A Practical Guide to Enterprise Risk Management

by | **Peter Muldowney** and **Sheri Wright**

plans & trusts
education | research | information

For boards overseeing pension and benefits programs, risk functions as both a constraint and a source of potential value. The authors offer practical steps that organizations can use to identify, assess and respond to risk while safeguarding the plans' reputation and long-term sustainability.

Risk weaves itself into everyday decisions—sometimes unnoticed, sometimes underestimated. Organizations that succeed over the long term are those that build the discipline to recognize uncertainty early and respond with clarity, structure and purpose.

Enterprise risk management (ERM) challenges leaders to look ahead and ask better questions about what could matter most. It provides a practical way to distinguish risk from uncertainty, define risk appetite and capacity, integrate an ERM framework, counter behavioural biases and build a culture in which risk information flows and actions follow.

Building Awareness

Organizations often operate on the assumption that future conditions will mirror past experiences. An initial step in risk management is developing awareness. This involves looking beyond the immediate tasks to identify potential obstacles and opportunities. Asking simple questions such as "What if?" can interrupt routine thinking and reveal new scenarios that may require consideration. This separates strategic risk awareness from routine oversight. ERM is as much about how people behave as it is about formal processes. It is therefore important for boards to practice reflective awareness and watch for group think, overconfidence or undue reliance on third parties.

Risk is not limited to the possibility of negative outcomes. It refers to the effect of uncertainty on objectives. As Dr. David Hillson ("the Risk Doctor") puts it, "Risk is uncertainty that matters." In other words, uncertainty alone does not constitute risk; it becomes relevant when it has the potential to influence an objective. This underscores the importance of clarifying objectives, as they provide the basis for identifying which uncertainties are significant.

Takeaways

- Risk is "uncertainty that matters." Clarifying what matters most to plans and organizations over the next three to five years is important before identifying risks. Enterprise risk management is about recognizing risks sooner, not eliminating risks.
- Defining risk appetite in relation to strategy provides parameters for decision making and supports translating broader goals into specific objectives. This alignment can help identify and address risks earlier.
- Reporting systems can enable consistent board oversight of how risks and opportunities may affect outcomes, improving alignment and transparency in decision making and supporting timely responses as conditions evolve.
- Behavioural biases often influence decision making and risk management protocols, sometimes without being recognized. Anchoring, loss aversion and decision fatigue can all skew judgement; thoughtfully designed processes, such as blinding scenarios, prioritizing important decisions early and using structured discussions, help reduce these biases.
- Regular communication and consistent reporting strengthen oversight and accountability. Communication practices are frequently cited as contributing factors to project outcomes, and gaps in information sharing are frequently associated with project and operational challenges.

Why Take Risks?

For boards overseeing pension and benefits programs, risk functions as both a constraint and a source of potential value. Objectives such as providing retirement income or health benefits inherently involve uncertainty; decisions taken to meet those objectives introduce varying levels of risk. At the same time, failing to account for the needs and expectations of plan members can create exposures related to reputation, stakeholder confidence and the sustainability of the benefits offered.

Target's failed expansion into Canada illustrates how these dynamics can unfold. The company's inability to deliver the familiar customer experience Canadians expected contributed to its withdrawal from the market and a reported pretax loss of $5.4 billion.[1] The outcome has been associated with several risk management shortcomings, including flawed assumptions, unclear objectives, limited operational constraints and insufficient oversight at the board level.

An ERM-aware pension board looks beyond the surface comfort and asks deeper questions: Is there pressure to keep contributions low to avoid discomfort for the sponsor? Is the board relying too heavily on single-point estimates instead of considering a range of outcomes and scenarios?

Enterprise Risk Management

ERM integrates risk assessment with governance, strategy and performance by embedding risk considerations across organizational activities. It establishes defined roles, processes and reporting structures that support consistent board oversight of how risks and opportunities may influence outcomes. This approach can improve alignment and transparency in decision making and support timely responses as conditions change.

