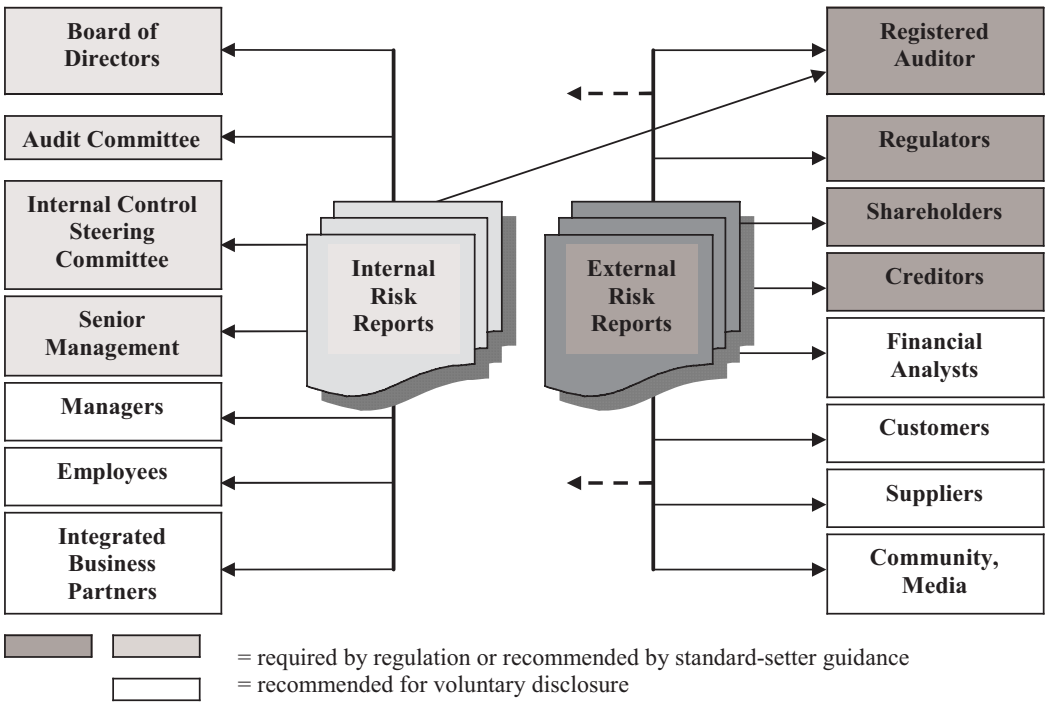
Although internal risk reports aim exclusively at internal audiences, from a broader perspective external risk reporting, including corporate annual reports, may include both external users and interested internal groups (see the two dashed arrows in Exhibit 6).

As Exhibit 6 shows, both internal and external audiences can be further divided into two subgroups. On one hand, some audiences (audit committees, internal control steering committees, boards of directors, and senior management among internal audiences, and registered auditors, regulators, shareholders, and creditors among external audiences) must or should be informed about the organizational risks and risk management processes because of regulation or recommendations in standard-setter guidance. Voluntary disclosure to other internal audiences (managers, employees, and integrated business partners), and external stakeholders (financial analysts, customers, suppliers, community, and media), is recommended because of anticipated benefits to improved decision-making.

Responsibilities of some within the internal audiences are listed below:

- The board of directors has the primary oversight responsibility for developing and implementing the organization's mission, values, and strategy, and must carefully review corporate processes of risk identification, monitoring, and management. The board also originates risk philosophy, risk appetite, and risk tolerances. Specific reviews of financial objectives, plans, major capital expenditures, and other significant material transactions also typically fall within a board's responsibility. These responsibilities require broad and transparent reporting on the various organizational risks—strategic, operational, reporting, and compliance risks.

Exhibit 6: Internal and External Audiences Interested in Risk Reports



- Regulations require audit committees to be informed about significant deficiencies and material weaknesses in internal control over financial reporting. More specifically, the audit committee has been given delegated responsibility from the board of directors to direct oversight over internal control, and must receive assurance of, and other information regarding, internal control from members of management directly responsible for achieving internal control objectives.
- The internal control steering committee is an important recipient of internal risk reports, since it must ensure that internal control oversight and internal controls function as intended. Although their risk interests are therefore primarily oriented to reporting and compliance risks, they are also interested in strategic and operational risks. The committee is made up of the president, the vice-president and the CFO, the vice-president and Chief Audit Executive, the senior functional officers, and heads of the operating units of the organization.
- Senior management's needs for information on organizational risks are of specific importance. They need relevant, accurate, and reliable risk reports on a real-time and periodic basis for effective decision-making and control. Only by generating a wealth of risk-related information can organizations inform senior management with facts, not intuition, so that they can then appropriately integrate that information into management decisions and make more effective decisions to optimize company strategy and goals.
- Similarly, managers need relevant and accurate real-time and periodic risk reports. Without proper internal reporting on organizational risks—strategic and operational, in particular—managers cannot (a) make optimal strategic and tactical decisions, (b) evaluate the payoffs of specific risk management initiatives, or (c) make new capital project decisions while explicitly acknowledging the potential risks and their costs on organizational profitability.
- Employees, for example, prefer to work for companies with safe and healthy working conditions. Thus, they also often want information on the various risks the organization faces.
- In a growing number of entities, integrated supply chain partners are considered internal rather than external participants. Interdependence of partners in an extended supply chain requires cooperation and collaboration in risk management. Integrated supply chain partners need real-time information on various organizational risks, particularly those related to integrated processes and technologies so that they can contribute to maximum customer satisfaction and achieve optimal performance for the supply chain as a whole.

For years, reporting has often been based on mistrust, as senior management questioned the willingness of outsiders to handle corporate information responsibly. Today, the premise is not just that senior management should base the risk reporting communication policy on trust to be more accountable; organizations can also expect tangible benefits from fair and broad disclosure of organizational risk management. With respect to external stakeholders, owners of the organization were typically considered the principal external audience for external risk reporting. However, with increased recognition of the role of customers, suppliers, creditors, and communities in successful achievement of organizational goals, external risk reporting should not be fragmented but unitary.

- Owners primarily rely on financial reporting to assess the current financial condition of the organization, its financial performance over time, and its prospects. However, current and prospective owners have interests beyond the relative transparency of an entity's material costs and liabilities, and expect information on all organizational risks (including reputation risks) that could adversely affect the organization's future financial condition and performance. More specifically, shareholders have an interest in a broad set of risks, including compliance and reporting risks as well as strategic ones. These strategic risks would include risks such as: changes in supply and demand, changes in competitive structure, introduction of new products and services, concentration risks, risks of technological obsolescence of product assembly or the product itself, engineering failures, risks of poorly managed government relations, and environmental risks. In addition, shareholders, creditors, and financial analysts are particularly interested in some operation risks, such as financial risks (foreign exchange, strategic equity, commodity, asset liquidity, and employee stock option program risks), R&D and innovation risks, reputation risks, health and safety risks, etc.
- Creditors have a particular vested interest in complete and timely disclosure of organizational risks, to assess credit risks and potential joint liability for loans secured by, for

example, contaminated properties. They may be interested in strategic risks as well.

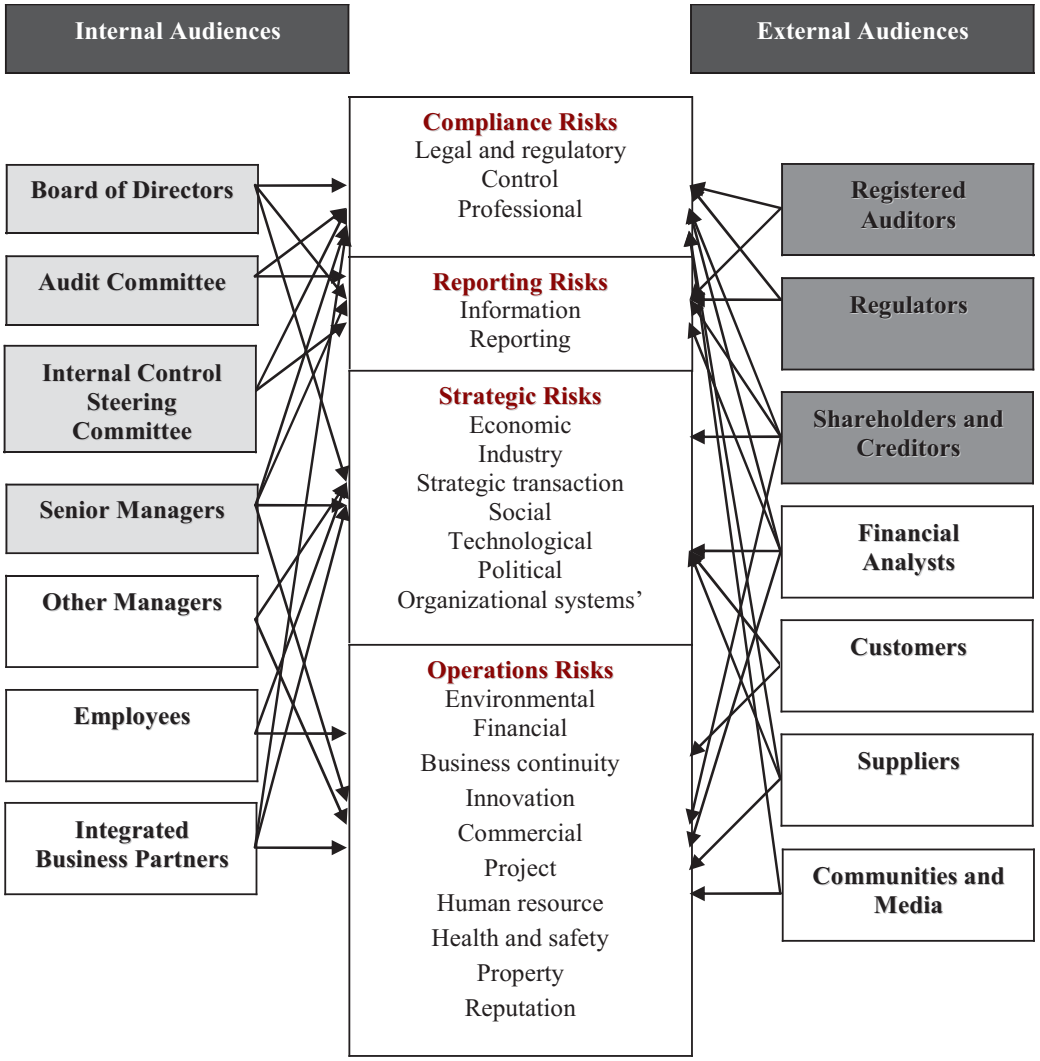
- With increased regulation of internal control over financial reporting, representatives of regulators and registered auditors are interested in both external and internal risk reporting. Primarily, however, they are interested in (a) compliance risks, such as risks of unreliable and incomplete financial information for internal decision-making and for external reporting, and (b) reporting risks, such as risks of data accuracy and reliability. In addition, they may also be interested in operations risks, such as risks related to product quality and product safety, environmental compliance, etc.
- The list of external audiences for risk reporting also includes customers, suppliers, and communities (interest groups, media, the scientific community, and the general public). This extended external audience has wide-ranging interests in the risks organization face, and how it manages risks and turns them into business opportunities.

Exhibit 7 lists the major risk areas of interest to identified internal and external audiences.

Exhibit 7 will not universally apply, and the identified stakeholders' interests should not be considered exclusive. Those audiences that have become particularly important with the new internal control regulations are primarily interested in reporting and compliance risks, while other audiences' interests span strategic and operational risks as well.

The appropriateness of risk report frequency, content, format, and placement can now be discussed in the light of known audiences.

Exhibit 7: Risks of Primary Interest to Internal and External Audiences



GUIDANCE ON THE REPORTING OF ORGANIZATIONAL RISKS FOR *INTERNAL DECISION-MAKING*

As shown in the previous section, internal audiences for risk reporting include the board of directors, the audit and internal control steering committees, senior management, other managers, employees, and integrated supply chain partners. The interests of these various internal constituents vary both in scope and the detail of required risk information. From the strategic and business perspective, i.e. for improved strategic planning and execution as well as for more informed and improved operational decision-making, the primary internal audiences for risk reports are boards of directors, senior management, and other managers. These decision-makers must receive comprehensive risk reports covering strategic, operational, reporting, and compliance risks, detailed when reported on a real-time basis, and aggregated when reported periodically. Other internal audiences' requirements or needs are narrower, focused on specific risks that are not necessarily detailed. For this reason, the subsequent sections provide guidance on internal risk reporting specifically oriented to boards of directors, senior management, and other managers.

2 Choosing the Frequency of a Risk Report

The Frequency of Internal Risk Reports

How to decide which risks to report, and in what detail, must be discussed in the light of risk reporting frequency. Internal risk reports can be either real-time or periodic. Reporting frequency therefore importantly influences the content, format, placement, distribution, and communication of risk reports.

