hi@solanasis.com
303-900-8969
solanasis.com

Your Mission Is Built for Generations. Your Technology Should Be Too.

Private foundations steward irreplaceable records: trust agreements, planned giving documentation, donor information, and beneficiary data. Let's face it: most do this on infrastructure that was never designed for that level of sensitivity. The mission is built for generations; the systems protecting it are often running on good intentions and a thin IT budget.

We help foundations close that gap.

The Quiet Risks Foundations Carry

Wealth management-grade data, minimal IT budgets

Foundations handle trust records, donor PII, and estate documents with the same sensitivity as any financial services firm. But most operate without dedicated IT staff, let alone a security team. That mismatch is where quiet failure begins.

Irreplaceable records

Trust agreements, planned giving documentation, and beneficiary records. If these are lost, corrupted, or exposed, there is no rebuilding them. These documents represent decades of relationships and legal commitments.

Untested backups

Most foundations have never verified whether their backups actually produce a usable restore. That's not disaster recovery; that's false comfort. The first test of your backup should not happen during an actual crisis.

Breach exposure is real

The Blackbaud breach cost $59M+ in settlements and exposed data from 13,000 nonprofits. Foundations are targets, not bystanders. State data breach notification laws apply regardless of organization size.

Foundation Compliance Readiness Assessment

10 days. Fixed fee. Board-ready reporting.

$5,000 to $7,500 depending on the number of systems and users. We'll give you a specific number after a short intro call.

Nonprofit Data Protection · NIST CSF · Disaster Recovery Verification

What we do

- ✓ Gap analysis mapped to nonprofit data protection standards
- ✓ **Real disaster recovery test.** We restore your backups and prove they work
- ✓ Systems inventory and risk prioritization
- ✓ Board-ready reporting your leadership team can present with confidence

STEP	WHAT HAPPENS
1	Intro call about your foundation
2	Kickoff and scope lock
3	Assessment + real restore test

What you get

- Gap analysis with nonprofit-specific mapping
- Risk register: prioritized, evidence-backed
- 90-day resilience roadmap with owners and deadlines
- Maturity scorecard
- Disaster recovery report with documented restore verification
- Board-ready executive summary

STEP	WHAT HAPPENS
4	Readout + board-ready roadmap
5	Optional remediation

Your team's time: 3-5 hours over 10 business days. We designed this for lean teams.

How We Fit

We coordinate with your compliance counsel and your IT provider (or vendor, if you don't have internal IT). We handle cybersecurity verification, disaster recovery testing, and technical remediation. We replace no one.

Most foundations we work with don't have dedicated IT staff. That's fine. We work directly with your team and any vendors you already use. The goal is to give your board confidence that your mission-critical data is actually protected, not just backed up somewhere.

What Happens Next

1. **Hand off cleanly.** Take the roadmap and execute with your existing team or IT vendor.
2. **Remediation sprint.** We close the top gaps in 2-4 weeks. Fixed scope, fixed fee.
3. **Ongoing resilience partner.** Quarterly testing and board reporting so your security posture doesn't drift.

Book a 30-minute conversation: go.solanasis.com/intro

Download the free compliance checklist: go.solanasis.com/checklist

BOOK A CALL