OODP | Ontario Organizational Development Program

Strategic Risk Management and Financial Oversight Checklist for Non-profit Boards

Prepared by: Dionne Falconer, OODP Consultant
January 2014

Updated by: Radha Nayar, OODP Director
May 2026

Copyright & Disclaimer Statement

Production of *Strategic Risk Management and Financial Oversight Checklist for Non-profit Boards* has been made possible through financial contributions by the by the HIV and Hepatitis C Programs (HHP), Ontario Ministry of Health.

Board Risk Management and Financial Oversight Checklist

This checklist serves as a practical framework for boards to operationalize your fiduciary duties, transforming abstract governance obligations into actionable oversight. By systematically reviewing these critical areas, Boards can proactively safeguard organizational assets, navigate complex regulatory landscapes with confidence, and ensure that every decision aligns with long-term strategic interests and ethical standards. Boards can also cross-reference this checklist with OODP's Critical Compliance List for Non-profit Boards to ensure you are acting in the best interests of the organization.

1. Strategic Risk Management

- **Risk Framework Review**: Review and approve the **Enterprise Risk Framework**[1] annually to ensure it covers strategic, operational, financial, and reputational risks, including a **current risk register or risk dashboard** that offers accurate and unbiased information that compiles all current risks across the organization and is reviewed at least quarterly (including expected impact, and actions being taken to prevent or mitigate the risk).
- **Emerging Risks Scan**: Actively monitor for emerging risks (e.g., cyber threats, data privacy incidents, business continuity and disaster/pandemic preparedness and recovery, geopolitical shifts, regulatory changes, climate impact) and ensure management has a proactive mitigation plan.
    - **Crisis Preparedness**: Review and test the organization's **Crisis Management Plan** (including communication protocols, succession planning, and business continuity) at least annually.
    - **Cyber & Data Privacy**: Oversee the organization's cybersecurity, data governance and privacy compliance, ensuring regular audits are conducted.
- **Technology Governance**: Ensure the Board understands the organization's reliance on technology and the associated risks (e.g., Artificial Intelligence ethics, digital transformation).
- **Reputation Management**: Periodically review your organization's public reputation and brand integrity, including social media sentiment and stakeholder trust.

[1] The ERM Framework is a policy document that sets the rules, culture, and governance for the *entire* entity. A risk register or dashboard is a living document that reports (typically quarterly) on current risks an organization is facing and plans for mitigation. Risk Management Plans are used at program levels to manage risks at that level (e.g., risks specific to provision of clinical services for HIV/AIDS).

- **Contractual & Funder Compliance**: Verify that the organization meets all contractual obligations to major funders and donors.
- Oversee compliance with **applicable legislation and regulations**, including:
    - Ontario Not-for-Profit Corporations Act (ONCA)
    - Employment standards, health & safety
    - Privacy legislation (e.g., PHIPA/PIPEDA where applicable)
- **Board Competency & Skills Matrix**: Regularly assess the Board's collective skills against the organization's risk profile; recruit directors with specific expertise where gaps exist (e.g., cybersecurity, legal, finance).
- **Governance Execution**: Confirm the Board is actively fulfilling its fiduciary duties and adhering to its own stated purposes, Bylaws, policies and other governing documents.
- **Policy Adherence**: Ensure strict organizational compliance with internal policies, including the Code of Conduct, Conflict of Interest, and Whistleblower protections.
- Oversee **leadership continuity and succession planning** for the Executive Director and key roles.

2. Financial Oversight and Stewardship

- **Budget Approval:** Approve the annual operating budget and (if applicable) capital budget, ensuring alignment with strategic goals and realistic revenue projections.
- **Performance Monitoring:** Review monthly/quarterly financial statements, focusing on:
    - Variance analysis (budget vs. actuals).
    - Cash flow liquidity and reserve levels.
    - Revenue diversification and funding risks
    - Investment performance and risk exposure.
- **Financial Policy Governance:** Approve and annually review **financial policies (and their compliance)**, including:
    - **Delegation of Authority:** Clear spending limits and approval hierarchies for expenditures and contracts.
    - **Internal Controls:** Robust processes for segregation of duties and fraud prevention.

    - **Whistleblower Mechanism:** A safe, anonymous channel for reporting financial irregularities.
    - **Procurement Framework:** Transparent guidelines for sourcing goods and services to ensure value and fairness.
    - Expense reimbursement and approval processes
- **Audit Integrity:** Ensure the annual independent audit is completed on time, review the audit findings, and track the implementation of management's corrective action plans.
- **Insurance Coverage:** Review and approve insurance policies (D&O, General Liability, Property, Cyber) to ensure coverage limits match the organization's current risk profile.
- **Investment Policy:** Approve and review the organization's **investment and reserve policies**, ensuring alignment with risk tolerance and liquidity needs and ethical investment standards.
- **Solvency & Sustainability:** Assess long-term financial sustainability, including endowment management, diversification of revenue streams, and reserve adequacy ratios.

References

An introduction to emerging risks and how to identify them. (n.d.). IRM Charities Special Interest Group Report. https://www.theirm.org/media/9230/charities-sig-an-introduction-to-emerging-risks-and-how-to-identify-them.pdf

Lindsay, H. (2009). *20 questions directors of not-for-profit organizations should ask about risk.* Chartered Professional Accountants of Canada. https://governance.ca/wp-content/uploads/2020/05/20-questions-about-risk-compressed.pdf

Herman, Melanie (n.d.). *All Aboard: Embracing ERM in Your Nonprofit.* Nonprofit Risk Management Center. https://nonprofitrisk.org/resources/all-aboard-embracing-erm-in-your-nonprofit/

Wares, A. (n.d.). *Getting started with enterprise risk management: A guide for nonprofits.* ERM Initiative, North Carolina State University. https://erm.ncsu.edu/wp-content/uploads/sites/436/migrated-files/Getting_Started_with_ERM_-_A_Guide_for_Nonprofits.pdf