

University of Mississippi

eGrove

Guides, Handbooks and Manuals

American Institute of Certified Public
Accountants (AICPA) Historical Collection

2004

Managing Risk in the New Economy

American Institute of Certified Public Accountants (AICPA)

Canadian Institute of Chartered Accountants

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_guides



Part of the [Accounting Commons](#)



**Risk is about
putting the odds in your favor.**



Managing Risk in the New Economy

American Institute of Certified Public Accountants
The Canadian Institute of Chartered Accountants

COMMITTEE AND TASK FORCE MEMBERS

AICPA

Assurance Services Executive Committee

Robert L. Bunting, *Chair*
Gari Fails
Louis J. Grabowsky
Everett C. Johnson, Jr.
John Lainhart
George Lewis
Edward F. Rockman
Susan C. Rucker
J.W. Mike Starr
Wendy E. Visconti
Darwin Voltin

AICPA Staff

Anthony J. Pugliese
Director, Assurance Services

CICA

Assurance Services Development Board

John W. Beech, *Chair*
Sheila Fraser
Douglas C. Isaac
Marilyn Kuntz
Doug P. McPhie
Steven E. Salterio
David W. Stephen
Keith S. Vance

CICA Staff

Gregory P. Shields
Director, Assurance Services Development

Written by Hugh Lindsay under the direction of the
AICPA/CICA Risk Advisory Services Task Force

Louis J. Grabowsky, *Chair*
Mark Bagaason
Stephen W. Bodine
Diana Chant
Brad Davidson
Michael A. Gunns
David Gurnham
Colin Lipson
Michael J. McGourty
Tony Maki
Susan Menelaides
Thaddeus (Ted) J. Senko
Gregory S. Steiner
Paul L. Walker

AICPA Staff

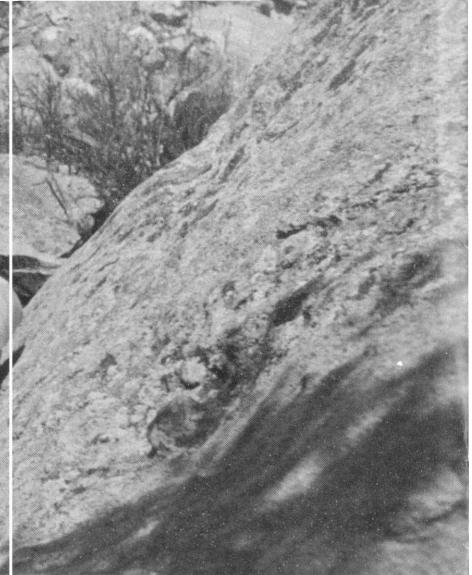
Alan W. Anderson
Senior Vice President, Technical Services
Anthony J. Pugliese
Director, Assurance Services

CICA Staff

Cairine M. Wilson
Vice President, Innovation
Karen M. Duggan
Principal, Assurance Standards
Gregory P. Shields
Director, Assurance Services Development



Preface



Managing Risk in the New Economy is a publication of the American Institute of Certified Public Accountants (AICPA), and The Canadian Institute of Chartered Accountants (CICA).

Chartered Accountants (CAs) and Certified Public Accountants (CPAs) are trusted business advisers who help business managers to maximize their potential for success. The profession has taken a leading role in the field of risk, and firms increasingly include risk management in the wide range of services they provide to their clients. The goal of the Risk Advisory Services Task Force (the Task Force) is to expand risk advisory services across the profession by developing—

- A common language and framework for understanding and communicating this important issue.
- A series of practice guides describing tools and techniques that support the risk management process.

The Task Force has written this document primarily for CAs and CPAs who provide or plan to provide risk services to their clients or employers. "Managing Risk in the New Economy" describes a generic framework or set of steps for risk management based on

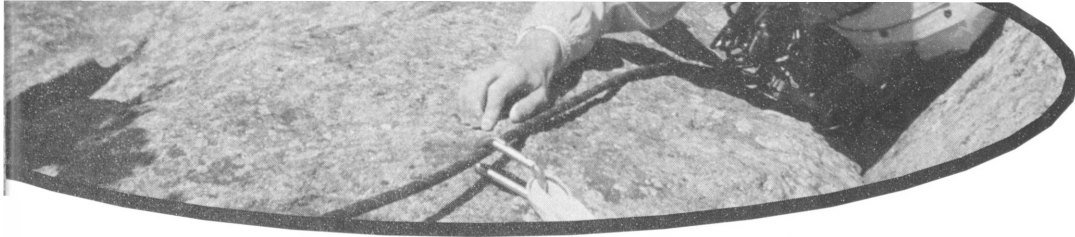
current best practices and is applicable to any size or type of organization.

The related practitioners' guides will provide guidance on implementing risk management systems. The materials will support CAs and CPAs in building on and adapting their existing skills and experience to provide risk management services.

The Task Force recognizes that many public practitioners have developed various approaches to risk management. This document is neither intended to replace any of these approaches nor to establish a uniform model for risk management.

The Task Force has reviewed current literature on the emerging topic of risk services and has incorporated concepts from authoritative sources around the world. The sources are acknowledged in Appendix A, "References and Suggested Reading."





Contents

Committee and Task Force	i
Preface	ii
Executive Overview	2
1. Understanding Risk	3-5
2. Establishing the Context	6-8
3. Identifying Risks	9-10
4. Analyzing and Assessing Risks	11-12
5. Designing Strategies for Managing Risk	13-14
6. Implementing and Integrating Risk Management	15-18
7. Measuring, Monitoring, and Reporting	19-21
8. Cases	22-25
Appendix A – References and Suggested Reading	26-27
Appendix B – Control Frameworks	28
Appendix C – Self-Assessment	29
Appendix D – Glossary	30



Executive Overview

Risk: The chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood.

People want results

Consumers demand high-quality goods and services at competitive prices from businesses, governments, and not-for-profit entities. Investors expect outstanding performance and growth from their stocks.

The challenge for organizations is to deliver results in the New Economy. A world that is fast-paced, ever changing, globally competitive, and technologically innovative. This puts heavy pressure on business owners, boards, and management, who can no longer rely on old-established strategies and practices. They must do a better job of taking and managing risks.

Organizations that manage risk well are more likely to achieve or exceed their objectives because they have the capacity and ability to—

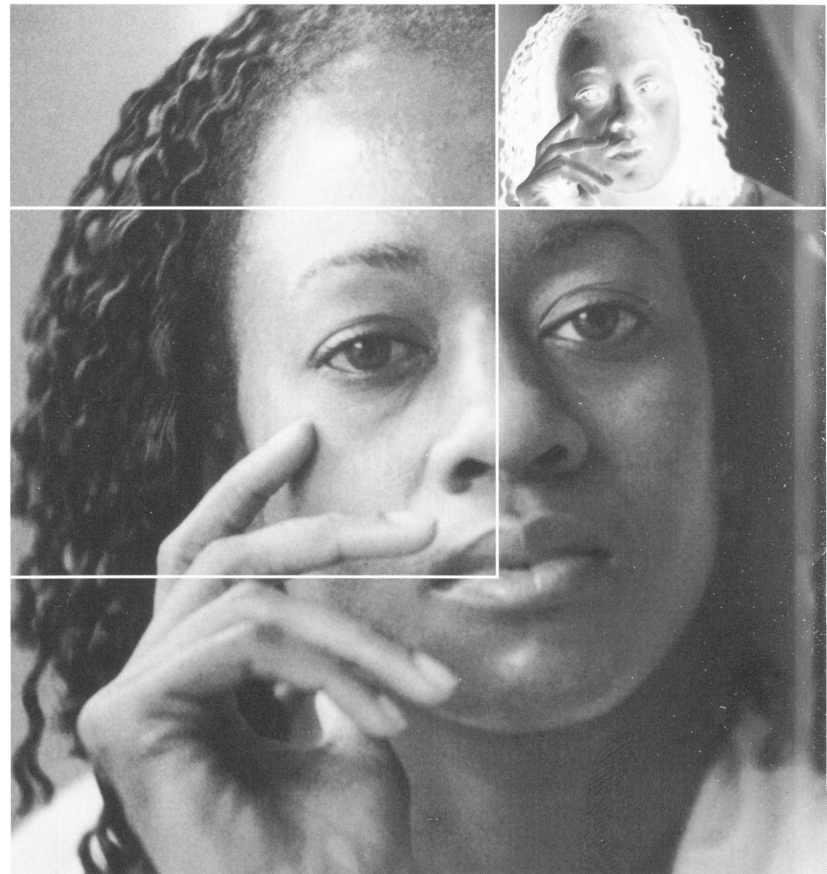
- Identify and exploit opportunities.
- Identify and manage risks that could affect achieving their objectives.
- Make good decisions quickly.
- Respond and adapt to unexpected events.

