

# RESILIENCE UNDER REGULATION:

Regulatory Pressure &  
Compliance Fatigue in  
Financial Services



New research reveals how growing regulatory pressure is straining cybersecurity and compliance in the financial sector – and how modernization and managed partnerships can transform compliance into proof of resilience.



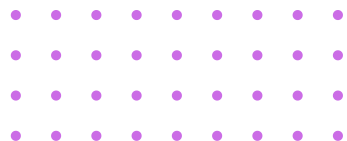
# Table of Contents

|                                              |    |
|----------------------------------------------|----|
| Executive Summary                            | 03 |
| Regulatory Pressure Is Mounting              | 04 |
| Compliance Fatigue Across Financial Services | 05 |
| Manual Processes: Compliance at a Standstill | 06 |
| Uncertain Signals from Regulators            | 07 |
| From Manual to Managed: The MSSP Advantage   | 08 |
| Modernization as the Compliance Multiplier   | 09 |
| What Firms Want from Compliance Technology   | 10 |
| Conclusion: Proof Over Promises              | 11 |
| About Omega Systems                          | 12 |
| Survey Methodology                           |    |





of financial executives cite staying current with evolving requirements as their biggest compliance roadblock



# Executive Summary

For U.S. financial institutions, the compliance burden has become inseparable from cybersecurity. From the SEC’s new disclosure rule to NYDFS Part 500 and FINRA’s expanding oversight, regulators have turned resilience into a baseline requirement – not a best practice.

Omega Systems’ 2025 Financial Services IT and Cybersecurity Survey of more than 300 executives reveals the growing strain:

- 42% cite staying current with evolving requirements as their biggest compliance roadblock.
- 36% lack sufficient internal compliance expertise.
- 29% say budgets are stretched too thin.
- 54% still rely on spreadsheets or in-house tools to benchmark security controls.

**The result is compliance fatigue** – where the pressure to keep pace with regulation outstrips the resources to execute. When confidence is the currency of finance, compliance is what keeps it in circulation.

# Regulatory Pressure Is Mounting

Over the past 18 months, the U.S. has seen an unprecedented tightening of cybersecurity oversight.

The SEC's Cybersecurity Disclosure Rule now requires public companies to report material incidents within **four business days**.

NYDFS Part 500 mandates **annual certification, executive accountability, and continuous monitoring** for New York-registered entities.

The FTC Safeguards Rule and FFIEC Cybersecurity Assessment Tool continue to **widen expectations** for financial institutions that manage consumer data.

FINRA has expanded its business continuity guidance to include **documented cybersecurity testing**.


Together, these frameworks are redefining compliance as **proof – not policy**.

In fact, many firms acknowledge they're struggling to meet these accelerated expectations. More than one-third (35%) of our survey respondents say it would take a week or longer to detect and contain a security breach – a timeline that would put firms out of step with new disclosure requirements. Detection delay has become not just a security weakness, but a compliance liability.

 **Detection delay has become not just a security weakness, but a compliance liability.**

More than one-third of our survey respondents say it would take a **week or longer to detect and contain a security breach**



