

Guide to Risk



The board's risk oversight role is not a one-time event. Thinking about risk management as a matter of course, in quieter times, gives an organization a leg-up when it comes to responding to unanticipated events.

Taking an action in the face of uncertainty brings with it the potential for negative outcomes.

But keep in mind that same action has the potential to bring rewards and opportunities. That is the upside of taking risks.

Every organization is exposed to and takes risks daily. It's important to manage the balance of risk and reward.

Risk management

Risk is defined as the potential for uncontrolled loss of something of value. For an organization, a risk is something that could prevent it from achieving its goals.

The process of identifying and minimizing the consequences of a negative occurrence - to the extent possible - is referred to as the risk management system.

Risk management is how an organization identifies, assesses and mitigates its risks. The sophistication of an organization's risk management system depends to a certain extent on its size, complexity and resources, as well as on the industry it operates in.

The board's role in risk

The board of directors is not involved in day-to-day risk management. Instead, the board has a risk oversight role. In fulfilling that role, board directors should be able to satisfy themselves that effective risk management processes are in place and functioning effectively.

The risk management system allows management to bring to the board's attention the company's material risks and to assist the board to understand and evaluate how these risks interrelate, how they may affect the organization, and how they are being managed.

"The board's role in risk oversight is similar in some ways to the role of the audit committee. The audit committee does not prepare financial statements, draft disclosures, or maintain the system of internal controls. Rather, the audit committee bears responsibility for overseeing the financial reporting and related internal control processes." - John E. Caldwell, CPA, CA. 'A Framework for Board Oversight of Enterprise Risk'

The board needs to keep risk in mind at an enterprise-wide level, but also at a project level. When assessing and making decisions about a proposed course of action, a board director's 'risk antenna' should be on high alert.

As board directors, we need to look beyond the risks that management has identified and consider what additional unexpected risks might be out there.

This is an area where each board member's unique background and experience becomes invaluable and where diversity of viewpoints pays off. Let's face it, your view of risk is not the same as anyone else's. A robust discussion of risk strengthens the decision-making process and ensures that the board and management

are forging ahead with a common view of the risk environment.

Risk categories

Categorizing risk into different 'buckets' can really help when it comes to identifying risks that are less obvious. It's useful to consider risk in the following categories:

- **External risk.** External risks typically include economic volatility, industry cyclicality, industry structural change, and political change.
- **Financial risk.** The possibility that an organization may lose money or be unable to pay its debts. Types of financial risk include liquidity, capital availability, capital structure, currency exchange rates, and interest rates. In crisis situations, liquidity risk – the risk of being unable to meet short term financial demands – is often paramount. As one CEO put in during the pandemic, "Cash is king right now. A great set of financial statements counts for nothing if you don't have enough cash to get you through this crisis."
- **Operational risk.** This category includes broad risks that are often unique to each specific type of organization, such as customer dissatisfaction, product and service quality, technological and cost competitiveness, capacity constraints, production disruptions, IT security, vendor dependencies, and input quality and cost. Two specific types of operational risk came to the fore in the pandemic crisis:
 - **Supply chain risk:** Disruptions to the supply chain affected many organizations.
 - **Cyber security risk:** With so many employees working from home, IT systems became more vulnerable than ever to security breaches.

- **Compliance risk.** The possibility that the organization may breach applicable laws, regulations, and codes of conduct. These differ widely according to the industry sector and type of organization. New, and ever-changing, regulations around preventing the spread of the virus creates additional risk in this area during the pandemic.
- **Strategic risk.** The possibility of loss that arises from pursuing an unsuccessful business plan such as making poor business decisions, poor execution, allocating inadequate resources, or failing to respond properly to changes in the business environment.
- **Organizational risk.** The possibility of loss due to ineffective leadership, the lack of a succession plan, poor performance of management and/or staff, an inability to attract and retain talent, and a negative organizational culture.
- **Hazardous risk.** Threats to property, environment or health posed by natural disasters, environmental hazards, and occupational safety and health hazards.
- **Reputational risk.** The possibility that the perception of the organization by its stakeholders may be harmed on account of negative publicity about its products or services, its operations, or its people. Stakeholders include investors, customers and suppliers, employees and volunteers, governments and regulators, and the public.

Assessing risk

A typical risk assessment involves trying to pinpoint the probability, or likelihood, that it will occur, and the severity or impact that will result if it does occur. There are sophisticated ways of performing a risk assessment, but it almost always involves a high degree of personal judgment.



For instance, how would you assess the risk of a pandemic? If you were asked that question before the COVID-19 pandemic, your response would have been different that it would be today. And if you were affected by the 2003 SARS epidemic, your response would have been different from someone who did not.

Management usually has the expertise and intimate knowledge of the facts that allows them to properly assess the organization's risk. Here, the board can play its oversight role by probing to ensure management's opinions are objective and that their view is not distorted by rose-colored glasses. So, if the CFO says, "There's nothing to worry about," that's an occasion for the board to trust but verify on the topic of risk.

Choices in dealing with risk

An organization can deal with its risks in one of four ways. This set of choices represents an additional lens through which the board can oversee risk.



- **Accept.** If the organization decides that the degree of risk is manageable because the costs of mitigating are too high, or it is considered highly unlikely, or the potential rewards are too great, it can simply accept it and move on with the course of action.
- **Mitigate.** If the level of risk is too high, the organization can put in place steps to lower the risk to reduce it to a level that balances the rewards. Typically, these steps include process changes, equipment, training, etc.
- **Transfer.** The organization can transfer the risk to another party, usually by buying insurance.
- **Avoid.** If the organization decides that there is no way to reduce or transfer the risk to an acceptable level, it may decide to avoid the risk and forego the rewards.

The individual director's role

When it comes to risk oversight, you as an individual director can best contribute by remaining objective and maintaining a healthy scepticism.

Your takeaways:

- The board director's role is not to manage risk, but to oversee it.
- Categorize risks into buckets to help surface hidden risks or unanticipated events.
- Ask probing questions of management to ensure they are not seeing their pet projects through rose-colored glasses.

Resources:

- [20 Questions Directors of Not-For-Profit Organizations Should Ask About Risk.](#) Hugh Lindsay, FCA, CIP, CPA Canada
- [A Framework for Board Oversight of Enterprise Risk.](#) John E. Caldwell, CPA, CA, CPA Canada.
- [Calibrating Risk Oversight.](#) KPMG Board Leadership Centre.

This guide is adapted from The Savvy Director blog "[What do I need to know about risk?](#)" posted May 24, 2020.
