SAFE

TPRM Program Blueprint: Your Guide for Transforming Third Party Risk Management

Table of Contents

Executive Summary

The verdict is clear: Third-Party Risk Management (TPRM) needs a complete rehaul. Legacy methods are outdated, manual, and ineffective at mitigating real business risk. These practices persist not because they deliver value—but because they check compliance boxes and satisfy audit requirements. In today's digital-first world, where cybersecurity risk is inseparable from business risk, organizations must ask: Are we justified in devoting significant time, effort, and investment into processes that do little to reduce actual exposure?

The answer is a resounding "no". **A radical course correction in TPRM is essential.**

As vendor ecosystems grow in size and complexity, and integrate more deeply into core business operations, third-party risk management must evolve into a proactive, intelligence-led discipline. The need of the hour is not more checklists it's an AI-powered, autonomous, and risk-based TPRM approach that delivers real-time visibility, precision, and scale.

To truly reduce risk while supporting business growth, organizations must move beyond redundant processes and toward systems that prioritize action over assessment. This whitepaper explores the systemic flaws in traditional TPRM and outlines a blueprint for **reimagining the function as a scalable, outcome-oriented, and strategic business enabler.**

Highlights

- **Ditch the Redundancy:** Identify and focus on key controls that matter, so you and your third parties can utilize limited resources efficiently
- **Embrace Automation:** Leverage AI and automation to scale your TPRM program efficiently.
- **Real-Time, Continuous Evaluation:** Move beyond static assessments. Continuously monitor and evaluate the effectiveness of your vendors' controls.
- **Focus on Business Risk:** Use financial metrics and cyber attack likelihood to prioritize critical risks.
- **Optimize Costs:** Implement predictable, cost-effective strategies to maximize the return on your TPRM investment.

Escalating Third-Party Risk Requires an Autonomous Approach

Enterprises today are rapidly scaling through external vendors, SaaS tools, and third-party services opting to buy rather than build. This shift enables agility, cost-efficiency, and faster innovation. But it also expands the digital attack surface exponentially, making third-party risk management (TPRM) one of the most critical and complex areas of cybersecurity. As the threat landscape evolves, businesses must move beyond legacy frameworks and embrace new, intelligent solutions to stay ahead. Forrester echoes this sentiment:

> *"TPRM is shifting from a nice-to-have tool for compliance checks and onboarding automation to a must-have technology for leveraging the benefits of third-party relationships without creating undue risk to the organization, complete with new AI-enabled use cases and the ability to support the entire lifecycle of a third-party relationship."*

The Real Problem Isn't Just Risk. It's How We're Managing It

Despite rising exposure, **69% of organizations still rely on manual TPRM processes**, and **57% depend on generic cybersecurity ratings** to make high-stakes decisions. These outdated approaches fail to deliver continuous, contextual, or actionable insights.

Most current tools are reactive, fragmented, and heavily reliant on questionnaires and static data. They provide only a narrow snapshot of vendor risk and lack the automation or intelligence to scale effectively. Security rating services also fall short—offering black-box scores without context or real visibility into business impact. The result? TPRM programs that are labor-intensive, blind to real risk, and fundamentally unscalable.

The Shortcomings of Traditional Third-Party Risk Management (TPRM)

