Wizard
Intelligence beyond the perimeter

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Continuous Risk Intelligence for US-Based Financial Company with Wizard, AI-Powered TPRM

letsconnect@ampcuscyber.com

www.ampcuscyber.com

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

01 Executive Summary:

A mid-sized US financial services firm managing nearly 340 active third-party vendors faced mounting regulatory pressure and severe operational bottlenecks due to manual, spreadsheet-driven risk assessments. Ampcus Cyber overhauled the firm's third-party risk management (TPRM) program by deploying ComplyX Wizard, transitioning the organization from static, point-in-time reviews to automated, continuous risk monitoring. Within two quarters, vendor onboarding time dropped by nearly 67%, and audit preparation time shrank from two weeks to three days.

67%	**100%**	**78%**
Drop in Onboarding Time	**Critical Tier Monitored**	**Faster Audit Prep**
Cut from 6 weeks to under 2 weeks for standard vendors.	135 critical and high-risk vendors moved to 24/7 monitoring.	Evidence-gathering reduced from 2 weeks to approximately 3 days.

02 Customer Profile

- **Industry:** Financial Services (Digital Banking, Core Payments)
- **Organization Size:** Approximately 2,200 Employees
- **Geographic Footprint:** Multi-state operations within the United States
- **Vendor Ecosystem:** Approximately 340 active third-party vendors (Cloud, Core Banking, SaaS, Outsourced Support)
- **Regulatory Frameworks:** Subject to FFIEC Guidance, GLBA, and SOC 2 Type II attestation requirements

03 The Challenge: Regulatory Exposure Meets Commercial Bottlenecks

While the firm maintained robust internal cybersecurity controls, its TPRM program relied on decentralized spreadsheets, email chains, and annual SIG questionnaires. This legacy workflow created three severe operational risks:

- **Point-in-Time Blind Spots:** Vendor risk was evaluated once a year. If a vendor suffered a credential leak or allowed a SOC 2 attestation to lapse mid-cycle, the security team had zero visibility until the next annual review.
- **Severe Procurement Friction:** Every vendor cleared the same manual questionnaire-and-review cycle regardless of risk tier. Security reviews averaged six weeks per vendor, creating deal desk bottlenecks that delayed key digital banking initiatives.
- **Regulatory Scrutiny:** An FFIEC examination flagged the firm's reliance on annual, static assessments as a material gap, specifically highlighting that fewer than half of critical vendors had current SOC 2 Type II attestations on file.

04 Solution: Wizard, AI-Powered TPRM

Ampcus Cyber approached the engagement as a complete program modernization rather than a simple tooling upgrade. The team deployed Wizard to serve as the unified operating system for third-party risk across the entire vendor lifecycle:

- **Centralized Single Source of Truth:** Replaced siloed spreadsheets with dynamic vendor risk profiles accessible across Security, Legal, and Procurement teams.
- **Tiered Onboarding Orchestration:** Automated intake workflows so low-risk vendors clear rapid-track reviews, while high-risk vendors route directly into deep technical evaluations.
- **Continuous Attack Surface Intelligence:** Real-time external scanning for DNS hygiene issues, misconfigured or exposed ports, and leaked credentials tied to vendor domains.
- **Event-Driven Risk Triggers:** Instant alerting on newly disclosed vulnerabilities affecting vendor technology stacks, expiring SOC 2 bridge letters, and subcontractor (fourth-party) concentration risks.
- **Audit-Ready Dashboards:** Consolidated portfolio-wide reporting that translates technical vendor telemetry into board- and regulator-ready metrics

05 Phased Implementation for 14-Weeks

- **Phase 1:**
  Assessment & Baselining (Weeks 1 to 3): Ampcus Cyber inventoried all vendors, harmonized disparate questionnaire templates, and established a standardized tiering rubric (Critical, High, Medium, Low).

- **Phase 2:**
  Platform Configuration (Weeks 4 to 7): Configured ComplyX Wizard to match the firm's SIG-based questionnaire library, risk appetite thresholds, and role-based access permissions across departments.

- **Phase 3:**
  Migration & Tiered Activation (Weeks 8 to 11): Migrated legacy records into the platform. Incomplete historical files (nearly 15%) were triaged directly into fresh automated assessments. Continuous monitoring was activated immediately across all approximate 40 critical vendors.

- **Phase 4:**
  Rollout & Enablement (Weeks 12 to 14): Delivered cross-functional training for Security, Compliance, Legal, and Procurement teams to ensure full adoption and pipeline visibility.

06 Business & Operational Impact

- **Real-Time Risk Mitigation:** Within the first six months of deployment, event-driven monitoring flagged 11 lapsed or expiring SOC 2 attestations among critical vendors. These issues would previously have remained undetected until the next annual review.

- **Accelerated Business Velocity:** By routing vendors through risk-tiered intake paths, standard onboarding time fell from approximately 6 weeks to under 10 business days, turning security from a procurement bottleneck into an agile business enabler.

- **Seamless Regulatory Compliance:** During the subsequent FFIEC examination cycle, the compliance team produced complete vendor audit trails, continuous telemetry, and remediation history directly from ComplyX Wizard, reducing audit prep time from two weeks of staff effort to three days.

07 The Result: From Periodic Reviews to Continuous Risk Intelligence

The firm transitioned from a reactive, questionnaire-driven TPRM model to a more continuous, risk-based approach.

With Wizard, vendor assessments became part of a broader risk management process that combined vendor onboarding, risk tiering, security evidence, external exposure monitoring, and remediation tracking.

This gave Security, Compliance, Legal, and Procurement teams a more current view of third-party risk while reducing manual effort across the vendor lifecycle.

The result was a more proactive and audit-ready TPRM program that could better support the pace and risk requirements of modern financial services operations.

Modernize Your Third-Party Risk Management

Move beyond periodic questionnaires with continuous vendor risk visibility, automated assessments, and risk-based workflows.

Explore how Wizard can help strengthen your TPRM program