Successful organizations take calculated risks to achieve objectives. They weigh opportunities against threats and act decisively. The traditional, negative definitions of risk, harm, loss, danger, and hazard, are only part of the story. The other, and equally important part, is opportunity.

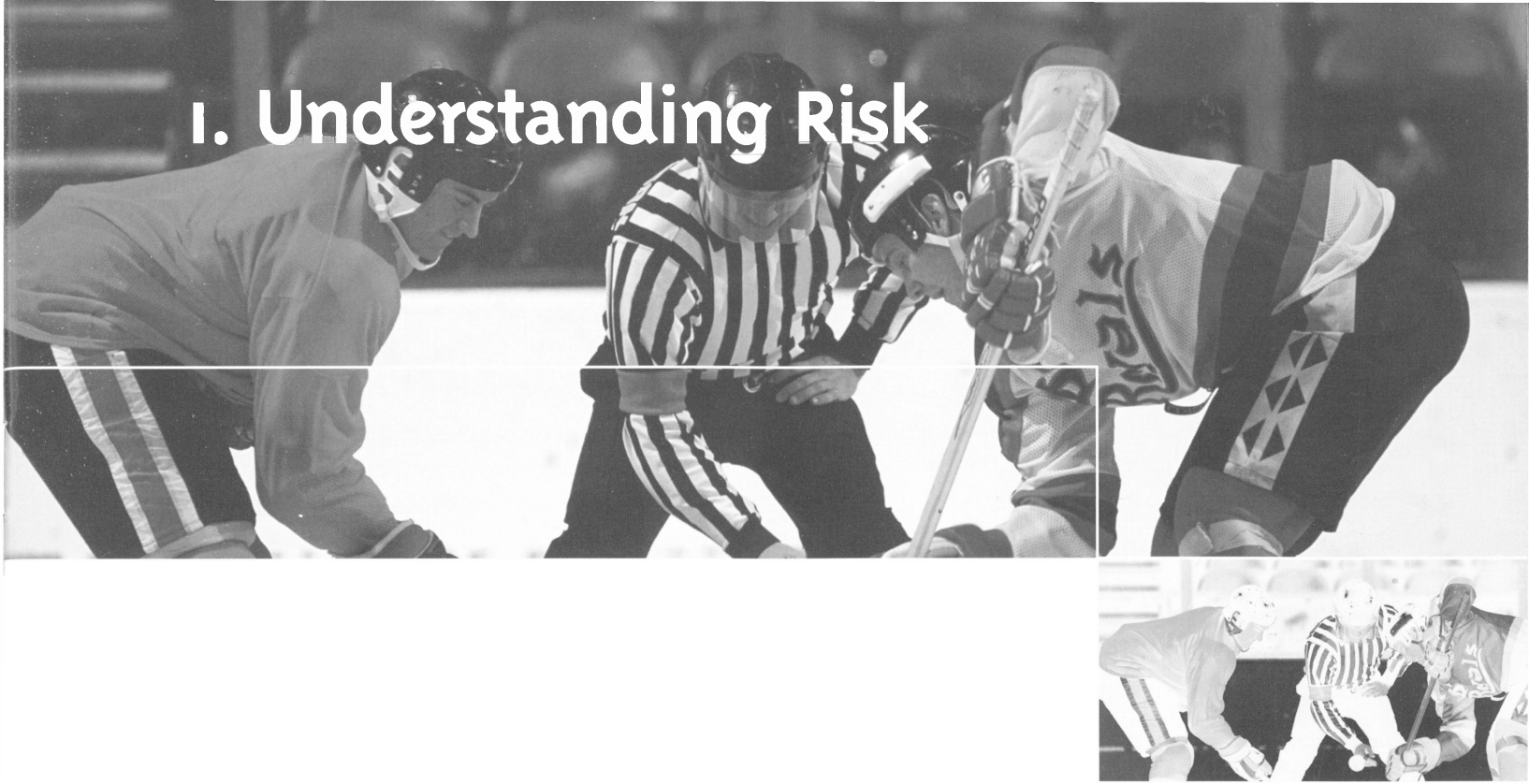
Although each organization has its own unique approach to risk management, a number of consistent steps have emerged and represent current best practice as follows.

- Establish the context.
- Identify risks.
- Analyze and assess risks.
- Design strategies for managing risk.
- Implement and integrate risk management.
- Measure, monitor, and report.

These steps can be applied to an entire enterprise, to a part of the organization or to a specific project. Although an enterprise-wide program is the most effective, there is considerable value in beginning in a local or limited way.



I. Understanding Risk



Objectives and Risks

“First, I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth.”

With these words to a joint session of the U.S. Congress on May 25, 1961, President John F. Kennedy launched one of the world’s greatest adventures. His speech continued:

“No single space project in this period will be more impressive to mankind, or more important for the long-range exploration of space; and none will be so difficult or expensive to accomplish.”

Eight years later, on July 20, 1969, the world heard Neil Armstrong say, “One small step for man, one giant leap for mankind.”

President Kennedy believed the United States had the resources, talent, and courage to achieve the goal of landing a man on the moon. His role was to inspire the nation to seize the opportunity and take the risk. The Apollo Program was not without danger and setbacks, but the project team skillfully managed the risk. The space project succeeded and transformed societies around the world. Universities were founded and expanded to meet the need for educated people and research into high technology. Businesses have built on these foundations to achieve the technological miracles of the New Economy. The story of the

space project illustrates and links the key concepts of objectives and risks. The people involved took and managed risks to achieve the objective of landing a man on the moon and returning him safely to the earth.

Risk and Opportunity in the New Economy

The dawn of the new millennium is a time of unprecedented economic and technological change. The term New Economy is often used to describe the businesses that create and use high-technology products and services, but it equally affects the activities and expectations of every individual and organization. Consumers demand high-quality goods and services at competitive prices from businesses, governments, and not-for-profit entities. Investors expect outstanding performance and growth from their stocks.

Government deregulation and deficit cutting have created a favorable climate for investment and global trade. Powerful computer hardware and software together with high-speed communications technology and the Internet make it possible to meet consumer and investor expectations in a way that was impossible a few years ago.

Meeting these expectations puts heavy pressure on business owners, boards, and management who can no longer rely on old-established strategies and practices. They must do a better job of taking and managing risk.



Does risk mean?

- Opportunity
- Chance
- Threat
- Hazard
- Uncertainty
- Upside
- Downside
- Some of the above?
- All of the above?

I. Understanding Risk

Objectives and Risks

Organizations that take and manage risks well are more likely to achieve or exceed their objectives because they have the capacity and ability to do the following:

- Identify and exploit opportunities.
- Identify and manage risks that could affect achieving their objectives.
- Make good decisions quickly.
- Respond and adapt to unexpected events.

Definitions

Successful organizations take calculated risks to achieve objectives. They weigh opportunities against threats and act decisively. The traditional negative definitions of risk, harm, loss, danger, and hazard are only part of the story. The other and equally important part is opportunity.

There are many definitions of *risk*. The dictionary entry is just a beginning and does not include the many risk-related terms used in business. Each organization has its own terms for talking about risk. It is important that everyone within the organization share a common risk language since universally accepted definitions of most risk-related terms are still being formulated.

The following definitions reflect the current view of risk as embracing both opportunity and threat.¹

- *Risk* is the chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood
- *Risk management* includes the culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects
- *Risk management process* includes the systematic application of management policies, procedures, and practices to the tasks of establishing the context, identifying, analyzing, assessing, managing, monitoring, and communicating risk.

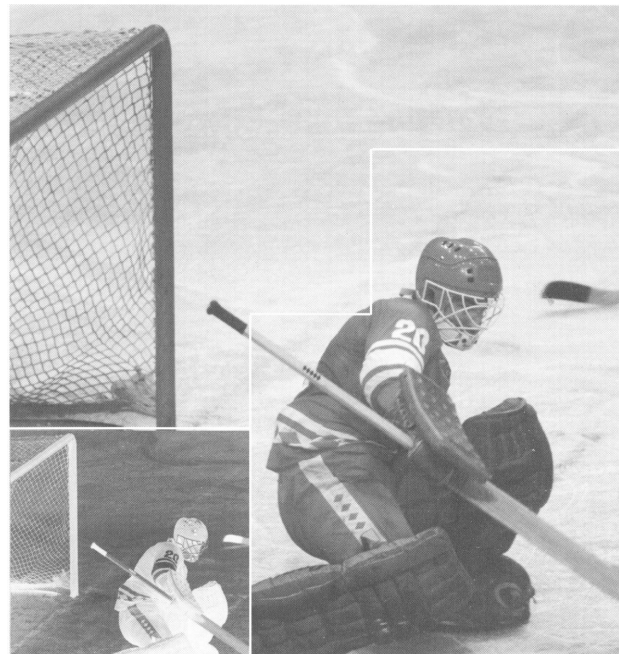
Integrated Risk Management

There is no single, right way to manage business risk. However, there is a strong consensus that risk management is not an isolated activity carried out by specialists. An enterprise-wide responsibility calls for "a common process developed centrally and implemented locally with the guidance of the risk management champion".²

This is integrated risk management. The concept of integration has a further dimension. It relates to the need to understand the relationship between multiple risks and the integration of risks. This adds reality to risk management, as well as engaging more of the organization in an integrated process.

