CA Chartered Accountants of Canada

20 Questions Directors of Not-For-Profit Organizations Should Ask about **Risk**

WRITTEN BY
Hugh Lindsay, FCA, CIP

20 QUESTIONS

How to use this publication

Each "20 Questions" publication is designed to be a concise, easy-to-read introduction to an issue of importance to directors. The question format reflects the oversight role of directors which includes asking a lot of questions. For each question there is a brief explanatory background and some recommended practices.

The questions are intended to be relevant to most not-for-profit organizations, particularly to those with staff resources who can manage the organization's risks with policy direction, approval and support from the board. The "answers" or comments that accompany the questions summarize current thinking on the issues and practices of not-for-profit governance. There are many views on the best way to govern and manage not-for-profit organizations and a number of governance models. This document describes general principles that apply in most situations. If your organization has a different approach, you are encouraged to test it by asking if it provides an appropriate answer to these questions.

After the comments there are lists of recommended practices that directors can use to assess their understanding of their organization and to prompt further questions if they are not fully satisfied with the answers. They represent aspirations, not absolute standards that must be met immediately.

Directors who come from a for-profit business may find that their experience, although helpful, will not always provide the best answers in the not-for-profit environment. Appendix 1 compares and contrasts for profit and not-for-profit governance.

Readers who want more details on specific topics may refer to the section on "Where to Find More Information." Most of the CICA 20 Questions series of publications for directors were written for business boards but are relevant to not-for-profit boards.

WRITTEN BY
Hugh Lindsay, FCA, CIP

PROJECT DIRECTION
Beth Deazeley, LL.B.
Principal, Risk Management and Governance
CICA

INSTITUTE
OF CORPORATE
DIRECTORS

The CICA has granted permission
to the ICD to use this materials
in its Director Education Program

Chartered Accountants
of Canada

20 Questions
Directors of
Not-For-Profit Organizations
Should Ask about
Risk

Library and Archives Canada
Cataloguing in Publication

Lindsay, Hugh, date.

20 questions directors of not-for-profit organizations should ask about risk / Hugh Lindsay.

ISBN 978-1-55385-391-6

1. Risk management. 2. Nonprofit organizations —Management. 3. Boards of directors. I. Canadian Institute of Chartered Accountants, II. Title. III. Title: Twenty questions directors of not-for-profit organizations should ask about risk.

HD61.L5628 2008 658.15'5 C2008-907807-1

Canadian Institute of Chartered Accountants
277 Wellington Street West
Toronto, ON M5V 3H2

Printed in Canada
Disponible en français

RISK MANAGEMENT AND GOVERNANCE BOARD

Brian Ferguson, CA, Chair
Dan Cornacchia, FCA
Andrew J. MacDougall, LL.B.
Michael B. Meagher, FCA
Anne Marie O'Donovan, CA
Sue Payne, FCA, C.Dir
Peter W. Roberts, FCA, CPA (Illinois), ICD.D

DIRECTORS ADVISORY GROUP

Giles Meikle, FCA, Chair
James Arnett, QC
John Caldwell, CA
William A. Dimma, F.ICD, ICD.D
John T. Ferguson, FCA
Gordon Hall, FSA, ICD.D
Carol Hansell, LL.B.
Mary Mogford, F.ICD, ICD.D
Patrick O'Callaghan
Ronald W. Osborne, FCA
Thomas Peddie, FCA
Guylaine Saucier, CM, FCA

NOT-FOR-PROFIT ORGANIZATIONS TASK FORCE

Dan Cornacchia, FCA, Chair
L. Robin Cardozo, FCA, ICD.D
Sue Matthews, CA, ICD.D
Lyn McDonell, CAE, C.Dir
Giles Meikle, FCA
Larry Murray, FCA
S. Harlan Schonfeld, CA, CIRP
Catherine Smith, ICD.D., F.I.C.B.

CICA STAFF

Dave Pollard, CA
Vice President, Knowledge Development
Gigi Dawe
Principal, Risk Management and Governance
Beth Deazeley, LL.B.
Principal, Risk Management and Governance

Preface

The Risk Management and Governance Board of the Canadian Institute of Chartered Accountants (RMGB) has developed this briefing to help members of not-for-profit boards of directors understand their responsibility for the oversight of risk.

Not-for-profit organizations are very diverse and range from small all-volunteer groups to large, sophisticated enterprises. This document is primarily intended for organizations with an executive director and staff resources who can manage the organization's risks with policy direction, approval and support from the board. It covers the same principles of risk management that are described in CICA's *20 Questions Directors Should Ask about Risk* but from the perspective of a not-for-profit organization. In particular, it assumes that members of not-for-profit boards may not be familiar with business practices and terminology and would appreciate explanations and examples that are more relevant to the not-for-profit sector.

A Board is most likely to be effective in managing risk when it has members chosen for the experience, skills and knowledge they bring to the organization—and practices good governance as described in CICA's *20 Questions Directors of Not-for-profit Organizations should ask about Governance*.

The Risk Management and Governance Board acknowledges and thanks the members of the Not-for-Profit Organizations Task Force for their invaluable advice, Patrick Doig of Marsh Canada Limited and Monica Merrifield of the YMCA of Greater Toronto for their helpful suggestions and reviews, Hugh Lindsay, FCA, who wrote this briefing under their guidance and the CICA staff who provided support to the project.

Brian Ferguson, CA
Chair, Risk Management and Governance Board

Introduction

Risk is a reality for every individual and organization. Anyone who serves on the board of a not-for-profit organization quickly learns that things don't always run smoothly. Board members work hard with staff and volunteers to have an organization that earns the support of members, donors, funding agencies, customers and other stakeholders because it has a good reputation for delivering relevant, valued programs and services. But this is not easy. There is always a degree of uncertainty about how things will turn out.

There are many things that can go wrong — from minor, day-to-day incidents to major crises — that may adversely affect the delivery of programs and services, damage the organization's reputation or, at worst, threaten its capacity to survive. These "risks" can generally be reduced or avoided by good risk management — the oversight of which is one of the key responsibilities of a board of directors.

As in other aspects of governance, the board is responsible for establishing policy, approving decisions that are beyond the authority of staff, and overseeing the management of risk. A board may delegate much of the work involved in managing risk, but can never delegate its responsibility for oversight.

The nature and extent of the board's role in risk management can vary with the size and sophistication of the organization and its staff. In larger organizations, the board can often rely on staff to manage day-to-day risks and provide much of the information and analysis the board needs when considering approval of policies, strategies and major decisions. In organizations whose staff have less knowledge, experience or skill to manage risks effectively, the board may find it necessary to be more "hands-on" — providing guidance and information to staff and requiring board approval of relatively small decisions. In situations where it is apparent that "letting management manage" isn't working, the board may need to become even more actively involved; taking charge, if necessary, to prevent problems from becoming crises.

The capacity of staff to manage risk will be an important consideration in how the board organizes itself to oversee risk issues. Risk isn't always an agenda item in itself. It's often a consideration in other board activities, including: strategic planning, policy and decision making, approval of projects and programs, reviewing operational and financial performance, and the work of the audit, investment, compensation and other committees.

Although risk is a reality of life, it's not something most people are comfortable discussing. This can be particularly true for not-for-profit organizations where trusting relationships are valued. Raising the issue of risk may be embarrassing because it implies a lack of trust and confidence, but it is essential if the organization is to survive and succeed.

This document explains what "risk" and "risk management" mean, describes how risks can be identified and managed, and provides guidance for boards on how to carry out their oversight responsibilities. There are three sections:

- Risk Context and Policy — describes how the board can prepare itself to oversee the management of risk, support a risk-aware culture, and establish risk-related policies.
- Managing Risk — describes what the board should expect to hear from staff about their techniques for identifying and assessing risks, and developing strategies and procedures for managing them.
- Monitoring and Learning — discusses the information the board should expect to get from staff on the measurement of risk and performance, and their learning from crises and other experiences. The section also discusses how the board can evaluate its own effectiveness in overseeing risk management.

Risk Context and Policy

Effective risk management—like other aspects of governance—begins at the top. It calls for a board of directors with the knowledge and ability to approve risk policies and to oversee their implementation.

