Nonprofit Risk Assessment & Reduction Guide

June 2025

Developed by Big Change Consulting for Cuyahoga County Human Services Chamber

This guide assists organizations in evaluating their vulnerabilities and developing action plans to address them. Sections are as follows:

Overview....1
Financial Risks....3
Legal and Compliance Risk....5
Tax Status....5
Governance Risks....6
Operational Risks....6
Technological Risks....7
Personnel Risk....8
Reputational Risks....8
Programmatic Risks....8
External Risks....9
Anything Else?....9
Resources....9

Overview

Running a nonprofit organization is hard. Beyond delivering services to your community, you must secure funding, manage compliance, and mitigate risks. This guide provides a structured approach to identifying and reducing common risks in nonprofit operations.

Each category of risk can be addressed using the following process:

Step 1: Identify Your Requirements

- Review grants, contracts, policies, governance documents, and legal requirements.
- Consult experts, board members, and legal advisors to ensure you capture all compliance obligations.

Step 2: Assess Risk Levels

- Assign a risk score to each item and calculate an average risk score per category to prioritize action.

Risk Level	Description
0 - None	No compliance, financial, or operational exposure.
1 - Low	Minimal potential impact; minor consequences if not addressed.
2 - Medium	Some potential for compliance issues, financial loss, or operational disruptions.
3 - High	Significant threat to funding, operations, or legal standing. Immediate action required.

Step 3: Develop Policies

- Draft clear policies outlining responsibilities, timelines, and required actions.
- Ensure policies are reviewed and approved by the appropriate team or governing body (e.g., board of directors).

Step 4: Document Procedures

- Create Standard Operating Procedures (SOPs) for consistent compliance with policies.
- Clearly define:
    - Who is responsible for each task.
    - When tasks should be completed.
    - Where to find key documents.
    - How to handle questions and decision-making.
- Set a timeline for reviewing and updating policies and procedures.

Step 5: Implement and Monitor

- Train staff and volunteers to follow the established procedures.
- Assign accountability to ensure compliance and effectiveness.

Step 6: Maintain and Adapt

- Regularly review and update policies and procedures as:
    - Regulations change
    - Grant or funding requirements evolve
    - Staffing adjustments occur
- Conduct periodic risk assessments to stay ahead of potential issues.

Financial Risks

Revenue: Assess the vulnerability of your revenue, including:

- ☐ **Funding is too restrictive**: Do your funding restrictions allow you to cover all necessary operations?
- ☐ **Too much funding from a few sources**: If one of these funders decreases or is eliminated, how will it affect your organization?
- ☐ **Too much funding from unstable sources**: If these funders don't have a history of maintaining funding for your organization, are dependent on certain relationships, or are tied to a specific project, does that pose a risk to your organization?
- ☐ **Failing to maintain strong funder relationships**: If the economy were to suffer a downturn, then would your funders continue to prioritize supporting your organization?
- ☐ **Funder confidence in the organization**: Funders may cut or reduce funding if they lack trust in the organization's leadership, financial management, or mission impact.
- ☐ **Investment security**: Make sure funds are invested safely in case of stock market fluctuations.
- ☐ **Federal grants** are changing. Check out this guide from the National Council of Nonprofits

Insurance: Determine how much insurance is appropriate for your current size, facilities, activities, and risk tolerance. Key coverages to consider include:

- Cyber
- Directors & Officers (D&O)
- Events (may be ad hoc)
- General Liability (GL)
- Hired/Non-Owned Auto
- Property

Contact Charity One Insurance for an assessment or quote.

Financial Mismanagement:

Financial mismanagement—whether due to error, weak oversight, or fraud—can jeopardize an organization's funding, credibility, and operations. Reduce risk by establishing clear policies, ensuring oversight, and using secure systems for financial transactions. In addition to other recommendations in this guide to reduce financial risk, segregation of financial duties is critical to reduce the risk of financial mismanagement.

