whistic

The Whistic Insight Edition 1

A WHISTIC WHITE PAPER

SPEED-TO-TRUST: THE NEW METRIC FOR FINANCIAL VENDOR RISK MANAGEMENT

How Financial Institutions Are Modernizing Vendor Risk Through Automation and Shared Trust

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For years, financial institutions have measured third-party risk management (TPRM) success through compliance checklists and audit readiness. But today, **speed-to-trust** has become the new competitive metric.

In a world where fintech partnerships and SaaS integrations drive business growth, **delays in vendor assessments translate directly into delayed revenue.** Gartner estimates that inefficient risk reviews can delay onboarding by up to **12 weeks,** while the **2025 Verizon Data Breach Investigations Report (DBIR)** shows that **30% of all breaches now involve a third party** — nearly double the prior year.

The message is clear: traditional, manual questionnaires can't keep pace with modern risk.

This white paper explores how forward-thinking financial institutions are transforming their TPRM programs by embracing automation, shared trust profiles, and event-driven reassessments — building vendor relationships that move at the speed of business while strengthening compliance and security oversight.

INTRODUCTION: THE TRUST LAG PROBLEM

Every financial institution depends on vendors — from cloud platforms and payment processors to fintech startups and data analytics firms. Each new relationship introduces opportunity and risk.

The challenge? Traditional vendor assessments move far slower than the pace of innovation. Manual questionnaires, spreadsheets, and endless email chains remain the norm, leaving risk and procurement teams buried in administrative work.

The result is what we call the Trust Lag: the costly delay between when a business wants to move forward and when security feels confident enough to say yes.

12 weeks

average delay in vendor onboarding due to inefficient risk reviews (Gartner, 2024).

Gartner®

$4.88 million:

average cost of a data breach (IBM, 2024).

IBM®

30% of breaches:

involve a third-party vendor (Verizon DBIR, 2025).

verizon

This isn't just an IT problem — it's a business performance problem. Every week a vendor sits in onboarding purgatory, potential revenue and innovation sit idle.

THE BUSINESS COST OF DELAY

In financial services, time equals trust — and trust equals revenue.

When vendor reviews are slow, the consequences cascade across the organization:

Revenue delays:
The result is what we call the Trust Lag: the costly delay between when a business wants to move forward and when security feels confident enough to say yes.

Operational drag:
Risk teams spend hours manually parsing documents instead of managing strategy.

Vendor fatigue:
Repeated questionnaires create frustration and inconsistent data.

Compliance risk:
Outdated responses leave blind spots regulators will question.

Gartner research shows that inefficient onboarding can delay deals by up to three months, costing millions in lost opportunity. Meanwhile, **the Financial Stability Board's (FSB) 2023 Toolkit** urges continuous vendor oversight — not just point-in-time reviews — as global regulators demand more dynamic risk management.

For financial institutions, accelerating speed-to-trust is now both a business imperative and a compliance expectation.

THE RISK LANDSCAPE HAS CHANGED — YOUR ASSESSMENT MODEL HASN'T

Financial institutions today operate in the most interconnected ecosystem ever. Every API, fintech partnership, and cloud platform extends the perimeter of trust — and with it, the potential for risk.

Then	Now
• Vendor list updated once a year • Manual questionnaires • Fragmented visibility	• Ongoing due diligence • Real-time monitoring • Integrated systems and alerts

Recent frameworks make one thing clear: vendor oversight can't be a once-a-year task.

- **NIST SP 800-161r1 (2024):** Calls for "ongoing due diligence proportional to risk."
- **FSB Third-Party Risk Toolkit (2023):** Defines continuous supply chain monitoring as critical for resilience.
- **OCC & ECB:** Now require lifecycle visibility — from onboarding to offboarding.

Takeaway: *Speed-to-Trust isn't optional — it's the new benchmark for regulatory maturity.*

MANUAL ASSESSMENTS DON'T JUST SLOW YOU DOWN — THEY LEAVE YOU EXPOSED.

Despite new technology and regulatory pressure, **60% of organizations** (Ponemon, 2024) still rely on spreadsheets for vendor risk management. The result: **stale data, frustrated vendors, and missed opportunities.**

Point-in-Time Risk

Risk changes faster than your review cycle. By the time a spreadsheet is updated, the data's already outdated.

Manual Chaos

Spreadsheets and email chains make it impossible to maintain version control or track evidence across teams.

Vendor Fatigue

When vendors complete hundreds of questionnaires a year, accuracy and engagement plummet — and errors multiply.

> *"Organizations using manual processes are 3x more likely to experience incomplete or outdated vendor data."*
> *— Ponemon Institute, 2024*

Traditional tools weren't built for continuous risk. Modern programs use automation and shared data to turn assessments from roadblocks into real-time insights.

INTRODUCING THE SPEED-TO-TRUST FRAMEWORK

The **Speed-to-Trust Framework** is a new approach that blends automation, intelligence, and collaboration. It's built on four pillars:

Automation

AI processes vendor documentation (SOC 2, ISO 27001, SIG) in minutes, mapping controls automatically.

Shared Profiles:

Vendors publish one always-current profile, reducing questionnaire fatigue.

Event-Driven Reassessments:

Triggered automatically when risk changes — not just annually.

Auditability

Continuous updates provide defensible, transparent documentation for regulators and auditors.

Together, these pillars turn vendor assessments from bottlenecks into accelerators — enabling faster decisions, stronger oversight, and measurable cost savings.

