IMPACT EXCHANGE 2026

Medium nonprofits: practical risk guide

Tailored actions for organizations with 11–50 paid employees • companion to the 16-risk reference

WHAT MATTERS AT THIS SIZE

Management designs, operates and checks safeguards. The board assures itself that sound risk practices exist and reviews the risk dashboard twice yearly, with urgent exceptions escalated promptly.

FIRST FIVE PRIORITIES

- [ ] Assign a management owner for each top risk.
- [ ] Use service capacity, incident and funding signals in monthly management meetings.
- [ ] Document supervisory and safeguarding practices across teams.
- [ ] Sample-check payments, user permissions and backup tests quarterly.
- [ ] Provide a board dashboard twice yearly; promptly escalate major issues.

A risk-by-risk action checklist

01 Financial sustainability and funding concentration

MAKE ROUTINE Set board-agreed triggers, three scenarios and a quarterly funding-concentration review. Assign a team owner and keep evidence in a shared location.

WATCH FOR Falling unrestricted cash; recurring deficits; late receivables; a major funder approaching renewal.

DASHBOARD INPUT Cash forecast reviewed; funding concentration monitored; trigger and decision recorded.

02 Demand exceeding safe and sustainable service capacity

MAKE ROUTINE Review capacity indicators monthly and test a surge or staff-loss scenario. Assign a team owner and keep evidence in a shared location.

WATCH FOR Increasing wait times; vacancies; overtime; more shortcuts, near misses or complaints.

DASHBOARD INPUT Wait-time trends; staff workloads; triage decisions; quality and complaint evidence.

03 Client safety, safeguarding and incident response

MAKE ROUTINE Practise incident response and review exceptions/near misses independently. Assign a team owner and keep evidence in a shared location.

WATCH FOR Unapproved one-to-one contact; boundary exceptions; incidents not logged; gaps in supervision.

DASHBOARD INPUT Training, supervision, incident reviews and appropriate reporting records.

04 Staffing, burnout, management capability and workplace safety

MAKE ROUTINE Develop supervisor training, workforce backup and OHSA-informed workplace-violence/harassment controls. Assign a team owner and keep evidence in a shared location.

WATCH FOR Turnover; sick time; unfilled roles; avoidable conflict; postponed supervision; staff reporting fatigue.

DASHBOARD INPUT Workload and vacancy trends; completion of supervision; training and issue-resolution records.

05 Cybersecurity, privacy and information stewardship

MAKE ROUTINE Complete annual access reviews, formal incident exercise and supplier/security review. Assign a team owner and keep evidence in a shared location.

WATCH FOR Shared logins; MFA gaps; excess access; no proven backup restore; unusual email/payment requests.

DASHBOARD INPUT MFA coverage; restore test result; access-review sign-off; incident log.

06 Board oversight, renewal and risk-aware governance

MAKE ROUTINE Prepare a board risk dashboard at least twice yearly; plan board succession. Assign a team owner and keep evidence in a shared location.

WATCH FOR No reporting of changes or exceptions; vacant officer roles; repeated deferred decisions.

DASHBOARD INPUT Board minutes show decisions, exceptions, owners, due dates and follow-up.

07 Volunteer capacity, screening, boundaries and supervision

MAKE ROUTINE Review role changes, volunteer retention and incident learning each quarter. Assign a team owner and keep evidence in a shared location.

WATCH FOR Unscreened new duties; role drift; missed orientation; shifts covered by a few individuals.

DASHBOARD INPUT Role/screening records; supervision and refreshers; coverage and incident trends.

08 Fraud, theft, financial controls and misuse of assets

MAKE ROUTINE Sample payment approvals, separate access permissions and test fraud response. Assign a team owner and keep evidence in a shared location.

WATCH FOR Urgent bank-detail changes; delayed reconciliation; one person controls authorization and review.

DASHBOARD INPUT Dated independent review; callback log; reconciliations and exceptions.

09 Business interruption and emergency service continuity

MAKE ROUTINE Run scenario exercises and rehearse recovery priorities with partners. Assign a team owner and keep evidence in a shared location.

WATCH FOR Single-location dependence; no contact tree; backups not tested; unclear decision authority.

DASHBOARD INPUT Exercise results; updated contact list; restored systems; tested referrals.

10 Executive succession and concentration of key knowledge

MAKE ROUTINE Test interim authority and maintain a board-approved CEO succession protocol. Assign a team owner and keep evidence in a shared location.

WATCH FOR Only one person knows passwords, relationships, restricted-funding details or payroll routines.

DASHBOARD INPUT Accessible transition checklist; backup successfully completes a critical task.

11 Fundraising volatility, donor influence and mission drift

MAKE ROUTINE Monitor concentration, restricted obligations, donor influence and fundraising returns. Assign a team owner and keep evidence in a shared location.

WATCH FOR Funders influence service priorities; unusual gift restrictions; fundraising expenses rise without return.

DASHBOARD INPUT Approved gift review; funding terms register; board-documented exceptions.

12 Artificial intelligence and third-party technology

MAKE ROUTINE Maintain approved-tool list, training, privacy review and human accountability for significant decisions. Assign a team owner and keep evidence in a shared location.

WATCH FOR Sensitive information entered into consumer tools; no owner for vendors; unchecked AI-generated decisions.

DASHBOARD INPUT Tool inventory; privacy assessment; sampled outputs and incident reporting.

