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

Wills, Trusts, and Powers of Attorney Deserve Better Protection Than a Shared Password and Good Intentions

Estate planning firms handle some of the most sensitive documents in professional services. ABA Model Rules 1.1 (Competence) and 1.6 (Confidentiality) require "reasonable efforts" to protect client information. The question most firms struggle with: what counts as reasonable for a 10-person practice? We help you answer that with evidence, not guesswork.

The Gaps We See Most Often in Estate Practices

Document security

Wills, trusts, and beneficiary designations stored in shared drives with broad access controls. If everyone in the firm can read everything, your access permissions don't match the sensitivity of the data. Here's the thing: that's a hidden risk most firms have learned to live with.

Untested recovery

If your document management system goes down tomorrow, how long until you're operational? Most firms have backups; few have tested whether those backups actually produce a usable restore.

Vendor access nobody tracks

Your practice management software, cloud storage, and email provider all touch client data. Do you know exactly who has access? Messy handoffs with former vendors create exposure that compounds over time.

Breach notification exposure

Your state's data breach notification laws create real liability if client information is exposed; without detection capabilities, you may not know a breach occurred until weeks or months after the fact.

10-Day Compliance Readiness Assessment

Fixed scope. Fixed fee. Minimal disruption.

ABA Rules 1.1 & 1.6 | State Bar Guidance | State Breach Notification Laws | NIST CSF

What we do

- ✓ Security assessment mapped to ABA rules and your state bar's data protection guidance
- ✓ **Real disaster recovery test.** We restore your data, time the process, and prove it works
- ✓ Vendor access inventory and risk review
- ✓ Prioritized readiness roadmap you can actually execute

What you get

- Gap analysis with ABA and state-specific regulatory mapping
- Risk register: prioritized, evidence-backed

TIMELINE	STEP
Day 1	Kickoff and scope lock
Days 2-6	Assessment + real restore test
Days 7-9	ABA-mapped deliverables
Day 10	Readout with your team

Your team's time: approximately 3-4 hours over 10 business days. We

- 90-day readiness roadmap with owners and deadlines
- Readiness maturity scorecard
- Disaster recovery report and restore runbook
- Executive summary for your managing partner

handle everything else.

How We Fit

Your Compliance Counsel	**Solanasis**	Your IT Provider / MSP
ABA rules interpretation, state bar guidance, legal strategy	Cybersecurity verification, DR testing, vendor risk, remediation	Daily operations, help desk, infrastructure

We coordinate with everyone. We replace no one.

What Happens Next

1. **Take the plan and run.** The deliverables are yours. Many firms execute the roadmap independently.
2. **Remediation sprint.** We close the critical gaps in 2-4 weeks. Fixed scope, fixed fee.
3. **Fractional Cybersecurity Partner.** Ongoing oversight 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