Good governance practices by the board are essential to risk management because they establish the tone of the organization and provide the context in which the board exercises oversight of the organization's activities.

A board's policies and decisions on risk-related matters are more likely to be accepted as legitimate when it has earned the respect of members, staff and other stakeholders for its competence and integrity. This can be valuable when tough decisions and actions are necessary and emotions run high.

The questions in this section explore the board's role in three areas:

- Supporting a risk-aware climate or culture (Questions 1, 2 and 3)
- Developing and maintaining the board's capacity to oversee risk management (Questions 4, 5 and 6)
- Approving the risk tolerance policy (Question 7)

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.

Based on definitions developed by the Joint Technical Committee OB/7, Risk Management. Standards Australia and Standards New Zealand, *Australian/New Zealand Standard 4360:2004: Risk Management.*

1. What does "risk" mean in this organization?

Before the board can effectively oversee the management of risk, it needs to know what the term "risk" means for the organization. To some people, "risk" means "threat" — something that could harm the organization or prevent it from achieving its objectives. Others see risk as including "opportunity" — something that could help the organization to achieve new objectives or improve its ability to achieve existing ones. Both definitions are valid. In this document, "risk" generally refers to threats and potential barriers to opportunities. The management of opportunities is discussed in *20 Questions Directors of Not-for-profit Organizations Should Ask about Strategy and Planning.*

Risk takes many forms but, essentially, is anything that affects an organization's ability to meet its objectives and preserve its reputation. Organizations are more likely to consistently meet their objectives when they have effective processes for identifying and managing risks. They may do so by considering and addressing risk under a number of categories which include:

- Compliance risk — the risk of fines and other regulatory penalties for such offences as failure to remit payroll deductions, violation of privacy laws, etc. Also restrictions on the use of funds from donors and funding agencies.
- External risk — the risk of becoming irrelevant, losing the support of the public and funding sources, and failing to respond to economic, demographic and other trends.
- Financial risk — the risk of fraud, financial failure and decisions based on inadequate or inaccurate information.
- Governance risk — the risk of ineffective oversight and poor decision-making.
- Information technology risk — the risk that the information technologies used in the organization may not provide dependable service and accurate, secure information that is available when needed.
- Operational or Program risk — the risk of poor service delivery, day-to-day crises, and misuse or neglect of human capital and other resources.
- Reputation risk — the risk of losing goodwill, status in the community, and the ability to raise funds and appeal to prospective volunteers.
- Strategic risk — the risk of inappropriate or unrealistic programs and initiatives, and failure to keep the organization strong and relevant.

Because there are different ways of defining risk, it is of critical importance that the board, staff and (where appropriate) volunteers, all have a common understanding of what the term "risk" means in terms of their individual responsibilities.

Recommended practices

- The organization's policies and procedures for risk management include definitions and categorization of risks
- These definitions and categorization of risks are communicated, as appropriate, to staff, volunteers and other stakeholders
- The organization should have specific policies for accepting and managing key risks (i.e. Investment management, insurance coverage, etc.)

2. What are the organization's ethical values?

A reputation for integrity is essential to most not-for-profit organizations. Members, donors, funding agencies and others may be unwilling to support organizations they don't trust. The users of programs and services need to feel that they will be treated with respect and receive value from their participation. Similar considerations apply to other stakeholders. The loss of an ethical reputation can be devastating.

The integrity of an organization depends on the behaviour and actions of the people in it, who should all share the same understanding of ethics—the values and standards that determine how board members, staff, volunteers and other stakeholders behave and treat others. The standards, which are usually set out in a Code of Conduct (Code), establish the boundaries of acceptable behaviour and sanctions for lapses. Organizations that have a strong Code reduce the risk and associated costs of fraud, conflicts and other events that could harm the organization and its reputation.

FOR MORE INFORMATION, SEE THE CICA PUBLICATION *20 QUESTIONS DIRECTORS SHOULD ASK ABOUT CODES OF CONDUCT*

The Code should be approved and championed by the board, communicated to staff, volunteers, contractors, suppliers and business partners, and be enforced. If this is done well, the organization is likely to develop a reputation for honesty, integrity and principled behaviour.

Ethics in practice

Oxfam has a zero-tolerance policy on fraud and corruption. Our approach is to reduce their likelihood and impact by education and awareness-raising, risk management, internal controls, and having dedicated resources to help management prevent, reduce or recover any losses suffered as a result of fraud and corruption. This is true in all cases no matter how high the level of corruption is in the countries where we work. As a policy, Oxfam staff do not pay bribes in order to go about their business.

Source: Oxfam: Accountability Report 2006/07

There are several areas of risk that may be addressed in a Code of Conduct, including:

- Individuals, acting on behalf of the organization, committing illegal acts or failing to comply with laws and regulations
- Individuals, acting on behalf of the organization, behaving in ways that, while not illegal, are damaging to the organization's reputation: e.g. disrespectful treatment of others, providing misleading information, etc.
- Individuals behaving illegally for personal gain: e.g. committing fraud or theft
- Individuals inappropriately benefitting from their association with the organization: e.g. receiving gifts from suppliers, making personal use of computers and other resources, hiring close family members, etc.

An effective Code will include provisions for "whistle-blowing" by individuals who wish to communicate their concerns candidly and confidentially. The provisions should include describing how and to whom concerns may be reported and the rights of whistle-blowers to be protected from retaliation from those who might be adversely affected by their action.

Recommended practices

- The board approves the Code of Conduct
- The board supports the Code and leads by example
- Directors should sign the Code of Conduct annually evidencing they have read it and are complying with it
- The Code is communicated to staff, volunteers and key stakeholders
- The Code includes sanctions against those who deviate from it
- The Code is enforced
- The Code contains provisions for whistle-blowing

3. What are the major risks and uncertainties facing the organization?

The board's responsibility for the oversight of risk includes making sure that the organization has procedures for identifying, assessing and managing risks and uncertainties. This applies to all the risks that an organization faces. There are usually just too many risks for the board to follow individually, so, in most cases, the board will confine its oversight role to satisfying itself that risk management procedures exist and are followed. The processes for identifying and managing risks are discussed in questions 9 through 15.

Some risks, however, could severely affect the organization's ability to achieve its objectives and continue operations. It is important that the board and staff know and understand what these major or "key" risks are, and what is being done to manage them.

Major risks can be important considerations for the board when reviewing strategic and operational plans, capital projects and new programs. It is advisable to consider a range of scenarios — what might happen if, for example: key components of operating costs increase by 10%, 50% or 100%, an expected grant is reduced or cancelled, a fund-raising event only achieves 50% or 75% of its goal, or the computer system goes down at a critical time.

Recommended practices

- The organization has a structured process for identifying, monitoring and managing the organization's major risks and providing regular briefings to the board
- Planning includes considering a range of scenarios (including the worst-case) for major changes in costs and funding, catastrophic events and other major risks

Examples of major risks

- Loss of a major source of funding
- Reductions in the market value of investments and the income from them
- Unsuccessful fund-raising projects
- Fraud
- Failure of a project or strategic initiative
- Inadequate responses to emergencies
- Irrelevance because programs or services are no longer in demand or distinctive
- Excessive increases in the cost of human and other resources
- Actual or alleged sexual misconduct or abuse by an employee or volunteer
- Loss or theft of information
- Inability to perform critical functions that depend on technology

4. How does the board get the knowledge and experience it needs to oversee risk management?

A board of directors can be very effective in overseeing risk when its membership includes people who are familiar with the kinds of risk the organization is likely to face. A well-balanced board will typically include members who, collectively, have knowledge and experience of the field in which the organization specializes as well as such professional fields as law, accounting and other relevant disciplines.

FOR MORE INFORMATION, SEE THE CICA PUBLICATION *20 QUESTIONS DIRECTORS SHOULD ASK ABOUT BUILDING A BOARD*

The knowledge and experience of board members should be supplemented by regular training and updates on risk issues. This begins with an overview of risks in director orientation sessions and continues in board meetings, planning sessions and meetings of committees that have responsibility for the oversight of risk.

