The Enterprise Risk Intelligence Buyer's Guide

How to evaluate platforms for third-party risk, ownership transparency, and defensible investigations

Buyer Guide · Enterprise Risk

74% **86%** **15×**

of risk leaders say siloed [illegible] entity intelligence vs. manual rese

Gartner, 2025

Forrester, 2025

Sayari Analytics

The Market Has Shifted

Enterprise risk buyers are no longer purchasing narrow screening utilities. They are being asked to justify investment in a system of record for third-party intelligence: a platform capable of resolving ownership, linking adverse and sanctions signals across jurisdictions, supporting defensible investigations, and fitting into procurement, compliance, legal, and security workflows.

Perfect Storm Driving Demand

Gartner identifies trade volatility, cyberattacks, new regulatory requirements, and supply chain disruptions as core drivers of platform investment. Siloed approaches to third-party management frequently do not work well in practice.

Why vendors are winning on breadth over depth

Many enterprises currently rely on multiple TPRM solutions for different use cases. Gartner research confirms that these siloed arrangements tend not to perform well operationally. In Sayari's 2025 Enterprise Survey, 67% of decision-makers reported their risk management stack was only partially integrated with their enterprise IT environment, and 14% said it was not integrated at all.

The integration imperative

The modern enterprise risk problem is less about the absence of data and more about the absence of integration, traceability, and cross-functional usability. Enterprise risk teams are now being asked to answer more exacting questions: Can we identify beneficial owners? Can we connect ownership to sanctions and adverse history? Can we demonstrate the basis for our risk decisions to auditors and regulators? Can we monitor change without building unsustainable manual processes?

02 The Real Obstacle Is Alignment

The internal approval challenge is often underestimated. Many buyers assume the decision will turn on product functionality, but in practice it turns on whether the buyer can answer four critical internal questions:

1. **Why now?**
2. **Why this platform rather than the status quo?**
3. **What economic value justifies the spend?**
4. **How will this reduce friction?**

Buying complexity is structural

Forrester research shows that 86% of B2B purchases stall during the buying process, 81% of buyers are dissatisfied with their final provider selection, and the average decision now involves 13 internal stakeholders across two or more departments. The evaluation process must produce institutional alignment, not just vendor preference.

> **This is where many evaluations fail**
> The product may appear compelling in a demo, but the internal champion cannot translate it into a form that the CFO, procurement, legal, or security organization can approve with confidence.

What the CFO needs to hear

A sophisticated CFO is unlikely to approve this category on the basis of vague claims about 'better intelligence.' The business case needs to be framed around measurable outcomes:

Reduction of fragmented tooling: If teams currently rely on multiple subscriptions, spreadsheets, or manual reconciliations, the platform should be framed as reducing duplicative spend and operational drag.

Greater operating leverage: The strongest argument is headcount productivity: the ability for existing analysts to cover more third parties and move faster on escalations.

Better defensibility: A platform that cannot preserve source evidence, ownership logic, and change history may save time in a demo but create downstream cost in reviews and escalations.

Monitoring coverage without linear cost growth: In Sayari's survey, respondents reported continuously monitoring only 49.6% of third parties they manage, even though 86% said continuous monitoring is essential.

9 What a Mature Program Looks Like

Mature third-party risk programs are characterized by integration, not fragmentation. They move through distinct phases of operational maturity:

Stage	Characteristics	Platform requirements
Reactive	Isolated screening; event-driven investigations; limited monitoring	Single-point tools; manual research
Coordinated	Onboarding diligence across teams; periodic reviews; basic monitoring	Multiple tools with manual handoffs; fragmented data
Integrated	Unified platform; automated diligence; meaningful monitoring coverage; streamlined workflows	Single platform supporting the full lifecycle; integrated monitorin
Intelligent	Predictive escalation; ownership automation; cross-domain insights	Advanced analytics; API-driven integrations; explainable reasoning

Most enterprises evaluating a platform purchase are attempting to move from the reactive or coordinated stage toward integration or intelligence. This shift requires not just better data, but better operating processes and stronger alignment across stakeholders.

