waystone | Compliance Solutions

Preparing for Regulation S-P Exams in 2026: SEC Priorities and Key Takeaways from the January 2026 Outreach Session

Julie Majka January 27, 2026

On January 22, 2026, the SEC's Division of Examinations held a detailed outreach session to highlight expectations under the amended Regulation S-P and to help advisers understand how the updated safeguarding and incident response requirements will be evaluated during examinations.

The program featured staff from the Division of Examinations' technology teams and offered clear insights into the SEC's priorities for firms of all sizes. This session provided important clarity on how the SEC intends to assess Regulation S-P compliance throughout 2026 and highlighted the areas where firms should expect deeper scrutiny. This session provided important clarity on how the SEC intends to assess Regulation S-P compliance throughout 2026 and highlighted the areas where firms should expect deeper scrutiny.

The SEC noted that this session marked the conclusion of its recent series of public outreach events and was structured to be especially relevant to smaller advisers with less than $1.5 billion in assets under management, while reinforcing that amended Regulation S-P is a top supervisory priority across the industry.

Expanded Definition of Customer Information and Compliances Dates

The SEC began with historical context, noting the expanded definition of customer information under the amended rule. The scope now captures any nonpublic personal information, including customer information received from other financial institutions, as well as information handled in the course of acting as a financial institution. This expanded definition is a significant shift that firms should incorporate into their compliance planning and data governance programs.

The staff then outlined the agency's forward-looking approach, including upcoming risk alerts and additional publications that firms can use as reference points. Importantly, firms were reminded of the compliance dates that frame implementation efforts: larger entities were expected to meet the December 3, 2025, deadline, and smaller entities are expected to comply by June 3, 2026.

How Examiners Approach Technology Related Reviews

The central focus of the discussion involved how examiners approach technology-related reviews. According to the SEC, the examination process is not changing structurally; rather, the emphasis is on understanding each firm's operational workflow, the nature of its business lines, where its customer information resides, and how data moves through the organization. Examiners will look closely at a firm's staff structure, physical and virtual office footprint, and the way client data is ingested and ultimately decommissioned when retention requirements no longer apply. They will also evaluate how firms monitor, track, and secure data across its lifecycle.

Expectations for Smaller Advisers

For smaller firms, the SEC acknowledged that technology practices vary widely. Examiners will assess data-protection controls in the context of the firm's size, complexity, and reliance on custodians or other service providers. The agency stressed that smaller advisers must still maintain policies and procedures that accurately reflect their operational model and the types of customer information their providers hold. The SEC noted that proportionality does not reduce the expectation that firms understand and document how customer information is protected within their specific operational model.

Risk Management Program Expectations

The SEC also emphasized that examinations will look closely at each firm's risk-management program. **Examiners expect to see a risk matrix or similar risk-assessment program that identifies risks, assigns risk levels, and maps mitigation strategies.** The staff noted that **cyber security and technology risks are often not adequately included** in firm assessments,

Key expectations include the following:

- Capturing criticality, business impact, and likelihood of occurrence
- Updating risk assessments periodically to reflect evolving business lines
- Maintaining documentation showing how risks are tracked and addressed over time.

While no single methodology is mandated, the staff pointed to established frameworks such as the NIST Cybersecurity Framework as useful reference points when organizing a thorough assessment, and encouraged advisers to consider their specific services, office locations, and network architecture when calibrating scope and depth.

Service Provider Oversight Requirements

Service provider oversight remains a significant exam priority. The SEC reiterated that registrants, not vendors, retain responsibility for protecting customer data.

The staff expects firms to conduct both initial and continuing due diligence. This includes ensuring that service providers can meet breach-notification requirements, support contractual obligations, and maintain controls consistent with the rule. The SEC noted that firms may rely on attestations or structured service agreements but must take responsibility for understanding vendor risks and ensuring continued engagement. They also commented on **instances where firms lacked log data to prove whether a breach had occurred**, highlighting the importance of maintaining tools that can demonstrate whether client data was impacted. The staff urged firms to remember that **it is not enough to purchase a solution–firms must enable the necessary modules and configure the tools properly**, and that it can be **helpful to engage a third party, independent of the vendor, to validate what the vendor is doing.** The SEC also wants firms to consider **fourth party risks**, particularly when a vendor outsources part of its operations without the firm's awareness.

Relevant SEC Resources

The session included an overview of SEC resources that registrants should consider, including the following Risk Alerts:

- April 2023 Risk Alert Risk Alert: Safeguarding Customer Records and Information at Branch Offices: Focused on protection of data at branch offices (still relevant even for firms without branch offices), including:
  - Patching
  - Email configuration
  - Use of service providers.
- Other Risk Alerts:
  - Cloud storage and ransomware (May 2019 – September 2020). OCIE Risk Alert – Network Storage.pdf
  - Risk Alert – Ransomware.pdf

- January 2020 SEC examination report: Cybersecurity and reliance on reports; OCIE Cybersecurity and Resiliency Observations 2020
  - Mobile security and data-loss prevention considerations.

Initial Document Request (as presented during the January 22 SEC Outreach Session)

At the beginning of a Regulation S-P examination, the SEC explained that examiners are likely to request a defined set of core materials to understand a firm's safeguarding program, technology environment, and incident-response readiness.