Recommended practices

The board's nominating practices recognize the need to include directors who are familiar with the fields in which the organization is active, and the risks it faces

The board takes steps to raise the awareness and understanding of risk among directors by:

- Including an overview of the organization's risk management processes and major risks in orientation sessions for new directors
- Holding periodic educational sessions on risk issues and processes

The board uses internal and external experts to advise the board and committees on specific risk issues

5. How does risk get on the board's agenda?

Board agendas are often very full. Important issues such as risk can be easily overlooked—especially when there are seemingly more "urgent" issues to consider. Although the Executive Director may have considerable influence in setting the agenda, it is the Chair and the board that should ultimately decide what to include. The Chair of the board plays a valuable role in raising risk issues by including them in board agendas and supporting debate at board meetings.

There are a number of occasions that are appropriate for discussing risk at board sessions, including:

- Strategic planning sessions
- Reports at board meetings from staff on performance and risk issues
- Motions at board meetings to approve major programs or projects
- Periodic sessions specifically to discuss the major risks
- In-camera board sessions

Recommended practices

The board:

- Participates in the strategic planning process
- Schedules specific times for receiving and discussing reports on risk from staff
- Encourages members to ask questions and provide advice and direction at appropriate times during board meetings
- Includes in-camera sessions in all board meetings

6. How does the board organize itself to oversee risk management?

Although the entire board is responsible for the oversight of risk, some areas of risk management can be complex and time consuming to review. Boards may find it more effective to delegate the detailed work of overseeing certain aspects of risk to one or more committees. In such cases, the board must make sure that it is informed of the findings of the committees and that no significant aspect of risk is overlooked.

As a general rule, board committees should be responsible for overseeing the risk management processes in the area for which the committee is responsible: e.g. investments, finance, construction projects, member discipline (in professional organizations), etc. Recognizing that this can leave gaps, organizations may delegate responsibility for overseeing the co-ordination of risk management to a specific committee—typically the Audit Committee (sometimes known as the Audit and Risk Committee).

Recommended practices

- The board and its committees have written policies and procedures that define their responsibilities for overseeing risk management
- Where the board elects to delegate specific risk-related responsibilities to board committees, the committees are required to report their activities to the full board at least annually

The Audit Committee and Risk

Oxfam's Audit Committee meets regularly with the external auditors, both with and without the presence of management. The group agrees the external audit plan, reviews the external auditor's management letter, and monitors implementation of actions required as a result. The Committee also has the responsibility of ensuring that the audit, risk management, and control processes within Oxfam are effective... The Committee undertakes a detailed review of the draft Annual Plan, the Risk Register and the Annual Report and Accounts prior to their submission to Council.

Oxfam Annual Report & Accounts 2006/07

7. How does the board decide how much risk the organization can take on?

Organizations are more likely to succeed and survive when they understand their risk tolerance — the amount of risk they are willing to assume. Boards of directors can provide direction by approving risk tolerance levels that "optimize" risk by balancing risk and opportunity. Risk tolerance has, essentially, two components: appetite for risk and capacity for risk.

Appetite for risk reflects the willingness of an organization's members to take risks. Some organizations take the position of "nothing ventured, nothing gained". They see taking risks as the best way to succeed. Others are "risk averse", fearing that risky strategies could destroy an organization that knows its limitations and does a good job of meeting its modest objectives.

Most successful organizations find a balance. They recognize that risks that appear to be barriers to innovative and potentially valuable strategies may be manageable by sound planning and control activities. For example: organizations that promote and support high-risk sports (e.g. skydiving, rock climbing, etc) are at risk of litigation over deaths and injuries from accidents. They can reduce their risk by having training programs and standards that make the sport safe and enjoyable for informed participants and spectators.

An organization's capacity for risk is based on the strength of its finances, donor support, reputation and credibility, and the experience and competence of volunteers and staff. A well-financed organization with experienced, competent and well-equipped staff and volunteers is in a good position to succeed in new initiatives and to survive setbacks.

Tolerance for risk

Endowment funds balance safety and possible low investment returns against the potential for higher income but higher risk.

Not-for-profit organizations that operate in war-torn regions recognize that they put their staff and volunteers at higher risk than would be acceptable in their home countries and take steps to minimize the risks.

The board ideally should approve a formal "risk tolerance" policy and guidelines that establish the level of risks the organization is prepared to accept as it pursues its objectives. It can be valuable to record the discussion and decisions for future reference.

Points to consider in risk-tolerance discussions and policies include:

- The amount of money that the organization is prepared to lose if a revenue-generating or fund-raising project is less successful than anticipated
- The potential risk to the organization's reputation and credibility if a strategy or project is poorly received or otherwise unsuccessful
- The limits of the authority of the Executive Director or CEO — beyond which board approval is needed
- The information the board should receive before making its decision to approve strategies, policies and projects

Recommended practices

The board approves a risk tolerance policy that:

- provides guidance to staff and volunteers as to how much risk they may take
- is consistent with the organization's values and capacity for taking risk
- is reviewed at least annually

When the board is called upon to approve a specific proposal or action the board receives a balanced picture with information about:

- The potential risks and how they will be managed, as well as the potential opportunities
- The alternatives that were rejected as well as the proposal being advanced
- The worst case scenario
- Staff's concerns and uncertainties as well as its optimistic expectations

Managing Risk

Managing risk involves everyone in an organization — the board, staff and volunteers. But, in most cases, risk is only one aspect of an individual's responsibilities. Without clear policies and procedures, risk management can be everyone's job and no one's job. It is important to establish who is responsible for managing certain types of risks and what they should do.

Risk management involves asking:

- What could happen that would affect our ability to meet our objectives?
- How likely is it to occur?
- How serious might it be?
- What should we do to reduce the risk?
- How can we be prepared to respond to problems?

Boards of directors need to know, in general terms, how the organization identifies, assesses and manages risks.

The questions in this section are those that members of a board could ask about processes the organization has for managing risk in the following areas:

- Assigning responsibility for risk management (Question 8)
- Identifying, assessing and managing risk (Questions 9 – 13)
- Communicating and coordinating risk management (Question 14)
- Crisis management (Question 15)

8. Who is responsible for managing risks?

Although the board has overall responsibility for risk management, it generally delegates to the Executive Director and staff most of the detailed aspects of identifying, assessing, and managing the risks that the organization faces — subject to board policy and approval.

A major policy decision for a board is the amount of authority it gives to the Executive Director — who manages risk on a day-to-day basis. To avoid misunderstanding it is important to have a written job description that establishes the powers and limitations of the Executive Director in the context of the risk tolerance policy.

The amount of authority the board wishes to delegate to staff is a key consideration in hiring and assessing the Executive Director. The board's Compensation Committee can help by including risk management skills, experience and performance in their hiring and assessment processes.

Recommended practices

The board approves:

- A written job description for the Executive Director
- Written policies specifying the Executive Director's authority and requirements for board approvals (Executive Director limitations)

9. How does the organization identify the risks that it faces?

Identifying the risks that an organization faces, and assessing how serious they might be, is a challenging task. Planning for the risks you know about is relatively straightforward. It can be very difficult to anticipate the unexpected. The problem is made harder by our reluctance to think the unthinkable.

