Cybersecurity Risk Assessment Checklist

A practical self-assessment for association and nonprofit leaders

Use this checklist to evaluate your organization's cybersecurity posture across six critical domains. For each item, check the box if your organization has fully implemented the measure. Items left unchecked represent opportunities for improvement.

Tip: Complete this assessment with your leadership team and IT provider together for the most accurate picture.

1. Governance & Executive Ownership

- [ ] An executive leader (ED, CEO, or board member) is designated as the cybersecurity owner
- [ ] Cybersecurity is a standing agenda item at board or leadership meetings (at least quarterly)
- [ ] The organization has a written IT Acceptable Use Policy that all staff have signed
- [ ] There is a documented Incident Response Plan that defines roles, escalation paths, and communication protocols
- [ ] Cybersecurity risk is integrated into the organization's Enterprise Risk Management (ERM) framework
- [ ] You have identified and documented all critical digital and physical assets (data, systems, devices)

2. Identity & Access Management

- [ ] Multi-Factor Authentication (MFA) is enforced for ALL users across all critical systems
- [ ] Executive, finance, and admin staff use phish-resistant MFA (FIDO/YubiKey hardware keys)
- [ ] Least-privilege access is enforced — staff only access systems their role requires
- [ ] Former employee and vendor accounts are deactivated within 24 hours of departure
- [ ] Admin/privileged accounts are inventoried and reviewed at least quarterly
- [ ] Single Sign-On (SSO) is implemented where possible to centralize access control

3. Email & Endpoint Security

- [ ] Third-party email filtering is deployed beyond built-in Microsoft 365 or Google protections
- [ ] DMARC, DKIM, and SPF records are configured for your email domain
- [ ] External email banners warn staff when messages originate outside the organization

- [ ] Endpoint Detection & Response (EDR) is installed on all organizational devices
- [ ] Mobile devices accessing organizational data are enrolled in a Mobile Device Management (MDM) solution
- [ ] USB and removable media policies are defined and enforced

4. Data Backup & Recovery

- [ ] Automated backups run on a defined schedule for all critical systems and data
- [ ] Backups follow the 3-2-1 rule: 3 copies, 2 media types, 1 offsite/cloud
- [ ] Backup restoration is tested at least quarterly (with documented results)
- [ ] Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are defined and achievable
- [ ] Backups are protected from ransomware via immutable storage or air-gapped copies
- [ ] A documented disaster recovery plan exists and has been rehearsed within the past year

5. Security Awareness & Culture

- [ ] All staff, volunteers, and board members complete security awareness training at least annually
- [ ] Simulated phishing tests are conducted regularly to measure and improve awareness
- [ ] A blame-free reporting culture exists — staff are rewarded for reporting suspicious activity
- [ ] New employee onboarding includes cybersecurity training and policy acknowledgment
- [ ] Staff understand how to identify phishing, smishing (SMS phishing), and social engineering
- [ ] Security reminders are integrated into regular team communications (not just annual training)

6. AI Usage & Governance

- [ ] A written AI Acceptable Use Policy exists and has been communicated to all staff
- [ ] Data classification (Green / Yellow / Red) guides what information may be used with AI tools
- [ ] An approved list of AI tools exists, with unapproved tools explicitly prohibited
- [ ] Staff have been trained on safe AI use, including risks of entering sensitive data
- [ ] All AI-generated external content is reviewed by a human before publication
- [ ] AI use is disclosed in externally facing content per your transparency policy

Quick Reference: AI Data Classification (Traffic Light System)

GREEN — Safe to Use	Public info, general research, non-sensitive content
YELLOW — Use with Caution	Internal reports without personal data; review before sharing
RED — Never in Public AI	Donor names, health data, financials, member PII

How to Score Your Assessment

30-36 items checked: Strong posture — focus on continuous improvement and testing.
20-29 items checked: Good foundation — prioritize unchecked items using the 30-60-90 day roadmap.
10-19 items checked: Significant gaps — start with the Big 5 measures immediately.
Under 10 items: Critical risk — engage professional support and address governance first.