During the session, the staff presented the following items:

General Request Items

- Registrant Compliance Manual
- Written Policies & Procedures addressing administrative, technical, and physical safeguards for the protection of customer information
- Information Technology Managed Service Provider Contract
- Organization Charts
- Risk Assessments related to technology/cybersecurity risk, controls, threats, and vulnerabilities

These documents provide examiners with baseline information about the firm's structure, governance, oversight relationships, and how safeguarding responsibilities are operationalized.

Incident Response – Specific Requests

Examiners are likely to request:

- Incident Response (IR) Plan including the firm's documented program to detect, respond to, and recover from unauthorized access to or use of customer information, such as customer-notification procedures
- Procedures supporting the IR Plan including policies and procedures that demonstrate how the registrant detects incidents, escalates them internally, assesses scope, contains the issue, and manages recovery activities
- Listing of staff, vendors, contractors, or other persons responsible for incident-response activities and should clarify who performs which IR functions, including internal personnel and external service providers
- Listing of all tools that facilitate detection and monitoring of the registrant's environment including a current inventory of the monitoring infrastructure (e.g., EDR, SIEM, DLP, email security, IDS/IPS, vulnerability scanning)
- Monitoring evidence that confirm the firm's information systems, networks, and personnel activity to detect incidents are enabled and functioning properly
- Documentation related to any security incidents during the review period to show that the firm followed its IR program for each event, including step-by-step response, investigation findings, customer-notification determinations, and any remediation or "lessons learned."

Data Location and Mapping

While a formal data-mapping matrix is not required by rule, examiners are likely to request either a matrix **or** an equivalent narrative explanation showing where customer information is stored, how it is ingested (e.g., email), whether it resides on-premises, in the cloud, with custodians, or with other service providers, and how and when it is decommissioned.

What to Expect During a Regulation S-P Examination

The SEC also provided a detailed explanation of what firms should expect during a Regulation S-P examination. The workflow begins with the SEC's internal risk assessment used to determine the scope of the exam. Firms will receive an initial document request, which is the first step in the review process.

Examiners will review the submitted materials, conduct interviews–preferably in person–and test whether the firm's practices align with written policies and procedures. Follow-up requests may occur if additional clarification is needed. At the conclusion of the exam, the SEC may share observations, when applicable, to provide firms with an opportunity to enhance their compliance programs.

During the mock exam discussion, the SEC explained that exam teams will evaluate how well the firm understands its risk areas and where improvement is needed. They will review websites, historical and current exams, regulatory filings, and complaints to gain a holistic understanding of the firm. Examiners may initiate the review with either an introductory meeting or a direct document request. They will want to see evidence of the tools used to detect and monitor for potential breaches and the reports that demonstrate ongoing oversight and anomaly remediation. Firms should expect questions about the incident response program, the steps taken during incidents, and the root-cause analysis process. In addition to describing how data is protected, firms should be prepared to show where customer information actually resides across systems and environments.

Interview Expectations

The SEC also described its expectations regarding interviews. While personnel titles may differ, firms should ensure that knowledgeable individuals are available to address questions about technology, data ingestion, email infrastructure, data-loss-prevention controls, custodian-managed data, and cloud-based environments. Examiners may ask firms to produce a data-mapping matrix or an equivalent explanation of where data resides. They may also inquire about meeting frequency with service providers, exposure to fourth-party risk, patch-management practices, and the activation status of security-tool modules.

Common Examination Findings

Common examination findings were also discussed. The SEC noted that firms often maintain policies that are not designed to meet Regulation S-P requirements or have policies that are not effectively implemented. Before issuing a deficiency letter, exam teams will meet with the registrant to clarify findings and address any misunderstandings.

Q & A Highlights

During the Q&A portion, the SEC addressed the broad definition of service providers under the rule, confirming that any entity that receives or processes customer information is a service provider, with no exclusions. The staff also reiterated that risk matrices for small firms may leverage different frameworks and none are prescriptive, and reminded firms that helpful resources include risk alerts, historical Reg S-P videos, the adopting release, and the Small Entity Compliance Guide.

Conclusion

As the SEC moves firmly into the examination phase of the amended Regulation S-P, firms should expect heightened scrutiny of their safeguarding programs, incident-response readiness, and service-provider oversight. The January 22 session made clear that examiners are looking not only for well-written policies, but for evidence that those policies are fully implemented, monitored, and aligned with each firm's unique operational realities. By preparing early, documenting clearly, and maintaining strong engagement with service providers and internal stakeholders, firms can position themselves to navigate upcoming exams with confidence.

How Waystone Can Help

Waystone supports advisers in building and maintaining robust, Regulation S-P-aligned compliance frameworks that are tailored to the size, complexity, and technology footprint of the firm.

Our US Compliance Solutions and Cyber Security Solutions team can assist with:

- Enhancing written policies and procedures
- Reviewing incident-response programs
- Strengthening service provider oversight documentation
- Prepare for examinations by conducting mock reviews
- Conduct Risk Assessments to identify vulnerabilities in current systems and prioritize updates
- Service Provider Oversight in real time using best-in-class third-party risk management platform OneTrust.

If you have any questions or want to learn more about how Waystone can help you prepare for the June 2026 compliance deadline or meeting the amended Regulation S-P requirements, please reach out to your usual Waystone representative or contact us via the link:

Contact us →