2025 // 2026

Visory

Future-Proofing Compliance & Cybersecurity

An E-Guide on What RIAs Need to Know Now

AUTHORED BY

Tammy Jutras
Director of Cybersecurity Services, Visory

Leila Shaver
Founder, My RIA Lawyer

Inside

In 2025, the SEC withdrew proposed rules around outsourcing, custody, and cybersecurity—moves that were largely welcomed by firms weary of prescriptive mandates. However, regulatory relief doesn't equal reduced responsibility.

Cybersecurity and legal compliance experts Tammy Jutras (Visory) and Leila Shaver (My RIA Lawyer) agree: now is the time for RIAs to modernize their internal frameworks and reaffirm best practices. Regulatory expectations haven't vanished—they've evolved.

This guide offers practical, actionable insight to help firms move beyond compliance as a checklist—and toward a proactive strategy for resilience and growth.

Why the Pullback Doesn't Mean "No Compliance"

> "Just because some rules were withdrawn doesn't mean the SEC has stopped caring about the risks they were meant to address."
>
> **— Leila Shaver**

The SEC may have halted specific rule proposals, but its focus on risk management, investor protection, and fiduciary responsibility remains intact. The reality is that many withdrawn proposals were rooted in principles that are already enforceable under existing law.

"Even though the prescriptive cybersecurity and outsourcing rules were withdrawn, the fiduciary framework hasn't changed," says Shaver. "Firms are still expected to demonstrate that they're acting in their clients' best interests—and that includes protecting sensitive data and vetting third-party vendors."

Her advice? Stay vigilant. "Don't pause your compliance strategy—update it."

A Cybersecurity Wake-Up Call

> "Cyber threats don't wait for formal rulemaking. Your infrastructure and controls need to evolve constantly."
>
> **— Tammy Jutras**

Jutras warns against mistaking regulatory inaction for risk mitigation. Cyberattacks remain a top threat to RIAs of all sizes—especially smaller firms that may lack robust defenses.

Top cybersecurity risks include:

Phishing and Business Email Compromise (BEC)
Still, the most common and costly vector.

Unvetted Third-Party Access
Vendors handling sensitive client or firm data can be high-risk entry points.

Shadow IT and Unsanctioned AI Use
Employees deploying tools outside of IT visibility can compromise firm-wide protections.

"The key is to align cybersecurity efforts with real-world threats —not just compliance deadlines," Jutras says.

Vendor Oversight Isn't Optional

> "You can outsource services, but not accountability."
>
> **— Leila Shaver**

Even without a rule mandating enhanced vendor oversight, regulators expect firms to identify and mitigate third-party risks. Both experts agree that a lapse in vendor due diligence could carry significant regulatory and reputational consequences.

Shaver adds that when vendors handle client PII or impact operational continuity, your oversight obligations increase. "If a third-party fails you, the SEC still holds you accountable," she says.

Jutras's Recommendations

- Maintain a vendor inventory including access levels and data scope.
- Use formal agreements that define expectations, confidentiality, breach notification, and audit rights.
- Conduct annual due diligence, including reviewing SOC 2 reports or independent assessments.
- Integrate vendor risk into your incident response plan, including notification protocols.

"Compliance isn't just a checklist—it's a mindset."

— Leila Shaver

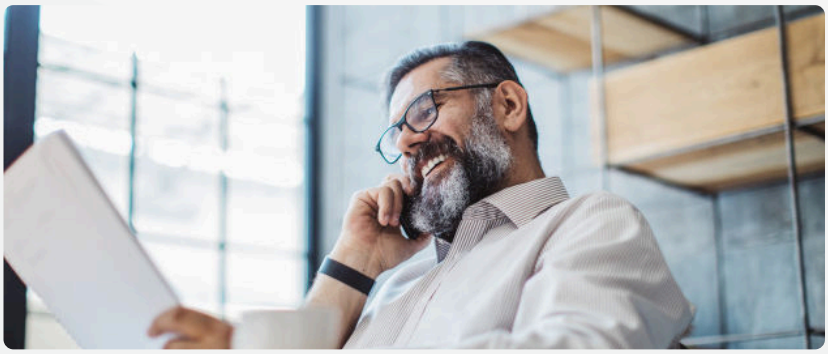
Turn Compliance Into a Culture

A common shortfall, especially among growing firms, is treating compliance as an annual event rather than an ongoing business function. According to Shaver, the most successful RIAs operationalize compliance throughout their organization.