Internal real-time risk reporting is specifically important for operational decision-making. Senior management, for example, needs timely information on risks to make informed investment decisions. Other managers responsible for resource allocations also need real-time information on the risks an organization faces. Such risk reports are provided when specific circumstances require it, such as the occurrence of a risk event. The time available to receive data on a specific risk, process it, and respond to the external process is dictated by the time constraints imposed by the organization's risk management process. Exhibit 8 represents the process of determining the risks to be reported on a real-time basis to internal audiences.

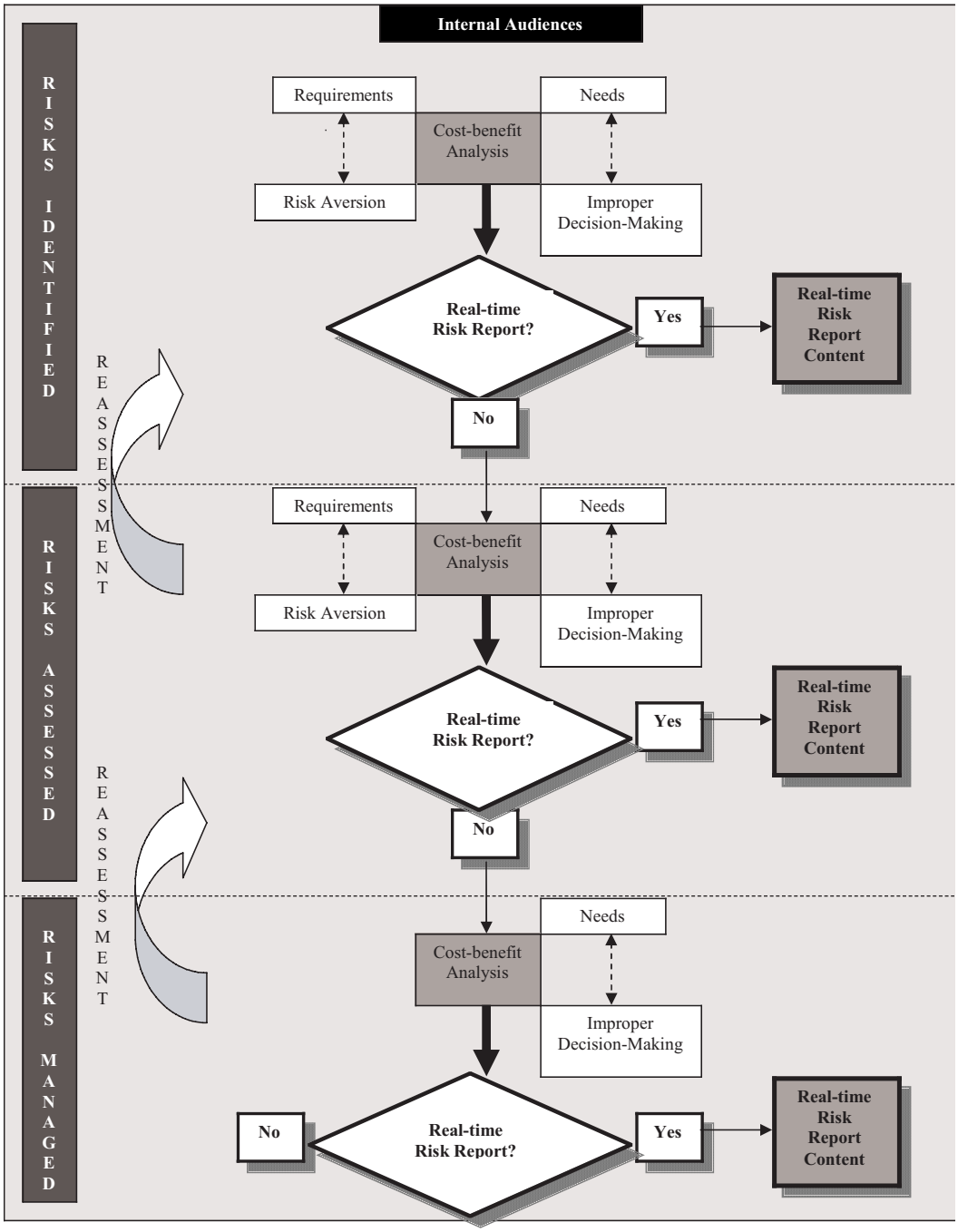
When deciding on what risks to disclose on a real-time basis, organizations need to compare the costs and benefits of disclosure. As seen in Exhibit 8, the cost-benefit analysis of risk disclosure must be made throughout the risk management process. The completeness and accuracy of risk information will increase in moving from risk identification to risk assessment, and then to the risk management (risk response) phase. Consequently, the cost-benefit analysis may provide different results.

For identified but not yet assessed risks, a brief cost-benefit analysis must first take place to determine if they should be reported on a real-time basis. Senior management needs are considered, along with the benefits of improved decision-making, and the potential reduction in appropriate risk-taking by managers. The cost-benefit analysis must specifically consider reporting of risks that endanger the critical success factors, i.e. those aspects of an organization's business that are especially important to its success. Critical success factors include a handful of activities or unique capabilities of overriding importance to the strategic and operational success of a particular organization. More generally, to determine which risks to disclose internally, organizations must consider whether disclosure of a specific organizational risk would adversely affect the organization by stimulating managers to make inappropriate strategic or operational decisions. Even though definitive quantification of all costs and benefits of risk reporting is complex and difficult, often requiring judgment, organizations must attempt to assess both. Whenever the benefits of a real-time risk disclosure exceed its potential costs, real-time risk reporting is appropriate.

Some identified risks not disclosed in the first phase because of the unfavorable output of the preliminary cost-benefit analysis may be disclosed when they are fully assessed. With new and more reliable data on the actual dimensions of a specific risk, the cost-benefit analysis may show that the previously undisclosed risks should now be disclosed to internal audiences on a real-time basis.

Finally, some risks that—although assessed—still have not been disclosed to senior management, for example, may pass the test of the cost-benefit

Exhibit 8: Determining Risks to Be Reported on a *Real-time* Basis to Internal Audiences



analysis when they are managed. As shown in Exhibit 8, different phases of risk management influence which risks to report on a real-time basis. The more information an organization has about a specific risk, the higher is the reliability of the decision on reporting, and the content of the risk report if it is issued, and the less the concern over making a real-time risk disclosure. An effective system of real-time risk reporting calls for a good risk management process, including event identification, risk assessment, risk management, and risk response.

A template for more detailed calculation of the cost-benefit analysis of real-time risk reporting is provided in Exhibit 9. It describes the necessary steps in a typical cost-benefit analysis, regardless of the phase where the cost-benefit analysis of real-time risk reporting is taking place. In the first step of the cost-benefit analysis, the benefits

Exhibit 9: Calculating the Costs and Benefits of Internal *Real-Time* Risk Disclosure

CALCULATE THE BENEFITS OF INTERNAL REAL-TIME RISK DISCLOSURE

Outputs	Benefits	Monetary Value
Compliance with Regulation	Reduced costs of prosecution and penalties	$.....
Improved Operational Decision-Making	Labor hours saved, machine hours saved, increased on-time deliveries reducing cost of grievances etc.	$.....
Enhanced Working Environment	Increase in output (units produced, services offered)	$.....
Improved Resource Allocation	Savings in costs based on efficient capital allocations	$.....
Improved Strategic Decision-Making	Revenues generated from new strategic initiatives	$.....
	Total Benefits	$.....

CALCULATE THE TOTAL COSTS OF INTERNAL REAL-TIME RISK DISCLOSURE

Costs		Value
Real costs of risk reporting	Cost of gathering data, analysis, reporting etc.	$.....
Potential costs of managerial risk aversion	Cost of lost business opportunities	$.....
Potential costs related to employees	Bargaining disadvantage with employees	$.....
	Total Costs	$.....

COMPARE THE BENEFITS AND COSTS OF INTERNAL REAL-TIME DISCLOSURE

$$\text{COST-BENEFIT ANALYSIS} = \frac{\text{Total Benefits}}{\text{Total Costs}}$$

of a real-time risk disclosure must be expressed in monetary terms. The key potential benefits of internal risk reporting include, for example, improved internal decision-making that leads to cost savings or increased revenues. An enhanced working environment may also be a benefit of risk disclosure to employees, leading to increased employee trust, commitment, creativity, and productivity. Potential costs of internal risk reporting relate to dysfunctional behavior of different internal audiences, such as a reduction in appropriate risk-taking of managers that is necessary for business success.

Expressing benefits of internal *real-time* risk disclosure in monetary terms is illustrated through short examples in Exhibit 10. Specific risk disclosure outputs that result in benefits are presented, followed by the relevant calculations to capture the monetary value of realized benefits.

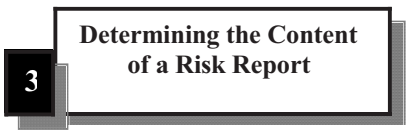
On the other hand, ***Internal periodic risk reporting***, provided on a monthly, quarterly, or yearly basis, allows more precise cost-benefit calculations of risk disclosure, if deemed necessary. In Exhibit 8, two reassessment loops are presented, indicating the need for subsequent cost-benefit analyses to confirm the results of the preceding judgments or analytical results. The primary purpose of periodic internal risk reports is to provide boards of directors, senior management, and other managers with well-processed and aggregate information about various relevant organizational risks, with trend indicators and periodic comparisons, to improve their decision-making. The results of reassessment loops during the real-time risk reporting process contribute to decisions on what information to include in periodic risk reports.

Exhibit 10: Calculating Monetary Benefits from Internal *Real-Time* Risk Disclosure

DISCLOSURE OUTPUTS	BENEFIT	CALCULATION OF MONETARY BENEFIT
Compliance with Regulation	Reduced costs of prosecution and penalties	Monetary benefit equals the reduced costs of prosecution and penalties; estimates of the costs should be based on historical evidence
Improved Operational Decision-Making	Labor hours saved	Benefits equal to the number of hours saved, multiplied by the standard labor wage, and adjusted with a benefits factor
	Machine hours saved	Benefits arise out of optimal use of existing resources and are equal to the costs of amortization that relate to machine hours saved
	Increased on-time deliveries reducing cost of grievances	If the result is reduction in grievances, the average cost per grievance provides a basis for estimating the benefits
Enhanced Working Environment	Increase in output (units produced, services offered)	Benefits can be calculated as additional sales minus marginal sales expense
Improved Resource Allocation	Savings in costs based on efficient capital allocations	Benefits can be traced to reduced debt financing or lower weighted average cost of capital
Improved Strategic Decision-Making	Revenues generated from new strategic initiatives	Benefits are equal to the generated new sales or the discounted cash flow from new strategic initiatives

Periodic internal risk reporting contributes to strategic oversight and decision-making, and improved operational business decisions. This type of risk reporting provides general information to interested audiences on the risk management processes, without unnecessary detail. Exhibit 11 summarizes the process of selecting risks for periodic risk reporting to internal audiences.

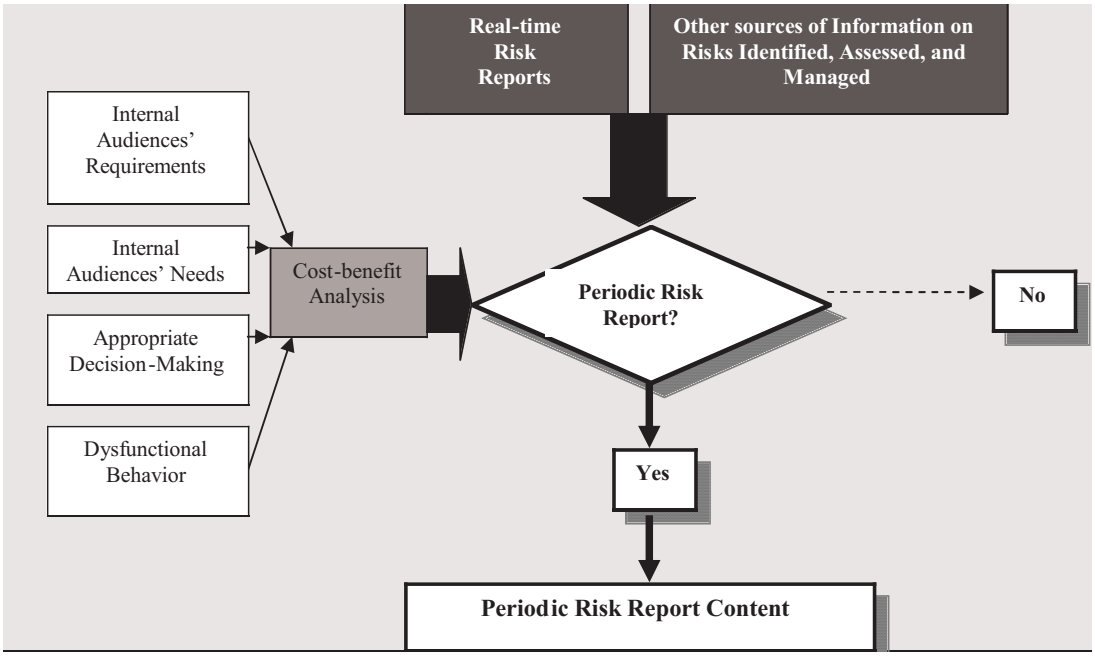
Determining the content of an internal periodic risk report starts with listing risks in the specific phases of risk management process (risks identified, risks assessed, and risks managed), including those identified in real-time risk reports. A listing of those risks that have already been assessed and appropriately managed would typically be accompanied with a detailed description of their characteristics and potential effects. The consideration of risk disclosure will start with the primary internal audiences' requirements. Audit committee risk reporting requirements related to compliance and reporting risks are an example. Organizations must disclose risks to internal audiences that are required by regulation. Otherwise, detrimental costs of non-compliance may result. An organization should then consider other internal audiences' needs, and compare them to the costs of disclosure. Organizations will decide on periodic risk disclosure based on a cost-benefit analysis (which is similar to the cost-benefit analysis provided in Exhibit 9).