- ☐ No single staff member should be responsible for authorizing, processing, and reconciling financial transactions. Assign different people to approve expenses, make payments, and reconcile bank accounts.
- ☐ Use dual approval for payments and purchasing when possible.
- ☐ Budget-to-actual reports should be prepared and reviewed monthly.

- ☐ The Board should receive financial updates at least quarterly.
- ☐ Leadership should use financial data to monitor organizational health and identify irregularities early.
- ☐ Ensure the Board is Trained on and Engaged in Proper Oversight: Provide training or onboarding on how to read financial statements, understand the Form 990, and assess cash flow and reserves. Board members should ask questions, review financials, and understand their fiduciary responsibilities.

Fraud: Financial fraud is a growing threat to businesses of all sizes. Protect your organization by implementing strong internal controls and following best practices for financial transactions.

Key Fraud Prevention Steps include:

- ☐ Establish Financial Policies and Procedures
  - Verify the segregation of financial duties (e.g., dual approvals for payments).
  - Ensure compliance with audit requirements (internal and external).
- ☐ Confirm Financial Reporting and Accountability
  - Review the accuracy and timeliness of financial reports.
  - Evaluate expense monitoring processes and budget adherence.
  - Ensure the Board is trained on and engaged in proper oversight
- ☐ Utilize Secure Financial Practices
  - Ensuring all bank account users have their own confidential login and password.
  - Implement practices on the Business Fraud Mitigation Checklist
- ☐ Practice the most secure payment methods whenever possible.

  Most Secure Methods (Highly Recommended)
  ✔ Credit Cards – Uses your organization's credit, reducing direct exposure to bank funds.
  ✔ Multi-Approver Payment Systems – Require multiple levels of approval before processing payments. Examples: Ramp, Bill, or your bank's ACH with dual authorization

  Moderately Secure Methods (Use with Caution)
  ✔ Single-Approver Payment Systems – Your bank's online bill pay (if well-monitored).
  ✔ Keyed-In ACH Payments – Requires entering account details manually, but offers some security.
  ✔ Hand-Delivered Checks – Less risk than mailed checks, but still susceptible to fraud.

  Least Secure Methods (Avoid When Possible)
  ❌ Debit Cards – Directly linked to bank accounts, offering minimal fraud protection.
  ❌ Mailed Checks – Prone to theft, forgery, and interception.

Legal and Compliance Risk

Nonprofits must adhere to legal and regulatory requirements to maintain good standing.

- ☐ Tax and Regulatory Compliance

- Tax-Exempt Status Compliance: Regularly confirm that the organization meets all IRS requirements to maintain its nonprofit tax-exempt designation.
- Accurate and Timely Filings: Review all state and federal filings, such as Form 990 and charitable registrations, to avoid penalties or loss of good standing.
- Lobbying and Advocacy Restrictions: Ensure compliance with lobbying limits applicable to 501(c)(3) organizations to prevent jeopardizing tax-exempt status.

☐ Contractual and Employment Compliance
- Legally Reviewed Contracts and Agreements: Keep contracts, Memoranda of Understanding (MOUs), and other agreements up to date and legally vetted.
- Employment Law Compliance: Verify compliance with labor laws, including minimum wage, overtime regulations, harassment prevention policies, and workplace safety requirements.

☐ Data Protection and Governance Policies
- Data Privacy and Security: Ensure compliance with applicable data protection laws, such as GDPR, CCPA, or HIPAA, if handling protected health information. Maintain secure data management practices.
- Documented Policies and Governance: Maintain clear, accessible policies such as whistleblower protections, conflict of interest policies, and financial oversight guidelines to promote transparency and accountability.

☐ Financial and Intellectual Property Protections
- Intellectual Property Protections: Safeguard the organization's trademarks, copyrights, and logos to prevent unauthorized use. Ensure proper licensing for any third-party content.
- Grant Compliance and Reporting: Track and report on grant deliverables, ensure proper use of restricted vs. unrestricted funds, and submit all required reports to funders on time.