Experienced risk managers know that no single approach to identifying risk is good enough in itself so they use a number of approaches in combination. Commonly-used approaches may include a combination of:

- Internal processes — interviews, questionnaires, brainstorming, etc.
- Self-assessment and other facilitated workshops
- Strengths, weaknesses, opportunities, and threats (SWOT) analysis
- External sources — comparison with other organizations, discussion with peers, benchmarking, risk consultants, etc.
- Tools, diagnostics, and processes — checklists, flowcharts, scenario analysis, etc.
- Audits (e.g. a safety or environmental audit)

These approaches can be used to identify risks from a variety of perspectives or categories, including:

- Sources of risk — governance, strategic, operational/program, financial, external, informational, compliance and information technology (see Question 1)
- Objectives — the risks that could keep the organization from achieving each of its objectives: e.g. events, programs, building projects, etc.
- Areas affected — reputation, assets, revenues, costs, performance, staff, volunteers, customers and other stakeholders
- Specific hazards or perils — fire, theft, earthquake, liability, etc. The hazard-based approach is usually based on the policy coverages available from insurers
- Capacity gaps — inexperienced or inadequate human resources (human capital), or inadequate systems and processes to track performance
- Risk drivers — pressure points that if left unchecked contribute to increased risk exposure, for example, *growth* or speed of operational expansion, *culture* or degree of information-sharing, and *information management* or flow of information within an organization[1]
- The degree of control that the organization has over the risk, e.g.:
  - — Natural disasters and political, economic, social, and financial risks over which an organization has very little control
  - — Factors such as public expectations, reputation, competition, and changes to legislation and regulations, over which the organization may have some influence but very little control
  - — The choice of programs, events and major projects over which an organization can have a great deal of control

Recommended practices

The organization has a methodical process for identifying risks that involves an appropriate variety of approaches, techniques and participants

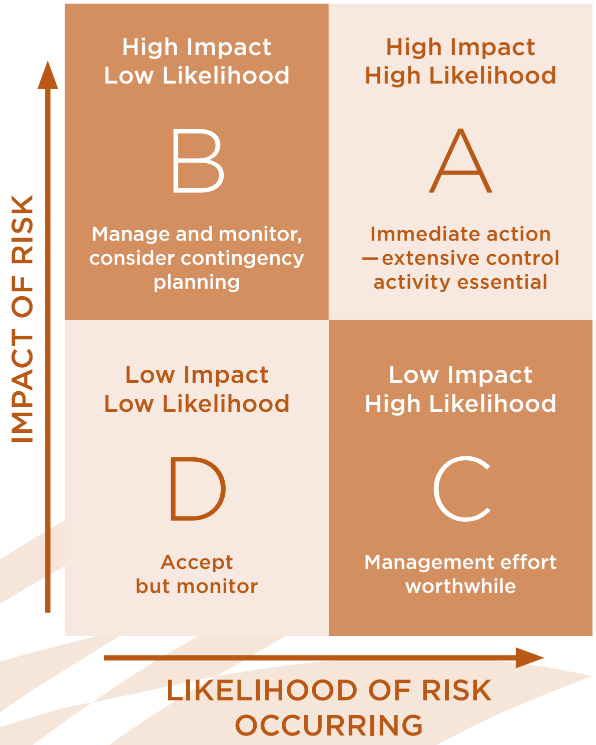
[1] Robert Simmons, "*How Risky is Your Company*", Harvard Business Review, May-June, 1999

10. How does the organization assess the risks that it faces?

Before an organization decides how it will manage each of the risks it has identified, it needs to assess them to determine how they might affect the organization and its objectives.

This usually involves considering how frequently the risk is likely to occur and how severe its consequences might be. A commonly-used technique for doing this is known as “risk mapping” which uses a matrix that can be used to assess specific risks by displaying the relationship between their potential frequency/likelihood and severity/impact.

Risk mapping[2]



High Impact Low Likelihood B Manage and monitor, consider contingency planning	High Impact High Likelihood A Immediate action —extensive control activity essential
Low Impact Low Likelihood D Accept but monitor	Low Impact High Likelihood C Management effort worthwhile

The results of the assessment can be used to decide how to manage the risks.

[2] The risk map model is reproduced with the kind permission of the YMCA of Greater Toronto.

Recommended practices

The organization has processes and criteria for assessing risks

Risk scoring

The risk map may be used in combination with a scoring system that assigns a value to the potential frequency and severity of each risk. (e.g. 1 = least frequent or severe 5 = most frequent or severe.) Multiplying the scores gives a risk score that can be used to rank risks and identify those that are considered “major” and to be reported to the board (Question 3).

11. What strategies does the organization use to manage risk?

Once risks have been identified and assessed, it is time to decide how to manage them. For example: small risks that occur frequently can often be managed by good procedures and training. Big, but infrequent, risks may also require insurance (see Question 13) and/or contingency planning (Question 15).

There are, essentially, four ways to manage risk:

Avoiding risk — Just don't do something that seems too risky. This can be a legitimate strategy but it can stop good things from happening if people are too cautious and "risk averse". Avoiding risk may seem like a conservative or safe approach but can result in missed opportunities and poor results for the organization. Before abandoning a promising idea, it makes sense to weigh the potential risks and benefits and explore control activities and other ways to manage the risks.

Transferring risk — Share the risk with someone else. Buying an insurance policy is one way to do this, especially for perils like fire, theft and liability. Another way to transfer risk is to establish contractual relationships with other organizations that have the expertise and resources to handle specialized issues and risks.

Mitigating risk — Develop procedures with checks and balances (control activities and procedures) to detect and reduce the likelihood and/or severity of risks. High-risk fields like medicine have sophisticated processes to protect patients and staff. Accountants use internal controls to protect assets and keep accurate financial records. Arts groups balance artistic merit with potential box office success in creating programs that will attract and retain audiences.

Accepting risk — Provided that the risk is unlikely or would not cause serious harm to the organization, it may make more sense to accept and monitor it. An annual outdoor event might be less successful if it rains or snows. However, the organizers believe that many participants will feel it is so important to them that they prefer to show up and get wet rather than have it cancelled.

Take care when you share risk

Sharing risks can be risky if your partner lets you down, damages the organization's reputation or exposes it to litigation. Great care is needed in selecting insurers, outside service providers and other partners.

The organization and its partners should put their expectations and responsibilities in writing to avoid costly misunderstandings.

Residual Risk

Risk management may include more than one approach. For example: the organization may establish procedures and controls to mitigate some risks – then buy insurance to cover the "residual" risk of things that procedures can't cover.

In selecting risk management strategies, cost is an important consideration. The cost of managing a risk should generally be compatible with its potential consequences. For example: it may make more sense to trust volunteers who collect small amounts of money than to spend staff time on trying to control the funds; renting a tent for an outdoor event, or letting people get rained on may make more financial sense than buying insurance against rain.

Recommended practices

The organization's strategies for managing risk are:

- Compatible with its values, objectives and risk tolerance
- Realistic in balancing cost and protection
- Supported by strong internal processes and reliable partners

12. What records does the organization keep on its risks?

Identifying and assessing risks and developing strategies and procedures for managing them can be time consuming—particularly when doing it for the first time. Having a good system can save the information in a way that can be quickly and easily updated and provides a strong basis for managing risks.

One way of doing this is to use a "risk register" that contains details of risks, who is responsible for managing them and how they are to be managed and reported. A register can be a simple worksheet or spreadsheet, or a sophisticated computer software product that records, analyzes and provides reports on risk information. For an example of a risk register, see Appendix 2.

It can be valuable to have a record of the decisions that were made in developing items for the risk register and the information on which they were based. This can be done by keeping minutes of the decisions or by adding notes to the risk register.

Recommended practices

- A senior employee is responsible for the maintenance of the risk register
- The risk register is updated and reviewed at least annually

13. What is the organization’s financial capacity to take on risk?

An organization’s capacity to take opportunities, respond to urgent needs and prevent disasters all require it to have the capacity to “finance” risk. Not-for-profit organizations frequently have limited financial resources for funding new projects and recovering from unexpected setbacks. There are essentially two ways in which they can strengthen their financial position: maintaining financial reserves, and buying insurance.

Financial reserves—money set aside for specific or general purposes (restricted or unrestricted net assets)—can provide the funding for new projects, programs and other initiatives before they are funded by grants, donations or earned revenues (fees, ticket sales, etc). They can also provide a cushion in cases where, for example, a fund-raising project fails to meet its targets, an anticipated grant is reduced or eliminated, or costs run higher than expected.

Financial Reserves Policy

The Society effectively budgets its operations on a break-even basis and uses unrestricted excess revenue over expenses to maintain adequate financial reserves and develop its humanitarian programs.

The Society has set aside $43.5 million in permanent reserves to ensure the capability of operations should there be unexpected events.

Canadian Red Cross: Annual Report, 2007/08

There are, however, many risks that cannot be completely mitigated by security, procedures and other control measures—and that could result in losses that an organization could not absorb from its operating budget or financial reserves. Insurance can provide protection at reasonable cost for some of these risks. It is generally preferable to have all insurance coordinated by one staff person, working with an experienced insurance broker who is familiar with the risk management needs of not-for-profit organizations and the fields in which the organization is active.