The Content of Internal Risk Reports

The most important content issue relates to what risk information to provide for optimal internal-decision-making, without causing

Exhibit 11: Determining Risks to Be Reported *Periodically* to Internal Audiences



unnecessary alarm that would inhibit appropriate risk-taking. More specifically, how detailed should the reports be in specific circumstances? Generally, risks can be classified into one of the following four broad categories—strategic, operational, reporting, and compliance (see also Exhibit 2). *Strategic risks* relate to an organization's choice of strategies to achieve its objectives. By their nature, these risks can endanger the organization's achievement of high-level goals that are aligned with and support its mission. To assess strategic risk calls for questioning whether management has misread its environment. *Operational risks*, on the other hand, relate to (a) threats from ineffective or inefficient business processes for developing, acquiring, financing, transforming, and marketing goods and services, and (b) threats of loss of firm assets, including its reputation. *Reporting risks* relate to the reliability, accuracy, and timeliness of information systems, and to reliability or completeness of information used for either internal or external decision-making. Finally, *compliance risks* address the inadequate communication of laws and regulations, internal behavior codes and contract requirements, and inadequate information about failure of management, employees, or trading partners to comply with applicable laws, regulations, contracts, and expected behaviors (Epstein and Rejc, 2005).

In determining risks to be reported internally, the cost-benefit analysis will provide a general answer, but not identify the level of risk detail to disclose. What detail to include will vary with the frequency of risk reporting, and with the phases of the risk management process. ***Internal real-time risk reports*** for senior management and other managers responsible for resource allocations and other strategic and operational decision-making may often include very little information on the risk event. This may be because specific circumstances may have required quick reaction to a risk, allowing insufficient time to gather all necessary information. ***Internal periodic risk reports*** allow and require more careful consideration of included details. Reliability of risk information, on the other hand, should increase with each subsequent phase of risk management. To achieve this, the risk information detail should increase with each phase as well.

Exhibit 12 details the risk information that should be disclosed at different risk management levels—at the risk identification, the risk assessment, and the risk response levels respectively.

As presented in Exhibit 12, a risk report may include the following sections, depending on the phase of the risk management process where a specific risk occurs:

1. **Risk description.** It can be general (the risk identification level) or detailed (required at the

Exhibit 12: Details of Risk Information Disclosed at Various Phases of the Risk Management Process

INFORMATION	RISK IDENTIFICATION LEVEL	RISK ASSESSMENT LEVEL	RISK RESPONSE LEVEL
Risk Description	General	Detailed	Detailed
Impact	• Potential operational • Potential financial • Potential impact on other risks	• Current operational • Current financial • Impact on other risks • Future financial	• Current operational • Current financial • Impact on other risks • Future financial
Prevention Plans and Goals	NO	YES	YES
Controls Put in Place	YES	YES	YES
Recommendations	YES	YES	YES
Effects of a Risk Response	NO	NO	Potential/ Actual

risk assessment and risk response level). In real-time risk reports, risks will often be reported when they occur at the event identification level; periodic risk reports, on the other hand, will typically include risk information from all three levels.

2. **Impact.** Internal audiences must be provided with enough clear and sufficient information to allow them to understand the potential or existing operational and financial impact of the reported risk. In addition, an explanation of the impact of combined risks on the organization as a whole may be provided. Risk managers need to explain the link between high risk events and risk response activities, and their financial consequences. Understanding these links and the financial impact is critical for improved decision-making. The internal risk report's ability to report across the organization will allow internal users to identify risks in the aggregate, and determine gaps in the risk management strategy.
3. **Previous plans and goals.** These should be disclosed with the risks, to permit comparisons between actual achievements and planned results. This content item is relevant at the risk assessment and risk response level.
4. **Controls put in place.** These may be specifically important for boards of directors, audit committees, and steering committees, all of whom have responsibility for oversight, and senior management and other managers who are responsible for decision-making. The role of this type of information is important in all phases of the risk management process, as it relates to actions taken and those responsible for them.
5. **Recommendations.** Risk reports must also include recommendations for the intended internal audiences. Risk reports cannot determine how the CEO, CFO, and other senior managers should respond to individual findings. However, the recommendations should be precise, business-focused, and pragmatic, so that the recipients of reports feel sufficiently informed to act. For example, an organization may face a human resource-related risk within a process that is found to be dependent upon the skills of one individual. The risk report recommendations might suggest an additional hire, cross-training, or alternatively improving documentation so that a non-specialist could operate the process.
6. **Effects of a risk response.** Internal risk reports to the board of directors, senior management, and other managers should also include details on the potential or actual effects of a risk response. This information can only be disclosed at the risk response level.

To determine the content of a risk report, the following questions also need to be answered:

1. **Type of data.** The type of data must be selected. Different details of risk reporting call for different types of data—qualitative or

quantitative, different metrics, and other tools (such as graphs, exhibits, or scenarios). Graphs and exhibits are specifically useful. However, the report must include sufficient relevant technical detail needed by those responsible for taking action.

2. **Metrics.** More detailed risk reports should explain presented metrics. In periodic reports, metrics must be disclosed consistently from period to period, to the extent they still are relevant. However, a decision to report on a specific risk with a specific metric in one period does not require continuing disclosure if it is no longer relevant, or if a more relevant metric becomes available.
3. **Context.** The context of reported risks must be appropriately explained. Managers seeing only facts without context in risky situations may react inappropriately. In addition, reporting of specific risks must include sufficient evidence to influence proper decisions. For example, some managers may require overwhelming evidence before they accept a problem's existence; others may simply need sufficient evidence to understand the nature of the problem. Risk managers may therefore decide to include information on strategy, actions, and performance in addition to information specifically focused on risk. This broader description should be narrative, and accompany a quantitative presentation of the risks. Alternatively, the risk report should clearly describe the status of the organization's processes and activities related to risk management initiatives.

Exhibit 13 provides an example of how the content of a risk report can be structured when providing real-time information on an assessed risk. The structure of this report follows the information details outlined in Exhibit 12. It does not provide all relevant details, but it does provide guidance on what to report on a real-time basis when there is available data. The first section provides a detailed risk description of two risk events resulting in understaffing; both are assessed. Subsequent sections include details on the current operational and financial impact, impact on other risks, and future financial impact and its probability. Further, previous plans and goals are revealed, as are the controls put in place and recommendations to managers.

The real-time risk reports on the risk identified or responded to should be prepared using a similar structure.

As outlined earlier, risk managers striving to provide the internal audience with the desired level of understanding must assure that risk reports are stated in business terms, and with sufficient detail. In many cases, organizations may supplement risk reports with graphical representations of the causal relationships between various drivers of risk management, and the impacts of these on organizational success. Such representations can be very useful in describing the potential operational and financial impact of risks, or their impact on other risks to which the organization is exposed. They are also useful to present the expected consequences of an appropriate risk response, thus providing managers with a better understanding of controls put in place and expected results. Exhibit 14 provides an example that describes the potential effect of an appropriate risk response to a business continuity risk.

Exhibit 14 shows numerous drivers of success in the risk management process. At the bottom of Exhibit 14, the critical drivers include ongoing monitoring of various risks and increased risk awareness (inputs). These are expected to lead to improved event identification and assessment, and the response of appropriate risk management spending. In this specific example, the appropriate level of risk management spending relates to increased investments in flexibility, which will lead to the desired output—business process continuity. Consequently, productivity will increase and organizational reputation will improve, both of which generate greater sales. These beneficial outputs will lead to increased revenues, while business process continuity will also help contain overall costs. Finally, the increased revenues and sustained costs will lead to increased organizational success (outcome).

Internal audiences will be interested not only in disclosure of specific risks, but also in the risk management process. A well established and properly managed process will assure internal audiences about the reliability of risk reports. Organizations must therefore include information on the quality of their risk management process, particularly in their periodic risk reports.

TELUS Corporation, Canada's second largest telecommunications company, developed a risk reporting approach that is based on *annual risk assessment*, *quarterly risk assessment review*, and *engagement/project specific risk assessments*. The annual risk assessment, reported to the CEO, CFO, and Audit Committee and updated quarterly throughout the year, is a key input to strategic planning. The engagement/project specific risk assessment process performs detailed real-time

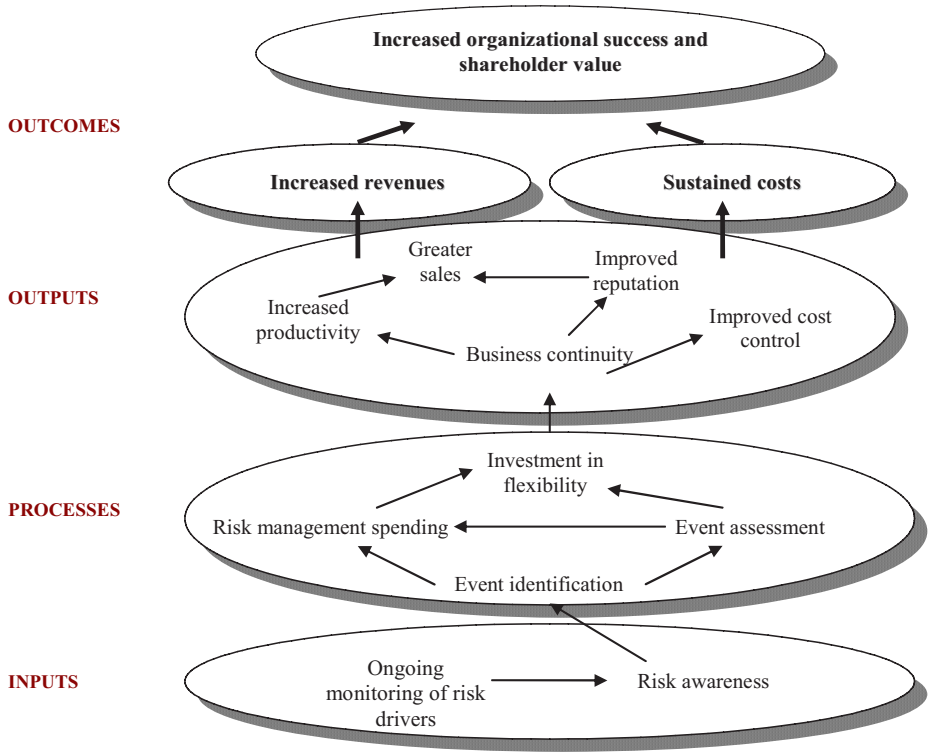
Exhibit 13: Example of a *Real-Time* Risk Report Content Disclosing an Assessed Risk

REAL-TIME RISK REPORT ON A HUMAN RESOURCE RISK: UNDERSTAFFING		
Detailed risk description	• Unexpected trend in higher compensation and expanding job opportunities in the job market caused fewer offers being accepted, resulting in too few staff • Inadequate needs/specifications description resulted in hiring unqualified staff	
	Risk assessment	
	10% reduction in hiring due to fewer offerings— 18 unfilled positions	Likelihood: 100%
	5% reduction in hiring due to poor candidate screening— 9 unfilled positions	Likelihood: 100%
Current operational impact	• Breakdown in business process continuity in manufacturing divisions resulting in a downturn of on-time deliveries from 85% to 75% • Two customers canceled their contracts	
Current financial impact	$ 5,000,000 of lost revenues	
Impact on other risks	The lack of staff in the manufacturing division imposes additional productivity burdens on existing employees, which may endanger their safety in the workplace (health and safety risks) and/or cause lower product quality (commercial risks)	
Future financial impact	$3,000,000 of lost revenues	Likelihood 18%
Previous plans and goals	Organization decided to hire 180 new qualified staff across all manufacturing divisions to meet customer demand without overstaffing and to maintain 22% staff cost per dollar order	Tolerance: • 165-200 new qualified staff; • staff cost between 20% and 23% per dollar order
Controls put in place	• Strengthened quality control in manufacturing divisions • Ensuring proper fit and suitability of employees' personal protective equipment • Regular reviews of staff competencies	
Recommendations	• High quality supervision and leadership • Change in compensation schemes to additionally reward productivity and quality of manufacturing staff	

This draws on an example from Committee of Sponsoring Organizations of the Treadway Commission, 2004b.

risk assessments, and provides updated and new risk and control exposure information to the annual and quarterly reports. In an internal quarterly risk report, for example, a bubble chart indicates the key risk profile of the company (Exhibit 15 provides a modified example of a TELUS bubble chart). Bubbles relating to critical risk areas, such as security, business operations, technology, information, financial, strategic initiatives, people, and others, include most relevant risk items that change with circumstances, as do critical risk areas. The 'Security' bubble may include the following risk items: IT security, physical security, and network

Exhibit 14: Causality of Risk Management Drivers to Describe Potential Effects of a Risk Response



security. The 'People' bubble may include security awareness, employee skills, retention and recognition, vandalism, and legal and ethical compliance. Each of these specific risk items is colored with yellow, orange, or red (see the shading legend under Exhibit 15), indicating the severity of threat (TELUS, 2006).

