

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

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

72-Hour SLA

Mandatory Vendor Breach Notice

30-Day Rule

SEC Reg S-P Client Notification

100% WORM

Immutable Comms Archive (204-2/17a-4)

4 Minutes

24/7 Identity Token Containment



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

[] PASS [] GAP / REMEDIATE

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



02. Mandatory 72-Hour Service Provider Breach Notice Addendum

[] PASS [] GAP / REMEDIATE

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.



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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.



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

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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



07. Wire & Disbursement Fraud Verification Protocol

[] PASS [] GAP / REMEDIATE

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



08. Proper Disposal & Sanitization of Customer Information

[] PASS [] GAP / REMEDIATE

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



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

[] PASS [] GAP / REMEDIATE

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.



10. Quarterly CCO Examination Binder & Annual Tabletop Documentation

[] PASS [] GAP / REMEDIATE

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).