In reviewing insurance coverage, directors should pay particular attention to:

- Adequacy of coverage and policy limits—the amount and extent of coverage should be tailored to the risks the organization faces and the amount it can afford to pay
- Exclusions—policies may exclude, or limit, coverage of important perils such as liability for sexual abuse or harassment
- Deductibles—increasing the amount the organization must pay towards each claim can reduce the insurance premium but could be costly if there are numerous claims
- Protection of directors—some policies cover the organization, its employees and Directors for errors and omissions. This form of coverage may be beneficial for the organization but may not provide adequate protection to directors

FOR MORE INFORMATION, SEE THE CICA PUBLICATION *20 QUESTIONS DIRECTORS SHOULD ASK ABOUT DIRECTORS’ AND OFFICERS’ INDEMNIFICATION AND INSURANCE.*

Be prepared for claims

Records and broker contact information should be accessible in case a claim occurs when the staff person coordinating and responsible is on vacation or out of the office.

Appendix 3 describes the kinds of insurance policies that are available for not-for-profit organizations.

Recommended practices

- The organization has policies for setting and spending financial reserves, and maintaining them at an appropriate level
- The organization’s insurance programs are an integral part of the risk management program
- The organization makes use of knowledgeable and experienced professionals when buying insurance
- The board reviews the scope of the insurance program and adequacy of coverage limits for the organization and for directors, officers, staff and volunteers
- The board approves an investment policy when there are material funds on hand (e.g. during a building campaign) stipulating the quality of investments and the risk profile that is desired

14. How are the board's expectations for risk management coordinated across the organization and communicated to staff and volunteers?

Every department and committee in an organization has — or should have — some degree of "risk ownership". In most cases, staff and volunteers are responsible for the risks directly related to their day-to-day activities. There may also be specialists who handle specific aspects of risk such as insurance, credit and environment. All the risk management activities should be coordinated so that no major risk is overlooked. In larger organizations, this can be accomplished by designating a risk manager or other senior staff person to be responsible for coordinating risk management across the organization. In smaller organizations, the Executive Director may need to assume responsibility for risk management. The individual responsible for risk management maintains the risk management process and advises and collaborates with senior staff members on risk issues.

Risk Awareness

- If I don't follow procedures, someone might get hurt
- If I'm rude to a customer, I could damage the organization's reputation
- If I cannot resolve a customer complaint myself, I should promptly refer it to someone who can
- If I see something that looks wrong, I should talk about it to my supervisor

When people know what they are expected to do and understand how to recognize and respond to risks, problems are less likely to occur — and easier to resolve. People also need to know and understand the risks that affect other departments and the organization as a whole, and the consequences of their own actions for others. This requires management to provide training and guidance to staff and volunteers as well as written policies, procedures and job descriptions. The goal should be to create a "risk-aware culture" in which people are encouraged to take appropriate action to manage risks or report them to others.

Organizations that have structured volunteer programs that are led or coordinated by experienced staff or volunteers can include risk awareness in their training programs and procedures. Those with less formal ways of involving volunteers need to carefully assess the risks and decide how to address them. This may require considerable tact and diplomacy, particularly when approaching long-time volunteers who are not used to being told what to do.

Recommended practices

The organization has:

- A risk manager or other senior staff person who is responsible for coordinating risk management across the organization
- A program of communication and training on risk that includes creating awareness of risk, promoting a risk-aware culture, and providing guidelines on policies and procedures for managing specific risks to staff and volunteers

15. What plans does the organization have for responding to crises?

Even the best-run organizations will experience crises from time to time. Most of these can be described as "operational incidents"—the day-to-day, minor crises of running the organization and serving individual customers. With good management, these can be avoided or promptly resolved by staff and volunteers. Directors are not normally involved in operational incidents unless they are symptoms of problems in executive performance or strategic planning.

A more serious situation is the "potential crisis"—a problem that grows larger over time and becomes critical if it is not addressed. Boards should pay close attention to potential crises and insist on plans and action to resolve them. This is not always easy. It is tempting to deny the threat and to procrastinate.

A third category is the "sudden crisis"—an event that occurs unexpectedly and has a major effect on the organization. Sudden crises include natural disasters, sabotage and outages of vital services such as power, water or computers. They may also result when operational incidents are mismanaged or when a neglected potential crisis becomes a real crisis.

Do we have a crisis?

Recognizing that there is a crisis or an impending/evolving crisis is often the most difficult aspect of crisis management. One approach is to apply a "litmus test." The following questions are from *Crisis Management: Planning for the Inevitable* by Steven Fink.

1. Is there a good chance that this situation will, if left unattended, escalate in intensity?
2. Might the situation foster unwanted attention by outsiders, such as the news media or some regulatory agency?
3. Is it likely that the situation might interfere with normal business operations in some manner?
4. Could it make you look bad or cause people (the public at large, or investors) to lose confidence?
5. How is it going to affect your bottom line?

This test can apply to any kind of crisis.

Sudden crises call for prompt, decisive action, effective communication and teamwork between the Executive Director and board. They also call for leadership, discipline, calmness, and sound judgment. The board should ensure that the organization has a commonly understood approach to crisis management and plans for business continuity. Board members need to know what to look for and make sure it happens. Anything less can make the crisis worse.

FOR MORE INFORMATION, SEE THE CICA PUBLICATION *20 QUESTIONS DIRECTORS SHOULD ASK ABOUT CRISIS MANAGEMENT*

Being prepared for a sudden crisis involves more than the capacity to manage the crisis itself, it means having the resources and resilience to continue operations. Organizations that have survived crises were best able to recover if they:

- Had a well-tested Business Continuity Plan
- Had a leader who could rise to the occasion and take prompt, decisive action to deal with the immediate crisis
- Communicated promptly and frankly with staff, customers, suppliers, other important stakeholders and the news media
- Demonstrated practical compassion for the injured, frightened and bereaved
- Were prepared for the mundane and predictable problems of business continuity: alternative computer and communication systems, off-site back up of vital records, contact information and more
- Had the financial and other resources to absorb the effects of the crisis and return to normal—strong balance sheets, positive cash flow and good cost control

Appendix 4 has more information on crisis and business continuity planning.

Recommended practices

- The organization has a board-approved Business Continuity Plan which is regularly tested
- The board's agenda planning includes regularly scheduled briefings to the board or designated committees on the organization's preparedness for foreseeable emergencies, such as the sudden death or incapacity of the Executive Director, major fire, facility failure, natural disasters, disease outbreaks (e.g. SARS) and terrorism
- The organization has a board-approved crisis management plan including escalation and communication protocols

Crisis response

Effective crisis response happens when:

- There's a written plan that describes what to do in a crisis
- Employees are trained in the use of the plan
- The plan is always available and accessible in print and electronic format
- The plan is regularly tested under realistic conditions
- Employees are empowered to act on their own initiative in times of crisis

Monitoring and Learning

Ignorance may be bliss, but not when it comes to risk management. The sooner you know about a problem, the better are your chances of resolving it before it gets out of hand. That's why effective organizations have systems for collecting, analyzing and reporting information they can use to take corrective action. They also take the time to learn from their experiences and grow stronger.

The diversity and uncertainty of risk make it impossible to have only one definitive risk measurement that can be monitored. Monitoring and learning from risk involves questions such as:

- 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?
- How well are we doing in managing risk?
- Are "near misses" recorded, tracked and used for learning?

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

This section describes techniques for developing and using information to manage risk and to learn from risk-related events.

Performance Monitoring

The CICA's success in achieving its vision, strategy, and priority commitments is assessed on the basis of several primary indicators and is reported on annually to the CICA board of Directors.

Deliverables — monitoring to confirm that they are completed on time, within budget and at the highest quality

Stakeholder satisfaction — formal and informal surveys of members, volunteers, partners and external stakeholders

Work environment — employee surveys, analysis of staff turnover statistics and investment in training

Canadian Institute of Chartered Accountants
Annual Report 2007/08

16. How does the organization's performance compare with its plan and budgets?

When things start going wrong, there are often warning signs — costs get out of control, expected income doesn't come in, plans and projects slip behind schedule, etc. Many of these signals can be picked up by monitoring the organization's key performance indicators or drivers against plans and budgets.