In addition to the bubble chart, historical (quarterly) risk ratings present the risk areas and their specific risk items (see Exhibit 16 for an example). Again, colors yellow, orange, and red (see the shading legend under Exhibit 16) indicate the risk rating status. In addition, management owner, management actions, and internal audit actions are indicated (TELUS, 2006).

4 Designing the Format of a Risk Report

The Format of Internal Risk Reports

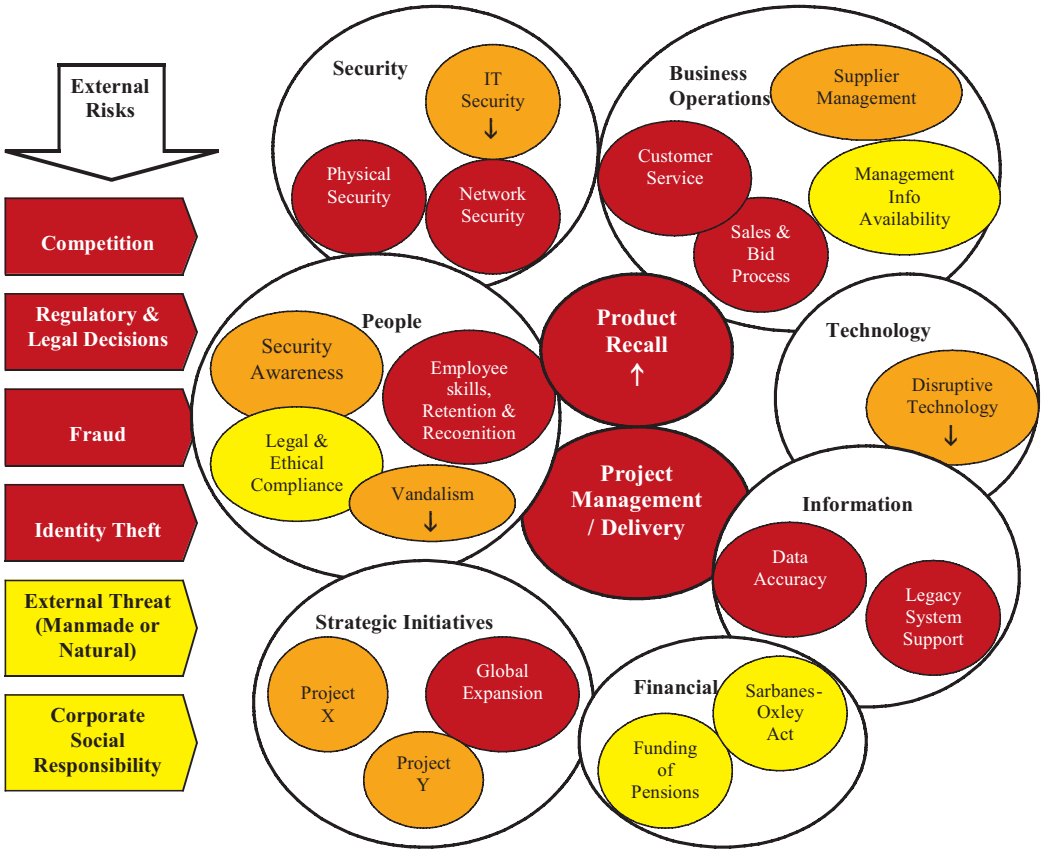
Risk information must be presented in an appropriate structure. If the format of the risk report obscures risk information, time and additional resources may be required for clarification, and users of risk reports may make less informed decisions that could adversely affect the organization's success.

Internal real-time risk reports for senior management and other managers responsible for resource allocations, investment decisions, and other strategic and tactical decision-making should allow users to drill down to examine the underlying data. Exhibit 17 provides an example of a real-time risk report for senior management that is presented in a 'dashboard'-style.

Organizations use dashboard-style reports to enable management to quickly determine the degree of alignment of the entity's risk profile with risk tolerances. Where misalignment occurs, and any existing risk responses or controls are not performing as expected, management can take corrective actions.

As Exhibit 17 shows, the first reporting level provides key risk categories (operations, strategic, compliance, and reporting) with risk sub-categories (such as environmental, financial, and innovation risks). Each relevant risk sub-category, previously identified as appropriate for real-time risk disclosure, is marked according to the phases of the risk management process: risk identified, risk assessed, or risk responded to. As senior management drills down to examine the risks in more detail, the next reporting level identifies whether the risks are safely within, near, or beyond risk tolerances. Colors green, yellow, or red (see the shading legend) may be

Exhibit 15: An Example of a Bubble Chart with Key Risk Profile for the Internal Quarterly Risk Report



Adapted from TELUS, 2006.

Shading legend: yellow = 

orange = 

red = 

used for this purpose. Correlated risks (two or more independent risks that, if they occur, cause far greater loss than the sum of individual losses), must be marked specifically, for example with a black color. Further drilling down the information source provides specific information on that risk.

To the extent possible, the risk-related information should always be supplemented with charts, graphs, and exhibits to improve and expedite the user's comprehension. An example of such an exhibit has already been shown in Exhibit 14, which graphically shows the causality of risk management drivers.

Internal periodic risk reports (see Exhibit 18) will include more general information on the risks, indicating trends or changes in risks. Risk information may be organized around specific key risk categories rather than around phases of the risk management process. Dashboard-style reports may be very useful for periodic risk reporting as well. Arrow directions indicate a periodic trend in expected loss from the underlying risks, with a down arrow indicating a decline in expected loss trend, and an up arrow indicating an increase. In addition, arrow color indicates residual risk in relation to tolerances, where green indicates expected loss safely within risk tolerance, yellow indicates expected loss near or at risk tolerance, and red indicates that tolerance is exceeded (see the shading legend). Periodic risk reports can also be designed for drill-down operations, but their

EXHIBIT 16: Key Risk Profile—Trending & Tracking

Key Risks		Risk Rating Q1	Q2	Q3	Management Owner	Management Actions	Internal Audit Actions
Business Operations	Supplier Management				A		
	Sales & Bid Process				B	Update plans quarterly	Audit planned for Q4
	Customer Service				C&D		
People	Security Awareness				D		
	Employee Skills, Retention & Recognition				A		
External Risks	Manmade and Natural Disasters				B		
	Changing Laws and Regulations				F,E,&A	Monitor planned changes	Include question in risk survey
	Supplier Viability & Reliability				D		
	Market Negativity				F&E		
	Economic Downturn				F,E,&A		

Adapted from TELUS, 2006.

Shading legend: yellow = orange = red =

primary purpose is to provide general information on the risks of interest.

To avoid misunderstandings, those responsible for risk reporting must establish a common language on the risks and risk management process. Otherwise, the reports may be misinterpreted, resulting in wasted time, the need for clarification, and lack of business buy-in. Thus, narrative explanations must accompany charts and graphs explaining (a) trends and changes in operating data and performance measures, (b) comparison of performance to previously disclosed risk information, (c) plans and goals for risk assessment and risk management, and (d) potential impact on future operations and financial performance. In addition, a description of the assessment techniques used for evaluations may be provided. This should contribute a common understanding of the level and nature of risks, in business terms, to the discussions of risk reports

5 Placement, Distribution, and Communication

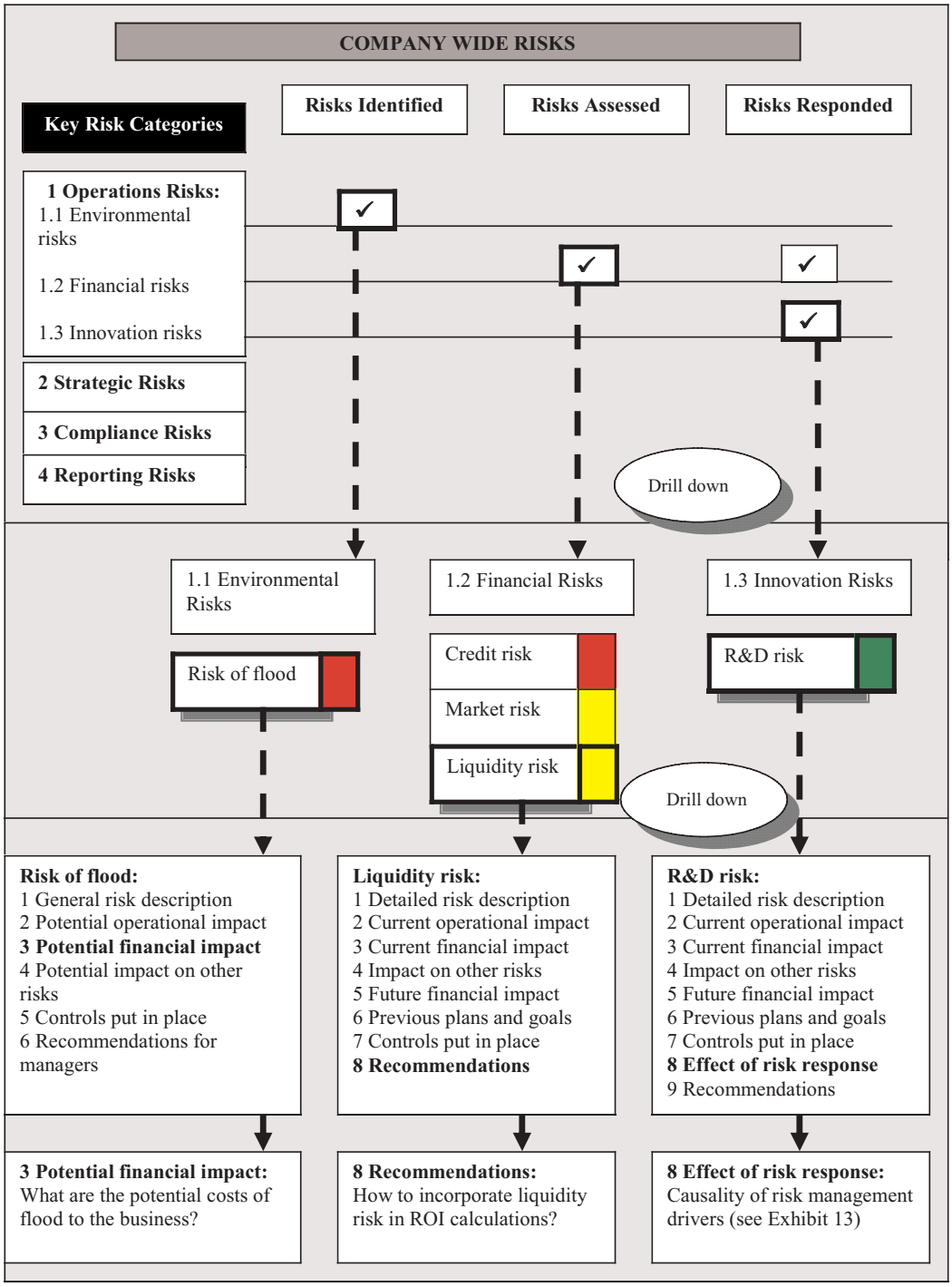
The Placement, Distribution, and Communication of Internal Risk Reports

Real-time internal risk reports are best communicated through dashboard reporting.

Draft internal periodic reports should be provided to the audit committee for review and comment before distribution.

