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

SEC Examiners Will Ask About Your Cybersecurity Controls. Will Your Answers Hold Up?

Examination priorities for 2026 put cybersecurity at the top of the list. So if your firm can't demonstrate tested recovery, documented vendor oversight, and a practiced incident response capability, the gap between what you have and what examiners expect could become a problem.

REGULATION S-P COMPLIANCE DEADLINE: JUNE 3, 2026

The SEC's updated Regulation S-P requires a written incident response program, expanded service provider oversight (including 72-hour breach notification), and client notification within 30 days of discovering unauthorized access.

The Blind Spots Examiners Find Most Often

Untested disaster recovery

Most firms have backups running; few have tested a full restore and documented the results. When an examiner asks "when did you last verify your recovery works?" the answer needs to be specific, not a guess.

Vendor blind spots

Your custodian, CRM, and cloud providers all handle client data. Reg S-P now requires expanded oversight, including contractual provisions for breach notification within 72 hours.

Documentation that doesn't match reality

Having a WISP is one thing. Having one that reflects what your firm actually does is something else entirely. Drift is the hidden risk here; the policy stays the same while systems change.

Incident response never rehearsed

SEC examination guidance identifies practiced incident response as an "observed good practice." A plan nobody has walked through is false comfort.

10-Day Compliance Readiness Assessment

Fixed scope. Fixed fee. Minimal disruption.

SEC Cybersecurity Exam Priorities | Regulation S-P | Colorado DORA | NIST CSF

What we do

- ✓ Gap analysis mapped to what SEC and state securities examiners actually look for
- ✓ **Real disaster recovery test.** We restore your data, time the process, and prove it works
- ✓ Vendor risk review against Reg S-P service provider requirements
- ✓ Prioritized readiness roadmap you can actually execute

TIMELINE	STEP
Day 1	Kickoff and scope lock
Days 2-6	Assessment + real restore test
Days 7-9	Regulatory-mapped deliverables

What you get

- Gap analysis with regulatory mapping (SEC, state, NIST CSF)
- Risk register: prioritized, evidence-backed
- 90-day readiness roadmap with owners and deadlines
- Readiness maturity scorecard
- Disaster recovery report and restore runbook
- Executive summary for your managing partner or board

TIMELINE	STEP
Day 10	Readout with your team

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

How We Fit

Your Compliance Consultant	**Solanasis**	Your IT Provider / MSP
Regulatory strategy, exam prep, Form ADV	Cybersecurity verification, DR testing, vendor risk, remediation	Daily operations, help desk, infrastructure

We coordinate with everyone. We replace no one.

Do you work with our existing compliance consultant?

Absolutely. Your compliance consultant handles the regulatory interpretation, policy development, and examination coaching. We handle the technical implementation and verification: testing whether backups actually restore, reviewing vendor security posture, documenting evidence that controls are operational. We coordinate with your consultant and your IT provider; we compete with neither.

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

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

BOOK A CALL