04 Aligning Your Buying Committee

A strong internal champion should assume that each stakeholder is trying to answer a different question. The evaluation and approval process must generate evidence that answers all of them.

Stakeholder	Primary question	What they need to see
CFO / Finance	Why is this worth the spend?	Economic logic, reduced fragmentation, productivity, risk reductio
Procurement	Will this integrate into sourcing workflows?	Implementation model, workflow fit, vendor viability, commercial c
Compliance / Legal	Will outputs stand up to audit or challenge?	Source traceability, audit trail, defensibility
IT / Security	Will this create risk?	Architecture, controls, API/integration model, data handling
Risk / Operations	Will this materially improve decisions?	Coverage, explainability, alerting, escalation usability

This is not merely a messaging exercise. It should shape the evaluation design itself. A platform that looks attractive in a generic product demonstration may still fail if the buying process does not generate evidence for each of these stakeholder groups.

The Evaluation Framework

The most important evaluation mistake is to over-weight data volume and under-weight traceability, operational fit, and defensibility. A sophisticated buyer should focus on five core capabilities:

1. Primary-source traceability The ability to trace a finding to underlying source material: registry documents, filings, court records, sanctions references. Without that, the platform functions as a black-box assertion engine.

2. Ownership resolution depth Many vendors can identify a direct shareholder. Fewer can resolve beneficial ownership through layered control structures. This matters because hidden control is where the highest-risk exposure sits.

3. Explainability and audit trail Risk scores may help triage, but they do not replace evidence. Buyers should evaluate whether an analyst can later reconstruct why a third party was flagged.

4. Workflow integration Gartner advises buyers to define must-have capabilities and assess implementation and API requirements. The value of a platform is often destroyed by weak integration.

5. Jurisdictional fit, not just 'global coverage' 'Global coverage' is too imprecise. Buyers should understand where the platform is strongest and how it performs in jurisdictions most relevant to actual exposure.

The vendor scorecard

Criterion	Weight	What strong looks like	Why it matters
Primary-source evidence	20%	Findings link back to reviewable source material	Supports defensibility
Ownership depth	20%	Handles complex multi-layer structures across jurisdictions	Reduces hidden exposure
Workflow integration	15%	Fits existing processes with minimal operational friction	Lowers adoption risk
Explainability / auditability	15%	Preserves evidence, logic, and case history	Strengthens governance

Cross-domain coverage	10%	Connects ownership, sanctions, legal, and adverse signals	Improves investigation completeness
Monitoring capability	10%	Supports meaningful continuous monitoring and alerting	Improves detection coverage
Jurisdictional fit	10%	Performs well where your actual risk resides	Avoids false confidence

Common Failure Modes

1. The Score-Only Trap

The evaluation over-weights risk scores without establishing how outputs are derived or defended.

2. The Integration Debt Problem

The buyer validates research quality but fails to prove operational fit, resulting in another disconnected point solution.

3. The Coverage Illusion

The vendor claims broad global capability, but underperforms in the jurisdictions or entity types that matter most.

4. The Monitoring Fiction

The system claims continuous monitoring, but in practice cannot support the population size or escalation requirements needed.

5. The Committee Collapse

The internal champion runs a product evaluation, but not an approval process. Necessary stakeholders are brought in too late.

Lessons from the Field

What mature buyers have learned

Sayari's survey of 139 decision-makers revealed consistent patterns among enterprises that have successfully moved from reactive to integrated programs:

• Most successful implementations treated the platform as a system of record, not a supplementary tool. This required executive sponsorship from the CFO or Chief Risk Officer.

• The evaluation design itself determined the outcome. Buying committees that mapped stakeholder evidence requirements produced more defensible decisions.

• Workflow integration was the primary driver of adoption. Platforms that required new processes or standalone case management tools struggled to achieve expected value.

• Monitoring coverage was only achievable with automated escalation and alert routing. Manual monitoring approaches remained limited to small populations.

• Source traceability became increasingly important during the first 12 months, when business decisions made on platform evidence came under scrutiny.

How to design the proof of concept

A strong proof of concept should be designed as an approval artifact, not merely a product demonstration. It should generate evidence that can be used with finance, procurement, compliance, and legal reviewers:

Use your hardest real entities. Include complex ownership structures and cases with known ambiguity. Do not use curated test data.