Method	Limitations
Cybersecurity Ratings The scoring is usually via black box methodologies that are based on data collected from outside-in (external and public) scans.	• Cybersecurity Risk Ratings are fast becoming a compliance requirement, even though they do not provide any insight into a third-party's internal control environment. • Scores from these services should not be confused with Cyber Risk Quantification which provides insight into a business' risk exposure: the financial impact of cyber risks and the likelihood of cyber attacks.
Questionnaires Often 150- 200+ questions which vendors are required to fill and update periodically. Typically an annual requirement.	• The information may be misleading since questionnaires do not assess the vendors' control maturity (coverage, capability, and reliability) For example, if a company deploys multi factor authentication on only a few cloud servers, it will still respond by checking "yes" to MFA on the questionnaire – when in reality, the coverage of the control is not up to the mark. • There is limited knowledge of who on the third party's side is filling out the questionnaire, therefore its reliability is questionable. • Questionnaires are derived from compliance requirements, making the entire process regulatory and compliance-oriented when in reality, enterprises need to be reducing their risk from third-party related breaches by proactively measuring risk.
Integrated Methods Combines the findings of questionnaires and cybersecurity ratings to a single solution	• Considered more beneficial than isolated CRR and questionnaire analysis, however it does not reduce the workload on enterprises or third parties. • The limitations of both above methods still apply • There is a high demand for automation in the process
Compliance Framework Reports These tools map a vendors cybersecurity program against a framework of controls.	• The scope of the analysis is usually incomplete. • Usually based on internal reporting instead of external audits.

The solution? An autonomous third-party risk management platform powered by Agentic AI one that continuously validates controls, quantifies real exposure, and prioritizes vendors based on actual business risk, not just checkboxes.

The Problem Isn't Just the Data- It's the Lack of Intelligence

Why Enterprises Struggle

Traditional third-party cyber risk assessments—based on static surveys, outdated risk ratings, or one-off questionnaires—leave businesses drowning in data but starving for insight. These tools operate in isolation, offering no real-time feedback, no prioritization, and no understanding of actual risk impact.

Without AI-driven context, these methods remain checkbox exercises offering little value in reducing risk or informing high-stakes decisions.

Why Vendors Struggle Too

Effective cyber risk management is a shared responsibility—but current systems fail to support vendors in building better security. Most tools ignore the vendor's internal control maturity and rely on manual follow-ups and fragmented communication.

Without insight into control maturity or guided feedback, vendors are left guessing. Manual follow-ups, long questionnaires, and unclear expectations create frustration on both sides.

The Blueprint to Transform Your TPRM Program

Why TPRM Needs an Autonomous, AI-Powered Shift

In this whitepaper, we explore how forward-thinking organizations are moving beyond outdated, compliance-heavy vendor risk management toward a smarter, scalable approach one powered by autonomous AI and grounded in real business risk.

Today's CISOs are shifting to risk-based third-party risk management that delivers measurable outcomes not just audit checkboxes. This paper outlines actionable strategies to modernize your TPRM program using the latest advancements in AI, automation, and continuous risk quantification.

STEP 1

Automate Onboarding & Tiering with AI from Day Zero

Traditional vendor onboarding is slow, manual, and often misses real risks. Static forms and generic tiering don't tell you which vendors truly matter—or which ones may be dangerous.

AI can speed up onboarding, uncover hidden vendors (shadow IT), and sort them by real business risk, without waiting on spreadsheets or endless emails.

AI tools can now read vendor data, understand risk signals like breach history or exposure, and automatically decide which vendors need more attention. What used to take weeks now takes hours, with fewer blind spots and better decisions from day one.

PRO TIP

Use AI agents to instantly process intake forms, auto-tier vendors by real business risk, and surface shadow third parties, before a single email exchange.

1. **AI-Driven Intake Processing**
2. **Autonomous Risk Tiering**
3. **Hidden Vendor Discovery**

STEP 2

Turn Risk Chaos into AI-Driven Intelligence

Most risk assessments are slow, manual, and only offer a partial view. Teams rely on point-in-time reports and siloed tools, which means risks often go undetected until it's too late.

Modern tools can combine multiple data sources, like breach history, threat intel, and internal assessments: into a single, real-time risk profile. By connecting both internal and external signals, you can spot misalignments, hidden threats, and changes in vendor posture as they happen.

Instead of reacting to problems after they occur, you can prioritize vendors based on real business exposure, not just generic risk categories.

PRO TIP

Don't wait for annual reviews to detect risk.

Use tools that continuously scan for changes in vendor risk, from new breaches and regulatory filings to threat intel and domain exposure. When signals are unified, you get fewer false alarms and more time to act on real risks.

