FINANCIAL SERVICES

FINRA and SEC IT Checklist for Advisory Firms

The controls examiners, custodians, and clients expect to see documented.

Regulators expect advisory firms to protect client information and prove it. The amended Regulation S-P now requires a written incident response program and customer notification for many breaches. This checklist covers the technical side so your compliance binder reflects what is actually running.

How to use it: tick what you have in place today. Anything left unticked is a conversation worth having.

01 Safeguard client information

- [ ] **Written information security program that matches your actual systems**
  Examiners compare the policy to reality.
- [ ] **Multi-factor authentication on email, CRM, custodian portals, and remote access**
  No exceptions for principals.
- [ ] **Encryption on laptops, phones, backups, and outbound email with client data**
  Account statements and tax documents leave every day.
- [ ] **Role-based access to CRM, portfolio, and file systems**
  Staff see only the clients they serve.
- [ ] **Data loss prevention rules for account numbers and SSNs**
  Catch sensitive data before it leaves by email.

02 Monitor, record, and retain

- [ ] **Email and messaging archiving that meets books-and-records rules**
  Including texts and collaboration tools used for business.
- [ ] **Audit logging on key systems, reviewed on a schedule**
  Who accessed client data and when.
- [ ] **Endpoint detection and response monitored 24/7**
  Ransomware and credential theft happen after hours.
- [ ] **Vendor due diligence file for every provider with client data**
  Custodians, CRM, planning software, IT, and backup.
- [ ] **Annual penetration test or vulnerability assessment**
  Keep the report and the remediation notes.

03 Respond and recover

- [ ] **Written incident response program with customer notification steps**
  Regulation S-P sets a notification deadline for covered incidents.
- [ ] **Wire and distribution requests verified by phone at a known number**
  Business email compromise targets advisor-client money movement.
- [ ] **Daily backups with an immutable copy, restores tested quarterly**
  Proof of recoverability is part of business continuity.
- [ ] **Business continuity plan that covers hurricanes and regional outages**
  Gulf Coast firms need an alternate site or cloud-first setup.
- [ ] **Annual cybersecurity training with completion records**
  Phishing simulations show the training works.

Red flags we see most

- The security policy was written from a template and never updated.
- Text messages with clients are not archived.
- Distributions are approved over email alone.
- Nobody has tested a restore this year.

Where to start

Before your next exam, have your IT partner walk through your written policies line by line and confirm each control is really in place.

Want a second set of eyes?

Book a free 30-minute IT assessment. A senior technician walks through this checklist with you and tells you what to fix first. No sales script, no obligation.

Book a free assessment

(813) 999-0086
swfit.io/free-consultation