As part of its reporting to the board, staff should provide regular information on the status of plans and budgets. Staff should monitor the differences (variances) in financial and non-financial (e.g. people served, satisfaction ratings, etc.) indicators between actual results and board-approved plans and budgets. When the variances are significant, staff should bring them to the attention of the board and describe what they will do to get things back on track. This may require further board approval if plans and budgets need major revision.

Recommended practices

The board receives regular reports on:

- Performance against board-approved strategies and plans
- Variances from plan and budget
- Results of periodic testing of crisis plans

17. What is the status of the risks facing the organization?

When boards approve strategic and operating plans, they do so on the basis of assumptions about factors, both within the organization and in the external world, that can change at any time and significantly affect the risks facing the organization and its plans.

Comparing performance against plans to detect problems and manage risks is a useful technique, but one that reacts to problems that have already happened. It is important, in addition, to review the planning assumptions and the status of major risks to identify trends and warning signals before they cause problems. The board should expect staff to report:

- What is happening
- How it might affect the organization
- How staff plan to respond

Some factors are relatively easy to monitor —currency exchange rates, commodity prices, interest rates, etc. Others, such as political, regulatory and social trends are harder to quantify and assess. In either case, it may be difficult to predict the consequences. Even if the information is incomplete or partial, it can stimulate valuable discussion and reduce the risk of complacency and inaction.

Recommended practices

Staff report to the board regularly on:

- The status of major risks including current exposure and effectiveness of risk management techniques
- How the strategic environment is changing, what new risks and opportunities are appearing, how they are being managed and what, if any, modifications in strategic direction should be adopted
- Progress on closing major gaps in risk management capabilities
- Reviews of compliance with risk tolerance policy limits
- Breaches of the Code of Conduct
- Litigation against the organization
- Formal and potential complaints against the organization, e.g. harassment allegations, human rights complaints, labour board investigations
- New and potential crises
- The status of any crises that are currently being managed

18. How can the board be sure that the information it gets on risk from management is accurate and reliable?

Boards generally have a close relationship with the Executive Director who attends board and some committee meetings to provide most of the information and answer most of the questions. The result can be that the board receives information that supports the Executive Director's viewpoint and, at worst, could be slanted or misleading. To get a broader perspective on the organization and its risks, the board should arrange to meet and hear from a number of sources in addition to the Executive Director.

This can be a sensitive area. Boards should be alert to the risks when the Executive Director is the only source of information to the board and be concerned when an Executive Director unreasonably restricts board access to senior staff. Effective Executive Directors usually look for opportunities to develop senior staff by encouraging them to make presentations and answer questions at board meetings, and to talk freely to board members at other times.

Does this make sense?

Experienced board members listen carefully to reports from staff. They are not afraid to ask questions if they don't understand what they are hearing or if it doesn't make sense to them. They persist until they are satisfied. They may ask that the board discuss their concerns without staff present, or take up the matter with the Chair after the meeting.

Regardless of the source, board members should demonstrate healthy skepticism and ask themselves if the information they get is consistent and rings true. In larger organizations, the board may periodically request a formal review and report on the effectiveness of the risk management process from an objective and independent source outside of senior management (e.g. internal audit, external auditor, consultant, etc.).

The board should also be informed of concerns reported by whistle-blowers and the action taken or proposed by staff (see Question 2).

Recommended practices

- The board gets information from a cross-section of knowledgeable and reliable sources in addition to the Executive Director, such as senior staff, auditors and external advisors
- The board receives reports on concerns expressed by whistle-blowers

19. What has the organization learned from its experiences with risk?

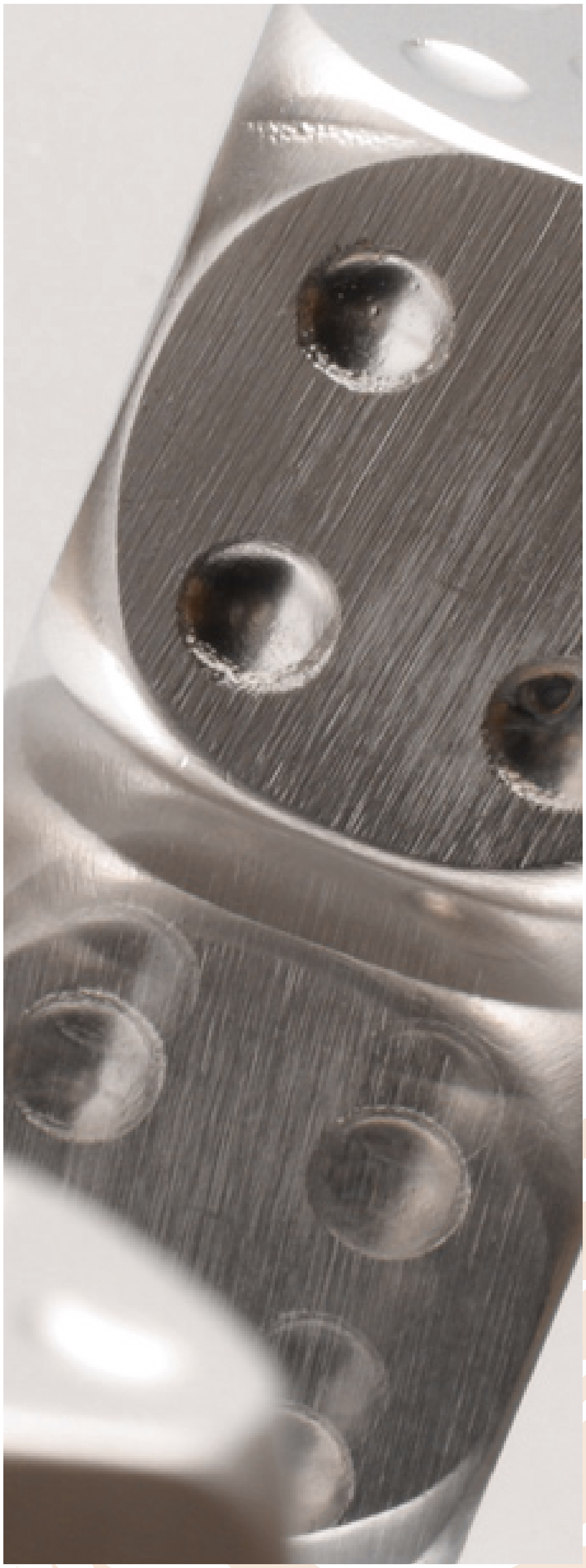
Organizations that review and analyze their response to crises, problems and successes can profit from their experience if they take advantage of the opportunities for improvement. This is a particularly important factor in building and maintaining an organization's reputation. Making mistakes can be understandable and forgivable. Failing to learn from them is not.

When things go wrong it's usually a combination of factors — human error, poor communication, inadequate inspection and maintenance, and more. An after-the-fact review can help diagnose underlying causes and suggest solutions that could reduce the risk of similar problems in the future. This usually works best when the focus of the review is on problem-solving rather than fault-finding.

Recommended practices

The organization:

- Promptly reviews the most significant lessons learned from each major event, surprise and disaster and how it has responded to these findings
- Takes action to improve the handling of similar events in the future
- Has effective knowledge transfer processes so that significant findings and lessons learned (both positive and negative) can be transferred quickly and effectively across the organization



20. What does the board do to assess its effectiveness in overseeing risk?

The board's responsibility for overseeing risk includes assessing how well the board and its committees perform. This can be done as part of a regular (preferably annual) governance assessment and after a serious crisis or event in which the board was, or should have been, involved.

The annual assessment would be based on the points raised in this document and consider, in particular:

- Does the board champion and support risk management?
- Does the board support the Code of Conduct and lead by example?
- Does the board have members with the knowledge and experience to manage risk?
- Do the board members receive orientation and updates on risk issues?
- Does the board agenda provide for regular reporting and discussion of risk issues?
- Are the board and its committees effectively organized to oversee risk management?
- Does the board make use of opportunities to integrate risk management with other board processes, such as strategic planning, business planning, annual budget reviews, new program approval, etc?