"Even solo advisors must document their policies and processes," Shaver notes. "Smaller firm size doesn't exempt you from regulatory scrutiny."

Build a Culture of Compliance

Leadership Buy-In	Senior management must prioritize and model compliance behaviors.
Ongoing Training	Establish a cadence of quarterly sessions and document employee participation.
Embedded Workflows	Make sure compliance checkpoints are part of vendor onboarding, data governance, and new hire orientation.



What's Next: Regulation S-P & AML

Two major rule updates are scheduled to go live:

Regulation S-P (December 2025)
Requires firms to implement a formal data breach response plan.

Anti-Money Laundering (AML) Rule (January 2026)
Mandates the detection and reporting of suspicious activity, even for smaller firms.

"These are real and enforceable," says Jutras. "Firms that treat them as 'future problems' risk being caught flat-footed."

Key Actions to Prepare

- Assign clear roles across leadership, compliance, IT, and operations.
- Update and test your incident response plan, including communication flows and vendor integration.
- Run tabletop exercises to simulate a breach and assess team readiness.

From a legal perspective, Shaver emphasizes documenting your decision-making process. "If the SEC comes knocking, they'll want evidence—not intent," she says.

The Business Case for Compliance

> "Compliance done right is a **differentiator**."
>
> **— Leila Shaver**

Many firms view compliance as a drain on resources—but both Shaver and Jutras argue that proactive compliance enhances business value.

"We've worked with firms where strong documentation helped them close deals faster or attract new clients," says Jutras. "That's the ROI."

Strategic Advantages

- Reduces regulatory risks and fines
- Accelerates M&A or succession planning
- Inspires client trust
- Boosts operational efficiency
- Improves vendor relationships

Common Gaps & How to Fix Them

From firsthand client experience, Shaver and Jutras identify frequent trouble spots and how to remediate them.

TOP GAPS

Missing or outdated vendor agreements

No formal cybersecurity governance

Inconsistent training and documentation

Weak or nonexistent incident response plans

Failure to leverage technology to track compliance

BEST PRACTICES

Schedule quarterly compliance reviews

Use frameworks like NIST or ISO for cybersecurity planning

Involve legal and IT early—not only during audits

Implement workflow tools to standardize documentation and accountability

"You don't need to do it all at once," says Jutras. "Start with high-risk areas and build outward."

Cybersecurity Myth-Busting

MYTH #1 **"We're too small to be a target."**

"Small firms are often the most vulnerable," says Jutras. "Bad actors know they're less likely to have detection and response systems."

MYTH #2 **"If the rule was withdrawn, we don't need to worry."**

"The absence of a rule doesn't remove your fiduciary duty," says Shaver. "Expect the SEC to ask: what did you do to protect clients—regardless of regulation?"

Tools & Resources to Bookmark

Both experts recommend building these resources into quarterly leadership meetings:

- NIST Cybersecurity Framework
- Regulation S-P Final Rule
- FFIEC IT Examination Handbook
- Vendor Due Diligence Checklist
- AML Risk Assessment Template
- Incident Response Playbooks
- Compliance Calendar (internal or third-party)

These are internal documents that your company should create with guidance from compliance experts.

"Quarterly isn't just a suggestion—it's a rhythm that keeps you ahead," says Jutras.

Final Word from the Experts

"Future-proofing cybersecurity starts with culture. Tools help, but leadership is what sustains it."

Tammy Jutras

"Compliance is the cost of entry—but doing it well is how you grow."