1 **Unified Risk Visibility**

2 **AI-Powered Contextual Analysis**

3 **Truly Risk-Based Tiering**

STEP 3

Make Vendor Resilience Part of Daily Operations

Manual processes for managing third-party risk make it hard to stay ahead of disruptions. Security and risk teams are stuck reacting to issues—often after damage is already done.

By automating vendor interactions and using AI to detect early signs of risk, you can shift from reactive to resilient. Risk signals can trigger real-time insights, suggesting fixes before issues escalate—like hygiene improvements, architectural gaps, or weak processes.

Resources are automatically prioritized by risk impact, and AI-generated summaries support faster, board-ready decisions—no spreadsheets needed.

PRO TIP

Resilience starts by identifying weak links before they break.

Use automation to surface gaps in vendor hygiene, flag critical vulnerabilities early, and ensure consistent follow-ups, even across thousands of vendors. Resilient teams don't just assess, they adapt in real time.

1. Automated Questionnaire Pre-Fills
2. AI-Driven Recommendations
3. Scalable Vendor Resilience

STEP 4

Shift from Periodic Reviews to Continuous, AI-Powered Oversight

Traditional risk programs rely on periodic check-ins that often miss fast-moving threats. Once a vendor is onboarded, risk visibility fades, until the next review (or the next breach).

Modern programs use autonomous monitoring to maintain 24/7 visibility. AI agents scan for breach disclosures, regulatory changes, trust center updates, and public threat intelligence, surfacing risks as they happen, not weeks later.

Teams are notified instantly. Follow-ups are triggered automatically. Communication workflows run without manual chasing, letting analysts focus on risk, not reminders.

PRO TIP

Risk doesn't wait for QBRs. Neither should you.

Use AI to stay ahead of emerging threats. Combine outside-in signals, breach alerts, and regulatory shifts into a single stream of actionable insight, before risk becomes reality.

1. Autonomous Monitoring Agents
2. Real-Time Risk Alerts
3. Zero-Touch Communication

STEP 5

Ensure Audit-Ready Compliance and Reduce Operational Burden

Compliance is no longer an one-time exercise it's an ongoing obligation across the entire vendor lifecycle. But for most teams, proving compliance means chasing evidence, compiling reports, and scrambling ahead of audits.

Automation turns compliance into a continuous, autonomous process. AI agents automatically map evidence to regulatory frameworks like NIST, ISO, GDPR, and HIPAA, monitor control effectiveness, and generate audit-ready reports without manual data wrangling.

