SIMAPTIC.

SEC Reg S-P Exam-Readiness Checklist

For registered investment advisers under **$1.5B AUM** — the **June 3, 2026** compliance deadline has passed; these requirements are now in force. Examiners can ask for evidence of your program at any exam.

> Work through each section below. Every unchecked box is a gap an examiner can find — and the SEC has been clear that it wants proof of implementation, not just written policies.

1. Risk Assessment

The risk assessment is the first step to understanding what controls are "reasonable" for your firm — and the best way to justify any control you have chosen not to implement.

- ☐ **Inventory of sensitive customer data (NPPI) your firm handles.**
  Include data held on third-party platforms (CRM, portfolio management, custodians) *and* local copies — a common pitfall is firms that believe everything lives on third-party platforms while also saving client correspondence on internal file shares.
- ☐ **Data flow map covering the full lifecycle of NPPI.**
  Where customer non-public personal information lives, how it moves through your systems, and how it is decommissioned.
- ☐ **Written IT/security risk matrix (likelihood × impact).**
  Examiners expect to see security and IT risks, not just business risks — with identification, rating, mitigation, and iteration over time.
- ☐ **Documented justification for any control deliberately not implemented.**
  Example: a firm whose client data is held entirely on third-party platforms can use the risk matrix to justify not adding controls to its own network.

2. Incident Response Program

The most substantial new requirement: a written program covering the four required components — detection, scoping, response, and customer notification.

- ☐ **Written incident response program** reasonably designed to detect, respond to, and recover from unauthorized access to customer information.

- ☐ **Documented detection method with a named owner.**
  Who detects an intrusion, from what data sources, and who decides whether customers must be notified. If detection is outsourced to an MSP, its responsibilities must be documented.

- ☐ **Documented process for determining whether sensitive customer information was accessed.**
  Detection ties directly to scoping — without it, you cannot know when notification is required.

- ☐ **Containment and response steps.**
  Isolating affected systems, cutting off unauthorized access, and the internal notification chain for an in-progress incident.

- ☐ **Customer notification procedure.**
  The channel (email, phone, letter), the content (what happened, what information was involved, protective steps customers can take), and the 30-day notification requirement after becoming aware of a breach involving sensitive customer information.

- ☐ **Records retained for every incident — even when no customer data was accessed.**
  Keep the incident record and the detection artifacts that supported the "no access" determination.

3. Vendor Oversight

Relying on third parties shifts some of the work — but not the responsibility. Your firm remains accountable for customer data compromised at a vendor.

- ☐ **Inventory of service providers that touch customer information.**
  Custodians, CRM platforms, email, IT support, cybersecurity monitoring — anyone with access to client data.

- ☐ **Contracts require vendor notification within 72 hours of a breach on their systems.**
  The requirement applies to all third-party vendors. Where existing contracts lack the clause, document the gap and a remediation plan.

- ☐ **Cybersecurity obligations negotiated into vendor contracts — not just assumed.**
  Examiners ask for contracts showing negotiated obligations, and your policies must cover how you verify vendor compliance with your data handling requirements.

4. Recordkeeping & Monitoring

Buying a security tool is not sufficient — the SEC expects to verify it is actually in use.

- ☐ **Five years of written documentation** covering your safeguards and disposal procedures.
- ☐ **Monitoring and logging capable of an affirmative determination** of whether customer data was accessed or exfiltrated in the event of an incident.
  If you can't answer that question with evidence, you have a gap.
- ☐ **Security tools enabled and properly configured — not just purchased.**
  A common SEC exam finding: firms buy security tools but never enable key modules.

5. What Examiners Request

When SEC examiners arrive, expect the document request to include:

01 Your written incident response plan with all three required elements: assess, contain, and notify.

02 Vendor contracts showing negotiated cybersecurity obligations and 72-hour notification provisions.

03 A data flow map showing where customer NPPI lives, how it moves, and how it is decommissioned.

04 Evidence that monitoring and detection tools are purchased, **enabled**, and properly configured.

05 Log data sufficient to determine whether customer data was accessed following an incident.

06 Your IT/cybersecurity risk matrix showing identification, rating, mitigation, and iteration over time.

SIMAPTIC.

Want the evidence before the examiner asks?

SIMAPTIC runs automated internal security assessments mapped to **NIST 800-53 Rev 5** and **MITRE ATT&CK**, generating the exam-ready documentation SEC examiners look for — proof that your controls are not just written, but working.

Assessments starting at $4,000.

Book a Call

https://simaptic.ai/contact/