☐ Proactive Compliance Tracking
- Use of a Compliance Calendar: Track key deadlines for filings, renewals, grant reporting, and other compliance requirements to stay on schedule and avoid lapses.

By proactively managing these legal and compliance risks, nonprofits can safeguard their status, maintain credibility, and avoid costly legal challenges.

Tax Status

Ensure you know the following requirements for your 501(c)(3) tax status.

☐ Pass the Public Support Test: An organization is a publicly supported charity if it meets one of two tests.

☐ Lobbying limits: Nonprofits may not have a substantial part of their activities on lobbying, unless they file a 501(h) application to significantly raise the limit. Note that this very simple application is automatically approved, and no confirmation is provided by the IRS.

Governance Risks

Strong governance is critical to a nonprofit's stability, transparency, and effectiveness. A well-structured board ensures ethical oversight, strategic decision-making, and long-term success. Review the following:

- ☐ Board Engagement and Oversight
    - Active and Diverse Board: A well-rounded board with varied expertise strengthens decision-making, oversight, and community representation. Board members should be engaged, regularly attending meetings, and fulfilling their responsibilities.
    - Thorough Meeting Documentation: Maintain accurate board meeting minutes and decision records to provide transparency, accountability, and legal protection.
    - Annual Leadership Evaluations: Conduct regular assessments of board and executive leadership performance to ensure accountability, effectiveness, and continuous improvement. Include staff in executive leadership's assessments.
- ☐ Governance Structure and Compliance
    - Meet minimum board membership, meeting, and quorum requirements.
    - Clearly Defined Roles and Responsibilities: Ensure that board members and committees have well-established duties to prevent governance gaps and inefficiencies.
    - Adherence to Bylaws: Regularly review and enforce organizational bylaws to ensure compliance with legal and governance standards.
    - Strong Onboarding and Training: Provide thorough orientation and training for new board members so they understand their roles, responsibilities, and the nonprofit's mission and operations.

Refer to BoardSource for more information.

Operational Risks

Effective operations are essential for nonprofits to fulfill their mission efficiently and sustainably. Minimizing operational risks ensures stability, safety, and continued impact.

- ☐ Program and Staffing Management
    - Program Effectiveness and Alignment: Review program delivery to ensure it meets established goals and objectives with sufficient, qualified staff.
    - Volunteer Management and Screening: Implement screening, training, and oversight processes to ensure volunteers are well-prepared and aligned with the organization's mission. Proper management helps mitigate liability, safety concerns, and service quality risks.
- ☐ Infrastructure and Safety

- Sufficient Physical Infrastructure: Assess the office space, equipment, and other resources to ensure smooth operations. Facilities should be safe, accessible, and well-maintained to prevent disruptions.
- Comprehensive Safety Protocols: Establish and enforce safety measures to protect staff, volunteers, and beneficiaries. This includes workplace safety guidelines, emergency procedures, and risk mitigation strategies for fieldwork or high-risk activities.

☐ Crisis Preparedness and Risk Mitigation

- Emergency Preparedness and Crisis Planning: Develop a well-defined emergency preparedness plan that outlines response steps for crises such as natural disasters, security threats, or operational disruptions. Regularly review and update the plan to ensure readiness.

Technological Risks

Nonprofits rely on technology for operations, fundraising, and communication. Ensuring strong cybersecurity, reliable systems, and compliance with standards reduces risks and protects data.

☐ Cybersecurity and Data Protection

- Cybersecurity Measures: Implement strong protections, such as firewalls and multi-factor authentication, to prevent cyber threats.
- System Access Controls: Regularly review who has access to systems and data to ensure proper authorization and limit vulnerabilities.
- Data Backups and Disaster Recovery: Confirm that regular data backups are in place and that a disaster recovery plan is established to prevent data loss.

☐ Hardware, Software, and IT Infrastructure

- Age and Functionality of Systems: Assess whether computers, servers, and other hardware are up to date and capable of supporting the organization's needs.
- Antivirus and Anti-Malware Protection: Verify that security software is current and effectively protecting against threats.