¹ The following are based on definitions developed by the Joint Technical Committee OB/7, Risk Management. Standards Australia and Standards New Zealand, Australian/New Zealand Standard 4360:1999: Risk Management.

² The Conference Board of Canada, *A Conceptual Framework by Integrated Risk Management*, by Lucy Nottingham. Ottawa, ON, September 1997, Executive Summary.





I. Understanding Risk

Objectives and Risks

The principles of integrating and championing risk management apply to any organization. The process need not be complex nor formal and the business owner or president may personally assume the role of champion and coordinator of the risk management activities.

Although each organization has its own unique approach to risk management, the following consistent steps have emerged and represent the current best practice.

- Establish the context;
- Identify the risks;
- Analyze and assess the risks;
- Design strategies for managing risk;
- Implement and integrate risk management; and
- Measure, monitor, and report.

These steps can be applied to an entire enterprise, to a part of an organization, or to a specific project. Although an enterprise-wide program is the most effective, there is considerable value in beginning in a local or limited way.

A Word of Warning

Risk management is necessary and useful, but not an absolute guarantee. Peter L. Bernstein, author of *Against the Gods: The Remarkable Story of Risk*, warns of the limitations of risk management and the possibility of increasing risk instead of managing it.³

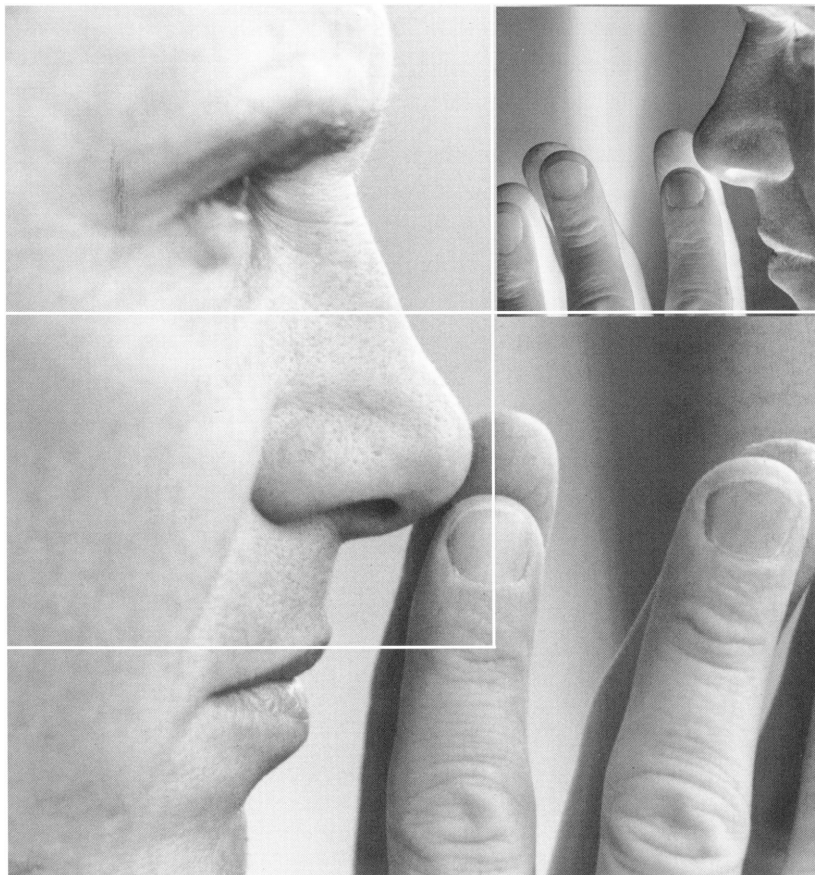
In periods of stability, Bernstein suggests, we come to assume that stability is the natural order of things. We forget about stock market crashes, hyperinflation, and massive price changes. If we do not expect wild things to happen, we do not build them into our risk management processes.

Risk management techniques often involve the use of historical

data to predict the future. The discipline of identifying and assessing risks is helpful but the resulting numbers are still guesses about uncertainty.

Finally, Bernstein warns that the sense of security that comes from having a risk management process in place may lead us to take risks we should not take. Taking more risk is usually beneficial. But we should be wary. The goal is to optimize risk not to maximize it.

³ Peter L. Bernstein, "The New Religion of Risk Management," Harvard Business Review, March-April, 1996, pages 47-51.



2. Establishing the Context

A leading liquor distributor offered to sponsor a children's festival organized by a charity.

The charity's executive director recognized the public image implications of the sponsorship and referred it to the board of directors. The charity's major constituents are public and parochial school systems that might have withdrawn funding to a charitable organization affiliated with liquor - which in turn could have been catastrophic to the charity.

The board was able to identify and manage this risk because the charity had (1) a board policy for determining potentially inappropriate sources, and (2) policies and procedures for staff to ensure that donations from questionable sources are identified immediately and referred to the board for approval.

Risk Context

The risk management process occurs within the context of the organization; its environment; and its goals, objectives, and strategies. By establishing its context, an organization is in a position to develop its approach to risk management.

Successful organizations know what they are and what they want to be. Their strategies are consistent with their vision and values. Investors, lenders, suppliers, and customers understand and respect them because they can rely on them. But organizations can be very different in their approaches to risk. Deposit-taking institutions place a high value on solvency and the preservation of capital. Their investors and customers expect a good return with little risk. Companies that prospect for minerals or develop high-tech products focus on big rewards for big risks. Their investors typically understand this trade-off between risk and reward and the significance of an organization's appetite and capacity for risk.

Appetite for risk, the amount of risk an organization is prepared to take, is closely linked to corporate philosophy, culture, and strategic perspective. Smart investors know it is impossible to make money in business without accepting risk. It is important to have an understanding with stakeholders as to how much risk they are willing to accept.

Capacity for risk includes the ability to exploit opportunities as well as the resilience to market setbacks and catastrophes.

It is related to the organization's structure and culture, and the strength of its human, financial and operational resources, systems, and processes. Organizations with a broad base of strengths are best positioned to withstand the individual and cumulative effect of risks.

Establishing the context for risk management begins with consideration of:

- The philosophy, culture, and strategic perspectives.
- The vision, mission, and values.
- Relationships with key stakeholders.
- The external environment.
- The internal environment.

These factors, which are key considerations in strategic planning, help the organization establish its objectives and its appetite and capacity for taking risk.

Objectives may be considered as steps on the way to achieving an organization's mission and vision. The mission and vision generally change little over time. Objectives are frequently established and revised. Since risks affect the achievement of objectives, the risk management cycle begins with identifying objectives and the strategies that are in place to achieve them.

Failure to achieve the objectives of the organization, or of specific activities or projects, is one set of risks that should be managed.





For Baxter International, building shareholder wealth was a key objective. The company saw shareholder risk and availability of capital as critical areas in which to manage risks.

The company turned employees into shareholders to manage resource allocation and build shareholder wealth. The international health care provider encouraged its seventy top managers to buy shares in the company.

"The result has been a sea change in thinking. In the area of resource allocation there's more discipline, more focus more prioritization, and trade-off" said CFO Harry Kraemer. —Economist Intelligence Unit & Arthur Andersen

2. Establishing the Context

Objectives and related plans should include measurable performance targets and indicators. These can include quantitative performance targets (such as budgets) and qualitative performance targets (such as customer satisfaction). The targets should be measurable and aligned with the objectives. Externally derived benchmarks can be used to help ensure the competitiveness of such targets.

Risk Management Approach

From an understanding of the risk context, the owners or management are in a position to develop a risk management approach. This may involve formal and structured policies and procedures, or an informal process, depending on the need of the organization. In developing the approach, an organization may ask the following four questions.

- What is our objective?
- What are our values?
- Who is accountable?
- Who has the authority?

Objective of Risk Management

An organization's objective for risk management will generally be to establish a process for optimizing risk. This will involve defining the degree to which risk management is integrated.