A post-crisis review might include considering:

- Did the board stay calm, get accurate information and assess the situation?
- Was the board's involvement timely and appropriate?
- Did the board recognize and reconcile dissenting views expressed by directors?
- Did the board stay on top of the situation?
- Was the board helpful to the Executive Director?
- Did staff conduct a thorough post-crisis review and report on it to the board?
- Did the crisis reveal any weaknesses in strategic planning, risk identification and risk management processes?
- How might the directors apply what they learned to improve the way the board functions and relates to the Executive Director?
- How can the board turn this crisis into an opportunity?

Recommended practices

- The board has a program for assessing how effective it has been in meeting its responsibilities for the oversight of risk
- The board conducts post-crisis reviews of the effectiveness of its response

Conclusion

Managing risk is an integral part of good governance. It is a consideration in everything a board, staff and volunteers do and the reason for establishing a risk-aware culture in an organization.

Risk management does not necessarily imply risk aversion. Rather, organizations should balance opportunities and threats to achieve objectives in a way that is compatible with their values and tolerance for risk. Successful risk management can seem boring — it's largely a matter of following good practices and procedures, and constant attention to detail. Failures in risk management can be more interesting, but also painful and expensive.

An effective board has members who knowledgeably promote the benefits of opportunities, members who wisely warn of threats, strong policies and procedures, and a chair who can guide the board in making sound decisions and overseeing management in the successful execution of strategies.

Appendix 1

A COMPARISON OF CORPORATE AND NOT-FOR-PROFIT GOVERNANCE.[3]

Corporate directors and others with business experience who become members of not-for-profit boards often experience culture shock in their new roles. Some of this is due to basic differences between the corporate and not-for-profit sectors — particularly the profit motive — but there are other significant factors including the size, sophistication and maturity of the organization and the field in which it operates. It would be nice to have a simple comparative chart that compares and contrasts governance in the two sectors. Unfortunately things are not that straightforward. The following observations on governance and operations may help newcomers from the corporate world to adapt to their roles as members of not-for-profit boards.

GOVERNANCE

Fundamentally governance is governance — there is no substantive difference in good governance between the corporate and not-for-profit sectors. This document is modeled after one written for corporate directors[4] and the scope is essentially identical. Many not-for-profit organizations have governance practices that equal the best in the corporate sector.

There is more variation in governance within a sector (business or not-for-profit) than there is between sectors. A director of a large public company would probably feel more at home on the board of a large not-for-profit than on the board of a small, start up business.

The directors of not-for-profit organizations, unlike their corporate counterparts, are not paid for their services and may be expected to cover out-of-pocket expenses and make donations. Experience shows that volunteer board members are no less seriously committed to the vision, mission and goals of their organizations than corporate directors. They work hard, believe in what they are doing and make a large contribution to its success — just like their business counterparts.

The underlying principles for nominating directors are essentially the same for both corporations and not-for-profits. In both cases the nomination process involves identifying the organization's needs — especially the strategic ones — and matching them to the skills and experience of prospective candidates. In practice, not-for-profits tend to be more open to diversity and to accept promising nominees with limited or no board experience.

Corporate boards have been shrinking in size and frequently have fewer than ten members. Boards of not-for-profits are often larger to accommodate representation from a range of stakeholders — but the value of this is being questioned.

[3] This material is based on CICA's *20 Questions Directors of Not-for-profit Organizations Should Ask about Governance.*

[4] CICA's *20 Questions Directors Should Ask about Risk*

OPERATIONS

Corporate directors are seldom expected to participate in operating activities — the “two hats” challenge for not-for-profit directors. They may, however, be expected to provide active assistance in their fields of expertise — particularly in raising capital — which could affect their governance objectivity.

Not-for-profit organizations, unlike for-profit businesses, frequently benefit from the contribution of time, ideas and expertise by volunteers. With no pay cheque or service contract, volunteers get much of their reward from a sense of achievement and contribution to the organization. These are important factors for paid workers but essential for volunteers who may quit if they do not feel valued or respected. Organizations that dedicate significant time and skilled effort to motivating and managing their volunteers, like those that have good human resource practices, are generally rewarded with dedicated and loyal service.

There is almost as much variation in the pay and working conditions of employees of not-for-profit sector as there is in corporations. Some not-for-profits have highly-paid professional staff and incentive-based compensation, others provide minimal pay and benefits — just as in the business world.

Many not-for-profits are quite entrepreneurial — this is increasingly the case as government support is reduced or matched to funds raised or earned by the organizations. Like companies, they use business techniques to improve their marketing, service delivery and customer service. On the other hand, businesses are becoming aware of the importance of stakeholders other than shareholders and recognizing the value of practicing social responsibility.

The accounting rules for not-for-profits are, for the most part, similar to those for businesses. There are, however, rules that will be unfamiliar to those whose experience is with business accounting. The differences are mostly related to the treatment of deferred revenues and of endowments, restricted and unrestricted funds. Any organization needs to have access to financially literate individuals who understand the specific accounting requirements of the field in which they operate.

Not-for-profit organizations generally have a little tolerance for deviations from budgets and low indebtedness on the balance sheet as compared to many corporations.

All organizations need ways to measure success. Although only corporations use measures related to shareholder value (earnings per share, return on investment, dividend yield, share price, etc.), both they and not-for-profits use many other measurements — both financial and non-financial.

Appendix 2 — Risk Register — example

The following is a simple, abbreviated example of the kinds of information that might be recorded in a risk register.

Risks identified	Likelihood	Severity	Overall (gross) risk	Control procedure	Retained (net) risk	Monitoring process	Responsibility	Action required	Date of review
Low investment returns	Medium	High	Medium/high	• Board-approved investment policy • Professional investment management	Low	Investment Committee reviews performance reports quarterly	• Chair, Investment Committee	Include reviews in board agendas	• Quarterly
Injuries to participants in sports programs	High	Medium	Medium	• Safety training for coaches and players • First aid training for coaches • Emergency procedures • Incident reports • Liability insurance	Low	Observe sports training	Sports director	• Report serious incidents to board • Include reviews in board agendas	• Ad hoc • Annual
Abuse of vulnerable individuals by staff and volunteers	Medium	High	High	• Screening of staff and volunteers • Awareness training • Anonymous reporting phone number	Medium	• Supervision • Review incident reports	• Volunteer coordinators • Managers and supervisors	• Report serious incidents to board • Include reviews in board agendas	• Ad hoc • Quarterly
Loss of information systems and information	High	High	High	• Frequent off-site back-up of files • Alternative processing resources • Emergency procedures and training	Low	• Review incident reports • Review of controls by auditors	• Vice President – Information Systems • Chair, Audit Committee	• Report serious incidents to board • Include reviews in board agendas	• Ad hoc • Annual

Appendix 3—Insurance

The following material is reproduced with the kind permission of the Insurance Bureau of Canada from their brochure "**Insurance for voluntary organizations: Things to consider**" [5]

WHAT TYPES OF PROTECTION CAN MY ORGANIZATION PURCHASE?

There are many, many types of insurance coverage available. The type and amount of insurance coverage you purchase will depend entirely on the type of service your organization provides. Some examples of types of coverage you may need are listed below

Commercial general liability insurance (otherwise known as CGL) is the most basic form of commercial insurance. If an organization has only one type of insurance, it is most likely commercial general liability. CGL policies cover claims in a number of basic categories of business liability:

- Bodily injury (e.g., a client or visitor is injured as a result of the work of your organization)
- Property damage
- Personal injury (including slander or libel)
- Advertising injury
- Tenant's legal liability
- Non-owned automobile insurance (e.g., volunteers using their own cars for the organization's business)

In addition to covering the claims listed above, commercial general liability policies also cover the cost of defending or settling claims—even if the claims are fraudulent.

Directors' and officers' insurance, or D&O, provides coverage for boards of directors against "wrongful acts," which might include actual or alleged errors, omissions, misleading statements, and neglect or breach of duty on the part of a board of directors.[6]

Errors and omissions insurance (sometimes called E&O, professional liability insurance or malpractice insurance) provides protection for those who give advice, make educated recommendations, design solutions or represent the needs of others. People who may benefit from this type of coverage include teachers, financial planners, consultants and placement services workers. It can be important coverage for anyone who deals with clients who could claim that something done on their behalf was done incorrectly, and that this error cost them money or caused them harm in some way.

