EMRY NETWORKS
IT Solutions That Click

2026 WEALTH MANAGEMENT & RIA AUDIT GUIDE • AMENDED SEC REG S-P • FINRA 4370 (MEMBERS)

Wealth Advisor & RIA SEC Regulation S-P & Rule 204-2 Books-and-Records Checklist

10 Cybersecurity & Vendor Oversight Controls for the Amended SEC Regulation S-P 72-Hour Service Provider Notice & 30-Day Client Notification Rules.

REG S-P (2025/2026) • SEC RULE 204-2

72-Hour SLA	30-Day Rule	100% WORM	4 Minutes
Mandatory Vendor Breach Notice	SEC Reg S-P Client Notification	Immutable Comms Archive (204-2/17a-4)	24/7 Identity Token Containment

WHAT'S INSIDE

- How to use this checklist and assessment details — p. 2
- 1 The 10 controls: status, owner, target date and evidence — p. 3
- 2 Your results and open items — p. 5
- Rules cited, related resources and next step — p. 6

Book a 30-Minute Risk Assessment →

USING THE INTERACTIVE VERSION

- **Type in any shaded box.** Press Tab to move to the next one.
- **Blue-outlined boxes are drop-downs** for each control's status.
- **Grey boxes calculate themselves:** the counts, readiness % and open items on your Results page.
- **Best in Adobe Acrobat Reader (free)** or another desktop PDF app. Browser viewers and Apple Preview let you type, but may not run the calculations; you can type those values in yourself.
- **Use the links** in the contents list, the header (Contents, Results) and the bookmarks panel to jump around.
- **Save often.** Prints on US Letter, landscape; the on-screen buttons do not print.

Print checklist | Clear all entries

STATUS KEY

In place: Implemented today and you can show evidence. Earns all of the control's points.
Partial: Started, or covers only some users, systems or sites. Earns 40% of the control's points.
Gap: Not in place yet. Earns 0 points, the same as a control you have not marked.

How to use this checklist

Reg S-P · Rule 204-2

1. Mark a status for each control. Use the drop-down next to each of the 10 controls: In place, Partial or Gap.

2. Assign the work. For anything Partial or a Gap, name an owner and a target date.

3. Note the evidence. Say where the proof lives (policy, screenshot, report, contract), so you can produce it on request.

4. Review your results. The Results page counts your answers, works out a weighted, self-rated readiness % and lists the open items.

5. Get a second opinion. Bring the results to a 30-minute risk assessment if you want an outside review.

Assessment details

Firm / legal entity		**Date completed**	
Completed by (name, title)		**Next review date**	
Systems, offices or sites in scope		**Reviewed with (IT provider, counsel, assessor)**	

The controls at a glance

01 Written Incident Response Program & 30-Day Customer Notification Workflow
02 Mandatory 72-Hour Service Provider Breach Notice Addendum
03 Phishing-Resistant FIDO2 Hardware MFA on Custodian & Portfolio Portals
04 Immutable Communications Archiving (RIAs: Rule 204-2 / Broker-Dealers: Rule 17a-4)
05 4-Minute 24/7 MDR Identity & Endpoint Isolation
06 Executive Mobile Device Management (MDM) & Remote Container Wipe
07 Wire & Disbursement Fraud Verification Protocol
08 Proper Disposal & Sanitization of Customer Information
09 Sub-24-Hour CISA KEV Edge & Remote Access Patching (Emry Recommended)
10 Quarterly CCO Examination Binder & Annual Tabletop Documentation

Disclaimer

This checklist is an educational self-check, not legal advice, a certification, or a formal assessment. Confirm requirements against the current regulation, your contracts, and your assessor or counsel. © 2026 Emry Networks.

1 The 10 controls

Reg S-P · Rule 204-2

For each control, pick a status, then add an owner, a target date and where the evidence lives. Your answers feed the Results page.

01. Written Incident Response Program & 30-Day Customer Notification Workflow

Establish a documented Incident Response Plan meeting amended SEC Reg S-P mandates, including assessment procedures and 30-day affected-client notification templates.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

02. Mandatory 72-Hour Service Provider Breach Notice Addendum

Enforce written contracts requiring all IT, custodian, CRM, and portfolio cloud vendors to notify your CCO within 72 hours of any unauthorized customer data access.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

03. Phishing-Resistant FIDO2 Hardware MFA on Custodian & Portfolio Portals

Block Adversary-in-the-Middle (AiTM) token theft across Schwab Advisor Center, Fidelity Wealthscape, Orion, Black Diamond, eMoney, Redtail, and Microsoft 365.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

04. Immutable Communications Archiving (RIAs: Rule 204-2 / Broker-Dealers: Rule 17a-4)

RIAs must keep required written communications under Advisers Act Rule 204-2 (five years, the first two in an appropriate office); Rule 17a-4 WORM or audit-trail storage applies to broker-dealers. Emry recommends immutable archives of advisor email, Microsoft Teams, Slack, Zoom, and approved SMS/mobile channels.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

05. 4-Minute 24/7 MDR Identity & Endpoint Isolation

Continuously monitor advisor laptops and cloud sessions for impossible-travel logins, unauthorized inbox forwarding rules, and anomalous bulk client-list downloads.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

06. Executive Mobile Device Management (MDM) & Remote Container Wipe

Enforce Intune/Jamf MDM with biometric lock, hardware encryption, and selective corporate container wipe on every advisor iPhone, iPad, and MacBook.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

07. Wire & Disbursement Fraud Verification Protocol

Combine DMARC p=reject anti-spoofing, Proofpoint/Avanan BEC behavioral AI, and out-of-band identity verification before any client ACAT or wire instruction.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

08. Proper Disposal & Sanitization of Customer Information

Maintain NIST SP 800-88 cryptographic erasure certificates for decommissioned advisor laptops, SSDs, and local scanner storage under Reg S-P Disposal Rules.