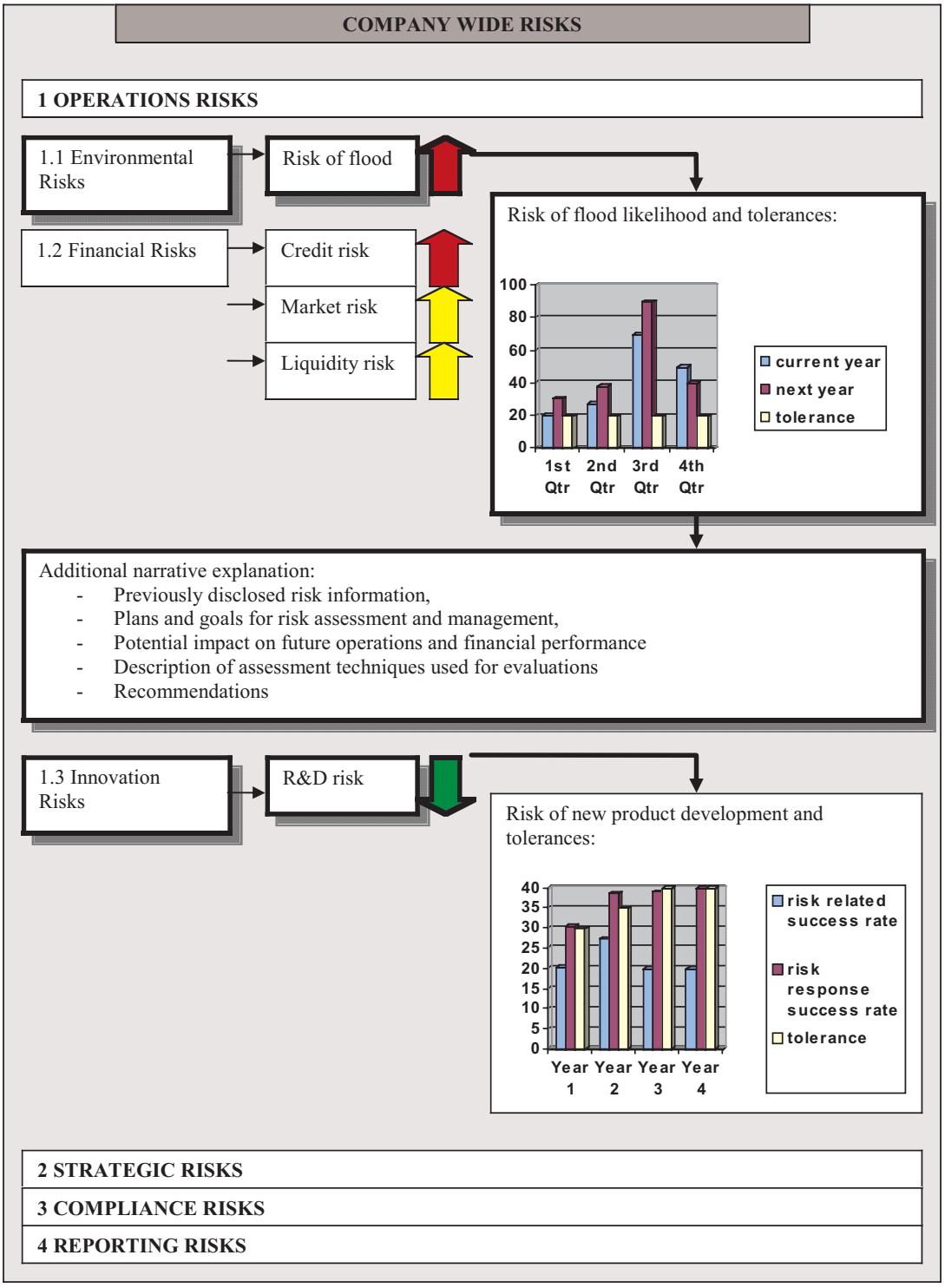
For the board and committees, risk reporting should be made at least quarterly. For senior managers and other relevant managers, real-time

Exhibit 17: A Dashboard for Internal *Real-Time* Risk Reporting for Senior Management



Shading legend:
green = = risk is within risk tolerance
yellow = = risk is near risk tolerance
red = = risk is beyond risk tolerance

Exhibit 18: A Dashboard for Internal *Periodic* Risk Reporting for Senior Management



Shading legend:

green = = expected loss safely within risk tolerance

yellow = = expected loss near or at risk tolerance

red = = risk tolerance is exceeded

risk information should be reported within a few days of the transaction or event. As the rate of change in business activities accelerates, and information technology reduces the cost of collecting and providing updated information, internal real-time risk reporting will likely be even faster. Further, as regulatory frameworks move towards real-time disclosure, management must see the information as quickly as possible.

The following communication vehicles may be used for a general communication of risk-based information across business units, processes, or functions: broadcast e-mails, broadcast voice mails, corporate newsletters, databases supporting specific risk issues, letters from the CEO, e-mail discussion groups, intranet sites capturing information regarding enterprise risk management for easy access by personnel, messages integrated into ongoing corporate communications, conference calls, posters or signs reinforcing key aspects of enterprise risk management, face-to-face meetings of 'risk champions', and newsletters from the chief risk officer. These broadcast vehicles generally promote awareness rather than guide decision-making.

GUIDANCE ON THE REPORTING OF ORGANIZATIONAL RISKS FOR *EXTERNAL DECISION-MAKING*

External constituents want more information about corporate activities. In a recent survey, investors identified communication to stakeholders to be one of the most important corporate governance aspects they monitor before making an investment. Nearly half of shareholder/investor respondents said that they would be prepared to pay a premium for companies that demonstrate a successful approach to risk management (Ernst & Young, 2005). Potential employees will typically seek organizations with more predictable working environments and risk management practices. Public interest groups and customers have also gained senior managers' attention. Organizations see increasing pressure for greater transparency, mandated or voluntary, and a better alignment of externally reported information with information reported internally to senior management to manage the business. Stakeholders expect and demand increased corporate risk disclosure to improve their various decisions. This requires effective external reporting of the risks the organization is facing, and of the management team's plans to capitalize on emerging opportunities or to minimize the risk of failures.

In our earlier discussion on risk reporting (see the section on "Importance of Organizational Risk Reporting") we suggested that organizations should move along the organizational risk reporting maturity line from compliance-based to strategy-based, and then on to business-based organizational risk disclosure. Organizations that have established proper risk management processes beyond compliance-based risk disclosure may consider disclosing broader organizational risks to external audiences as well. This sequential approach may be especially important, because external constituents expect disclosure of the risks as well as how the organization is prepared for and manages the risks. In the face of inappropriate risk management structures and processes, organizations cannot enhance corporate image and win the trust and loyalty of people outside the organization: the customers, shareholders, suppliers, and others they depend on to conduct business. The subsequent discussion on the frequency, content and format; and placement, distribution, and communication of external risk reports will therefore assume that organizations have established proper risk management processes.

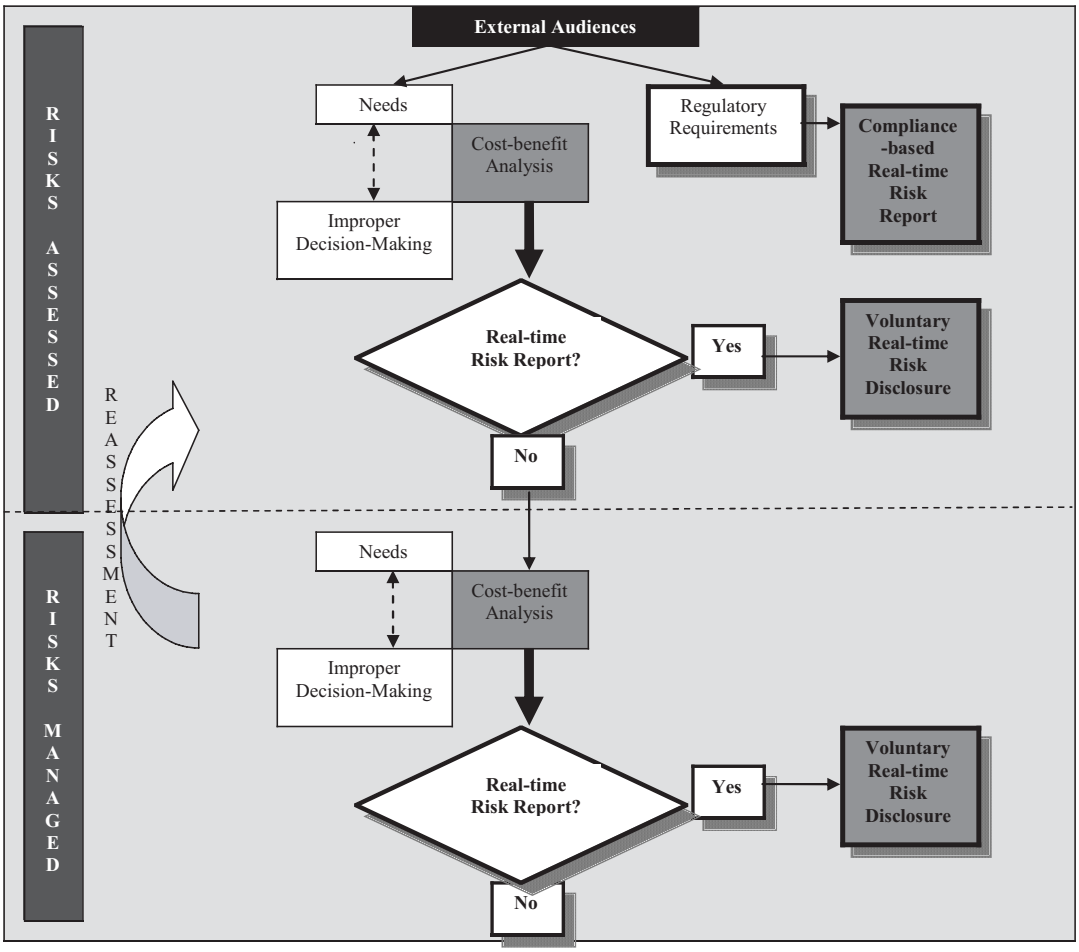
In the light of the known external audiences (registered auditor, regulators, shareholders, creditors, financial analysts, customers, suppliers, community, and media), and their risk interests (see Exhibit 7), the organizations may consider preparing different risk reports for different external constituents. Organizations can follow the uniform approach for all external audiences. except for the registered auditor and regulators, who may have specific reporting requirements.

Choosing the Frequency of a Risk Report **2**

The Frequency of External Risk Reports

Both real-time and periodic risk reporting may be needed for the general external audience. Some ***external real time risk reporting*** is required by regulation. Determining the risks to be reported externally on a real-time basis, however, may follow the steps indicated in Exhibit 19. Contrary to the internal reports (Exhibit 8), these external reports would not report risks if their probability of occurrence

Exhibit 19: Determining Risks to Be Reported on a *Real-Time* Basis to External Audiences



and magnitude of effect has not yet been assessed (risks identified).

As shown in Exhibit 19, disclosure of risk for regulatory purposes would not typically include a cost-benefit analysis. To determine which risks should be disclosed externally voluntarily, organizations must consider whether disclosure of a specific organizational risk would adversely affect the organization—by aiding its competitors, by creating a bargaining disadvantage with suppliers, customers, or employees, or by implicitly encouraging investors to withdraw their capital. Real-time risk reporting is appropriate whenever the benefits of a real-time external risk disclosure exceed its potential costs.

A more detailed cost-benefit analysis of external real-time risk reporting is provided in Exhibit 20. In the first step, the benefits of a real-time risk disclosure are converted to monetary terms. The primary potential benefits of external risk reporting to investors, creditors, and financial analysts, for example, are the reduced likelihood that they will misallocate their capital. As a consequence, organizations can benefit from (a) a lower average cost of capital, (b) enhanced credibility and improved investor relations, (c) access to more liquid markets with narrower price changes between transactions, (d) the likelihood that investors will make better investment decisions, (e) reduced danger of litigation alleging inadequate informative disclosure, and (f) improved defense of such suits. The key potential costs of external risk reporting relate to competitive disadvantage from informative disclosure, bargaining disadvantage because of disclosure to suppliers, customers, and employees, and litigation without merit that is attributable to disclosures. The greater the level of detail about a specific risk, the greater the likelihood of competitive disadvantage. Asymmetric risk reporting, when not all competitors in an industry adopt new guidelines, could also be important and a cost. Again, it is generally assumed that a specific

Exhibit 20: Calculating the Costs and Benefits of External *Real-Time* Risk Disclosure

CALCULATE THE BENEFITS OF EXTERNAL REAL-TIME RISK DISCLOSURE

Outputs	Benefits	Monetary Value
Compliance with Regulation	Reduced costs of prosecution and penalties	$.....
Corporate Reputation	Increased sales from existing and new customers Staff retention, improved recruitment	$..... $.....
Reduced Earnings Volatility	Increase in shareholder value	$.....
Reduced Cost of Capital	Savings in costs of equity financing	$.....
	Total Benefits	$.....

CALCULATE THE TOTAL COSTS OF EXTERNAL REAL-TIME RISK DISCLOSURE

Costs		Value
Real costs of risk reporting	Cost of gathering data, analysis, reporting etc.	$.....
Potential costs related to competitors	Provided risk information aids competitors to improve their competitive position	$.....
Potential costs related to suppliers	Bargaining disadvantage with suppliers	$.....
Potential costs related to customers	Bargaining disadvantage with customers	$.....
Potential costs related to investors	Potential withdrawal of their capital, absence of investments, etc.	$.....
	Total Costs	$.....