Values Related to Risk Management

An organization's values include its commitment to ethics, safety, customer service, product quality, and corporate citizenship; and respect for the risk tolerance and risk limits of its lenders, creditors, and investors. An important issue to consider is the organization's readiness to accept critical questions, objections, and other challenges from employees and other stakeholders.

Accountability for Risk Management

Although the owner-manager, chief executive officer (CEO), and board of directors have overall responsibility for the organization and risk, they may appoint a champion — a central coordination point for risk management. This individual, although not personally responsible for the total organizational risk, is accountable for ensuring that the risk management system is

implemented and sustained. It is also important to establish the accountability of line managers and individual employees for managing risk in their own areas.

Larger organizations divide activities and projects among a number of divisions and departments. The risk management approach establishes the roles, responsibilities, and relationships of the various parts of the organization and defines how they participate in risk management.

Authority for Risk Management

Authority includes the power to administer the risk management program. It also addresses the power of individuals to act in emergencies without consulting a superior or someone with specific risk management responsibility.



2. Establishing the Context

Criteria for Risk Assessment

A key objective of establishing context is the determination of criteria for risk management. The criteria provide a benchmark against which to make decisions and to measure and monitor performance. Criteria define what is important to the organization and how it will be measured. They reflect areas of particular sensitivity and the limits to the organization's appetite and capacity for risk.

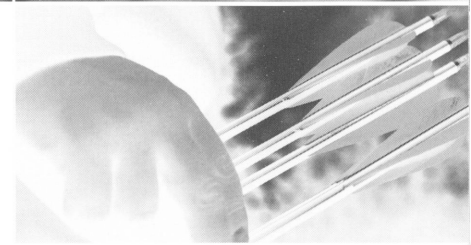
A systematic risk management process requires criteria against which risk can be evaluated. The criteria may be based on operational, technical, financial, legal, social, humanitarian, or other considerations. These often depend on the organization's internal policy, goals, objectives, and the interests of stakeholders. Risk criteria should correspond to the kind of risks and the way in which risk levels are expressed.⁴

Developing criteria is an iterative process, which begins by establishing risk levels in the context of the organization's appetite and capacity for risk. The criteria establish a common understanding of terms describing levels of materiality to the organization. The criteria will generally be further developed and revised as specific risks are identified, analyzed, and assessed.

⁴ Joint Technical Committee OB/7, Risk Management. Standards Australia and Standards New Zealand, *Australian/New Zealand Standard 4360:1999: Risk Management*.



3. Identifying Risks



The number of risks facing any organization can be enormous. It is not practicable to identify and assess all of them. People need a systematic approach to identify and address the risks related to the critical success factors for their organization. The risk identification system needs to have rigor, but also be flexible enough to deal with constant changes in the environment in which the organization operates.

Risk Identification Techniques

An organization's approach to risk identification will depend on the nature of the activities under review and the perceived degree of risk. The diversity and complexity of risk are best addressed by selecting from a variety of techniques, which may include the following:

- Internal interviewing and discussion made up of the following:
 - Interviews
 - Questionnaires
 - Brainstorming
 - Self-assessment and other facilitated workshops
 - Strengths, weaknesses, opportunities, and threats (SWOT) analysis.
- External sources including the following:
 - Comparison with other organizations
 - Discussion with peers
 - Benchmarking
 - Risk consultants.

• Tools, diagnostics, and processes including the following:

- Checklists
- Flowcharts
- Scenario analysis
- Value chain analysis
- Business process analysis
- Systems engineering
- Process mapping.

The most appropriate techniques are flexible and encourage openness. An effective approach is to involve employees at all levels in identifying the organization's risks to gain their insights and commitment.

Risk Categories

A systematic approach improves the likelihood of identifying significant risks and provides a basis for categorizing them. It also provides a common language for communication about risk and coordination of action. Categories are affected by the size and nature of the organization. An organization may develop its own in-house approach from a generic or industry-specific source, or use a proprietary product.





3. Identifying Risks

A starting point for categorizing risks may be the following:

- Objectives
- Areas of impact
- Sources of risk
- Specific hazards or perils, such as fire, theft and earthquake
- The degree of control that the organization has over the risk

There is risk for every objective. Breaking the value chain into subprocedures allows an organization to see each critical objective and the risks associated with that objective.

Areas of impact include the organization's reputation, assets, revenues, costs, performance, and people, which means employees, customers, and communities.

Models organized by sources of risk are the most common. They vary in detail but cover essentially the same ground. The principal categories are:

- *Environmental* — Risks from the world outside the organization can be natural, economic, political, and social. This kind of risk also includes financial risks such as volatility in interest rates, currency, or commodity markets
- *Strategic* — Risks of this kind are associated with strategic decisions to embrace opportunity and seek reward
- *Operational* — Risks of this kind can be prevented, detected, corrected, and managed through effective systems of control. They include breaches in compliance, inefficient operations, fraud, error, business interruption, and inaccurate reporting⁵
- *Informational* — Threats of this kind derive from the use of poor-quality information for financial or strategic decision making within the business and providing misleading information to outsiders.

The hazard-based approach is common among insurance buyers. It relates to the coverages available from insurers.

A number of organizations start from their relative ability to manage or influence risk, which may include:

- Political, economic, social, and financial risks over which an organization has very little control
- Factors such as reputation, competition, and regulation, over which the organization may have some influence but very little control
- Risks over which an organization can have a great deal of control.

Recording Risk

Documentation of the risk identification process provides a valuable record for the organization. There are a number of software packages available for recording risks. These usually include tools for assessment and analysis.

⁵ The Canadian Institute of Chartered Accountants; *Learning About Risk: Choices, Connections and Competencies*, 1998.



4. Analyzing and Assessing Risks



Consequence

The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage, or gain

Likelihood

A description of a probability or frequency



The process of analyzing and assessing risks helps the organization make better decisions and rank risks to establish priorities for action. An organization can assess how the identified risks affect its strategic objectives by considering their likelihood and consequence.

The terms *likelihood* and *consequence* recognize the element of uncertainty and the broad range of risks faced by most organizations.

The insurance industry uses the terms *frequency* and *severity*, which work well for that business. Insurance is based on the law of large numbers. Insurers know from experience the probable number (frequency) of claims that will flow from a given number of policies and the average cost (severity) per claim. With help from actuaries, the insurers can set premium rates and predict claims costs. They quantify their risk very precisely in numeric terms. Buying reinsurance or "insurance for insurers" protects them against catastrophic events.

A simple but powerful way to display the relationship between the likelihood and consequences of an event is to use a risk map. There could be a map by critical success factor, overall organization objective, or each of the categories used in identifying risk. Figure 1, "A Risk Map," provides an example of a risk map, a matrix that displays the relationship between the likelihood and consequences of specific risks.

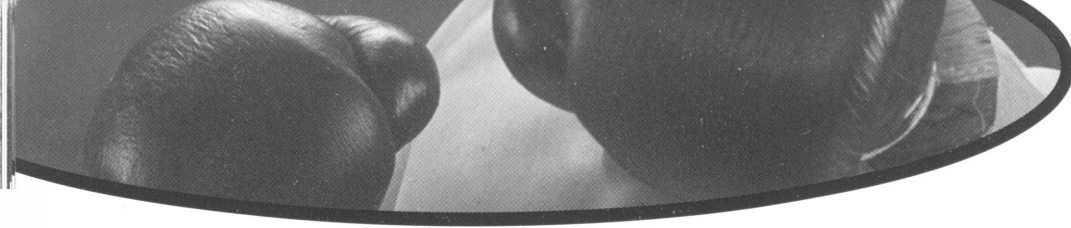
Figure 1

A Risk Map

Consequence	High			
	Moderate			
	Low			
		Low (Remote)	Moderate (Possible)	High (Probable)

Likelihood of Occurrence





4. Analyzing and Assessing Risks

Risk mapping can be used for both aspects of risk: opportunities and threats. Organizations may also find it useful to prepare risk maps for different time horizons.

One or more of the following kinds of measurement, which are also presented in figure 2, "Examples of Risk Measurement," may be used in risk analysis and assessment, depending on the size and complexity of the organization and the availability of information.

Qualitative analysis uses descriptive terms. This is a useful technique for getting a general indication of the level of risk before undertaking more rigorous analysis. Assigning a numerical "score" or approximate percentage creates a value that may not be completely accurate but is useful for ranking and aggregation purposes.

Quantitative analysis uses numerical measurements such as dollars, percentages, or occurrences. Risk assessment and analysis should also take into account the organization's ability to control or influence risk.