Commercial auto insurance is required if your organization or its volunteers operate a car as part of your organization's activities. It will protect your organization in the event of accident, theft, injury and other damages involving your organization's vehicles. It will also protect your employees while they are driving insured company vehicles. There are a variety of coverages available for your organization's cars. Your coverage will depend on how you use the cars.

[5] http://www.ibc.ca/en/Business_Insurance/documents/brochures/Volunteer-brchr_singles_ENG_oct-07.pdf

[6] For more information, see CICA's *20 Questions Directors Should Ask about Directors' and Officers' Liability Indemnification and Insurance*

Appendix 4 — Crisis and Business Continuity Planning[7]

Organizations need plans for responding to both the immediate and longer-term consequences of crises in three key areas:

Crisis response

- Take immediate action to protect lives, property and the environment
- Find out what's going on and identify what the organization knows and doesn't know
- Appoint a core team who has been trained to manage the crisis and free team members from their regular responsibilities
- Promptly notify the company's insurance company and legal counsel of potential claims
- Make sure that day-to-day operations continue as far as possible

Communications

- Designate a single individual to handle crisis-related communications and communicate frankly to stakeholders and the news media
- Demonstrate commitment to communities directly affected by the crisis by sending in the appropriate corporate representative — this may be the Executive Director, but not necessarily
- Communicate directly and frequently to the company's stakeholders including employees, customers, suppliers, shareholders and regulators — both during the crisis and subsequently
- Appoint a devil's advocate to provide a reality check on the organization's response to the crisis — this could include outside experts such as public relations consultants and lawyers
- Give the board regular briefings

Business resumption

- Implement or develop a plan to resume normal operations
- Continue to communicate with the company's stakeholders as the plan unfolds

[7] The material in this Appendix comes from *20 Questions Directors Should Ask about Crisis Management*, pages 6 and 7.

Where to find more information

CICA Publications on governance

THE 20 QUESTIONS SERIES*

20 Questions Directors and Audit Committees Should Ask about IFRS Conversions

20 Questions Directors Should Ask about Building a Board

20 Questions Directors Should Ask about CEO Succession

20 Questions Directors Should Ask about Codes of Conduct

20 Questions Directors Should Ask about Crisis Management

20 Questions Directors Should Ask about Crown Corporation Governance

20 Questions Directors Should Ask about Director Compensation

20 Questions Directors Should Ask about Directors' and Officers' Liability Indemnification and Insurance

20 Questions Directors Should Ask about Executive Compensation

20 Questions Directors Should Ask about Governance Assessments

20 Questions Directors Should Ask about Internal Audit (2nd ed)

20 Questions Directors Should Ask about IT

20 Questions Directors Should Ask about Management's Discussion and Analysis (2nd ed)

20 Questions Directors Should Ask about Responding to Allegations of Corporate Wrongdoing

20 Questions Directors Should Ask about Risk (2nd ed)

20 Questions Directors Should Ask about their Role in Pension Governance

20 Questions Directors Should Ask about Special Committees

20 Questions Directors Should Ask about Strategy (2nd ed)

THE CFO SERIES*

Deciding to Go Public: What CFOs Need to Know

Financial Aspects of Governance: What Boards Should Expect from CFOs

How CFOs are Adapting to Today's Realities

IFRS Conversions: What CFOs Need to Know and Do

Risk Management: What Boards Should Expect from CFOs

Strategic Planning: What Boards Should Expect from CFOs

THE NOT-FOR-PROFIT SERIES*

20 Questions Directors of Not-for-profit Organizations Should Ask about Fiducary Duty

20 Questions Directors of Not-for-profit Organizations Should Ask about Governance

20 Questions Directors of Not-for-profit Organizations Should Ask about Risk

20 Questions Directors of Not-for-profit Organizations Should Ask about Strategy and Planning

THE CONTROL ENVIRONMENT SERIES*

CEO and CFO Certification: Improving Transparency and Accountability

Internal Control: The Next Wave of Certification. Helping Smaller Public Companies with Certification and Disclosure about Design of Internal Control over Financial Reporting

Internal Control 2006: The Next Wave of Certification—Guidance for Directors

Internal Control 2006: The Next Wave of Certification—Guidance for Management

Understanding Disclosure Controls and Procedures: Helping CEOs and CFOs Respond to the Need for Better Disclosure

OTHER CICA PUBLICATIONS

CAmagazine:
Christopher K. Bart: “Lasting inspiration, May, 2000, pp. 49-50
Hugh Lindsay: “Plugging the holes”, December 1997, p. 43.

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

RISK MANAGEMENT STANDARDS

Implementing Turnbull—A Boardroom Briefing, Institute of Chartered Accountants in England & Wales, September 1999

AS/NZS 4360:2004 Risk Management, Standards Australia

Enterprise Risk Management—Integrated Framework, Applications Techniques, COSO, September 2004

*Available for purchase in hard copy or free download at www.rmgb.ca

OTHER REFERENCES

Broder, Peter, ed., *Primer for Directors of Not-for-Profit Corporations, Industry Canada*, 2002.

Carver, John, *Boards That Make a Difference: A New Design for Leadership in Nonprofit and Public Organizations* (Jossey-Bass, 1990 2nd edition, 1997 3rd edition, 2006)

Deloitte, *The Effective Not-for-Profit Board* (undated)

Dimma, William A., *Tougher Boards for Tougher Times: Corporate Governance in the Post-Enron Era*. John Wiley & Sons Canada Ltd, 2006. (Chapter 22 provides a comparison between corporate and not-for-profit governance.)

Fink, Steven, *Crisis Management: Planning for the Inevitable.* New York, NY: American Management Association, 1986

Gill, Mel D, *Governing for Results*, Trafford Publishing, 2005.

Herman, Melanie L, Head, George L, Jackson, Peggy M and Fogarty, Toni E, *Managing Risk in Nonprofit Organizations: A Comprehensive Guide*. John Wiley & Sons, Inc., 2004.

Kelly, Hugh M., *Duties and Responsibilities of Directors of Not-for-Profit Organizations*. Canadian Society of Association Executives, 2004.

WEBSITES

Alliance for Nonprofit Management, Washington, DC www.allianceonline.org

Altruvest Charitable Services www.altruvest.org

Canadian Society of Association Executives www.csae.com

The Charity Commission for England and Wales, Charities and Risk Management, 2007. http://www.charity-commission.gov.uk/investigations/charrisk.asp

Charity Village www.charityvillage.ca

Imagine Canada www.imaginecanada.ca

United Way of Canada: Board Development www.boarddevelopment.org

About the author

Hugh Lindsay, FCA, CIP

Hugh Lindsay is a founder and president of FMG Financial Mentors Group Inc. He specializes in writing, training and consulting in corporate governance, risk management and strategic planning. In addition to being a Chartered Accountant, he is a Chartered Insurance Professional and a member of Financial Executives International. Prior to entering full-time consulting in 1992, he held senior financial and internal audit positions with a university and a major insurance company. Hugh is an Associate Member of Continuing Studies at Simon Fraser University.

Hugh has served on the boards of a number of not-for-profit organizations including the Insurance Institute of British Columbia, the Institute of Chartered Accountants of BC, the Vancouver Little Theatre Association, Community Mediation Services Society, and the Vancouver Museum Commission. His current board memberships include the Canadian Academy of Independent Scholars and the Vancouver Chapter of FEI Canada. He was a member of the Criteria of Control Board of the Canadian Institute of Chartered Accountants and is now a writer and editor for their Risk Management and Governance Board. He has written or edited a number of publications in the CICA's 20 Questions and CFO series including *20 Questions Directors of Not-for-profit Organizations Should Ask about Governance*, and *20 Questions Directors of Not-for-profit Organizations Should Ask about Strategy and Planning*.

ISBN-13: 978-1-55385-391-6
ISBN-10: 1-55385-391-1

9 781553 853916
04000056

20 Questions
Directors of
Not-For-Profit Organizations
Should Ask about
Risk

277 WELLINGTON STREET WEST
TORONTO, ON CANADA
M5V 3H2
416.204.3400
WWW.CICA.CA