Magic Quadrant for Third-Party Risk Management Tools for Assurance Leaders

6 April 2026 - ID G00839681 - 36 min read

By Antonia Donaldson, Nicholas Sworek

In a crowded TPRM technology market, assurance buyers need to know which tools best fit their target use cases. Legal, risk and compliance leaders can use this Magic Quadrant to identify technology solutions for enterprise TPRM and key risk domains.

Market Definition/Description

The third-party risk management (TPRM) technology market offers solutions to identify, assess, manage, monitor and report on third-party risks associated with vendors, suppliers, distributors, agents, partners or other third parties. Solutions in this market can support a wide range of TPRM workflows across various risk domains. TPRM platforms in this market address the needs of a diverse range of customers and risk domains, including legal, compliance, procurement, supply chain, IT, cybersecurity and other teams that work with or provide routine oversight of third parties. Some technology solutions offer enterprise third-party risk management workflow as a feature, along with risk tiering, due diligence, risk mapping, metrics and reporting mechanisms. Other platforms may facilitate integration with risk data subscriptions, data aggregators or other subscriptions.

The TPRM technology market is a complex array of solutions servicing many business functions across an enterprise. TPRM solution providers can be categorized into technology platforms and tools, or risk-domain-specific data and insights.

TPRM Technology Platforms and Tools

These software platforms assess, monitor, report and remediate third-party risks. Some solutions focus on one type of third party, such as IT vendors or suppliers. Many TPRM solutions function as modules within governance, risk and compliance (GRC) platforms. The scope of risk domain coverage varies: Some vendors specialize in one risk domain, while others cover a wide range of third-party risk areas. The capabilities and integration requirements of TPRM technology platforms differ, and buyers should carefully evaluate them.

Risk-Domain-Specific Data and Insights

These data subscriptions provide specific risk insights into particular risk domains. The data from these subscriptions can be used in isolation, such as evaluating a third party's financial adequacy and public security intelligence data posture before signing a contract. Alternatively, the data can be integrated into the broader TPRM process or platform to support risk evaluation and ongoing monitoring requirements.

Mandatory Features

TPRM solutions must support the following activities:

- **Identifying third-party risk:** Determine which risk domains are relevant to a third party.
- **Analyzing risk:** Measure the potential impact on a customer's business or supply chain and provide an impact estimate.
- **Managing and escalating risk:** Offer platform functionality to surface and escalate risks, informing risk mitigation efforts. This may include escalation, tracking, action plans and risk tiering.
- **Continuous monitoring:** Provide visibility into risk events through dashboards, reports, alerts, reminders and notifications.
- **Third- and fourth-party risk mapping and metrics:** Offer risk mapping, risk visualization, metrics and the ability to export third-party risk data for reports and presentations.

Magic Quadrant

Figure 1: Magic Quadrant for Third-Party Risk Management Tools for Assurance Leaders

Gartner

Vendor Strengths and Cautions

Aravo

Aravo is a Leader in this Magic Quadrant. It is a private company headquartered in San Francisco, California, U.S., with a majority of customers in North America, followed by Europe. Aravo serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and consumer goods. Aravo's three primary third-party risk domains include compliance and regulatory risk; financial risk; and environmental, social and governance (ESG) risk.

Its TPRM product is Intelligence-First Platform. An innovative feature is the Aravo Evaluate Engine, a risk scoring and scorecard solution that supports its delivery of risk management across vendors, suppliers, service providers, partners and other third-party relationships. Aravo is advancing its new AI-centric platform solution, Aravo AI, which assists users in completing routine third-party workflow tasks and amplifies risk registers.

Strengths

- **Customer support and implementation:** Aravo's TPRM product supports numerous third-party risk domains while offering rapid and flexible configuration changes for assurance leaders. In Gartner client inquiries, customers report positive experiences with implementation and postimplementation support services.