COMPARE THE BENEFITS AND COSTS OF EXTERNAL REAL-TIME RISK DISCLOSURE

$$\text{COST-BENEFIT ANALYSIS} = \frac{\text{Total Benefits}}{\text{Total Costs}}$$

risk should be disclosed when the benefits of disclosure exceed the potential costs. Conversely, organizations will decide not to make some voluntary risk disclosures when the risks of harm outweigh the expected benefit. Still, some risks may need to be disclosed even at a high short-term cost, such as risks of product malfunctioning. Good corporate governance practice may, in some instances, promote disclosure despite a negative cost-benefit analysis. Bad news cannot simply be withheld because it would hurt the organization. Such a disclosure, however, depends on the probability that the risk could occur.

The conversion of benefits of external *real-time* risk disclosure to monetary terms is illustrated in Exhibit 21. Similar to Exhibit 10, specific risk disclosure outputs that result in benefits are presented, and followed by the relevant calculations that capture the monetary value of realized benefits.

External periodic risk reporting is also required by SEC regulation via the annual 10-K. Again, organizations may decide to provide broader and more frequent periodic risk reports, on a quarterly basis for example. The purpose of periodic external risk reports is to provide general external audiences with reliable, aggregated information about various relevant organizational risks, with trend indicators and periodic comparisons, to improve their decision-making. Exhibit 11, indicating the selection of risks for periodic risk reporting to internal audiences, can also be used for external periodic risk reporting. Using the cost-benefit analysis of external periodic risk disclosure (which is similar to the cost-benefit analysis provided in Exhibit 20), organizations will decide which risks to disclose.

EXHIBIT 21: Calculating Monetary Benefits from External *Real-Time* Risk Disclosure

DISCLOSURE OUTPUTS	BENEFIT	CALCULATION OF MONETARY BENEFIT
Compliance with Regulation	Reduced costs of prosecution and penalties	Monetary benefit equals the reduced costs of prosecution and penalties; estimates of the costs should be based on historical evidence
Corporate Reputation	Increased sales from existing and new customers	Benefits can be calculated as additional sales from existing and new customers minus marginal sales expense
	Staff retention	Benefits equal to monetary savings arising from decreased employee turnover (decrease in the cost of recruitment, orientation, and training)
	Improved recruitment	Benefits arise from lower cost of employee orientation and training
Reduced Earnings Volatility	Increase in shareholder value	Benefits relate to the increase in the share market prices
Reduced Cost of Capital	Savings in costs of equity financing	Benefits equal the reduced costs of equity financing

Determining the Content of a Risk Report 3

The Content of External Risk Reports

Generally, senior management must assure investors (and other stakeholders) that organizational risks are well-managed, and that reports include the actions taken and why they are appropriate. Two sets of information must, therefore, be provided in risk reports: information on the quality of risk management, and information on relevant organizational risks. This will enable external users of risk reports to make more informed business decisions.

When deciding on the details of ***real-time*** or ***periodic*** external risk reports, organizations may choose information from the template presented in Exhibit 12. However, the tendency should be to avoid reporting on risks that have not yet been appropriately assessed. In addition, reports will not be as detailed as for internal audiences, senior management and managers in particular, and recommendations may be omitted. Important additional guidance as to what risks to disclose externally can be found in Section 4.3 of the National Policy 51-201 Disclosure Standards (NP 51-201), issued by the Canadian Securities Administrators. The section contains a list, with examples, of the types of events or information that may be material (Canadian Securities Administrators, 2002):

- Changes in corporate structure, such as changes in share ownership that may affect control of the organization;
- Changes in capital structure, such as changes in an organization's dividend payments or policies;
- Changes in financial results, such as a significant increase or decrease in near-term earning prospects,
- Changes in business and operations, such as any development that affects the organization's resources, technologies, products, or markets;
- Acquisitions and dispositions, and
- Changes in credit arrangements, such as the borrowing or lending of a significant amount of money, or changes in rating agencies' decisions.

The specific dilemma of how much to report externally in bad times must be addressed. Organizations typically want to report more when they have something good to say. When they are performing poorly, some managers may want to

disclose less. The principles of good corporate communication, as well as regulation, require it to be consistent, honest, and forthright.

An example of an external periodic risk report is provided by K-Bro Linen Income Fund in its Management's Discussion and Analysis of Financial Condition and Results of Operation. The Fund was created for the purpose of acquiring, directly and indirectly, all of the issued and outstanding securities of K-Bro Linen Systems Inc., the largest owner and operator of laundry and linen processing facilities in Canada. In the 'Risks Related to K-Bro and the Laundry and Linen Services Industry' section of the MD&A, the risk report covers several topics, including a risk-related description of the competitive environment, acquisitions and integration of acquired businesses, industry risk, the Fund's ability to maintain profitability and manage growth, cost of linens, utility and energy costs, relocation of plants, workers' compensation costs, employee relations and collective agreements, changes in laws, reliance on key personnel, dependence on long-term contracts, credit facility, availability of future financing, and environmental matters. The content of the risk report, primarily narrative, is also supported with financial numbers. For example, when disclosing the K-Bro's business decision to relocate from its Calgary plant upon the expiration of its current lease in 2008, management included an estimate of the costs of such relocation ($2 million, assuming a new facility of comparable size and the relocation and installation of existing equipment). The disclosure further says that "Although management expects to finance any relocation through its cash reserves and/or credit facilities, …, difficulties in financing or inability to finance this relocation may have a material adverse effect on K-Bro's and the Fund's business, financial condition, liquidity, and operating results" (K-Bro Linen Income Fund, 2005).

Designing the Format of a Risk Report 4

The Format of External Risk Reports

External periodic risk reports may follow the 10-K form. However, when placed on websites or disclosed in annual reports, graphical disclosures are particularly appropriate to convey the results of risk response initiatives. Narrative descriptions of potential risks along with risk response initiatives, put in a business context, may help external users to better understand the importance of this information for decision-making. Such reports may accompany a more descriptive section on forward-looking information or prospective financial and non-financial information in an annual report, or in the management discussion and analysis section.

External real-time risk reporting, on the other hand, relates to risk information placed on the organization's web site, or disseminated in another real-time manner, such as in the form 8-K. Similar to periodic external risk reports, information should be general and aggregate, but related to recent risk-related analytical findings.

In broadening reporting, many organizations have issued special reports, on the environment for example, or for equal employment opportunity, philanthropy, or other issues. Many of these reports are issued to display 'a good corporate citizen' reputation and appeal to special interest groups. There is no need to segregate these reports from mainstream financial reporting.

Because of the rise of the Internet and the related trend toward electronic dissemination of financial and other information on the websites, concerns about the 'organization of information' may become obsolete. Users of corporate websites have greater control over which portions of the report to review and which to disregard. As these technologies develop, the sequence of information in a traditional paper annual report might become increasingly less important.

Placement, Distribution, and Communication 5

The Placement, Distribution, and Communication of External Risk Reports

Websites are particularly useful for ***external real-time risk reporting***. This allows organizations to provide aggregate information. Serious users can then delve into the on-line risk reports for detail. The 8-K form should also be considered an important placement tool.

With respect to ***external periodic risk reporting***, MD&A, other parts of annual reports, or quarterly reports, are generally viewed as the main channels for risk reporting to external stakeholders. As noted earlier, a model of risk reporting should first integrate,

not fragment, the mosaic of risk-related information that managers use for external disclosure. The president's letter, MD&A, financial statements, and footnotes, along with other voluntary disclosures, should offer a holistic reporting that includes organizational risks. Many organizations try to fill the risk reporting information gap with public relations. The problem with this approach is that public relations often implies that the organization is hesitant to come clean with all available facts, or is trying to paint a picture that may not be realistic. By relying on public relations alone, senior management risks losing credibility with their stakeholders.

Generally, the communication strategy may include analyst meetings, press conferences, formal documents, and other channels of communication, such as the Internet or websites. Some users will continue to want information on paper or orally. Others may access the information in electronic form. Whichever method is practiced, the reporting objective should be to provide a sound basis for external audiences to make comprehensive, albeit subjective, assessments of the reported data. The challenge for managers is to inform the average member of the external audiences, while being fair and balanced in covering all critical perspectives. The draft external periodic reports should be provided to the audit committee for review and comment before distribution.

CHALLENGES IN RISK REPORTING

Risk reporting inevitably confronts several challenges, such as controlling the risk report's effects on individual behavior, monitoring and evaluating these effects, and managing the costs of risk reporting.

The Impact of Risk Reporting on Individual Behavior

Reporting of organizational risks has either a direct or an indirect effect on the internal and external audiences' behavior concerning the perceived threats. Therefore, the managers' responsibility to present an accurate picture of the problems is vital. The reporting of organizational risks affects individual behavior through a number of phases, such as awareness, a sense of urgency or a demand for action, a search for solutions, reaction and resistance, wrestling with alternative choices, intellectual assent, resolution at the cognitive level, and full resolution—moral, emotional, and intellectual (Willis and Adelowo Okunade, 1997).

Proper communication and reporting of organizational risks is important to create risk awareness; but it is even more critical to attempt to influence the sense of urgency or a demand for action among the relevant audiences. Further, it should contribute to the difficult process of solving the problems. When communicating and reporting organizational risks, managers should (a) report on the complexities of the problem (b) define the conflicting values surrounding—and sometimes polarizing—an issue, and (c) define a common ground for effective action.

However, it is extremely difficult to influence these effects, since so many variables can alter the way the message is delivered or interpreted. The noise along the communication channel should be among the major concerns of the risk reporters. Further, how vulnerable do internal and external audiences feel to various organizational risks as a result of risk reporting? Relative personal invulnerability is not always a reflection of a person's ignorance of risk warnings. Rather, it could be an indirect effect of risk communication behaviors. When internal and external audiences are threatened by a serious risk, they will look for more information about the risk from media and interpersonal channels. Although these channels, often informal in nature, may increase the individual's perceived expertise about the risk, and enhance his or her perception of controlling it, they may also lead to false information, and cause high stress and wrong reactions. Thus, organizations need to control risk reporting channels and ensure accurate and reliable information.

Monitoring the Contribution of Risk Reporting

There is no way to measure precisely how many false internal and external decisions will be averted, and how many investment dollars will be saved, because of broader risk reporting. However, improved risk identification, measurement, management, and reporting generally is critical for improved internal decision-making and for increased investor confidence in the reliability of an organization's financial reporting and the capital markets.

With appropriate external disclosure of organizational risks and risk management initiatives, shareholders and financial analysts can more properly value company shares. The role of forward-looking information in voluntary disclosure is generally associated with more accurate analysts' earnings

forecasts and company valuations. Recent research shows that improving disclosures makes capital allocation more efficient and reduces the average cost of capital—lower costs of equity capital and lower debt costs (FASB, 2001). The reason is that an organization's cost of capital is believed to include a premium for investors' uncertainty about the adequacy and accuracy of organizational information. Voluntary disclosure also decreases price volatility and narrows bid-ask spreads, enhancing securities liquidity (Lev, 1992). Organizations with more informative risk disclosure have a wider analyst following, receive more accurate earnings forecasts, and have less volatility in forecast revisions (Lang and Lundholm, 1996).

Fair and favorable media publicity may also be a benefit, and customer loyalty may increase. By externally disclosing more comprehensive risk-related information, senior management increases transparency and improves goal alignment between the organization and its broad set of stakeholders. Strengthening the credibility of an organization's performance internally is also important. Employee morale and support for management can strengthen with accurate reporting of relevant risks and responsive risk management initiatives. Increased commitment to delivering results may lead to improved organizational success and shareholder value. Full accountability is accomplished only when an organization combines broad public disclosures with extensive internal performance reporting. By doing so, organizations create value for the stakeholders whose support is needed to prosper.

As with most reporting, the benefits of disclosure are hard to separate from the benefits of the actions and the process the reports represent.

Coping With Costs of Risk Reporting

Although the *Risk Reporting Contribution Scheme* (see Exhibit 4) responds to users' needs, risk reporting should reflect the organization's concern about the costs of disclosing, preparing, disseminating competitively sensitive information, and the potential for increased litigation. Organizations are typically sensitive to these costs, and will search for ways to limit them while still providing more useful information. Generally, if the organization prepares the right risk-related information to help managers make better strategic and operational decisions internally, the added cost of external disclosure should be small.

THE IMPORTANCE OF ACCURACY OF INFORMATION GATHERED AND PROVIDED TO INTERNAL AND EXTERNAL AUDIENCES

An important reporting rule for organizations is not to disclose any risk information without sufficient credible data for accurate reports. It is the risk reporter's responsibility to be accurate, but it is also the manager's responsibility to be truthful and make disclosures that represent economic reality. Inaccurate data can result in poor situation assessment and bad management decisions, while financial analysts and investors can draw incorrect conclusions and make improper business decisions. In addition, employee dissatisfaction with inaccurate reporting of risks may lead to a decline in trust, employee morale and support for management; customers may decide to switch to other providers; organizations may face adverse publicity; and investors and creditors may lose confidence in the organization's capability to deliver the required returns. As a consequence, the market value of the corporation may decline.

