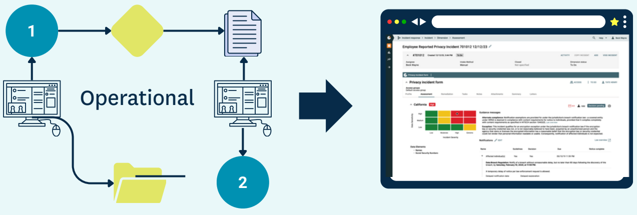
RadarFirst

EXECUTIVE ESCALATION MEMO

Regulation S-P: Enterprise Risk and Control Architecture Implications

WHAT CHANGED:



The SEC's amended Regulation S-P framework converts incident response into a documented supervisory control.

This elevates privacy incident handling from an operational function to a governance issue.

The exposure is no longer limited to the timing of breach notification.

The exposure is whether the firm's decision-making architecture is structured, consistent, and demonstrable under examination.

WHY THIS IS AN EXECUTIVE-LEVEL ISSUE

Regulation S-P now requires firms to prove:

- When awareness occurred
- How harm was evaluated
- Why were notification decisions made
- How vendor incidents were escalated
- Whether similar events were treated consistently
- Whether records are preserved in accordance with SEC standards

These requirements cut across:

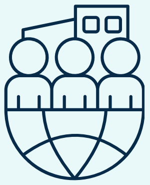
- IT and Security
- Legal
- Compliance
- Vendor Management
- Operations

Fragmented ownership increases regulatory risk.
This is not a departmental issue. It is a control architecture issue.

ENTERPRISE EXPOSURE PATTERNS

In larger organizations, risk most often arises from:

- Inconsistent decision logic across business units
- Separate systems used for detection, analysis, and documentation
- Decentralized vendor management
- Manual deadline tracking
- Lack of centralized supervisory visibility



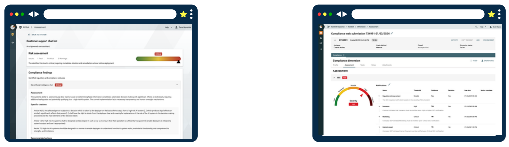
In smaller organizations, risk most often arises from:

- Lean staffing
- Informal awareness capture
- Manual documentation
- Dependence on third-party vendors

The regulatory standard does not vary by size.

GOVERNANCE QUESTION FOR LEADERSHIP

Does the firm manage incident response through coordinated email and spreadsheets?



Or through a structured, centralized, regulator-grade decision framework?

Under the amended rule, inconsistency itself can become a supervisory finding.

CONTROL STANDARDIZATION AS RISK MITIGATION

A DEFENSIBLE REGULATION S-P POSTURE REQUIRES:

- Centralized incident intake
- Defined decision logic
- Automated timeline controls
- Integrated vendor escalation logging
- Time-stamped documentation
- Reproducible audit trail

This is not automation for efficiency.
It is infrastructure for defensibility.

Radar Privacy™

Radar Privacy operationalizes Regulation S-P into a centralized system of record for incident decisions. It standardizes decision logic across business units, integrates vendor oversight into workflow, enforces timeline controls, and preserves regulator-ready documentation. The outcome is enterprise-level control visibility and reduced supervisory exposure.

LEARN MORE

WWW.RADARFIRST.COM