13 Organizational ethics, culture, complaints and reputation

MAKE ROUTINE Audit incident closure and incorporate themes into leadership and board reporting. Assign a team owner and keep evidence in a shared location.

WATCH FOR Repeat complaints; fear of raising issues; retaliation concerns; different rules for senior staff.

DASHBOARD INPUT Complaint response times; follow-through and non-retaliation checks.

14 Growth, partnerships, shared services and mergers

MAKE ROUTINE Review partner performance, shared incidents and renewal/exit options at set points. Assign a team owner and keep evidence in a shared location.

WATCH FOR New programs approved before staffing; partner boundaries unclear; no shared response agreement.

DASHBOARD INPUT Agreement register; service review; cost and incident evidence.

15 Legal, regulatory, contractual and insurance gaps

MAKE ROUTINE Run yearly compliance assurance and material-change reviews with board oversight. Assign a team owner and keep evidence in a shared location.

WATCH FOR Unassigned filing dates; no contract register; outdated policy; assumptions about insurance coverage.

DASHBOARD INPUT Filing confirmations; evidence of training; contract/insurance review notes.

16 Facility safety, property hazards and transportation

MAKE ROUTINE Use scheduled inspections, documented fixes and weather/transport continuity exercises. Assign a team owner and keep evidence in a shared location.

WATCH FOR Poor maintenance; unreviewed accessibility barriers; vehicle issues; extreme weather.

DASHBOARD INPUT Inspection checklists; incident data; completion of corrective work.

90-day implementation rhythm

Days 1–30	Days 31–60	Days 61–90
Choose 3–5 risks; assign owners; close an urgent safeguard gap.	Test safeguards; agree warning triggers; document escalation.	Present first dashboard to board; review at least twice yearly.

Size is not a measure of client-safety exposure. Apply all mandatory legal duties and adjust safeguards to program risk, sector licences and contracts.

Ontario and Canadian legal checkpoints — confirm what applies

CORPORATE GOVERNANCE (ONCA)

Ontario-incorporated nonprofits must identify their governing legislation, by-laws, financial-review requirements, annual-return and member-meeting obligations. Federally incorporated entities and other forms follow different rules. Read your own governing documents and obtain legal advice on material changes.

REGISTERED CHARITY OBLIGATIONS

Registered charities must file the T3010 within six months of fiscal year end, issue accurate donation receipts, maintain required books and records, and comply with charitable purpose and grant conditions. Other nonprofits do not automatically have the same CRA charity obligations.

SAFEGUARDING / MANDATORY REPORTING

Under Ontario CYFSA, s. 125, a person with reasonable grounds to suspect a child under 16 needs protection in a specified circumstance must immediately report directly to a children’s aid society. Different rules apply for 16- and 17-year-olds; sector-specific reporting can be additional.

WORKPLACE SAFETY

OHSA-covered employers must prepare and review workplace violence and harassment policies at least annually and implement the required programs. Written/posting requirements for policies apply when six or more workers are regularly employed at a workplace, subject to exceptions and orders. The written workplace-harassment program requirement is separate.

ACCESSIBILITY

Most Ontario businesses and nonprofits with 20 or more employees must file an AODA accessibility compliance report by December 31, 2026; designated public-sector organizations have different reporting cycles. Training and other standards can apply below the reporting threshold.

PRIVACY, FUNDRAISING AND INSURANCE

Privacy rules depend on activities and sector; do not assume all nonprofit personal information falls under PIPEDA. Confirm client record rules, contracts, cyber incident response, fundraising requirements and insurance terms with the appropriate specialist.

Source links and further reading

- Ontario Nonprofit Network, 2026 State of the Sector survey policy report (741 respondents, published October 15, 2026) — https://theonn.ca/topics/advocacy/nonprofit-sector-surveys/
- Ontario, ONCA overview — https://www.ontario.ca/page/not-profit-corporations-act-2010
- Ontario, Child, Youth and Family Services Act, 2017, s. 125 — https://www.ontario.ca/laws/statute/17c14#BK166
- Ontario, OHSA workplace violence and harassment guide — https://www.ontario.ca/document/guide-occupational-health-and-safety-act/part-iii0i-workplace-violence-and-workplace-harassment
- Ontario, AODA accessibility compliance reporting — https://www.ontario.ca/page/completing-your-accessibility-compliance-report
- Ontario, AODA rules for businesses and nonprofits — https://www.ontario.ca/page/accessibility-rules-businesses-and-non-profits
- CRA, T3010 filing deadline — https://www.canada.ca/en/revenue-agency/services/charities-giving/charities/operating-a-registered-charity/filing-t3010-charity-return/when-file.html
- CRA, charity books and records — https://www.canada.ca/en/revenue-agency/services/charities-giving/charities/operating-a-registered-charity/books-records.html
- CRA, official donation receipts — https://www.canada.ca/en/revenue-agency/services/charities-giving/charities/checklists-charities/issuing-complete-accurate-donation-receipts.html
- Canadian Centre for Cyber Security, guidance — https://www.cyber.gc.ca/en/guidance
- Melanie Lockwood Herman, Manage Risk With Intention This Year (NRMC, 2026) — https://nonprofitrisk.org/resources/manage-risk-with-intention-this-year/
- Office of the Privacy Commissioner of Canada, PIPEDA and nonprofits — https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Legal descriptions are issue-spotting guidance current to October 26, 2026, not a legal opinion. Confirm statute, current guidance, licences and funding agreements before acting.