Leila Shaver

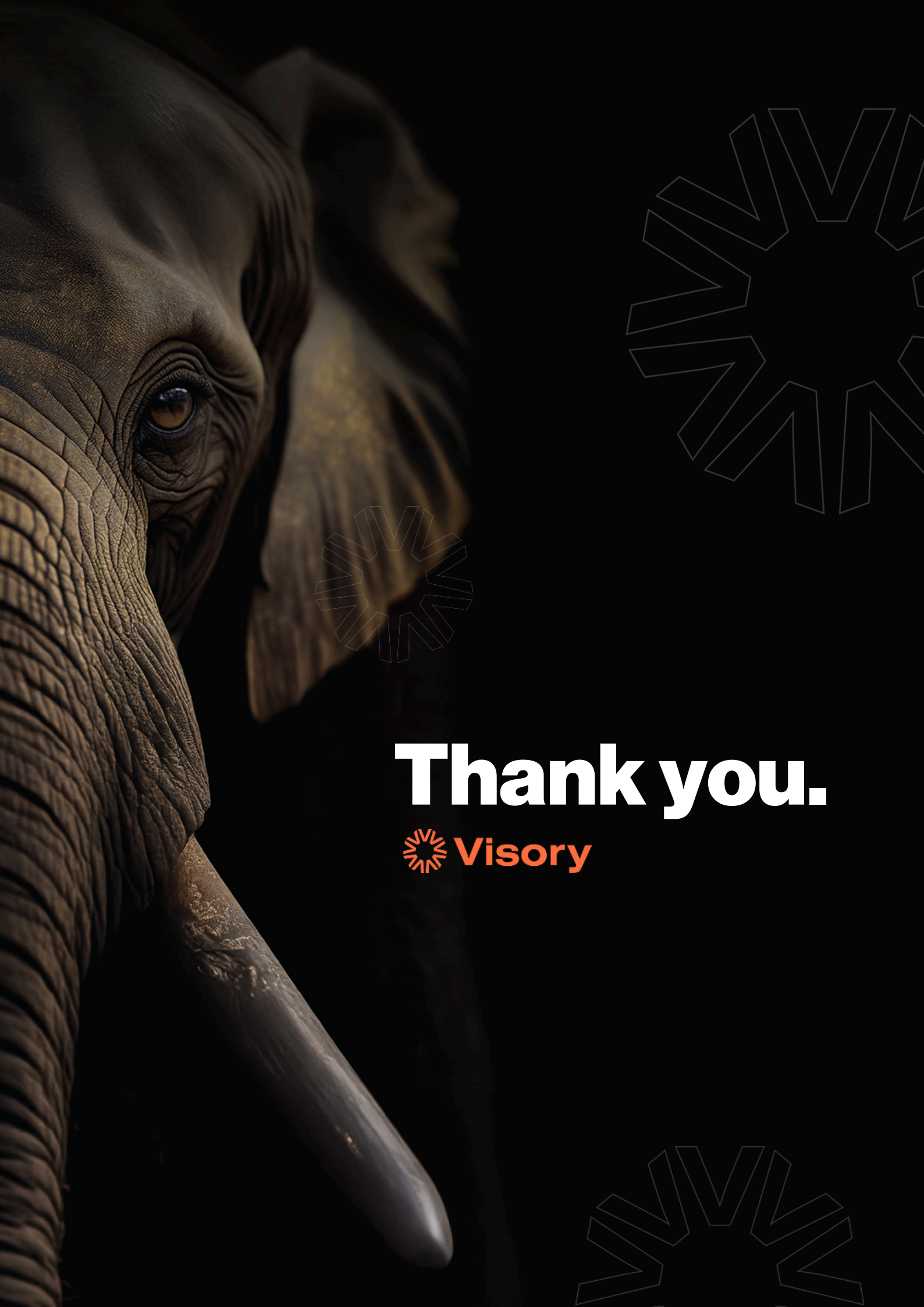
About the Authors

Tammy Jutras is the Director of Cybersecurity Services at Visory, helping RIAs modernize their IT environments while maintaining secure and compliant infrastructure tailored to their size and needs.

visory.net

Leila Shaver is the Founder of My RIA Lawyer, a boutique legal and compliance firm supporting RIA growth with regulatory guidance, legal strategy, and practical implementation support.

myrialawyer.com


Thank you.
Visory