On the other hand, even accurate information to stakeholders may also cause adverse publicity. When organizations provide accurate information, they may not improve their reputation. Full disclosure may stimulate customers to avoid purchase of the organization's products. Organizations thus face various risks related to both accuracy and inaccuracy of information, not just compliance risks.

Many risks of providing inaccurate information are related to the process of gathering information, since control weaknesses and risks are often due to people or process issues. Organizations also rely on others to provide information, such as suppliers and business partners, and in particular outside service providers. The extent of an organization's reliance on outside service providers may both complicate management's internal assessment of internal control over financial reporting, and make assuring accurate information more difficult. Management must obtain information from the service organization that allows it to assess the operational effectiveness of the service organization's internal control.

Accurate information may be more easily assured in a highly integrated enterprise. If the information from the three core transactional systems (Enterprise Resource Planning, Supply

Chain Management, and Customer Relationship Management) and other supporting functional automation systems is not integrated, financial data may be inaccurate, and considerable resources will be required to reconcile the differing, though overlapping, data from various sources. This data may then remain open to distortion, data loss, and corruption. There are several available integration technologies, and the CIO should consider the appropriate one based on the specific requirements and constraints of the organization.

RISK REPORTING RELATED TO MERGERS AND ACQUISITIONS

Reporting on various organizational risks related to due diligence is important not only in continuing operations, but also in acquisitions and mergers. Reports from financial analysts, media, and surveys reveal that poor due diligence is one of the failure determinants in failed mergers (Epstein, 2004). Risks associated with acquisitions and mergers include all aspects that relate to the initial different structures and systems, and the need for system changes or new systems. More specifically, they include legal and regulatory issues (compliance risks), lack of organizational culture alignment, and risks of misaligned management control systems or sub-optimal organizational policies (organizational systems' risks). More importantly, they also include other strategic and operational risks.

In considering acquisition and undertaking due diligence, organizations must:

- Consider the adequacy of the target's controls and its compliance efforts, if the target is a private or foreign company. Assessments of compliance risks, their probability of occurrence and magnitude of effect, must be made and reported to the board of directors and senior management of the acquiring organization.
- Carefully assess and report on all potential strategic and operational risks. Assessments should be made of preliminary inherent risks (with risk likelihoods and potential impacts), as well as of residual risks after a proper risk response is put in place (again with risk likelihoods and expected impacts).
- Provide the board of directors and senior management with a probability distribution of various outcomes of a merger or acquisition, particularly in relation to expected cost savings.

ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES FOR RISK REPORTING

With respect to internal control regulation, the ***board of directors*** bears ultimate responsibility for the effectiveness of internal control throughout the organization. It should also take responsibility for overall effective risk management and risk reporting. Boards of directors also have responsibilities related to developing and implementing the company's mission, values, and strategy. This responsibility also includes a careful review of corporate processes for identifying, monitoring, and managing risks. The board may delegate its oversight and reporting duties to certain committees, but it must receive and review risk reports of those committees and take actions necessary to ensure continued effectiveness of these corporate processes. Although the responsibility for risk may, in practice, be migrating from the wider board to the audit committee, it should stay firmly with the board. The audit committee is responsible for directing internal oversight and, therefore, for understanding internal control (risk) concepts, approaches, and issues.

The ***CEO*** is then responsible for organizing, planning, directing, and controlling the senior members of management to achieve risk management and risk reporting objectives. From the CEO's perspective, the organization needs to ensure that these reports clearly explain the critical risks, so that the users understand them and incorporate them in their decision-making. The ***CFO*** is responsible for designing and maintaining such internal control techniques in financial policies, procedures, processes, systems, functions, and undertakings as are necessary to achieve the company's financial and risk objectives. These include (a) maintaining a competitive capital structure, (b) providing relevant and reliable financial information and analysis to facilitate and support decisions on strategy, objectives, plans, and other initiatives, as well as (c) complying with applicable laws and regulations pertaining to financial matters. In addition, the CEO is responsible for making periodic risk reports in a form and content that enables management and the board to monitor performance and achieving risk objectives and business objectives.

The role of the ***internal audit function*** with respect to risk management is two-fold. In addition to identifying and evaluating risk exposures,

standards on internal auditing charge internal audit with the responsibility for monitoring and evaluating the effectiveness of the organization's risk management system. This responsibility requires internal audit to maintain its independence and objectivity.

To establish the right organizational risk management and risk reporting structures and systems, organizations should start with a written ***corporate risk disclosure policy***. That policy gives organizations a process for disclosure, and promotes an understanding of legal requirements among directors, senior management, other managers, and employees. It will focus on promoting consistent disclosure aimed at informative, timely, and broadly disseminated disclosure of risk-related information to interested audiences. Every disclosure policy should generally include the following (Canadian Securities Administrators, 2002):

- how to decide what risk information is 'material' and should be reported,
- policy on reviewing analysts' reports;
- how to release earnings announcements and conduct related analyst calls and meetings;
- how to conduct meetings with investors and the media;
- what to say or not to say at industry conferences;
- how to use electronic media and the corporate web site;
- policy on the use of forecasts and other forward-looking information (including a policy regarding issuing updating);
- procedures for reviewing briefings and discussions with analysts, institutional investors and other market professionals;
- how to deal with unintentional selective disclosures;
- how to respond to market rumors;
- policy on trading restrictions; and
- policy on 'quiet' periods.

The process of creating such a policy is itself a benefit, because it forces a critical examination of current disclosure practices. Although CFOs often assume responsibility for risk functions because of the broad perspective they have of their organizations, organizations should consider establishing a committee of company personnel (***Risk Management Committee***) or assign a senior officer (***Chief Risk Officer***) to be responsible for:

- developing and implementing the risk disclosure policy;
- monitoring its effectiveness and compliance;
- educating directors, senior management, other managers, and employees about disclosure issues and the risk disclosure policy;
- reviewing and authorizing disclosure (including electronic, written and oral disclosure) in advance of its public release; and
- monitoring the organization's web site.

The risk disclosure policy should be reviewed periodically, updated as necessary, approved by the board of directors, and widely distributed to senior management, other managers, and employees. Directors, senior management, other managers, and employees should be trained, so that they understand and can apply the disclosure policy.

In addition, the organization should authorize ***spokespersons***, limiting the number of people authorized to speak on behalf of the organization to analysts, the media, and investors. Ideally, spokespersons should be members of senior management. They should be knowledgeable about the risk disclosure record and aware of analysts' reports relating to the organization. Everyone in the organization must know who the organization's spokespersons are, and be directed to refer all inquiries from analysts, investors and the media to them. Having spokespersons helps to reduce unauthorized disclosures, inconsistent statements by different people in the organization, and statements that are inconsistent with the public disclosure record of the organization.

The ***unit responsible for risk reporting***, which directly reports to the risk management committee or CRO, should be elevated to the strategic level and organized as a separate entity. Its tasks include continuous gathering of data on risk events, providing risk assessments, and cost-benefit analyses. In addition, this unit prepares the risk reports to internal and external audiences. The risk management committee or CRO is responsible for supervising these activities and approving the analyses. On the other hand, the board of directors must approve the release of risk reports.

A firm commitment from the highest levels of management is clearly necessary to make risk management an organization-wide process. This is the only way to create a mindset in managers

and employees that builds risk into everyday decision-making. Without designated responsibility, proper training or even clear definition and communication of risks, various line managers may implement their personal risk approach, with varying tolerances for risk. This could lead to inconsistent risk management (The 2005 Oversight Systems Financial Executive Report on Risk Management, 2005).

CONCLUSION

Although internal control over financial reporting can be considered one of the most significant requirements resulting from the Sarbanes-Oxley Act of 2002, the internal control legislation and regulation also triggered a different and broader understanding of the risks organizations face, and the risk management process they implement. Managers increasingly understand the importance of effective risk reporting, internally and externally, and the value of delivering relevant and credible risk reports to internal and external audience that are articulated in business terms and supported by evidence. With the right information, internal and external audiences can make better decisions.

Broader real-time and periodic internal risk reporting provides senior management and other managers with on-time, detailed, and aggregate information on the various risks and the organization's risk management processes, thus contributing to more informed decision-making. Dashboard reporting systems allow managers to drill down for more detailed information on risks and relationships between them, and to include these in their ROI calculations. Improved resource allocations may result.

Broader external reporting should not hurt the organization's competitiveness. If specific risk-related information helps the organization make improved decisions and better track value creation, the information may also help attract new capital. Or, if information on employee satisfaction and well-being helps managers prevent the increase in personnel risks and cultivate a committed workforce, it may also help attract committed talent from outside. Data on business process continuity may lead to improved processes, which may also reassure customers and business partners externally. Organizations with poor external disclosure complicate informed decision-making by financial analysts, shareholders, customers, suppliers, and others with whom organizations interact.

This Guideline starts with a *Risk Reporting Contribution Scheme*, a framework for monitoring the outputs of risk reporting and financial outcomes from broader reporting of organizational risks, such as investors and creditors making more informed investment decisions, or managers making better strategic and tactical decisions. The *Risk Reporting Contribution Scheme* shows the benefits of a broad and well-managed risk reporting process, and provides the background to the *Risk Reporting Model* presented in this Guideline. The *Risk Reporting Model* provides useful guidance for senior managers on reporting of organizational risks internally and externally—the frequency of risk reports, what risks to report and in what detail, in what format, and where. This Guideline, therefore, helps senior management go beyond regulatory compliance regarding risk reporting, and seize the opportunity to improve reporting practices to drive better performance. In addition, this Guideline recommends a preliminary step, that all organizations establish appropriate organizational structures and responsibilities for risk management and risk reporting.

In the future, successful businesses will be those best able to balance coping strategies, which are defensive and focused on avoiding downside risks, with an increasing mix of exploitation and exploration strategies, which embrace risk and make the most of the opportunities it presents. This will require more than just an improvement in traditional risk management tools—it will involve a shift in mindset and focus, where reliable, relevant, and sufficient risk management and reporting is considered a value-added activity. Organizations should leverage the Sarbanes-Oxley Act compliance efforts and investments to build a comprehensive risk management and risk reporting system and drive significant new business value from a complex and mandatory process.

BIBLIOGRAPHY

American Institute of Certified Public Accountants. 1994. *Improving Business Reporting—A Customer Focus (Comprehensive Report of the Special Committee on Financial Reporting)*. New York: AICPA.

American Institute of Certified Public Accountants. 2004. *Improving Business Reporting—A Customer Focus: Meeting the Information Needs of Investors and Creditors*. New York: AICPA.

Accounting Standards Board. 2005. *Reporting Statement of Best Practice on the Operating and Financial Review.* London: ASB Publications.

Canadian Institute of Chartered Accountants. 2001. *Management's Discussion and Analysis: Guidance on Preparation and Disclosure*. Review Draft.

Canadian Securities Administrators. 2002. *National Policy 51-201 Disclosure Standards*.

Committee of Sponsoring Organizations of the Treadway Commission. 2004a. *Enterprise Risk Management—Integrated Framework: Executive Summary Framework*. New York: AICPA.

Committee of Sponsoring Organizations of the Treadway Commission. 2004b. *Enterprise Risk Management—Integrated Framework: Application Techniques*. New York: AICPA.

Companies (Auditing and Accounting) Bill 2003. Houses of Oireachtas, Ireland.

Epstein, Marc J. 2004. *The Drivers of Success in Post-Merger Integration.* Organizational Dynamics, Vol. 33, No. 2: 174-189.

Epstein, Marc J., and Rejc, Adriana. 2005. *Identifying, Measuring, and Managing Organizational Risks for Improved Performance*. Management Accounting Guideline. Hamilton: The Society of Management Accountants of Canada, New York: AICPA.

Ernst & Young. 2005. *Corporate Governance Web Survey: Key Findings and Valuable Insights*.

Financial Accounting Standards Board. 2001. *Improving Business Reporting: Insights into Enhancing Voluntary Disclosures*. Steering Committee Report, Business Reporting Research Project.

Institute of Chartered Accountants in England and Wales. 1993. *Guidance on the Operating and Financial Review.* London: Financial Reporting Committee—Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 1998a (revised in 2003). *The Combined Code: Principles of Good Governance and Code of Best Practice*. London: Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 1998b. *Financial Reporting of Risk: Proposal for a Statement of Business Risk.* London: Financial Reporting Committee—Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 1999a. *Inside Out: Reporting on Shareholder Value*. London: Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 1999b. *Internal Control: Guidance for Directors on the Combined Code.* London: Internal Control Working Party—Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 2000a. *No Surprises: The Case for Better Risk Reporting.* London: Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 2000b. *Prospective Financial Information: Guidance for UK Directors*. London: Institute of Chartered Accountants in England and Wales.

Institute of Chartered Accountants in England and Wales. 2003. *Preparing an Operating and Financial Review: Interim Process Guidance for UK Directors.* London: Financial Reporting Committee—Institute of Chartered Accountants in England and Wales.

International Federation of Accountants. 2002. *Managing Risk to Enhance Shareholder Value*. New York: International Federation of Accountants—Financial and Management Committee.