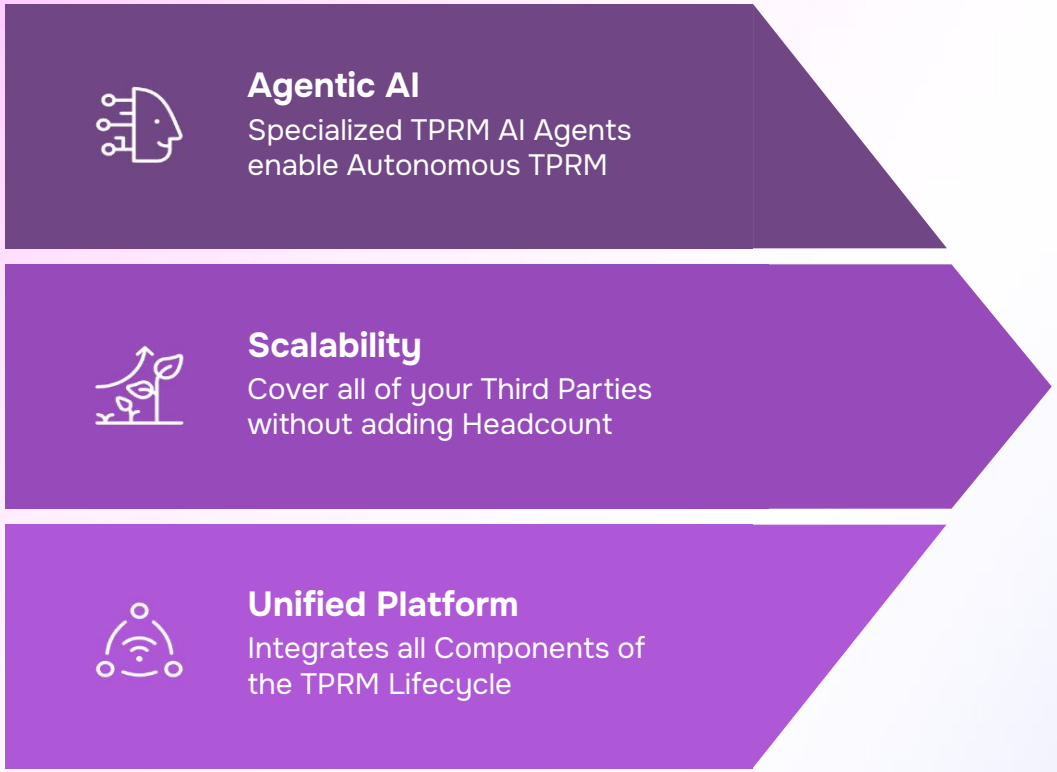
Whether you're preparing for an external audit, internal board review, or regulator inquiry, everything is version-controlled, traceable, and up to date reducing compliance risk and freeing your team to focus on higher-impact work.

PRO TIP

Automate your compliance stack.

Automate control mapping, evidence collection, and reporting with AI. Stay aligned to frameworks continuously, and make audit prep a non-event.

1. AI-Generated, Audit Reports
2. Automated Control Mapping
3. Always Audit-Ready

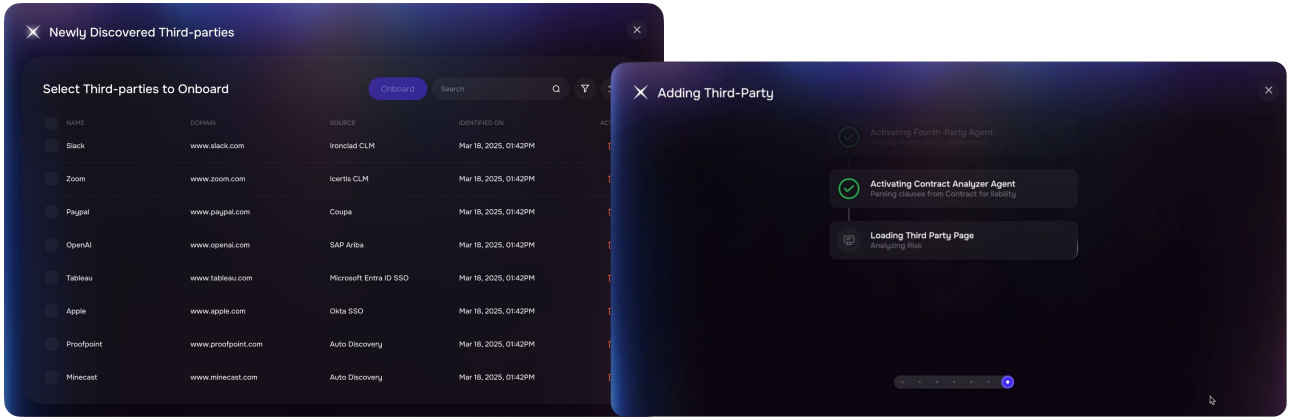


INTRODUCING SAFE'S 100% AUTONOMOUS TPRM

SAFE TPRM: AI-Powered. Fully Autonomous. Truly Risk-Based.