Figure 2

Examples of Risk Measurement

	Likelihood	Consequence
Qualitative	<ul style="list-style-type: none"> • Almost certain, likely, possible, unlikely, rare • Numerical scoring 1, 2, 3, and so on • Percentage probability 	<ul style="list-style-type: none"> • Insignificant, minor, moderate, major, catastrophic • Numerical scoring 1, 2, 3, and so on
Quantitative	<ul style="list-style-type: none"> • Time frame hourly, daily, weekly, yearly, and so on • Percentage of volume, and so on 	<ul style="list-style-type: none"> • Dollar ranges • Percentages • Per capita



5. Designing Strategies for Managing Risk

A company may have adopted the guiding principle that a smaller head count is better and accordingly downsized and outsourced—only to realize that business hasn't improved appreciably, and is doing worse in some respects. The benefits may have been exaggerated and the risks underestimated.

—Scott Lange, former Director of Risk Management, Microsoft Corporation

An infant car seat manufacturer had a goal to increase production by outsourcing assembly of the car seats. They would align their risk management strategy for controlling or managing product quality (defects that could contribute to death and injury) to address the processes performed by a third party, rather than at their own facilities.



Managing risk means that individuals make good decisions with respect to the following:

- *Strategic choices* — To embrace opportunity and seek reward
- *Operational choices* — To prevent, detect, correct, and manage risks through effective systems
- *Crisis choices* — In response to catastrophes
- *Resilience choices* — To build an organization that can survive catastrophes, major lawsuits, or the outcomes of unsuccessful strategic decisions.⁶

Each organization will establish its strategies on the basis of its own tolerance for risk and its respect for the risk tolerance and risk limits of its key stakeholders. Strategy options should be evaluated by balancing risk and reward to achieve risk optimization.

Strategies for managing risk tend to fall into one of four broad categories: Avoiding, Transferring, Mitigating, and Accepting.

Avoiding Risk

Risk avoidance can be a conscious strategic choice not to proceed with an activity likely to generate risk.

If the risk associated with an opportunity is too high relative to the potential reward, it may be appropriate to drop the idea.

Avoidance may also be the result of risk aversion. People are naturally inclined to be risk-averse and may be further influenced by an organization's internal systems and culture. Inappropriate risk avoidance may result in missing opportunities.

Transferring Risk

Organizations may reduce the consequence of losses by transferring risk to third parties. Examples include the following:

- Buy insurance.
- Use financial instruments.
- Outsource activities.
- Establish partnerships or strategic alliances.

Risk transfer is a valuable and legitimate strategy if the organization to which the risk is transferred can be relied on to manage the risk effectively.

Mitigating Risk

Successful organizations manage the risks they retain in a way that increases the probability of achieving objectives while reducing the likelihood and consequences of threats.

⁶ The Canadian Institute of Chartered Accountants, *Learning about Risk: Choices, Connections and Competencies*, 1998.



"The final act of business judgment is intuitive."

*—Alfred Sloan,
former President,
General Motors.*

5. Designing Strategies for Managing Risk

A way to increase the likelihood of achieving objectives is to establish and monitor critical success factors and key performance indicators. Effective control includes the information and reporting that support the achievement of objectives.

Preventive and detective controls anticipate and reduce or control the likelihood of risks. They include internal financial control and the controls built into manufacturing and other processes.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Criteria of Control (CoCo) project of The Canadian Institute of Chartered Accountants control models (see Appendix B, "Control Frameworks") provide guidance on the design and assessment of control in the context of achieving objectives.

Good crisis management and a resilient organization can reduce the consequence of risks. An effective risk management program will provide guidelines and procedures for catastrophe planning and disaster recovery. The program will also mitigate the consequence of everyday events that may affect customer satisfaction or customer loyalty.

A well-understood risk culture can help employees make informed and intelligent decisions to mitigate risk.

Accepting risk

Organizations may decide to accept some risks. For example, a gold mining company, recognizing the risk of fluctuating gold prices, may conclude that the opportunity of profiting from a rise in prices outweighs the benefits of hedging against the threat of falling prices. In such cases, they should take steps to identify, measure, and monitor the risk.

Intuition and the choice to deny or act

Experienced business people respect systematic processes. They also recognize the value of intuition as a source of innovative strategies, a reality check, and a powerful early warning device.

Intuition is fast and powerful. It sends gut-feeling messages that are usually worth acknowledging. Acting on intuition alone does not guarantee success or freedom from the risk of loss. Paying attention to its advice and warnings makes good business sense when it gets people to ask challenging questions and reassess strategies in light of all the other knowledge they have accumulated.



6. Implementing and Integrating Risk Management

Nine of every ten senior executives in the survey agreed that internal control is critical to effective management. Yet 80 percent of the same group agreed that when it comes down to compensation, "making the numbers is what really matters."

Virtually all CEOs (95 percent) state that they "truly have an open door policy and will reward employees who communicate potentially bad news."

However, half of all employees (48 percent) state that "the messenger of bad news takes a real risk in my company." Three-quarters of the chief executives surveyed answered "no" when asked whether their employees intentionally circumvent cumbersome corporate policies.

Yet, half of the non-CEOs surveyed indicated that such circumvention is common.

—Louis Harris and Associates, Inc., The Coopers & Lybrand Survey of Internal Control in Corporate America.

Implementing a program of integrated risk management involves the following:

- The creation of a risk-aware culture where each employee is accountable for managing risk
- The establishment of specific risk management objectives and performance measures
- The establishment of an infrastructure for risk management
- Communication and training in risk management
- The implementation and operation of the organization's risk management policies and strategies.

Responsibility for risk management starts at the top with one of the following:

- A board of directors that hires and supervises a chief executive to manage the enterprise on behalf of the owners, members or other stakeholders
- A management team that is not accountable to a board, as in owner-managed businesses and partnerships

Creating a Risk-Aware Culture

Management can show leadership by defining strategic objectives and values that are unmistakably clear and inspiring. They establish a consistent "Tone at the Top" by living and communicating the objectives and values. This leadership enables employees to link enterprise objectives and values to every level of the organization.

Establishing Risk Management Objectives

Successful organizations make business risk management and control strategic priorities for all operating units. An effective approach to integrating risk management across the enterprise is to align objectives, risks, and control. Implementation starts at

the top. Management sets and prioritizes business objectives. Each successive layer of the company establishes and prioritizes objectives that are consistent with the enterprise plan.

Establishing an Infrastructure for Risk Management

An organization's risk management infrastructure should be designed to reflect the nature of its business, its size, and the complexity of its organizational structure. Large, complex organizations will typically need a formal risk management infrastructure with written goals, objectives, policies, and procedures, as well as special departments and individuals devoted to maintaining the infrastructure. Smaller, less complex organizations will usually require a less formal infrastructure. Regardless of the degree of formality chosen, every organization should designate "owners" for all objectives, goals, and processes. Each owner from executive to entry level, understands his or her objectives, evaluates the related risks, and makes certain there are reasonable levels of control in place to mitigate those risks. The following three steps build accountability.

- Establish ownership for business objectives at all levels of the organization.
- Integrate the process for managing risk with other planning and management activities.
- Promote a "risk management competence" that provides employees with the tools to align objectives, risks, and controls.





6. Implementing and Integrating Risk Management

Business Areas

Each suborganizational area, department, program, project, or team activity is responsible for managing risk in accordance with the organization's risk management approach by—

- Incorporating control activities and risk strategies into processes and activities.
- Applying policies and procedures to day-to-day activities.
- Including control and risk strategies in new systems.
- Upgrading controls as needed to close gaps.
- Documenting risk assessments and controls.
- Sharing information on risk with other business units and the risk management team.

The Risk Management Team

The organization's risk management champion is accountable for establishing an integrated approach to risk management.

In smaller organizations, the risk management champion may be the owner/manager, president, general partner, or other high-ranking individual in the organization.

In larger organizations a number of specialist departments are already involved in aspects of risk management. These include controller, treasury, audit, compliance, public relations, human resources, security, and risk management professionals. Integrated risk management means linking these functions as an organization-wide team that also includes representatives of line management.

Identifying the risk management champion is a good first step in establishing an integrated risk management strategy. This individual may be a designated Chief Risk Officer or an executive within the risk management, finance, or internal audit groups.

The risk champion as leader (or sole member) of a risk management team is responsible for designing, communicating, and supporting the implementation of the organization's risk management approach. The team's primary objective should be to identify business risks and design strategies for managing them. The risk management team is not responsible for risk management but facilitates, challenges, and drives the risk management process by—

- Acting as the primary advocate for risk management at the strategic and operational levels of the organization.
- Providing a philosophy, framework, and methods to business units to identify, analyze, and manage their risks more effectively to achieve their objectives.
- Developing risk response processes (including crisis response) to assist appropriate kind and level of response required.
- Monitoring performance to provide assurance that the risk management approach is operating effectively to support achievement of the organization's objectives.
- Reporting to management on risk management.
- Acting as a troubleshooting team.⁷

⁷ International Federation of Accountants, *Enhancing Shareholder Wealth by Better Managing Business Risk*, 1999.