The Committee of Sponsoring Organizations (COSO) ERM framework, developed in response to major corporate

What to Do If an Employee Shows Signs of Burnout

FIGURE 1

Enterprise Risk Management

Source: *Enterprise Risk Management—Integrating with Strategy and Performance, Committee of Sponsoring Organizations of the Treadway Commission, 2017.*

Figure 1 depicts interlocking, colour-coded ribbons intended to represent the interrelated nature of ERM. COSO framework organizes ERM into five components, supported by 20 principles: governance and culture; strategy and objective setting; performance; review and revision; and information, communication and reporting. ERM can be understood as an approach embedded in how an organization plans, operates and adapts, rather than as a standalone function.

Governance and culture: Governance structures and organizational culture influence decision making, accountability and expectations. Clearly defined roles, responsibilities and authority can reduce gaps and provide additional oversight. While advisors and service providers may contribute, boards retain fiduciary responsibility for overseeing and protecting organizational interests.

Strategy and objective setting: Risk management is integrated with strategy and objective setting to establish direction. Defining risk appetite in relation to strategy provides parameters for decision making and supports translating broader goals into specific objectives. This alignment can help identify and address risks earlier.

Performance: Managing performance involves identifying risks that may affect objectives and assessing them in relation to impact and risk appetite. Responses may include accepting, mitigating or transferring risk, depending on context. Regular reporting supports awareness of decision makers.

Review and revision: Continuous assessment helps maintain the relevance of risk management practices. Periodic assessments can identify areas for adjustment, particularly in response to internal or external changes and incremental improvements over time.

Information communication and reporting: ERM relies on the availability of relevant information and effective communication channels. Mechanisms that support the timely sharing of information and the raising of concerns contribute to informed decision making. Consistent reporting practices support oversight and accountability.

failures to strengthen control practices, provides a structured, end-to-end approach for managing risk in relation to organizational objectives.

Practical Considerations

The following practices and tools illustrate how boards and management can apply ERM principles in practice.

Governance and Culture: Setting Expectations

Although governance is often defined by roles and responsibilities, many organizations still struggle to distinguish between board and management oversight. Unclear boundaries, competing priorities and governance complexities can weaken effectiveness. Culture also plays a decisive role. Shaped by skills, experiences and diverse perspectives, it thrives in environments where people feel safe to speak openly and where the board chair ensures inclusive, focused discussion.

Strategy and Objective Setting: Translating Appetite Into Action

A cornerstone of this component is the risk appetite statement, which documents a board's appetite, tolerance and capacity for accepting risk. This tool helps avoid fragmented judgments and supports consistent decision making:

- **Appetite:** The level of risk the organization is willing to accept to pursue value
- **Tolerance:** Acceptable variation from expected outcomes
- **Capacity:** The maximum risk the organization can sustain given its financial and operational position.

A robust risk appetite statement extends beyond investments to areas such as operations, administration and cybersecurity, and aligns decisions across related policies, including investment and funding.

Performance

Numerous tools support effective risk monitoring; the challenge is selecting those that are appropriate for your organization. Care is required when defining risks and responses, as behavioural bias can distort judgment. As Nobel laureate Daniel Kahneman demonstrated, losses sting about twice as much as equivalent gains feel rewarding.[2] This imbalance can skew probability assessments and lead to overly conservative or, at times, overly aggressive responses to risk.

Risk often breaks down at the board level not because information is unavailable, but because it feels abstract, technical or distant from today's decisions. Metaphors can help boards sharpen risk awareness by turning complex exposures into something easier to recognize and discuss. For example, the idea of "pulling a thread in a sweater" highlights how a seemingly contained decision, such as adjusting the asset mix, can trigger unintended and interconnected consequences elsewhere in the organization.