# Compliance Fatigue Across Financial Services

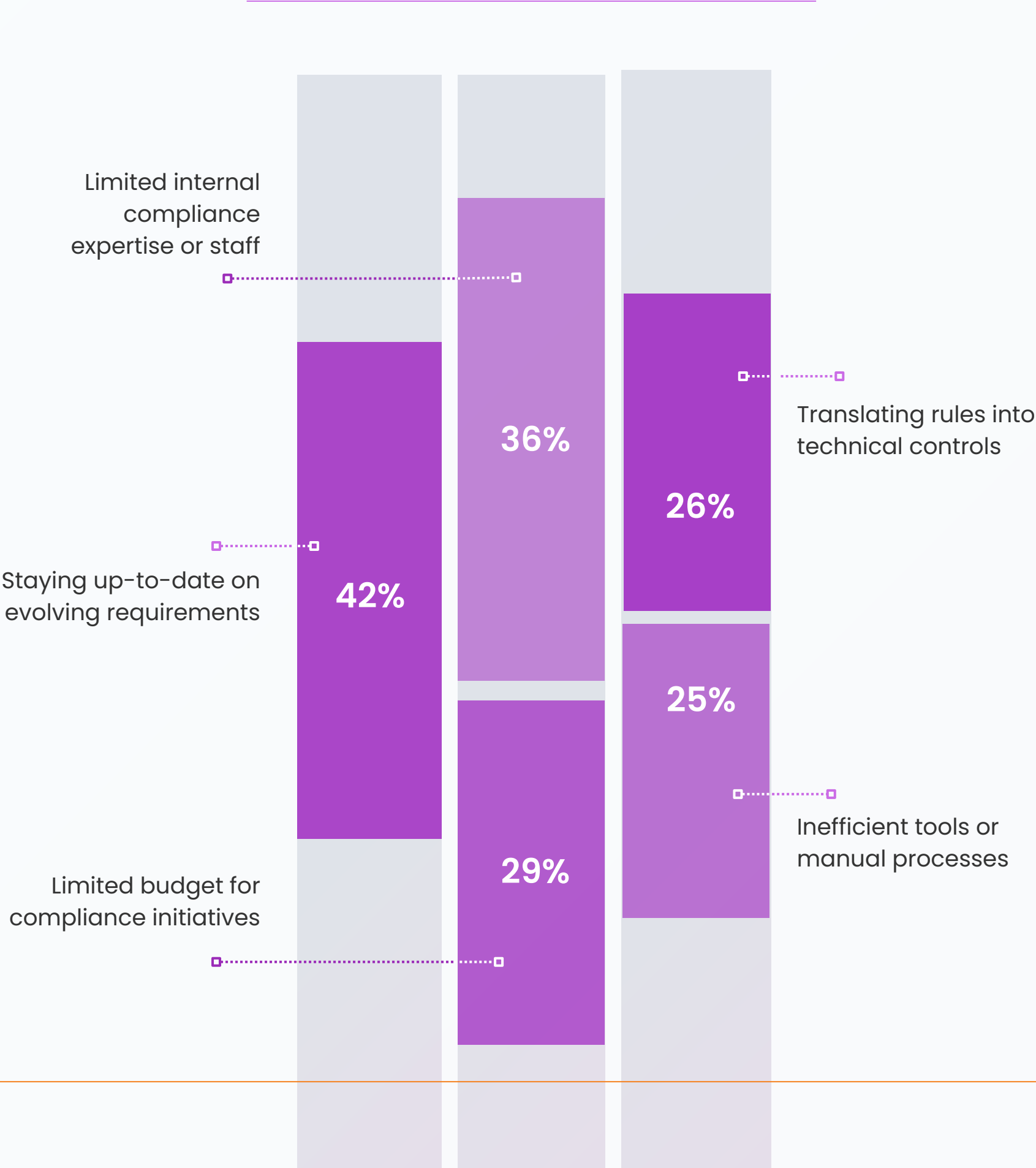
Financial leaders are caught between rising regulatory pressure and operational limits. Nearly half (42%) identify evolving requirements as their top challenge, followed by limited internal expertise (36%), budget constraints (29%), difficulty translating rules into technical controls (26%), and inefficient tools or manual processes (25%).

To complicate matters further, CFOs and CIOs often see the problem differently. 53% of CFOs cite staying current with regulations as a top concern, compared to 38% of CIOs – a gap that highlights how financial and technical priorities are misaligned. CFOs view compliance as a cost; CIOs view it as a process. Neither perspective, on its own, creates resilience.

When it comes to regulatory compliance readiness, financial services firms understand the mandate – they just don’t have the bandwidth to meet it.