01 | Onboarding & Due Diligence

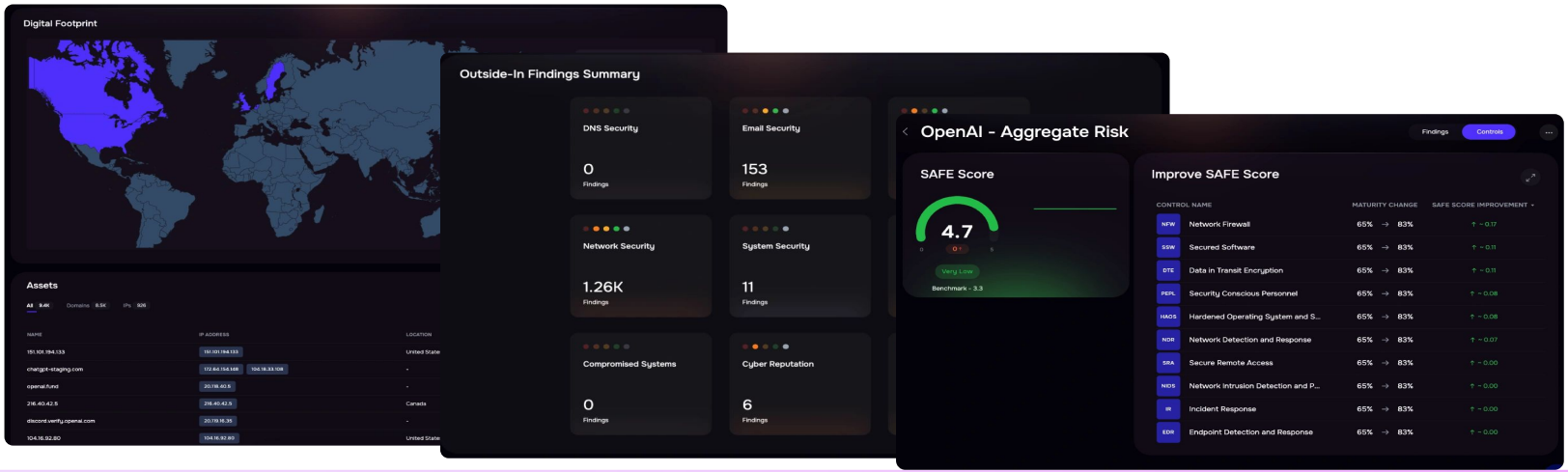
Traditional third-party onboarding is slow, manual, and prone to risk blindness. SAFE TPRM transforms this process using intelligent AI agents that automate discovery, intake, tiering, and risk analysis turning onboarding from a bottleneck into a strategic advantage. With SAFE, intake forms are parsed using LLMs to identify hidden risks instantly, while autonomous discovery tools validate all vendor connections including shadow IT. Vendors are tiered from day one based on business context, threat exposure, and potential financial loss, rather than generic categories.
Due diligence is enriched with external security posture, breach history, and firmographic data, all contextualized in real time. SAFE also enforces contractual safeguards early by linking required clauses to vendor tier and risk level. As a result, organizations dramatically shorten onboarding timelines from **weeks to hours**.



SAFE TPRM: AI-Powered. Fully Autonomous. Truly Risk-Based.

