REGULATION S-P

First SEC Exam Cybersecurity Checklist

[Firm name] | Completed by [Name] | [Month DD, YYYY]

Before You Start

Since June 3, 2026, the amended Regulation S-P has applied to every SEC-registered adviser, whatever its size. These are the items to have in place, and the proof to keep, before examiners ask.

For each item, mark Yes, Partial or No, and write down where the proof is kept. Items marked "Practice" or "Supports" are not named in the rule but help show it is met.

1. Your Program on Paper

Item	Rule	Proof to keep	Result
Written safeguards policies and procedures that describe your real systems, not a generic template	248.30(a)(1)	The policy or compliance manual section, with the date you approved it	☐ Yes ☐ Partial ☐ No
A dated risk assessment, with each control tied to a risk it addresses	Supports (a)(2)	The assessment, and how each risk is handled	☐ Yes ☐ Partial ☐ No
An annual review of your compliance program that includes cybersecurity	Supports 206(4)-7(b)	The review memo and who performed it	☐ Yes ☐ Partial ☐ No

2. Incidents and Client Notice

Item	Rule	Proof to keep	Result
An incident response program to detect, respond to, and recover from unauthorized access to customer information	248.30(a)(3)	The plan, the people and vendors on call, and your monitoring tools	☐ Yes ☐ Partial ☐ No
A client notice procedure: as soon as practicable, and no later than 30 days after you learn that customer information was, or likely was, accessed or used without authorization	248.30(a)(4)(iii)	A procedure step that records the date you became aware	☐ Yes ☐ Partial ☐ No
A notice letter template with the required contents, and a memo template for documenting a decision not to notify	248.30(a)(4)(i), (iv)	Both templates, ready to fill in	☐ Yes ☐ Partial ☐ No
A tabletop exercise that walks your team through an incident	Practice	Written results and the fixes that came out of it	☐ Yes ☐ Partial ☐ No

3. Vendors with Access to Client Data

Item	Rule	Proof to keep	Result
A list of every service provider that can access customer information. Review IT support, email, CRM, planning tools, backup, and e-signature, and decide on your custodian from the facts of the relationship	248.30(a)(5), (d)(10)	The inventory, with what each vendor can reach	☐ Yes ☐ Partial ☐ No
Due diligence before you sign, and monitoring after	248.30(a)(5)(i)	Security reports you reviewed, with your notes	☐ Yes ☐ Partial ☐ No
Each vendor's commitment to tell you within 72 hours of becoming aware of a breach of a system it maintains that holds your customer information	248.30(a)(5)(i)(B)	The contract clause, addendum, or written commitment	☐ Yes ☐ Partial ☐ No

4. Everyday Proof

Item	Rule	Proof to keep	Result
Disposal rules for paper, laptops, phones, and copier drives	248.30(b)	The written policy and disposal records	☐ Yes ☐ Partial ☐ No
Records showing who reviewed sign-in alerts, backups, and security warnings, and when	Supports (a)(3)	Recent reports or tickets	☐ Yes ☐ Partial ☐ No
Multi-factor authentication on email, your custodian portal, and your CRM. The rule does not name it; it is a common baseline control	Practice	Settings screenshots or an admin report	☐ Yes ☐ Partial ☐ No
The records Regulation S-P requires, kept in an easily accessible place for five years from the end of the fiscal year of the last entry, the first two in your office	Rule 204-2(a)(25), (e)(1)	A records index that points to each one	☐ Yes ☐ Partial ☐ No

Massachusetts firm, or clients in Massachusetts? 201 CMR 17.00 also requires a written information security program. Our Massachusetts WISP checklist covers it (saberguard.tech/resources).

Want the full list? The Regulation S-P checklist has 42 items, each with the rule paragraph and the proof to keep.

ABOUT

About This Checklist

A short checklist for advisers newly registered with the SEC, built from the text of the amended Regulation S-P (17 CFR 248.30) and the Advisers Act compliance and recordkeeping rules. Each item names the paragraph it comes from. For the full list, use the SaberGuard Regulation S-P Cybersecurity Checklist (42 items).

How to use it

- Work through it with whoever runs IT for the firm. The vendor and monitoring items need that person's answers.
- Fill in the proof for every Yes. If you cannot point to a document, a report or a setting, mark it No.
- Fix anything that could cause a missed client notice first: the notice procedure and the 72-hour vendor commitments.
- Run it again before each exam, at your annual compliance review, and after any incident or new vendor.

Before you rely on it

This checklist reflects 17 CFR 248.30 as amended in 2024 and Rules 206(4)-7 and 204-2, as published on eCFR in November 2026. It is not legal advice and it does not certify compliance. Massachusetts law (201 CMR 17.00 and M.G.L. c. 93H) can add requirements; have counsel confirm notification decisions.

Free to use

Use it, change it and share it inside your firm. If you want to go through it with someone, Jonathan DeLeon of SaberGuard keeps 15-minute slots for new advisers at book.saberguard.cloud/jonathan.

Jonathan DeLeon, CISM, CCSP

SaberGuard, LLC | jonathan.deleon@saberguard.tech | saberguard.tech