6. Implementing and Integrating Risk Management

The Board and its Committees

In organizations with boards of directors, the directors should demonstrate a clear commitment to risk management and explicitly assign responsibility. The board may discharge its risk management responsibility directly or through a committee of the board or a senior management group.

The process should ensure that the organization has a clearly defined and documented process for risk management.

Communication and Training

If an organization establishes or makes a significant change to its risk management approach, it needs to educate management and staff. The risk management team may be in the best position to coordinate and supervise the process of introducing the changes across the organization.

Most employees do not see managing risk as their primary responsibility. Their aim is to do their job properly. They want to know their objectives and how to achieve them. However, they also need to understand and be aware of the following:

- What might go wrong
- What would happen if it did
- How to prevent it from happening
- What to do if it happened

The objectives of communication and training should include the following:

- Raise awareness about managing risk
- Communicate and explain the organization's approach to risk management
- Implement a common risk language across the organization
- Establish a dialogue throughout the organization about managing risk
- Develop skills.

Implementing and Operating the Organization's Risk Management Policies and Strategies

Identifying and Filling Gaps

Once the infrastructure and communication programs have been established, the organization is in a position to assess the quality of its risk management, identify gaps, and begin a process of upgrading.

This uses and builds on the risk identification and assessment described in Chapters 3, "Identifying Risks", and 4, "Analyzing and Assessing Risks," and the risk management strategies in Chapter 5, "Designing Strategies for Managing Risk."





6. Implementing and Integrating Risk Management

Reinforcement

The "Tone at the Top" established by management needs constant reinforcement. Business unit managers and supervisors can demonstrate leadership by living and communicating the organization's objectives and values.

"Ultimately, an organization's employees will drive control and process improvement in the context of established core values and objectives. Therefore, a critical attribute of successful organizations is an alignment of human resource practices with the enterprises' business objectives and values. This is done through hiring the right people and then training them in both their job and control. Most importantly, the message must be reinforced through employee appraisals and incentives that not only reward financial results but also desired behavior. Ignoring or dealing inconsistently with unethical or uncontrolled actions creates a subtle erosion in corporate values that can lead to control failures".⁸

⁸ Moche, James, "Key Attributes of Well-Controlled Organizations: Making Control a Competitive Advantage," in *In Pursuit of the Upside: Leading Thinking on Issues of Risk*, 1998.



7. Measuring, Monitoring, and Reporting



“How Well Are We Doing At Managing Risk?”

The diversity and uncertainty of risk make it impossible to have one definitive risk measurement that can be monitored. The answer to the question is found in the answers to a series of more detailed questions such as the following.

- Are we achieving the results we planned?
- Are we monitoring and learning from control breakdowns and losses?
- What are we doing about the major risks we have identified?
- Do we have the necessary guidelines or policies and procedures?
- Do they work or will they?

The specific questions will depend on the organization. The answers will come from the processes for measuring, monitoring, and reporting risk.

Measuring Risk

The risk management process includes establishing measurable objectives and criteria for performance and risk and then collecting the relevant information. The measurements are established in the process of establishing the risk context described in Chapter 2, “Establishing the Context”.

Performance and risk measurements include the following:

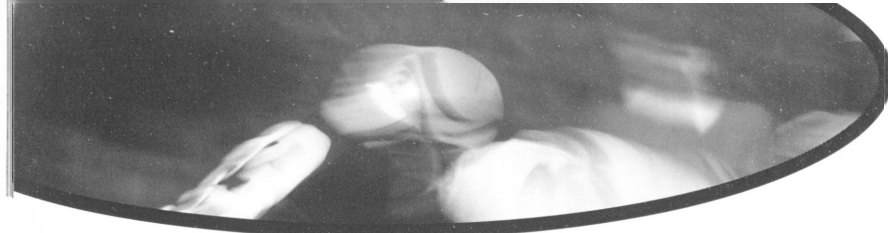
- Financial and other information that measure performance against objectives
- Records and analysis of control breakdowns and losses

Measurements can be problematic and hard to collect consistently at reasonable cost. However, the process of investigating and testing alternatives has proved very valuable to many organizations, which are also starting to develop some good measurements.

Monitoring Risk

Monitoring includes reviewing information and identifying the appropriate action to take. People in organizations learn from their experience and apply the knowledge to improving effectiveness.





Analyses of airplane crashes and hospital operating room incidents are powerful tools for identifying risks and improving control measures.

At Microsoft, risk analysis led one profit group to revise its pricing to include the cost of risk. The company was ready to license an innovative PC keyboard for production, charging a royalty for each unit. But the group that designed the keyboard failed to factor in the effect of "a very big storm brewing: repetitive stress injury and the potential for mass tort litigation."

—Scott Lange, former Director of Risk Management
Microsoft Corporation

7. Measuring, Monitoring, and Reporting

Monitoring processes include the following:

- Reviewing and acting on:
 - Performance and risk information
 - Control breakdowns and losses.
- Auditing and validating, including:
 - Audits of control systems and processes
 - Audits of financial and operational information systems
 - Self-assessments
 - Tests of contingency and disaster recovery plans
 - Confirmation that control deficiencies are remedied.
- Updating information and assumptions:
 - Assumptions made in planning and risk management
 - Measures used to track risks
 - Updates to risk identification and assessment
 - Changes to the external environment
 - Adequacy of the insurance program.

Reporting Risk

There are three main kinds of reporting on risk:

- Internal reporting to management and staff
- Reporting to the board of directors
- External reporting to regulatory agencies and other stakeholders.

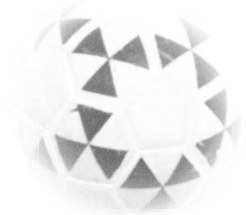
Internal Reporting

Internal reporting provides management and staff with the operational and strategic information they need to run the organization and meet its objectives. Reporting covers the performance and risk measurements that have been developed and monitored. It also covers the status of risk initiatives that were previously implemented or determined to be necessary. The primary purpose of reporting is to identify requirements for action.

A good reporting system is compatible with the management style and culture of the organization and need not be very formal.

Reporting to the Board of Directors

Boards need assurance that their organization has taken steps to identify and assess risk and that it takes appropriate measures to address identified risks. The CEO and risk management team should develop a process for reporting that meets the board's needs. This may include formal written reports and a series of presentations and discussions.





7. Measuring, Monitoring, and Reporting

The CICA publication, *Guidance for Directors – Dealing with Risk in the Boardroom*, recommends that directors should actively review information about future performance, opportunity, and risk. This includes taking time to review strategy and risk and receiving periodic updates from management on strategy and progress in managing previously identified risks. Directors should be briefed on the risks involved in major proposals, specific operational risks, and emergency preparedness.

The publication urges directors to watch for warning signs, make use of intuition and collective judgment, and be prepared to ask tough questions.

External Reporting

Regulatory agencies, lenders, and investors establish reporting requirements for organizations that use outside sources of financing. The principal regulatory requirements are those for prospect uses and annual reports.

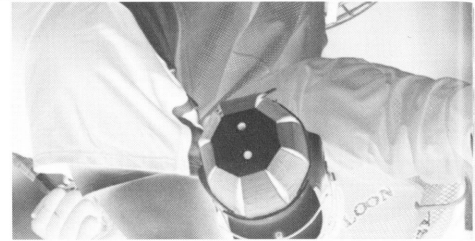
Prospect uses require a comprehensive disclosure and discussion of the risks that prospective investors should consider. The risk considerations are wide-ranging. Topics include the environment, operational matters, pricing, foreign exchange, labor relations, competition, and any other matters that may be relevant.

Annual report requirements are, at present, less demanding than those for prospectuses, but the gap is likely to shrink quickly. The management discussion and analysis sections of annual reports in the United States and Canada include disclosures about risk.

There are, at present, no generally accepted standards for risk measurement and reporting.



8. Cases



This chapter consists of a number of cases that illustrate aspects of risk management. These cases are selected from annual reports and from the sources indicated in the footnotes.

Establishing the Context

The Medicines Company, or TMC, a pharmaceutical development firm in Cambridge, Massachusetts, has become a skilled buyer and seller of risk as an offshoot of its core business. Developing a drug can cost about \$300 million and entails five distinct stages, from developing the chemical or biological compound to winning approval from the Food and Drug Administration (FDA). The potential upside, of course, is another billion-dollar blockbuster such as Tagamet[®], Zantac[®], or Viagra[®].