02 | Risk Assessment

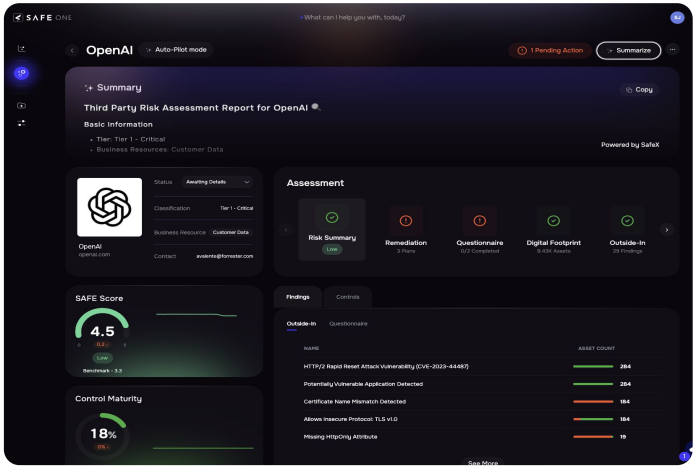
SAFE TPRM replaces the Risk assessment chaos with AI-driven automation that builds complete risk profiles from day one. The platform automatically populates third-party data from public and private sources combining firmographics, threat intel, breach data, and internal questionnaire responses into a single, unified view. SAFE's dual visibility approach uses both outside-in and inside-out telemetry to detect true security posture, while its LLM-powered engine & Agent reads and interprets vendor responses to identify gaps, evasive answers, or risky patterns. Risk tiering is driven by actual business context and financial exposure not just size or sector enabling truly risk-based prioritization. With continuous validation and auto-synced updates, SAFE ensures that every third-party risk profile stays accurate, actionable, and aligned to what matters most.

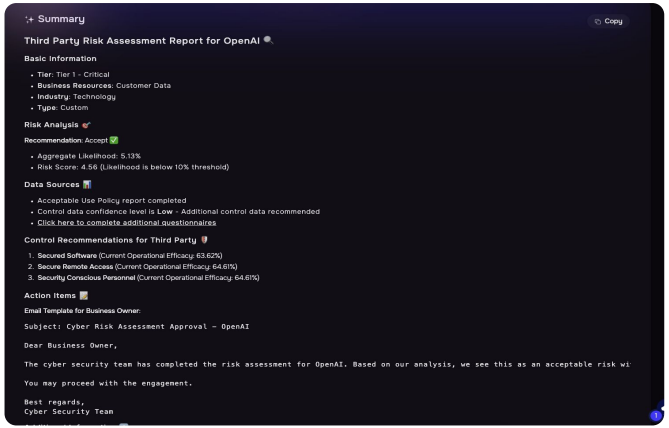


SAFE TPRM: AI-Powered. Fully Autonomous. Truly Risk-Based.

03 | Operational Resilience

SAFE TPRM embeds resilience into the fabric of your TPRM program with AI-powered insights, automated response workflows, and predictive modeling. As SAFE monitors vendors, it identifies potential points of failure and recommends targeted improvements that reduce risk to operations. These include suggestions for cyber hygiene, architecture hardening, and process updates all tailored to business-critical dependencies. Resources are automatically prioritized based on potential impact, allowing teams to act faster with fewer inputs. AI-generated summaries transform complex vendor data into board-ready insights that support faster, more confident decisions. With SAFE, resilience isn't reactive it's designed in.

