NONPROFIT IT HEALTH & RISK ASSESSMENT

Find the gaps that need a decision

A 45-minute worksheet for nonprofit, human-services and behavioral-health leaders. Review one organization or clearly defined program with your IT lead.

> Score each item: 0 = missing; 1 = partly in place; 2 = current evidence supports it; U = unknown; N/A = explain why. This is a Bitralynx Solutions prioritization worksheet, not a validated risk model or security certification. Scores do not measure breach probability.

Organization / program scope / review date / reviewers

01 Do current staff have individual, approved accounts? --

Evidence: active-user list matched to current staff and program roles.

02 Is MFA enforced for important and privileged access? --

Evidence: enforcement report, tested recovery and tracked exceptions.

03 Are administrative privileges limited and reviewed? --

Evidence: named administrators, separate admin accounts and review date.

04 Does offboarding remove access across every key service? --

Evidence: a recent departure record including vendor apps and devices.

05 Can authorized staff recover administrative access? --

Evidence: tested emergency-access procedure and a backup contact.

02 / BACKUPS AND DEVICES

Check the recovery path and endpoints

Continue the same scoring: 0 missing; 1 partial; 2 evidenced; U unknown; N/A with a written reason. Record evidence references on the final page.

06 Are all critical data locations in the recovery plan? --
Include mail, shared files, program applications, local systems and vendors.

07 Are recovery targets agreed with program leadership? --
Evidence: target restore time and acceptable data-loss window by service.

08 Has a recent test restored a usable staff workflow? --
Evidence: measured result and validation by authorized program staff.

09 Are recovery copies protected from common failure paths? --
Evidence: access, deletion protection and alternative recovery arrangements.

10 Does someone resolve backup failures and exclusions? --
Evidence: alert review, escalation and a record of closed failures.

11 Are work devices inventoried and supported? --
Evidence: device register covering shared, remote and mobile workflows.

12 Are security updates deployed and exceptions followed up? --
Evidence: update report and action on failed or unsupported devices.

13 Is endpoint protection monitored across the agreed scope? --
Evidence: coverage and alert handling, including inactive agents.

14 Are portable-device data and recovery keys protected? --
Evidence: verified encryption, access controls and retrievable keys.

15 Are routine admin rights and remote access controlled? --
Evidence: approved access methods and reviewed local administrator lists.

03 / VENDORS AND CONTINUITY

Make external dependencies visible

Technology risk includes responsibility, contracts, communication and recovery arrangements. Use evidence from the actual service, not general marketing claims.

16 Are critical vendors and escalation contacts documented?
Include program applications, identity, internet, telecoms and IT support.
--

17 Are vendor access and app permissions reviewed?
Evidence: purpose, approver, scope and end date for external access.
--

18 Are vendor recovery and data-export limits understood?
Evidence: service terms, recovery responsibilities and usable export options.
--

19 Is there a named incident lead with an alternate?
Evidence: contact list, decision authority and communication procedure.
--

20 Can priority programs use an approved downtime process?
Evidence: staff instructions, secure records and a reconciliation plan.
--

Calculate a coverage score, not a risk rating

Add numeric scores. Maximum = 2 x (20 minus N/A items). Count U as zero for this coverage calculation, and report the unknown count separately. Coverage = points / maximum x 100. If all items are N/A, do not calculate a percentage.

Points / maximum / coverage % / unknown count / N/A items and reasons

Example: 28 points, 2 N/A items and 3 unknowns = 28 / 36 = 78% coverage, with 3 unverified items. A high score does not cancel a critical gap.

04 / PRIORITIZE THE WORK

Leave with three practical priorities

Use service impact, exposure and dependency to choose actions. Do not rank work solely by the total score.

> Escalate: active incidents, exposed privileged access or no verified recovery for critical services. Then investigate unknown coverage and schedule remaining gaps.

Useful first moves: enforce MFA, test one recovery, reconcile the device list and clarify vendor duties. Choose based on local evidence.

Priority 1 / service impact / action / responsible person / due date

Priority 2 / service impact / action / responsible person / due date

Priority 3 / service impact / action / responsible person / due date

Evidence references / N/A explanations / next review date

Reference guidance

NIST: Cybersecurity Framework 2.0 - Small Business Quick-Start Guide

NIST informs the risk-management context; it does not endorse this questionnaire or scoring method. Keep completed assessments internal. Reviewed September 8, 2026.

> Bitralynx Solutions helps nonprofit leaders turn findings into a practical plan with clear responsibility and follow-through.
> Start with a complimentary Technology Readiness Review: one 45-minute conversation and a one-page list of practical priorities. Book your review or email info@bitralynx.com.