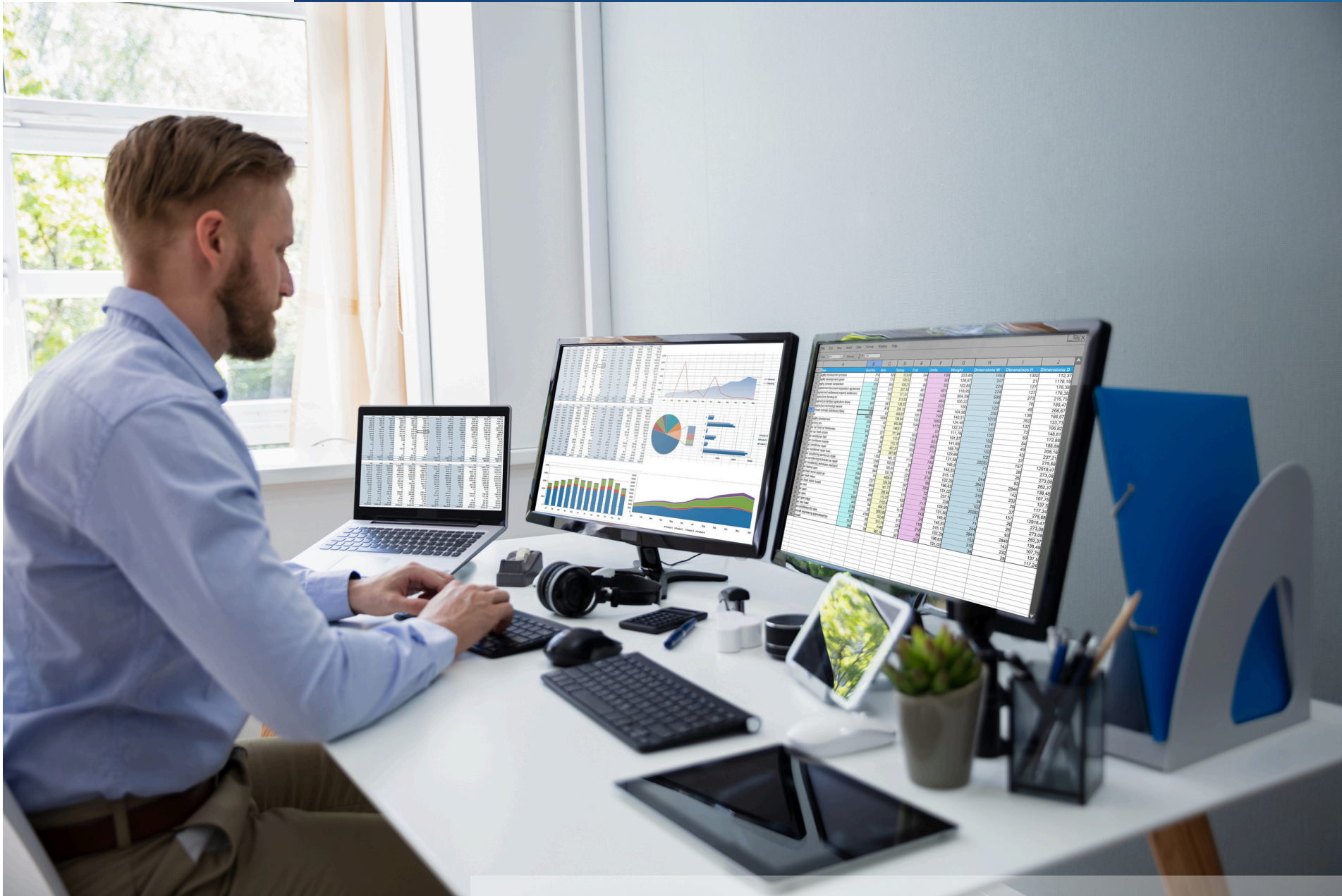
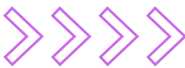
## Top 5 Compliance Roadblocks for Financial Firms



# Manual Processes: Compliance at a Standstill

Despite years of digital transformation, compliance itself remains remarkably manual across the financial industry. Fifty-four percent (54%) of firms still rely on spreadsheets or internally built systems to manage security control benchmarking and reporting. Smaller firms are particularly strained – 46% of those with fewer than 500 employees depend on manual methods, compared to just 21% of larger firms.

**Manual oversight limits visibility and creates risk.** Without automated logging, audit trails, and version control, firms struggle to produce the documentation regulators demand. Many discover too late that their compliance systems can't prove readiness when it matters most.



More than half of firms surveyed (54%) rely on manual spreadsheets/processes to benchmark their security controls.

# Uncertain Signals from Regulators

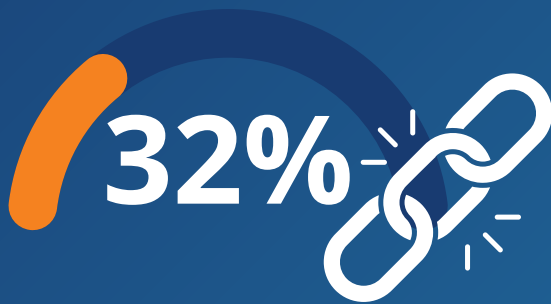
The SEC’s withdrawal of proposed cybersecurity rules in June 2025<sup>[1]</sup> added a layer of ambiguity just as expectations were tightening. Omega’s data shows a split reaction: 37% of firms believe the withdrawal weakened their posture, while 32% say it strengthened it by providing more flexibility.

In practice, this divide has created **inconsistent maturity across the industry**. Some firms are doubling down on documentation and governance, while others have paused investments until new clarity emerges. The risk, as regulators continue to enforce under existing laws, is that firms mistake uncertainty for relief.

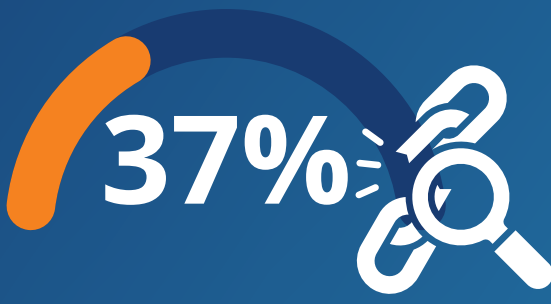


[1] Securities and Exchange Commission, Notice of Withdrawal of Proposed Regulatory Actions, Release Nos. 33-11377; 34-103247; IA-6885; IC-35635 (June 12 2025), [sec.gov](https://www.sec.gov).