Just as animals used in advertising create memorable brand associations, they are used in the investment world to describe three types of potential disruptive risks boards should recognize:

- **Black swans (unknown unknowns):** Rare, unpredictable, high-impact events. While they cannot be forecast reliably, their effects can be mitigated through portfolio diversification so that losses are not concentrated.
- **Gray rhinos (known unknowns):** Visible, growing threats that are often ignored, rising duration risk entering a rate-hike cycle. These call for timely, incremental adjustments before vulnerabilities build.
- **White elephants (known knowns):** Obvious risks sidelined due to politics or emotional attachment. Strong governance and disciplined processes help leaders act despite discomfort.

Another valuable tool is the environmental scan. This forward-looking process assesses external forces, demographic, technological, regulatory and climate-related, against organizational objectives. Regular scanning helps boards assess the likelihood and potential impact of emerging risks. For example, an environmental scan focused on economic and market conditions can help the board see how persistently volatile interest rates may drive larger swings in the plan's funded ratio, deepening the board's understanding of where future funding vulnerabilities could emerge.

Review and Revision

Regular performance reviews are essential, but they only add value when the oversight process itself is well designed. One proven approach is the three lines of defence model, which clarifies the framework for responding to risks, regardless of plan size or complexity.[3]

First line—Operational management: Teams directly responsible for day-to-day activities, such as internal teams, investment managers and call centers.

Second line—Risk and compliance oversight: Functions responsible for monitoring risk, compliance and internal controls. The scope of this role should reflect the size and complexity of the plan size; in smaller organizations, these responsibilities may sit within finance or another shared function.

Third line—Independent assurance: An independent review function that reports to the board and evaluates whether governance, risk management and controls are operating effectively, often through external risk audits.

Structured risk management supports the achievement of objectives, but its effectiveness depends on individuals identifying risks and control gaps in a timely manner and addressing them through established processes. When an individual initiative operates with clearly defined roles and accountabilities, organizations can apply risk management practices more consistently.

Risk assessment is only useful when it informs action. Responses are typically calibrated based on potential impact and implications for stakeholders. Certain categories, such as reputational risk, may be managed with very low tolerance levels. Common response options regarding risk include:

- **Accept:** Applied to risks with relatively low impact and likelihood, with a documented rationale
- **Mitigate:** Use of controls, diversification, hedging or process adjustments to reduced exposure
- **Transfer:** Allocation of risk through mechanisms such as insurance or contractual risk allocation
- **Avoid:** Discontinuing or declining activities that fall outside defined risk appetite or capacity.

Prioritization is based on the severity of risks in relation to the established risk appetite. When thresholds are exceeded, for example, when asset allocations move outside defined ranges following market changes, responses are typically guided by preestablished contingency plans rather than developed in real time.

Behavioural Biases: The Hidden Risks

Even the strongest frameworks can falter when human judgment is skewed. Behavioural biases often influence decision-making and risk-management protocols, sometimes without being recognized. Because these influences are subtle yet persistent, they can masquerade as good governance while quietly undermining it. Some examples include:

Anchoring. When reviewing asset mixes or major program changes, the current state often becomes a psychological anchor, constraining better options. One way to counter this is to mask which scenario represents today's asset mix when reviewing potential alternatives. This can reduce emotional bias and open the door to better outcomes.

Decision fatigue. Decision quality tends to decline as the day wears on, often unnoticed. Countermeasures include scheduling strategic decisions early, batching routine approvals and allowing for breaks (including snacks) to restore energy and focus.

Nudge theory in governance. Small design choices can shape behaviour. For example, renaming committees to reflect an expanded focus, (e.g., Governance and Risk) or using think–pair–share (brief, two-person discussions followed by group sharing) can reduce dominance by a few voices and improve participation.

Information, Communication and Reporting

Communication practices are frequently cited as contributing factors to project outcomes. The Project Management Institute reports that communication issues contribute to project failure in one-third of cases and can negatively affect overall project performance.[4] As a result, communication is commonly treated as a core element of risk management.