☐ Software and Digital Platform Management

- CRM and Donor Management Systems: Evaluate whether the nonprofit's CRM or donor database is effective, secure, and meeting organizational needs.
- Website Security: Check for vulnerabilities, such as outdated plugins or missing SSL certification, to protect against breaches.
- Accessibility Compliance: Ensure the website meets accessibility standards, such as WCAG, to provide equitable access for all users.

Personnel Risk

A strong, well-supported team is essential to nonprofit success. Reduce personnel risk by:

☐ Providing an Employee Handbook: Clearly outline policies, expectations, and procedures to ensure consistency and compliance.

- [ ] Supporting Your Staff: Address concerns promptly and foster an open, communicative workplace.
- [ ] Managing Uncertainty: Crises create fear; uncertainty worsens it. Keep staff informed, offer guidance, and provide reassurance to maintain morale and stability.
- [ ] Succession Planning: Create a plan for the sudden absence of the Executive Director or key staff and consider creating longer-term plans to build resilience within the staff and board.
- [ ] Organizational Culture: Establish values, assess the diversity of your staff, develop DEI framework, and a process for handling discrimination or bias-related complaints.

Reputational Risks

A nonprofit's reputation is one of its most valuable assets. Maintaining public trust, credibility, and transparency is essential for sustaining donor support, community engagement, and long-term impact. Reduce reputational risks by ensuring:

- [ ] Public Communications and Media Presence
    - Monitor Media Mentions: Implement media tracking to stay informed of how the organization is being perceived in the press and on digital platforms. Address any misinformation or negative coverage promptly.
    - Establish a Crisis Communication Plan: Develop a clear strategy for handling public relations challenges, including negative press, legal issues, or internal crises. Designate spokespeople and ensure staff are trained on appropriate messaging during a crisis.
- [ ] Stakeholder Trust and Engagement
    - Maintain Strong Conduct Policies: Implement and enforce policies for staff, board members, and volunteers to ensure ethical behavior. Address misconduct swiftly to prevent damage to the organization's reputation.

Programmatic Risks

Nonprofits must ensure their programs effectively fulfill their mission while remaining financially and operationally sustainable. Poorly designed or misaligned programs can lead to wasted resources, loss of stakeholder trust, or unintended harm. Reduce programmatic risks by ensuring:

- [ ] Confirm Program Alignment: Regularly review programs to ensure they align with the organization's mission and strategic plans.
- [ ] Review Evaluation Processes and Metrics: Establish clear performance metrics and outcome measurements to assess program success. Collect qualitative and quantitative data to determine effectiveness and areas for improvement.
- [ ] Identify Potential Risks in Program Activities: Evaluate whether programs could inadvertently cause harm, reinforce inequalities, or create dependency. Conduct risk assessments to mitigate unintended negative consequences.

External Risks

Nonprofits operate in an ever-changing environment influenced by external factors beyond their control. Proactively identifying and managing these risks ensures the organization's resilience and long-term stability.

Anything Else?

Stay proactive with a solid foundation:

- ☐ Conduct a SWOT Analysis: Identify strengths, weaknesses, opportunities, and threats to anticipate and address potential risks.
- ☐ Have a Crisis Plan: Prepare for emergencies to ensure organizational stability.
- ☐ Know Your Finances: Understand restricted vs. unrestricted funds, grant deliverables, and the true costs of fulfilling them.

Resources

- Big Change Consulting: Operations Consultant for Nonprofits
- BoardSource: Nonprofit Board Resources
- IRS: Charities and Nonprofits Information
- National Council of Nonprofits: Resources for Running a Nonprofit
- Nonprofit Insurance Alliance: Guidance and Broker Portal
- Nonprofit Quarterly: Compliance Checklist
- Nonprofit Risk Management Center: Resources on several risk categories
- Ohio Attorney General: Charitable Resources