## Split Reaction to SEC’s Cybersecurity Rules Withdrawal



of firms believe the withdrawal **strengthened** their posture and provided more flexibility.



of firms believe the withdrawal **weakened** their posture

### Compliance in Practice

Recent enforcement trends underscore how regulators are interpreting these rules. In 2024 and 2025, the SEC levied multiple fines exceeding \$1 million for delayed incident disclosure, weak vendor oversight, and insufficient documentation. The message is clear: process failures are now governance failures.

Omega’s findings mirrors those vulnerabilities – 20% of firms lack a defined incident response plan, and 18% say legacy systems hinder their ability to meet modern compliance standards. Documentation and testing are no longer optional; they’re the proof points regulators expect when resilience is questioned.

## From Manual to Managed: The MSSP Advantage

More than half of financial firms (52%) still manage cybersecurity internally, but those working with managed security service providers (MSSPs) or in co-managed models (17%) demonstrate stronger audit readiness and faster response times.

MSSP-supported firms test for vulnerabilities more frequently (56% conduct continuous or monthly testing vs. 38% of internally managed firms), detect and contain breaches faster (16% vs. 25% requiring two to four weeks), and maintain stronger documentation through continuous monitoring and audit logs. These capabilities give firms the verifiable evidence regulators now expect – turning compliance from a reactive obligation into a measurable operational discipline.

| Compliance Metric                       | Internal IT<br>(Shared Resources) | MSSP-Supported<br>Firms |
|-----------------------------------------|-----------------------------------|-------------------------|
| Continuous or Monthly Testing           | 38%                               | 56%                     |
| Breach Containment (2–4 Weeks)          | 25%                               | 16%                     |
| Lacking Defined Incident Response Plan  | 20%                               | 14%                     |
| Cyber Insurance Coverage                | 80%                               | 85%                     |
| Continuous Log / Audit Trail Visibility | Limited                           | Robust                  |



Partnering with a managed provider doesn't just fill resource gaps – **it operationalizes compliance, translating regulatory expectations into daily, measurable practice.**

## Modernization as the Compliance Multiplier

Compliance readiness depends on modernization. But half (50%) of firms admit they rely on outdated or on-premise systems today.

Legacy systems can't sustain the control visibility regulators now require. Modern platforms streamline compliance by centralizing logs, automating backups, and producing verifiable audit data on demand. But with such a heavy reliance on legacy IT within the industry, it's become clear that technology debt is now a compliance risk in itself.



**Half of financial services firms** admit they rely on outdated or on-premise systems today.

# What Firms Want from Compliance Technology

Financial firms are signaling that technology – not headcount – will close the compliance gap. The most valued features in a managed compliance platform include:

51%

**Data Discovery and Classification**

Helps firms locate sensitive information across cloud and on-prem environments to ensure nothing escapes regulatory scope.

45%

**Automated Evidence Collection**

Gathers audit logs, test results, and policy documentation continuously, eliminating manual proof-gathering at exam time.

45%

**Organized Document Management**

Centralizes controls, policies, and reports for easy retrieval during audits or investor due diligence.

41%

**Control Benchmarking & Progress Tracking**

Enables firms to measure improvement, identify compliance drift, and demonstrate governance maturity.

These capabilities transform compliance from an administrative burden into a measurable operational discipline. **Automation turns effort into evidence – and evidence into trust.**



## Conclusion: Proof Over Promises

In 2025, compliance has become the true measure of cyber resilience in the financial services industry – and resilience has become the foundation of trust. Regulators, investors, and clients are aligned: show the evidence.

Firms that modernize systems, automate documentation, and partner strategically won't just meet obligations – they'll lead with confidence. The next wave of compliance will reward those who can prove readiness, not just claim it.

As we move into 2026, documentation will carry the same weight as defense. The firms that build transparency into their technology and partnerships will be the ones investors trust most.

### Bottom Line

**Evidence, not promises, defines resilience.**





## Survey Methodology

Findings are based on an Omega Systems survey conducted in August 2025 of more than 300 U.S. financial services executives, including CEOs, CIOs, CISOs, CFOs, COOs, and other senior leaders. Respondents represented firms operating in the financial services sector including family offices, RIAs, wealth management firms, hedge funds, private equity, and investment advisory firms, with assets under management (AUM) ranging from less than \$1 billion to more than \$10 billion. Percentages are rounded to the nearest tenth.

## About Omega Systems

As a multi-award-winning MSP and MSSP, Omega Systems is passionate about delivering the security and compliance expertise today's businesses need alongside the responsive and reliable managed IT support they deserve. Omega's service-driven IT solutions portfolio includes 24x7 managed IT support, cybersecurity risk management, managed detection & response (MDR), backup and disaster recovery, multi-cloud connectivity, and much more. Omega Systems supports customers across the U.S. in key regulated industries such as financial services, healthcare, and professional services.



follow us: @omegasystemsMSP

learn more at [www.omegasystemscorp.com](http://www.omegasystemscorp.com)