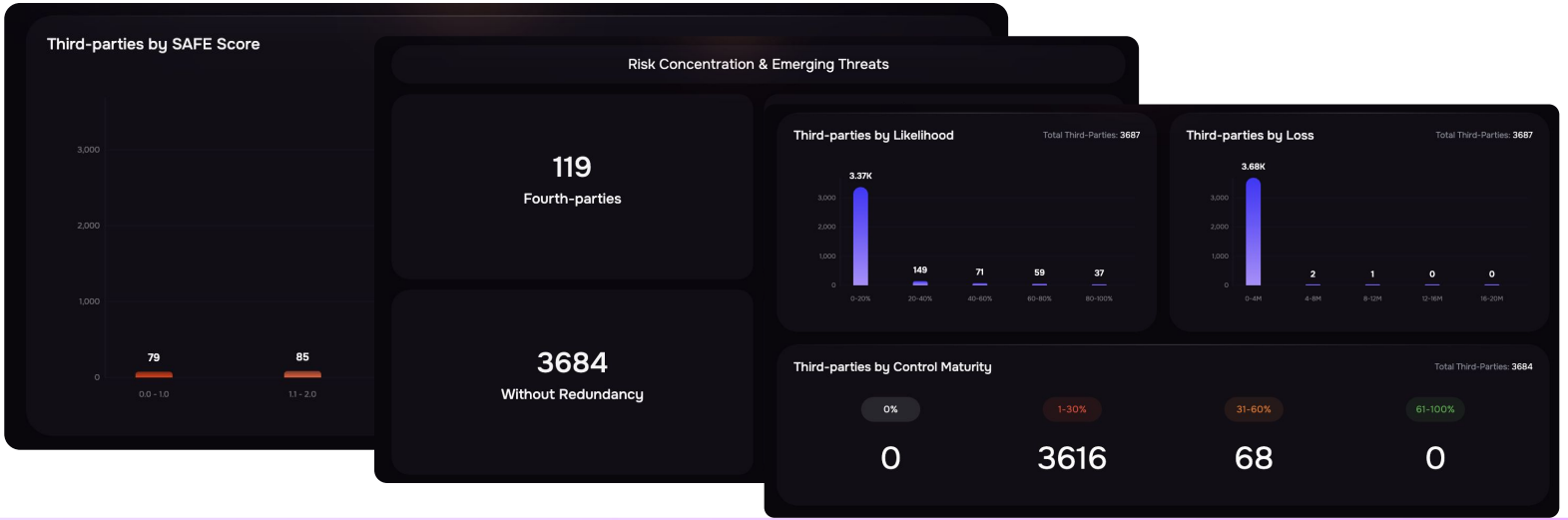




SAFE TPRM: AI-Powered. Fully Autonomous. Truly Risk-Based.

04 | Continuous Monitoring

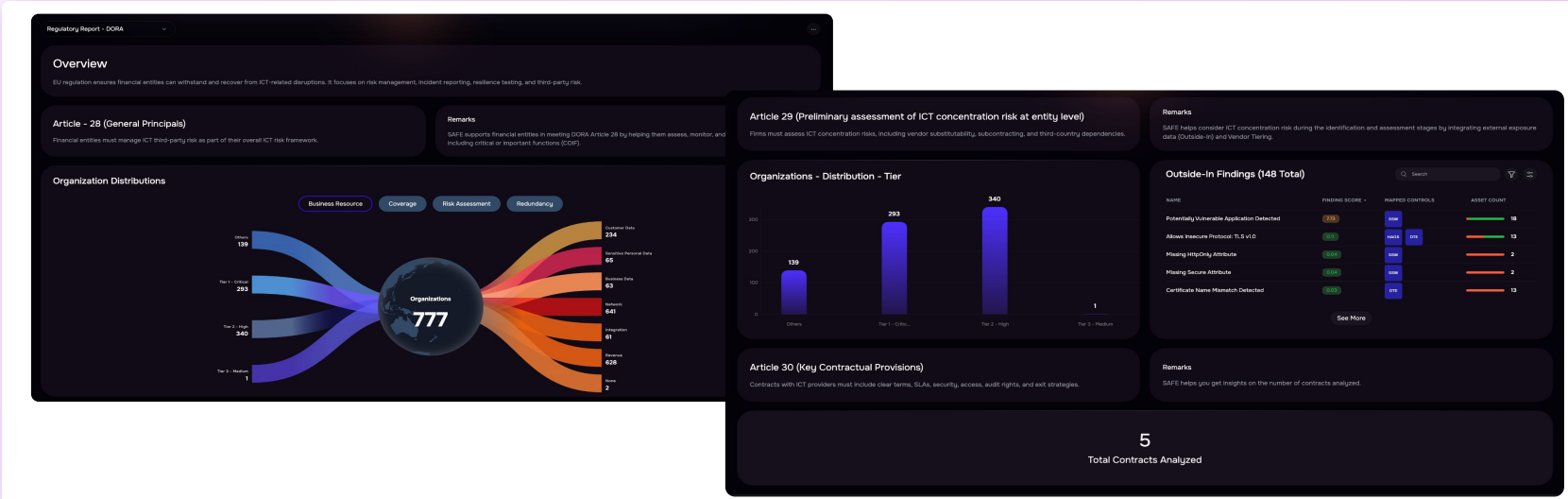
Most third-party assessments stop after onboarding—leaving organizations vulnerable to evolving threats. SAFE TPRM changes that with always-on, AI-powered monitoring. As soon as a vendor is onboarded, SAFE continuously scans for new risks using outside-in scanners, internal assessment signals, and public threat intel. The Public Data Agent tracks breach disclosures, regulatory filings, and industry alerts, correlating them to each vendor's profile. The Communication AI Agent notifies analysts immediately via email, Slack, or in-app alerts, and automatically follows up with vendors for resolution. When new risks emerge, SAFE auto-generates tasks and mitigation requests, driving collaboration without manual intervention.