Test evidence preservation. Require the vendor to show the source trail. Assess whether outputs can be preserved for audit or committee review.

Test workflow fit. Run the process through procurement, TPRM, legal, or case-management workflows. Document what still requires manual handling.

Measure operational value. Track time to answer, analyst effort, monitoring coverage, and ease of escalation. Compare against your current process.

Document disqualifiers. Define in advance: no intelligible source trail, weak handling of complex ownership, poor performance in priority jurisdictions, or inability to integrate without extensive custom work.

How to make the final decision

The best buying decision is rarely the platform with the most features. It is the platform that best combines defensibility, ownership visibility, workflow fit, monitoring scalability, committee confidence, and economic credibility. The core question is not whether the platform can produce answers. It is whether it can produce answers that are sufficiently reliable, traceable, and operationally usable.

A For the CISO / Head of InfoSec

Information security leaders evaluating third-party risk platforms need to focus on:

Data Security & Vendor Risk
How is third-party data encrypted, accessed, and governed? What is the vendor's own security posture and audit status? Does the platform support SAML/SSO integration, role-based access control, and audit logging of all data access?

Integration Model
Is the platform API-driven or does it require manual data imports? Can it integrate with your SIEM and identity management systems without creating new attack surfaces?

Scope of Access
Does the platform need read access to procurement systems or other sensitive internal systems? What data does it store, transmit, and retain? Can you control the geographic location of data storage?

A For the CRO / ERM Lead

Chief Risk Officers and Enterprise Risk Management leaders need to focus on:

Program Coverage & Control Completeness
Does the platform cover all entity types and jurisdictions relevant to your risk profile? Can it support continuous monitoring of your full third-party population?

Regulatory Defensibility
Can the platform produce audit-ready documentation of your diligence process and the basis for your risk determinations? Does it preserve source evidence and change history?

Audit Trail & Escalation
Can analysts reproduce their work and explain their conclusions to auditors? Does the system support case history and change logging? Can you escalate findings without losing the underlying evidence?

A For the CPO / VP Supply Chain

Chief Procurement Officers and Supply Chain leaders need to focus on:

Supplier Discovery Speed & Onboarding Efficiency
Can the platform accelerate supplier onboarding by automating basic diligence and research? How much analyst time does it save? Does it integrate into your RFX or vendor management system?

Forced Labor & ESG Compliance
Does the platform have specific coverage for forced labor risks and ESG concerns? Can it identify ownership chains that matter for ESG reporting?

Workflow Integration with Procurement Systems
Can diligence findings flow directly into your procurement workflow, or do they require manual export? How does the platform handle remediation and ongoing monitoring?

A For the General Counsel / CCO

General Counsel and Chief Compliance Officers need to focus on:

Legal Exposure & Litigation Defensibility
If a business decision made on platform intelligence is challenged, can the platform provide evidence of diligence and the basis for the decision? Can it demonstrate reasonable care?

Source Citation & Evidence Quality
Are sources authoritative and verifiable? Can you rely on them in regulatory submissions or customer disclosures? Can the platform distinguish between primary sources and derived findings?

Sanctions & Export Control Compliance
Does the platform integrate with your OFAC and export control workflows? Can it demonstrate compliance with regulatory screening requirements?

Sources & References

• Gartner. (2025). 'Perfect Storm of Third-Party Risks are Driving Growth and Maturity in Third-Party Risk Management Technology Solutions.' Market context and evaluation guidance on TPRM platform selection.

• Forrester. (2024-2026). 'The State of Business Buying.' Research on B2B buying complexity, stalled purchases, stakeholder dynamics, and buying-committee composition.

• Sayari Analytics. (2025). Enterprise Survey. Fielded survey of 139 decision-makers on risk management stack integration, monitoring coverage, platform investment drivers, and vendor evaluation priorities.

This buyer's guide was prepared for enterprise risk, compliance, legal, and procurement leaders evaluating third-party intelligence platforms. For additional research support or case studies, contact Sayari Analytics.