Oversight of Risk by the Board of Directors

The Question:

What is the Board's role in addressing risk?

The Answer:

Risk and risk management can be a real challenge for many not-for-profit organizations, and boards of directors often struggle with their role. Some boards run into difficulties by micromanaging and attempting to control every potential area of risk. Other boards allow fear of risk to paralyze the organization and stifle new initiatives. Still others move blithely from one meeting to the next, approving campaigns, events, and programs without ever discussing the potential risks involved. Obviously, none of these approaches is ideal. But how can the board of directors fulfill its responsibility to the organization when it comes to risk?

The role of the board may depend on the organization

The board's responsibility for the oversight of risk includes making sure that the organization effectively identifies, assesses and manages risks. The nature of the board's involvement may vary with the size and sophistication of the organization and its staff. In larger organizations with experienced management, the board can often rely on staff to manage day-to-day risks, and the board's role is limited to oversight of risk management activities and approval of policies, strategies and major decisions. In organizations with fewer experienced staff members, the board may need to be more hands-on.

Risk Tolerance Policy

The board sets or approves the risk tolerance policy for the organization. The risk tolerance policy sets out the amount of risk that the organization is willing to assume. It has two key components: appetite for risk and capacity for risk.

- **Risk appetite** reflects the organization's willingness to take on risk – some are very risk averse, whereas others are more daring.
- **Capacity for risk** reflects the ability to withstand risk and is based on the strength of the organization's finances, donor support, reputation and credibility, as well as the experience and competence of volunteers and staff.

Risk Identification

> ***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.
>
> 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.*

Not-for-profit organizations are very diverse, which means that risks can vary depending on mandate, stakeholders, funding etc. In order to ensure that all applicable risks are "on the radar", it can be helpful to consider categories of risk, such as:

- Compliance risk – the risk of fines and other regulatory penalties for offences such as failure to remit payroll deductions, violation of privacy laws, etc.
- External risk – the risk of becoming irrelevant, losing the support of funders or the public, or failing to respond to economic, demographic and other trends.
- Financial risk –loss of funding, the risk of fraud, or inability to meet financial obligations.
- Governance risk – the risk of ineffective oversight, poor decision-making or lack of direction.
- Operational or Program risk – the risk of poor service delivery, day-to-day crises, and misuse or neglect of resources, including human capital.
- 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, or failure to keep the organization strong and relevant.

It is important to use a variety of approaches in order to identify risk. Whether the board is doing risk identification itself or hearing a report from management on the process used, it is important that there is a process in place for identifying risks and that it involves a variety of approaches, techniques and participants to ensure that all the bases are covered.

Risk Assessment

The next step is to identify the highest priority risks so that steps can be taken to address them. This can be done by using processes like risk mapping or scoring, which involve assigning values to risks based on the likelihood of occurrence and potential impact. The goal is to classify risks in terms of priority, which will help determine how to manage them and also pinpoint major risks which the board should remain aware of.

Boards should not forget that risks are interconnected. Impact from one risk can affect the probability of other risks. Problems in one area can cause problems in another. Boards should also consider the effect of more than one risk coming to pass at the same time: while the organization might be prepared for the occurrence of one adverse event, the impact of two or more occurring simultaneously may be more than it is equipped to handle. Tools such as scenario planning can help in imagining these possibilities.

Risk Management

There are, essentially, four ways to manage risk:

- **Avoiding risk** –This can be a legitimate strategy but can also result in missed opportunities. Before abandoning a promising idea, it makes sense to consider other ways to manage the risk.
- **Transferring risk –** Share the risk with someone else, for example by buying an insurance policy.
- **Mitigating risk** – Develop procedures with checks and balances to detect and reduce the likelihood and/or severity of risks.

- **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.

In selecting risk management strategies, cost is an important consideration. The cost of managing a risk should generally be compatible with its potential consequences. The choice of risk management strategies should also be compatible with the culture of the organization and the risk tolerance policy as approved by the board.

Ensuring that risk is on the board's agenda

Risk isn't something that should only be discussed once a year, or only in response to a report from management. Directors should ensure that discussion of risk occurs regularly, for example, during strategic planning sessions and before motions to approve major programs or projects. Regular review of risk identification, assessment, and management should be part of the board's work plan, and frequent reports should be requested on areas of key risk.

Oversight of risk is an integral part of good governance. It should not imply risk aversion. Rather, boards of directors can help guide their organizations by balancing opportunities and threats to achieve objectives in a way that is compatible with their values and tolerance for risk.

Further information on risk for not-for-profit organizations can be found in the CICA publication *20 Questions Directors of Not-for-Profit Organizations Should Ask about Risk*, authored by Hugh Lindsay. Much of this discussion is based on that publication.