TMC understood that drug development represents a sequence of very different risks because a drug can fail for different reasons at any point in the approval process. The later the failure, the more expensive the failure. TMC had a clear sense of the risks it managed well, particularly the risk of failure during clinical trials. It was weak upstream in basic research and downstream in marketing drugs to physicians. So the company concentrates on buying the rights to chemical and biological compounds, developing them into drugs and then selling them to other pharmaceutical firms to bring to market. As a result, TMC has developed a successful business of buying and selling drug development projects. The company bears risk only for the pieces of the process where it best knows how to succeed.⁹

British Petroleum Exploration (BPX), like other companies in the global oil and gas industry, faces a new set of economic realities. In addition to fluctuating oil prices, BPX has identified the following four key external drivers it must accept and manage.

- Oil is getting tougher to find.
- Political risk reduces other options.
- The industry is losing its favored status with world governments.
- Old recovery techniques are often inefficient; new recovery technologies are often expensive.¹⁰

Identifying Risks

Guinness has defined seven business risks within its large but relatively straightforward businesses, which are United Distillers and Guinness Brewing Worldwide:

- Brand equity risk
- Customer satisfaction risk
- Product quality risk
- Catastrophic risk
- Regulatory risk
- Cultural risk
- Trade war risk.

It is the job of the treasurer to make certain the risks are addressed. Guinness's policy is to manage risks themselves where they can and to transfer risk to third parties where this is cost effective."¹¹

⁹ Stan Davis and Christopher Meyer, *Future Wealth*, 2000.

¹⁰ Economic intelligence Unit with Arthur Andersen, *Managing Business Risks: An Integrated Approach*, 1995.

¹¹ Economic intelligence Unit with Arthur Andersen, *Managing Business Risks: An Integrated Approach*, 1995.





8. Cases

Analyzing and Assessing Risks

Canadian Pacific is a diversified operating company active in transportation, energy, and hotels. Its results are affected by external market factors, such as fluctuations in the prices of crude oil, natural gas, and coal, as well as movements in interest and foreign exchange rates. The following table illustrates the estimated effect of changes, under certain conditions, in the foreign exchange value of the Canadian dollar, interest rates, and the prices of crude oil, natural gas, and coal, on consolidated 2000 earnings, based on the company's 1999 annual report:

	Effect on Net Income Excluding Hedging	Effect on Net Income Including Hedging
U.S. one-cent decrease in the value of the Canadian dollar	\$26	\$9
One percentage point decrease in interest rates	\$6	\$6
US \$1.00 per barrel increase in the price of West Texas Intermediate crude oil		
— Pan Canadian	\$34	\$29
— Other businesses	(\$14)	(\$14)
10 cent per thousand cubic feet increase in natural gas prices	\$17	\$17
US \$1.00 per metric ton increase in coal prices	\$13	\$13

Canadian Pacific utilizes various derivative financial instruments in order to mitigate the risks associated with changes in foreign currency exchange rates, interest rates and commodity prices.

Designing Strategies for Managing Risk

Managing customer service risk is critical to the survival and success of software developers. **ACT International** grew fast as a leading UK-based financial software maker until business and

profits plummeted in the early 1990's. A customer survey showed clearly that the company had failed to recognize the profound dissatisfaction of its customers. The solution began with the introduction of ongoing customer feedback into its system of performance evaluation and control. The survey asks questions concerning:

- Product functionality
- Account management and sales personnel
- Customer service center response quality
- Technical support timeliness
- Customization of installations
- Consultancy
- Administration and Communication
- General.

The customers rate ACT on a scale of 1 (very unsatisfied) to 5 (very satisfied) in a survey that takes between 15 and 30 minutes to complete. The response rate has been over 80 percent. Branch staff talk to clients who score less than 3 in a given area and take action to remedy the problem.



8. Cases

The focus on customer satisfaction helped the company return to profitability.¹²

Bombardier, a Canadian aerospace and snowmobile company, offered a \$1,000 rebate to buyers of its Ski-Doo machines in sixteen U.S. cities if the local snowfall was less than half the average of that in the past three years. Bombardier itself assumed the risk that its customers traditionally carried when buying machines in a snow-free season. Bombardier in turn hedged its bet with snowfall options. The company paid Enron between \$45 and \$400 for each snowmobile sold, and Enron agreed to reimburse Bombardier the full \$1,000 for every rebate paid. Ski-Doo sales in the sixteen cities soared 38 percent over the year before.¹³

Implementing and Integrating Risk Management

TD Bank strives to be the best risk manager among major Canadian banks. Meeting this objective requires a well-established infrastructure to manage the risks to which TD is exposed. A fundamental principle is the involvement of qualified risk management professionals acting independently from the business units to establish a policy framework and define TD's risk limits.

Policies and structures for managing each of the major financial risks are approved by Group Risk Management and reviewed at least annually by the Bank's Risk Policy Committee, comprised of senior executives of TD. In addition, the Audit and Risk Management Committee of the Board of Directors approves all such policies. (See the TD Bank Annual Report, 1999.)

The managers of the various businesses compete for capital on the basis of risk and return. This means that managers have an incentive to effectively manage and balance risk and return in the three kinds of risks: credit risk, market risk, and operational risk. The models used to determine risk-adjusted capital are sophisticated and dynamic.

Even at the branch level, there is a clear division of responsibilities developing between the sales and client

service people and the risk management people. In a very real sense, the branch risk manager is making strategic decisions within the policies and parameters provided from Head Office risk managers.¹⁴

Measuring, Monitoring, and Reporting

Internal Reporting

Chase Manhattan Bank empowers its organization towards specifically defined goals. It is committed to and measures a set of clear organizational objectives. The mission statement identifies three key objectives:

- *Provider of choice* — We will become the obvious product leader in each of our core businesses, making Chase the logical and inevitable choice for our customers.
- *Employer of choice* — We will show our employees a set of challenges, opportunities, and ongoing working environment unparalleled in our field.
- *Investment of choice* — We will deliver high quality and consistently excellent returns for our shareholders in both the near and especially the long term.

¹² Economic Intelligence Unit with Arthur Andersen, *Managing Business Risks: An Integrated Approach*, 1995.

¹³ Stan Davis and Christopher Meyer, *Future Wealth*, 2000.

¹⁴ Canadian Institute of Chartered Accountants, *Learning about Risk: Choices, Connections and Competencies*, 1998.





8. Cases

Chase established a creed: a quality pledge to customers, employees, and shareholders. These shared values are constantly reinforced at all levels of the organization, which uses Business Process Reengineering (BPR) and benchmarking to improve business processes.

The bank has established a menu of measurements to evaluate ongoing effectiveness. The following are examples:

- Objective: Provider of choice
Measure: Quality of product
 - Functionality of product
 - Speed of execution
 - Cost of delivery
 - Customer satisfaction.
- Objective: Employer of choice
Measure: Turnover ratios
 - Salary and benefit levels
 - Opportunities for development
 - Employee satisfaction.
- Objective: Investment of choice
Measure: Share price
 - Return on assets
 - Return on equity
 - Earnings.

Chase translates these broad metrics into an ongoing reporting system and selectively tracks and reports the most critical ones.¹⁵

External Reporting Environmental Factors

Brascan and its affiliates provide a diversified range of products and services to their customers and clients. The group's business operations are the subject of changing regulations, standards, and market expectations regarding their impact on the environment, particularly in the natural resource and energy sectors. Brascan subscribes to the principle of sustainable development and encourages its operating affiliates to design and operate their facilities in a

way which minimizes risks to the environment, to conduct regular environmental audits, and to communicate regularly with their regulators and various stakeholders regarding their environmental practices and impacts.

The Brascan group's natural resource operations include environmental management systems and auditing programs designed to ensure that these operations conform to the applicable laws, corporate policies, and industry standards. Its energy operations are committed to a policy of environmental protection and have management systems in place to ensure compliance with the relevant government regulations. (See Brascan's 1999 Annual Report.)

¹⁵ Economic intelligence Unit with Arthur Andersen, *Managing Business Risks: An Integrated Approach*, 1995.





Appendix A — References and Suggested Reading

Articles

Bernstein, Peter L., "The New Religion of Risk Management," *Harvard Business Review*, March-April 1996, pages 47-51.

Lam, James C., and Brian M. Kwamoto, "Emergence of the Chief Risk Officer," *Risk Management*, September 1999, pages 30-35.

Larsen, Terrence, "Perspectives on Managing Risk and Growth," *The Journal of Lending & Credit Risk Management*, February 1998, pages 22-25.

Moche, James, "Key Attributes of Well-Controlled Organizations: Making Control a Competitive Advantage," *In Pursuit of the Upside: Leading Thinking on Issues of Risk*, 1998, pages 17-20.