AUTOMATION IN PRACTICE

Automation is the engine of Speed-to-Trust.

- Parse vendor documents like SOC 2 reports or policies.
- Map findings directly to frameworks such as **NIST, SIG,** and **ISO.**
- Summarize long documents into control-by-control insights.
- Highlight gaps or inconsistencies instantly.

Deloitte's 2024 Future of Risk Report found that automation reduces manual workloads in TPRM by up to 90%, freeing teams to focus on strategic risk rather than repetitive review tasks.

Whistic AI applies these principles by leveraging AI to analyze documentation, generate responses, and flag potential risk indicators — all within minutes.

SHARED SECURITY PROFILES: TRUST THAT SCALES

In traditional TPRM, vendors complete the same questionnaires for multiple customers — hundreds each year. The result? Fatigue, errors, and inefficiency.

Whistic solves this through the Trust Center Exchange, enabling vendors to publish a single, always-current profile that can be securely shared across customers.

This model:

- Eliminates redundant questionnaires.
- Ensures every customer sees the same, verified information.
- Accelerates vendor onboarding and audit readiness.

For financial institutions, this shared-trust ecosystem means faster, higher-quality assessments and stronger vendor relationships.

EVENT-DRIVEN REASSESSMENTS

Static, calendar-based assessments leave blind spots. Real risk evolves dynamically.

Whistic helps teams move beyond annual reviews by enabling vendors to maintain a continuously updated security profile—so reassessments happen automatically when events occur, not once a year.

Event-driven reassessment replaces the "annual review" model with continuous visibility:

- When a vendor updates their SOC 2 report → automatic notification.
- When a product change affects data flows → reassessment triggered.
- When a breach occurs → instant review.

This aligns directly with NIST SP 800-161r1 and the FSB Toolkit, which both call for "ongoing risk monitoring proportional to criticality."

With Whistic, these reassessments happen automatically — allowing risk teams to stay proactive instead of reactive.

AUDITABILITY: BUILDING A DEFENSIBLE TPRM PROGRAM

Static, calendar-based assessments leave blind spots. Real risk evolves dynamically.

Whistic helps teams move beyond annual reviews by enabling vendors to maintain a continuously updated security profile—so reassessments happen automatically when events occur, not once a year.

Event-driven reassessment replaces the "annual review" model with continuous visibility:

- When a vendor updates their SOC 2 report → automatic notification.
- When a product change affects data flows → reassessment triggered.
- When a breach occurs → instant review.

This aligns directly with NIST SP 800-161r1 and the FSB Toolkit, which both call for "ongoing risk monitoring proportional to criticality."

With Whistic, these reassessments happen automatically — allowing risk teams to stay proactive instead of reactive.

Auditability: Building a Defensible TPRM Program

Auditors and regulators don't just want to see that you manage vendor risk — they want proof you can defend it.

Manual evidence collection and endless spreadsheets can't keep up with evolving standards like **NIST SP 800-161r1, DORA, and FSB's TPRM Toolkit**, which all require **continuous oversight and traceable documentation.**

Whistic builds auditability into every step of your TPRM program — creating real-time, defensible evidence without the scramble.

How Whistic Makes Audit Readiness Automatic

Built-In Audit Trail

Every vendor update, reassessment, and document upload is logged and time-stamped — no more manual recordkeeping or version confusion.

Continuous Evidence Collection

Whistic automatically captures and stores event-driven changes, like new SOC 2 reports or expired certifications, so your audit trail builds itself.

Framework-Aligned Reporting

Assessments are mapped directly to NIST, ISO, SIG, and PCI DSS frameworks, producing consistent, audit-ready outputs that satisfy regulators.

Proven Oversight, On Demand

When auditors or boards ask for proof, Whistic delivers it — structured, current, and instantly exportable.

Why It Matters

Auditability isn't just compliance — it's confidence. According to Deloitte's 2024 Future of Risk Report, automation cuts manual compliance workloads by up to 90%, freeing security teams to focus on risk reduction instead of paperwork.

Whistic turns oversight into evidence — so when regulators call, your team is ready.

BUSINESS IMPACT & ROI

When financial institutions modernize their vendor assessment process, the benefits are measurable:

Metric	Traditional Approach	Automated Approach (with Whistic)
Review Time	6–12 weeks	1–2 days
Manual Workload	100%	-90% (Deloitte, 2024)
Onboarding Delays	Up to 12 weeks (Gartner)	Reduced by 70%
Breach Cost Exposure	$4.88M avg. (IBM, 2024)	Reduced via continuous oversight

Beyond cost savings, the shift to Speed-to-Trust strengthens resilience, vendor collaboration, and regulatory confidence.

Case in Point:

A regional financial institution using Whistic reduced its average vendor assessment timeline from 8 weeks to under 10 days — freeing up over 500 staff hours per quarter.

CONCLUSION: CUT COSTS, NOT CONFIDENCE

In financial services, risk management has always been about trust. The difference today is **how fast you can build it.**

The financial institutions that thrive in the next decade will be those that modernize their vendor assessment programs — combining automation, shared profiles, and event-driven oversight to build **continuous trust at scale.**

The question isn't whether automation belongs in TPRM — it's whether you can afford to wait any longer to adopt it.

👉 See how Whistic helps financial institutions accelerate vendor assessments and build trust faster.

whistic

THANK YOU!