K-Bro Linen Income Fund. 2005. *Management's Discussion and Analysis and Interim Consolidated Financial Statements for the Period from February 3, 2005 to June 30, 2005*.

Lang, Mark H., and Lundholm, Russel J. 1996. *Corporate Disclosure Policy and Analyst Behaviour*. Accounting Review, Vol. 71, No. 4.

Lev, Baruch. 1992. *Information Disclosure Strategy.* California Management Review, Vol. 34, No 4.

TELUS. 2006. *Enterprise Risk Management and Internal Audit at TELUS: Engagement, Discussion, Shared Ownership and Governance.*

The 2005 Oversight Systems Financial Executive Report on Risk Management, Oversight Systems, Inc. May, 2005.

Willis, Jim, and Adelowo Okunade, Albert. 1997. *Reporting on Risks: The Practice and Ethics of Health and Safety Communication.* Westport: Preager.

APPENDIX 1: REGULATIONS ON REPORTING OF ORGANIZATIONAL RISKS

Under the ***Sarbanes-Oxley Act of 2002***, U.S. listed companies are subject to requirements for management and independent auditors' reporting on the effectiveness of internal control over financial reporting. This regulation requires a company's annual report on a Form 10-K, filed with the SEC, that includes management's assessment of internal control over financial reporting and the related auditor's report on that internal control. Management's report must identify the framework it used, and describe its success in evaluating the effectiveness of internal control over financial reporting. Regulators require management's report to disclose the nature of any material weakness in sufficient detail to enable investors and other financial statement users to understand the weakness and evaluate the underlying circumstances .

The ***8th Directive on Company Law*** introduces similar regulation in the European Union. Like Sarbanes-Oxley, at the core of the 8th Directive is a commitment to restoring investor confidence in the markets, which means that directors of U.S. listed companies with a dual European listing must be familiar with this directive as well. Directors and auditors have a particular responsibility to represent and protect investor interests through the quality, depth and breadth of their respective oversight activities. More specifically, the 8th Directive has an impact across two broad areas:

- Responsibilities of the audit committee: Public interest entities are required to appoint an audit committee, which will now have greater fiduciary responsibility for risk management, including oversight of the internal audit function and internal controls structure. The audit committee is required to monitor the effectiveness of the company's internal controls, internal audit, and risk management systems.
- The audit committee's relationship with the auditor: The audit committee now has responsibility for the selection of the external audit firm and oversight of auditor independence. The auditor is required to report to the audit committee on key matters arising from the statutory audit, including material weaknesses in internal controls in relation to the financial reporting process.

Regulatory bodies have made little attempt to provide an explicit integrated framework for broader corporate risk disclosure. The status of current regulation of broader risk reporting is primarily focused on narrower issues, such as market risk associated with the use of derivatives. In the United States, ***Financial Reporting Release No. 48*** (FRR 48), issued by The Securities and Exchange Commission (SEC) in 1997, requires the SEC registrants to disclose both qualitative and quantitative information about market risks (potential losses arising from adverse changes in interest rates, foreign currency rates, commodity prices, and equity prices). In practice, disclosure by listed companies varies widely in detail and clarity, and is spread throughout the Management Discussion and Analysis (MD&A) and the notes to financial statements. This makes it difficult for investors to gather information and make appropriate risk assessments. SEC rules contain many financial disclosure requirements, but they also address safe harbor provisions that protect management from liability for financial projections and forecasts made in good faith. FRR 48, therefore increases available risk information, but organizations often subvert the intent of the legislation by burying or defusing the data.

In the United Kingdom, ***guidance on the Operating and Financial Review*** (OFR) (similar to the MD&A), introduced in 1993 and revised in 2003 by the Institute of Chartered Accountants in England and Wales (ICAEW) for listed companies (and other companies voluntarily), recommends including a review of risks in the annual report, without specifying how detailed the review should be. Further, in 2005, the Accounting Standards Board (ASB) issued the Reporting Statement of Best Practice on the Operating and Financial Review. The Reporting Statement sets out a framework of the main elements that should be disclosed in an OFR, leaving it to directors to consider how best to structure their review, in the light of the entity's particular circumstances. It contains recommendations on the disclosures that should be made in respect of any key performance indicators included in an OFR, but it does not specify any particular performance indicators that entities should disclose, nor how many, on the grounds that this is a directors' decision.

The ***Combined Code on Corporate Governance*** is published by the Financial Reporting Council (FRC) and requires listed companies to maintain a sound system of internal control to safeguard shareholders' investment and the company's assets. The Listing Rules require companies to provide a statement in their annual report on how they have applied the Code Principle and Code Provision relating to internal control. Companies

also need to confirm that they need to comply with the provision or where they do not, to provide an explanation. Additional guidance was developed to assist listed companies to implement the code requirements relating to internal control. This is now commonly known as the Turnbull Guidance and is based on a risk-based approach to internal control. It emphasises the need to incorporate this approach into normal management processes and is designed to enable companies to adapt the guidance to its own circumstances.

Under current provisions, corporate risk disclosure is still generally at the discretion of the board of directors of individual companies, and a matter of voluntary disclosure rather than regulatory compliance.

APPENDIX 2: EXISTING GUIDANCE ON VOLUNTARY DISCLOSURE AND FRAMEWORKS FOR ORGANIZATIONAL RISK REPORTING

- The ***American Institute of Certified Public Accountants*** (AICPA, 1994, 2004) proposed a framework for voluntary disclosure aimed at improving the quality and effectiveness of financial reporting. To provide information for investors, companies should consider disclosing five different types of data and information: *financial and non-financial data, management's analysis of financial and non-financial data, forward-looking information, information about managers and shareholders*, and *company background*. The framework explicitly addresses external reporting, and is therefore primarily relevant to capital providers and financial analysts. It provides no specific guidance on the format, frequency of the report, or communication channels.
- The ***Canadian Institute of Chartered Accountants'*** reporting guidelines (CICA, 2001) suggested a reporting framework that includes information concerning company vision (core business and long-term business strategy), *critical success factors, capabilities (resources) to achieve desired results, expected results*, and *connected risks and opportunities*. Again, the framework provides general instructions along with the content of an external risk report, without specifying the format, frequency, design, and communication channels.
- The ***COSO Enterprise Risk Management—Integrated Framework*** (COSO, 2004a, 2004b) addresses risk management processes in general. It proposes that information is needed at all levels of an organization to respond to risks, and to otherwise run the entity and achieve its strategic, operational, reporting, or compliance objectives. Financial and non-financial information would include (a) external events, for example, market- or industry-specific economic data that signals changes in demand for an organization's products or services, (b) market intelligence on evolving customer preferences or demands, (c) information on competitors' product development activities, and (d) legislative or regulatory initiatives. Organizations should provide a risk map that displays significant residual risks that exceed the organization's risk appetite, or report on the target risk tolerances for specific performance measures and actual results. The framework also provides exhibits and application techniques, both qualitative and quantitative, that can be used in managerial reports on organizational risks. Qualitative techniques include likelihood risk rankings, impact risk rankings, or descriptive risk assessments. Quantitative techniques include probabilistic techniques (value at risk, cash flow at risk, earnings at risk, assessment of loss events, and back-testing) and non-probabilistic techniques such as sensitivity analysis, scenario analysis, and stress testing. The framework is very useful for overall risk management, but provides only limited specificity on the content, format, and frequency of the (internal and external) risk reports.
- Epstein and Rejc (2005) provide a specific model, ***Risk Management Payoff Model: Calculating a Risk Management Initiative ROI***, to calculate a risk management initiative ROI so that managers can integrate risks in their investment decisions. First, the monetary value of a risk management initiative benefit is calculated. Then, the total cost of a risk management initiative is summed, including front-end direct cost, disruption costs related to human and organizational factors, and operating costs of the risk management initiative. Finally, the risk management initiative ROI is calculated. Such a formula can be used to evaluate the payoffs of specific risk management initiatives and, as organizations make new capital project decisions, to

explicitly acknowledge the potential risks and costs of those risks on organizational profitability. This model is therefore primarily focused on internal risk reporting.

- The ***SEC*** encourages companies to disclose *forward-looking information* in their annual reports so that investors can better understand a company's future prospects and make informed investment decisions. In a typical annual report, MD&A would be preceded by a section on the 'Risks and Uncertainties That May Affect the Organization's Future Results', where the nature of forward-looking information would be explained and risk and uncertainties revealed. Here, words such as 'anticipate', 'project', 'intend', and 'believe', which describe future operating or financial performance, identify these forward-looking statements. Typical risks and uncertainties might include research and product development, financial risk management, international operations and foreign markets, patents and intellectual property rights, competition, government regulation and price constraints, litigation, tax legislation, and environmental law compliance. The SEC provides no specific directions on how risk and uncertainties information should be disclosed as to risk report structure and format, or what quantitative evidence is required. It is focused primarily on investors' risk reporting interests.

Guidance on general principles of risk disclosure is also offered by:

- Papers issued by professional bodies and research institutes (Institute of Chartered Accountants in England and Wales, 1998b, 1999a, 2000a, 2000b, International Federation of Accountants, 2002). All share the common goal of proposing principles and structures for approaching forward-looking disclosure and communication of a fair and integrated view of the company risk profile.
- The FASB Framework for Providing Voluntary Disclosure (Financial Accounting Standards Board, 2001). It includes identification of critical success factors, management's strategies and plans for managing those critical success factors, and metrics to measure and manage the implementation of strategies and plans. It also includes consideration of whether voluntary disclosure would adversely affect the organization's competitive position, and, if disclosure is deemed appropriate, a definition of how best to voluntarily present that information.

THE AUTHORS:

Marc J. Epstein is Distinguished Research Professor of Management at Jones Graduate School of Management at Rice University in Houston, Texas. He recently was Visiting Professor and Wyss Visiting Scholar at Harvard Business School. Prior to joining Rice, Dr. Epstein was a professor at Stanford Business School, Harvard Business School, and INSEAD (European Institute of Business Administration), Dr. Epstein has written previous MAGS for the AICPA and CMA Canada including co-authoring "Applying the Balanced Scorecard" and "Measuring and Improving the Performance of Corporate Boards Using the Balanced Scorecard", "Evaluating Performance in Information Technology" and "Identifying, Measuring, and Managing Organizational Risk for Improved Performance". He has also written other articles on strategic management systems and performance measurement, and over 100 articles and 15 books. In 1999, he wrote the award winning "Counting What Counts: Turning Corporate Accountability to Competitive Advantage".

Adriana Rejc Buhovac is presently Assistant Professor at the Faculty of Economics at the University of Ljubljana. An expert in the design and implementation of performance measurement and evaluation systems, Dr. Rejc Buhovac is the author of numerous papers including "Determinants of Performance Measurement System Design and Corporate Financial Performance", "Toward Contingency Theory of Performance Measurement", "How to Measure and Improve the Value of IT", and "What's in IT for You (and Your Company)". In addition to her research on the topic, Dr. Rejc Buhovac has worked with numerous companies on the evaluation of performance of the human resources function, and on the implementation of strategic performance measurement systems. She is a member of the Editorial Board of the Advances in Management Accounting (AIMA). With Marc Epstein, Dr. Rejc Buhovac coauthored two recent Management Accounting Guidelines for CMA Canada and the AICPA: "Evaluating Performance in Information Technology" and "Identifying, Measuring, and Managing Organizational Risk for Improved Performance".

This *Management Accounting Guideline* was prepared with the advice and counsel of:

Barry Baptie, MBA, CMA, FCMA
Board of Directors
VCom Inc

Richard Benn, MBA, CMA, FCMA
Vice President Knowledge and Program Development
CMA Canada

Ken Biggs, CMA, FCMA, FCA
Board Director and Business Consultant

Dennis C. Daly, CMA
Professor of Accounting
Metropolitan State University

William Langdon, MBA, CMA, FCMA
Knowledge Management Consultant

Melanie Woodard McGee, MS, CPA, CFE
Director of MBA Programs
The University of Texas at Arlington

David L. Tousley, MBA, CPA
Chief Financial Officer
airPharma, LLC

Robert Torok, MBA, CA
Executive Consultant
IBM Global Business Services

Kenneth W. Witt, CPA
Technical Manager, The New Finance
American Institute of Certified Public Accountants

For additional copies or for more information on other products available contact:

In the U.S.A.: **American Institute of Certified Public Accountants**
1211 Avenue of the Americas
New York, NY 10036-8775 USA
Tel (888) 777-7077, FAX (800) 362-5066
www.aicpa.org
Visit the AICPA store at www.cpa2biz.com

In Canada and elsewhere: **The Society of Management Accountants of Canada**
Mississauga Executive Centre
One Robert Speck Parkway, Suite 1400
Mississauga, ON L4Z 3M3 Canada
Tel (905) 949-4200
FAX (905) 949-0888
www.cma-canada.org

AICPA Member and
Public Information:
www.aicpa.org

AICPA Online Store:
www.cpa2biz.com

ISO Certified

030003