STATUS · 5 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

09. Sub-24-Hour CISA KEV Edge & Remote Access Patching (Emry Recommended)

Eliminate exposed office VPNs and patch critical workstation/browser/gateway vulnerabilities within 24 hours of disclosure with automated compliance timestamps. CISA's KEV deadlines bind federal civilian agencies only; for advisers they are a recommended best practice.

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

10. Quarterly CCO Examination Binder & Annual Tabletop Documentation

Generate turnkey SEC Division of Examinations evidence packages showing 365-day log retention, vendor due diligence, and quarterly tabletop sign-off. FINRA Rule 4370 business continuity plans apply only to FINRA member firms (e.g., dually registered broker-dealers).

STATUS · 3 PTS | OWNER | TARGET DATE

EVIDENCE / NOTES (where the proof lives)

2 Your results and open items

Calculated from the 10 controls

These totals fill in automatically from your answers in Adobe Acrobat Reader and most desktop PDF apps. If a box stays blank in your viewer, count from the controls pages and type or write the number in. Readiness is your own self-assessment, not a compliance determination.

In place	Partial	Gap	Assessed (controls marked)	Readiness (self-rated)	Gaps and partials with no owner

Points:

Readiness = points earned ÷ points available. Each control is worth 5, 3 or 1 points (shown next to its status). In place earns all of its points, Partial earns 40%, and a Gap or an unmarked control earns 0, so the score climbs from 0% as you mark controls.

Open items to close (calculated: Gaps first, then Partials, with owner and target date)

Sign-off

Reviewed by (name, title)	
Signature / date	
Date of next review	

Rules and documents cited in this checklist

Official sources for the rules, standards and documents named in the controls above. Check them for updates before relying on any requirement.

SEC final rule: Regulation S-P amendments (Release 34-100155, File S7-05-23): https://www.sec.gov/rules-regulations/2024/06/s7-05-23
Regulation S-P, 17 CFR Part 248, Subpart A (eCFR): https://www.ecfr.gov/current/title-17/chapter-II/part-248/subpart-A
Advisers Act Rule 204-2, 17 CFR 275.204-2 (eCFR): https://www.ecfr.gov/current/title-17/chapter-II/part-275/section-275.204-2
Exchange Act Rule 17a-4, 17 CFR 240.17a-4 (eCFR): https://www.ecfr.gov/current/title-17/section-240.17a-4
FINRA Rule 4370 (Business Continuity Plans): https://www.finra.org/rules-guidance/rulebooks/finra-rules/4370
NIST SP 800-88, Guidelines for Media Sanitization: https://csrc.nist.gov/pubs/sp/800/88/r2/final
CISA Known Exploited Vulnerabilities (KEV) Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Sources for the figures on the cover

72-hour SLA: 17 CFR 248.30(a)(5)(i)(B): service providers must notify the covered institution as soon as possible, but no later than 72 hours after becoming aware of a breach.
https://www.ecfr.gov/current/title-17/chapter-II/part-248/subpart-A/section-248.30
30-day rule: 17 CFR 248.30(a)(4)(iii): notice to affected individuals as soon as practicable, but not later than 30 days after becoming aware.
https://www.ecfr.gov/current/title-17/chapter-II/part-248/subpart-A/section-248.30
Compliance dates: Larger entities Dec. 3, 2025; smaller entities June 3, 2026 (SEC small entity compliance guide).
https://www.sec.gov/files/rules/final/2024/regulation-s-p-small-entity-compliance-guide.pdf
Rule 204-2 retention: 17 CFR 275.204-2(e)(1): five years, the first two in an appropriate office of the adviser. https://www.ecfr.gov/current/title-17/chapter-II/part-275/section-275.204-2

Related Emry Networks resources

RIA SEC Regulation S-P Checklist (web page): https://www.emrynetworks.com/ria-sec-reg-s-p-checklist
IT security for wealth advisors and RIAs: https://www.emrynetworks.com/services/regulated-industries/wealth-advisors-rias
All resources: https://www.emrynetworks.com/resources

Want a second set of eyes before your next exam?

Emry Networks helps RIAs and wealth managers put these controls in place and keep the evidence an examiner will ask for. Call (603) 202-3200 or Book a 30-Minute Risk Assessment.

EMRY NETWORKS • DEFENSIBLE IT, 24/7 MDR & LIVE COMPLIANCE ENGINEERING
Jacksonville, FL & Manchester, NH Operations Hubs • Serving Regulated SMBs Across All 50 States • (603) 202-3200 • www.emrynetworks.com/contact-us

Book a 30-Minute Risk Assessment →

Print checklist Clear all entries