Monitoring tools such as risk registers and dashboards support this function by maintaining an updated record of key risks, assigned owners, metrics, thresholds and response plans. When combined with defined escalation criteria, these tools help align responses with the level of exposure and reduce the likelihood of disproportionate reactions.

In addition to the COSO ERM framework, there are other models that could be used by boards that are overseeing risk. However, for pension and trust boards in Canada, an informal approach to risk management is no longer an option. The Canadian Association of Pension Supervisory Authorities (CAPSA) introduced Guideline 10 in late 2024. The guideline calls for boards to establish and document a framework for identifying, evaluating, managing and monitoring risks. Regulatory guidance generally establishes baseline expectations, which organizations may build upon to further integrate risk considerations into strategy, operations and organizational processes.

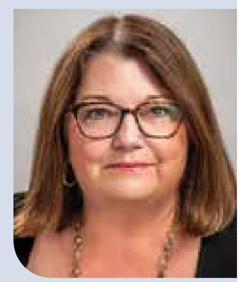
Practical Checklist for Boards

As boards strengthen their risk management practices, the following checklist highlights critical priorities.

1. **Clarify objectives.** Without clear objectives, risks cannot be identified. At a minimum, understand what matters most over the next three to five years.
2. **Define risk appetite.** Draft or refresh a Risk Appetite Statement covering both investments and operations.
3. **Establish a risk register.** Track top risks, owners, metrics and triggers, and make them the first agenda items in quarterly reviews.
4. **Embed ERM.** Integrate COSO ERM components into planning, performance reviews and reporting—avoid treating ERM as a separate function.
5. **Counter bias.** Blind current-state information in scenario reviews, schedule major decisions early and use think–pair–share to limit dominance in meetings.
6. **Design the three lines of defense.** Tailor the model to organizational size while preserving the independence of the third line.
7. **Scans and stress test.** Use environmental scan and scenario exercises to identify material risks and test response options.
8. **Overcommunicate.** Clear communication, reinforced by meaningful measurement, builds risk awareness and discipline.

BIOS

Peter Muldowney is the Senior Vice President Head of Institutional and Multi-Asset Strategy at Connor, Clark & Lunn Financial Group, in Toronto, Ontario. He has over 25 years of experience in the investment industry, during which time he has worked in Canada, the United States and the United Kingdom. Muldowney is also a member of the teaching faculty for the International Foundation of Employee Benefit Plans Master of Trust Management Standards (MTMS) credential program.



Sheri Wright, ICDD, is a governance guru devoted to supporting pension boards in Canada. She is a ten-year volunteer with the International Foundation of Employee Benefit Plans, an instructor of the Master of Trust Management Standards (MTMS) program, and an occasional conference speaker.

Review, Adapt and Communicate

ERM is an ongoing process rather than a one-time activity. Boards typically review risk management practices on a periodic basis, reassess underlying assumptions, identify emerging or previously unmonitored risks, and update risk appetite statements as conditions change. Communication remains a central element, as gaps in information sharing are frequently associated with project and operational challenges. Risk management focuses on established objectives, identifying relevant uncertainties, and maintaining processes that support timely and appropriate responses. When applied consistently over time, ERM can support organizational stability and inform decision making in changing environments.

Endnotes

1. Patterson, Craig. "10 Years Since Target's Exit from Canada: Lessons Learned." *Retail Insider.* January 15, 2025.
2. Tversky, Amos, and Daniel Kahneman. "Loss Aversion in Riskless Choice: A Reference-Dependent Model." *The Quarterly Journal of Economics* 106, no. 4 (November 1991): 1039–1061.
3. Anderson, Douglas J. and Gina Eubanks. *Leveraging COSO Across the Three Lines of Defense*, COSO, July 2015, 22 pages.
4. Project Management Institute (PMI). *The Essential Role of Communications*. May 2013.