Teach, Edward, "Microsoft's Universe of Risk," *CFO*, March 1997, pages 69-72.

Books

Bernstein, Peter L. *Against the Gods, the Remarkable Story of Risk*. New York: John Wiley & Sons Inc., 1996.

Davis, Stan, and Christopher Meyer. *Future Wealth*. Cambridge, MA: Harvard Business School Press, 2000.

Magazines

CAMagazine

CFO

Harvard Business Review

Internal Auditor

Journal of Accountancy

Journal of Lending and Credit Risk Management

Management Accounting

Practicing CPA

Risk Management

The CPA Journal





Appendix A – References and Suggested Reading

Other Publications

The Canadian Institute of Chartered Accountants, *Guidance for Directors – Dealing with Risk in the Boardroom*, April 2000.

—, *Guidance on Control*, 1995.

—, *Learning about Risk: Choices, Connections and Competencies*, 1998.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control – Integrated Framework*, 1992.

Conference Board of Canada, *A Conceptual Framework for Integrated Risk Management*, by Lucy Nottingham. Ottawa, ON: September 1997.

Deloitte & Touche LLP, *Perspectives on Risk*, 1997.

Economist Intelligence Unit with Arthur Andersen, *Managing Business Risks: An Integrated Approach*, 1995.

Institute of Chartered Accountants in England and Wales, *Financial Reporting of Risk: Proposals for a Statement of Business Risk*, Discussion paper 1997.

—, *No Surprises*, Report for Comment, 1999.

International Federation of Accountants, *Enhancing Shareholder Wealth by Better Managing Business Risk*, 1999.

International Standards Organization, ISO/TMB Working Group on Risk Management Terminology N23, *Risk Management Terminology*, Second Working Draft for Comment, 1999.

Joint Technical Committee OB/7 – Risk Management. Standards Australia and Standards New Zealand, *Australian/New Zealand Standard 4360:1999: Risk Management*, 1999.

Louis Harris and Associates, Inc., *The Coopers & Lybrand Survey of Internal Control in Corporate America: A Report on What Corporations Are and Are Not Doing to Manage Risks*, 1996.

PricewaterhouseCoopers LLP, *In Pursuit of the Upside: Leading Thinking on Issues of Risk*, 1998.



Boards and executives of organizations need and want to demonstrate that they are not negligent.

Negligence—Failure to use the degree of care expected from a reasonable and prudent person.

—*Dictionary of Insurance, Insurance Institute of Canada*

Appendix B — Control Frameworks

Risk management and control depend on the existence of effective control activities in a supportive control environment.

There is enormous pressure on governing boards and management to meet objectives. The objectives may be growth and profit, the delivery of social programs at lower costs, or something else. Customers, lenders, investors, and other stakeholders are more and more demanding. Meeting their expectations is challenging and hard to achieve unless organizations have effective control.

In the past ten years, the accounting professions in the United States, Canada, and other countries have undertaken initiatives to improve the quality of corporate governance and management. In so doing, they have radically changed the concept of control.

The North American initiatives were the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Criteria of Control (CoCo) project of The Canadian Institute of Chartered Accountants.

The COSO framework identifies five components:

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

The COSO definition of control is:

Control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

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

The CoCo Model of Control

A person performs a task guided by an understanding of its purpose (the objective to be achieved) and supported by capability (information, resources, supplies, and skills).

The person will need a sense of commitment to perform the task well over time.

The person will monitor his or her performance and the external environment to learn about how to do the task better and about changes to be made.

The same is true of any team or work group.

Exhibit 1
The COSO cube

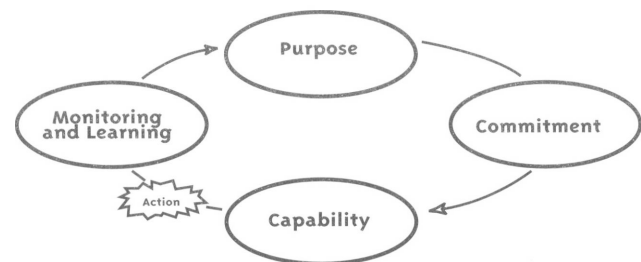


The CoCo definition of control is:

Control comprises those elements of an organization (including its resources, systems, processes, culture, structure, and tasks) that, taken together, support people in the achievement of the organization's objectives.

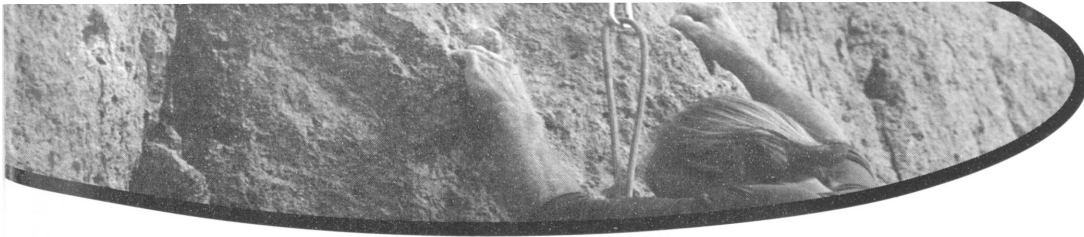
The twenty CoCo Criteria of Control provide a useful framework and context for considering risk assessment and management. The four groups of criteria fit a model, as shown in Exhibit 2, "The CoCo Model," that is comparable to management cycle models.

Exhibit 2
The CoCo Model



Although the CICA and COSO diverge somewhat in their approach and frameworks, both recognize risk assessment and risk management as key factors in control.





Appendix C – Self-Assessment

A powerful approach to risk management, one that is very effective when used in conjunction with other risk identification techniques, is the self-assessment based on a control framework such as Committee of Sponsoring Organizations of the Treadway Commission (COSO) or The Criteria of Control (CoCo) project of Canadian Institute of Chartered Accountants.

A self-assessment engages employees from across the organization in a structured review process. The assessment team works with employees at all levels to look at their organization in terms of a number of criteria or components. The team coordinates the results. It is a good way to measure the “fuzzy stuff” of corporate culture and to quantify the results.

There are a number of excellent tools for self-assessment, including software and hardware for computerized voting on questions put to employee groups. The software preserves individual confidentiality while accumulating and displaying the collective results. This is a good way to encourage people to speak freely.

Self-assessment may not identify all risks, but it is a very valuable technique for validating risk identification and for identifying gaps and weaknesses in control.





Appendix D – Glossary

The definitions in this glossary were selected or adapted from the sources indicated in the footnotes.

Consequence The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.*

Likelihood A qualitative description of a probability or frequency.*

Monitor To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.*

Opportunity The possibility that one or more individuals or organizations will experience beneficial consequences from an event or circumstance.†

Risk The chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood.*

Risk analysis A systematic use of available information to determine how often specified events may occur and the magnitude of the consequences.†

Risk management The culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects.*

Risk management process The systematic application of management policies, procedures, and practices to the tasks of establishing the context, identifying, analyzing, assessing (evaluating), managing (treating), monitoring, and communicating risk.*

Risk map A model or matrix that displays the relationship between the likelihood and consequences of specific risks.▼

Risk model A mathematical, graphical or verbal description of risk for a particular environment and set of activities within that environment; useful in risk assessment for consistency, training, and documentation of the assessment.†

Stakeholder Any individual, group, or organization able to affect, be affected by, or that believes it might be affected by, a decision or activity.†

Threat The possibility that one or more individuals or organizations will experience adverse consequences from an event or circumstance. (This is the definition of risk given in the CICA's publication entitled *Learning about Risk: Choices, Connections and Competencies*.)†

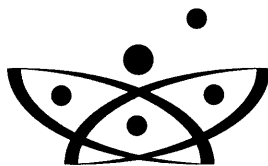
Uncertainty A condition where the outcome can only be estimated.†

* Joint Technical Committee OB/7, Risk Management. Standards Australia and Standards New Zealand, *Australian/New Zealand Standard 4360:1999: Risk Management*

† The Canadian Institute of Chartered Accountants, *Learning about Risk: Choices, Connections and Competencies*, 1998.

▼ International Federation of Accountants, *Enhancing Shareholder Wealth by Better Managing Business Risk*, 1999.





Managing Risk in the New Economy

American Institute of Certified Public Accountants (AICPA)

1211 Avenue of the Americas

New York, NY 10036-8775

Tel: (212) 596-6200 Fax: (212) 596-6213

The Canadian Institute of Chartered Accountants (CICA)

277 Wellington St. West. Toronto, ON. Canada

Tel: (416) 977-3222 Fax: (416) 204-3340