SAFE TPRM: AI-Powered. Fully Autonomous. Truly Risk-Based.

05 | Regulatory Compliance & Reporting

SAFE TPRM streamlines compliance with automated evidence collection, AI-generated audit reporting, and continuous control validation. SAFE aligns vendor actions with key regulatory frameworks such as NIST, ISO, GDPR, and HIPAA mapping telemetry and assessments directly to controls. Evidence is automatically collected and validated through uploaded documents, system integrations, and vendor interactions. When it's time for an audit or board update, SAFE generates comprehensive, defensible reports that highlight compliance status, open issues, and potential financial impact.



SAFE TPRM AI Agents

Public Records Agent

Surfaces critical risk signals from multiple sources like SEC filings, breach databases, trust centers, and more

Digital Footprint Agent

Builds a third party's digital risk profile using domain data and online presence

Outside-In Agent

Continuously scans a vendor's external attack surface to identify exposed assets and risks

Threat Intel Agent

Continuously checks for threat indicators from past breaches and assets including exposed S3 buckets

Trust Center Agent

Parses trust centers to auto-extract certifications, policies, and security artifacts

Fourth-Party Agent

Uncovers hidden fourth parties by mapping downstream vendors like AWS, Slack, Okta, and more

Contract Intelligence Agent

Analyzes contracts to flag missing clauses, compliance risks, and security misalignments

Auto-Fill Agent

Pre-populates 95% of questionnaires with known data to save time and ensure consistency

Communication Agent

Automates reminders, clarifications, and auto-drafts follow-ups to vendors

Assessment Reviewer Agent

Highlights incomplete, inconsistent, or expired responses across submitted assessments

Evidence Analyzer Agent

Reviews uploaded documents and auto-classifies them enabling quick analysis and review

Monitoring Agent

Tracks third-party risk posture over time and alerts on key changes, breaches, or reassessment triggers

The New Way With SAFE

OLD

MANUAL & REACTIVE
Vendor chasing, spreadsheets, emails

SLOW
Weeks to assess or onboard a vendor

CONTROL-BASED
Focus on questionnaire completion, not actual risk

FRAGMENTED TOOLS
Ratings, Questionnaires, GRCs, managed separately

LIMITED COVERAGE
Focus on top 10–20% vendors

NEW

AUTONOMOUS & PROACTIVE
AI agents handle end-to-end workflow

SCALABLE
Assess thousands of vendors in hours, not weeks

RISK-BASED
Business impact per vendor

UNIFIED PLATFORM
Integrating Ratings, Questionnaires, Contracts,...

COVERAGE AT SCALE
Including shadow 3rd parties and 4th parties

SAFE

Take the SAFE Advantage: **Schedule your 1:1 demo** with a TPRM expert!

CATEGORY LEADER IN CRQ

FORRESTER CRQ WAVE Q3, 2023

LEADER IN THIRD PARTY RISK MANAGEMENT

LIMINAL LINK INDEX™ REPORT, 2025

CYBER INSURTECH OF THE YEAR 2025

INSURTECH, 2025

RESEARCH SPONSOR

MITRE ATT&CK, TOP CONTRIBUTOR

www.safe.security | getintouch@safe.security