SOLANASIS

Don't Trip Over Your Untied Shoelaces

A Quick Compliance Gut-Check for Wealth Management Firms

Here's the thing about compliance: most firms think they're covered until someone actually checks. A regulatory examiner, a client's attorney, a due diligence questionnaire from a new custodian; and suddenly all those assumptions get tested.

This checklist covers the 35 things that matter most right now, mapped to what SEC and state securities examiners are prioritizing in 2026, including the updated Regulation S-P requirements taking effect June 3, 2026. It's not everything, but if you can check most of these boxes, you're in better shape than 80% of the firms we've seen.

If you can't check them? That's not a reason to panic. It's a reason to know where you stand.

RIAs (Registered Investment Advisors) | Estate planning attorneys | Family offices | Impact investing firms

Whether you're SEC-registered or state-registered, these items reflect what examiners prioritize. State securities regulators (like Colorado's Division of Securities under DORA) apply similar cybersecurity expectations.

Your Score	What It Means
28-35 checked	Solid foundation. You're ahead of most firms. Focus on maintaining and documenting.
18-27 checked	Gaps to close, but you know what they are. A focused sprint could get you there.
Under 18 checked	Significant exposure. Prioritize the highest-risk items, especially governance, access controls, and backup testing.

1. Governance & Written Policies

Why this matters: Regulators' 2026 examination priorities emphasize governance practices and senior management oversight of cybersecurity. If you don't have it written down, it doesn't exist.

- [ ] You have a Written Information Security Program (WISP) that's been reviewed in the last 12 months
- [ ] Your WISP names a specific person responsible for cybersecurity
- [ ] You have a written incident response plan that's been tabletop-tested
- [ ] Your acceptable use policy covers personal devices, remote access, and AI tools
- [ ] Board or senior leadership receives cybersecurity briefings at least annually

Examiner tip: Examiners want to see evidence of management oversight. Meeting minutes count.

2. Access Controls & Identity Management

Why this matters: Access controls are a top 2026 examination focus area. The question isn't just "who has access"; it's "can you prove only the right people have access?"

- [ ] You enforce multi-factor authentication (MFA) on all systems with client data
- [ ] You have a documented process for onboarding/offboarding user access
- [ ] You review user access permissions at least quarterly
- [ ] Admin/privileged accounts are separate from daily-use accounts
- [ ] You enforce a password policy (complexity, rotation, or passphrase standard)

Pro tip: Ideally paired with a password manager. "Summer2024!" doesn't count.

3. Data Protection & Loss Prevention

Why this matters: Data loss prevention (DLP) is a 2026 regulatory examination priority. Your clients trust you with sensitive financial data; you need to prove you're protecting it.

- [ ] Client data is encrypted at rest and in transit
- [ ] You know where all client PII and financial data lives across your systems
- [ ] You have controls preventing unauthorized data transfers (USB, personal email, etc.)
- [ ] Your email system has protections against phishing and unauthorized forwarding
- [ ] Sensitive documents have classification and handling procedures

Blind spot: Unencrypted backups are a common finding in examinations.

4. Vendor & Third-Party Risk

Why this matters: Your vendors' security is your security. Examiners evaluate how firms oversee their service providers, especially cloud and technology vendors.

- [ ] You maintain a current inventory of all vendors with access to client data
- [ ] Vendor contracts include data protection and breach notification requirements
- [ ] You conduct due diligence on vendor security before onboarding
- [ ] You review vendor security posture at least annually
- [ ] You have a plan for vendor transition if a critical provider fails

Reality check: SOC 2 from 2021 doesn't tell you anything about 2026.

5. Backup & Disaster Recovery

Why this matters: Most firms say they have backups. Very few have actually tested a full restore. There's a big difference between "backups exist" and "recovery works."

- [ ] You perform regular backups of all critical systems and client data
- [ ] Backups are stored in a separate location from production systems
- [ ] You've tested a full restore from backup in the last 12 months
- [ ] Your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are documented
- [ ] Your incident response plan specifically addresses ransomware scenarios

Examiner tip: Ransomware preparedness is explicitly called out in 2026 examination priorities.

6. Regulation S-P & Client Privacy

Why this matters: The SEC's updated Regulation S-P (compliance date June 3, 2026 for smaller entities) requires written policies for safeguarding customer records, an incident response program, and timely breach notification.

- [ ] You have written policies for safeguarding customer records and information
- [ ] Your privacy notice is accurate and has been updated for current practices
- [ ] You have a documented process for notifying clients within 30 days after discovering unauthorized access
- [ ] Your data retention and disposal policy is documented and followed
- [ ] Staff receive privacy and data handling training at least annually

Key deadline: Updated Reg S-P requires service providers to notify your firm within 72 hours of a breach. Your firm must then notify affected clients within 30 days. Training records matter; "we talked about it in a meeting" isn't documentation.

7. AI & Emerging Technology Governance

Why this matters: AI security controls are a new 2026 examination focus area. If your firm uses AI tools, examiners will want to see guardrails.

- [ ] You have a policy governing the use of AI tools in your firm
- [ ] AI tools that process client data have been vetted for data privacy
- [ ] You maintain activity logs for AI-assisted decisions affecting clients
- [ ] Staff are trained on acceptable AI use and its limitations
- [ ] You've assessed whether AI tools create new regulatory obligations

Reality check: AI governance isn't just a technology problem; it's a people problem.

Your Total Score: ___ / 35

Not sure what to do with your score?

Our 10-Day Compliance Readiness Assessment picks up where this checklist leaves off. We verify your answers, test what can't be checked on paper (like whether your disaster recovery actually works), and give you a prioritized roadmap with regulatory context.

BOOK A FREE INTRO CALL

No pitch deck. No pressure. Just a conversation about where you stand.

Your compliance consultant handles the regulatory strategy. Our assessment verifies the technical controls that back it up.

---

solanasis.com · hi@solanasis.com · (303) 900-8969

solid systems. fewer unknowns. clients protected.