- **Product:** Aravo's Intelligence-First Platform streamlines and automates third-party onboarding and due diligence. It captures third-party criticality, data sensitivity, service type and regulatory requirements. Configurable risk tiering dynamically adjusts TPRM workflows.

Cautions

- **Overall viability:** Aravo did not share profitability, growth rate or level of R&D investment with Gartner; therefore, we are unable to verify its profitability, growth prospects or market position.

- **Geographic coverage:** Aravo's customer base is heavily concentrated in North America. It targets a number of assurance buyer personas and serves several verticals; however, its installed base and geographic coverage outside the U.S. is limited. This may delay its ability to attract new customers and scale its presence in other regions.

Archer

Archer is a Challenger in this Magic Quadrant. It is a private company headquartered in Overland Park, Kansas, U.S., with a majority of customers in North America, followed by Europe and the Middle East. Archer serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and insurance. Archer's three primary third-party risk domains include information security risk, financial risk and ESG risk.

Its TPRM product is Archer Third-Party Risk Management (TPRM). An innovative feature is its proprietary enterprise risk quantification methodology for third-party risk, moving beyond qualitative heat maps to measurable, decision-ready metrics. Across 2026, Archer plans to expand its SaaS-based product offering, Archer Evolv, and embed AI agents.

Strengths

- **Overall viability:** Archer is a well-established and profitable governance, risk and compliance (GRC) and TPRM vendor with a demonstrated track record of financial stability. As an embedded solution, it maintains a high TPRM customer renewal rate, reflecting customer confidence in the stability of the platform.

- **Innovation:** Archer is investing in AI to enhance its TPRM product to reduce manual work in compliance and risk, support regulatory updates, and improve third-party oversight. Its solution successfully integrates assurance-specific use cases, such as operational risk, AI governance and ESG in highly regulated industries, enabling improved regulatory alignment.

Cautions

- **Vertical/industry strategy:** While Archer's platform provides strong functionality for regulated environments, it does not offer industry-specific TPRM configurations, extensions or add-ons. Organizations with specialized needs may require additional customization.

- **New customer acquisition:** Archer's TPRM product has demonstrated a low annual growth rate over the past two years, despite maintaining an exceptionally high renewal rate. While existing customers show confidence in the platform, this dichotomy suggests potential challenges attracting new buyers in a competitive market.

Certa

Certa is a Leader in this Magic Quadrant. It is a private company headquartered in Saratoga, California, U.S., with a majority of customers in North America, followed by Europe and the Asia/Pacific region. Certa serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and manufacturing. Certa's three primary third-party risk domains include privacy and data processing risk, antibribery and anticorruption, sanctions screening, and ESG risk.

Its TPRM product is Certa Third-Party Operating System. An innovative feature is its embedded AI, facilitating rapid integration of third-party risk signals, continuous assessment and escalation. Certa expects to enhance data reporting and analytics capabilities along with its AI concierge to support core TPRM use cases.

Strengths

- **Vertical/industry strategy:** Certa offers multiple industry-specific configurations, extensions or add-ons across several verticals such as financial services, manufacturing and consumer goods. This enables tailored TPRM workflows for industry-specific requirements.

- **Product:** Certa provides comprehensive TPRM workflow solutions with embedded AI, including centralized third-party onboarding and offboarding, real-time third-party risk visibility, live status tracking, continuous risk and compliance monitoring, and auditability across the third-party life cycle.

Cautions

- **Marketing strategy:** Certa targets a broad range of buyer personas, including procurement, sourcing and information security leaders, in addition to several assurance-led roles. This diluted focus may limit its ability to grow its installed base and follow through on product development plans.

- **Overall viability:** Founded in 2017, Certa is a relatively new entrant to the TPRM technology market. Its installed TPRM customer base remains relatively small in comparison to other Leaders in this Magic Quadrant.

Diligent

Diligent is a Leader in this Magic Quadrant. It is a private company headquartered in New York, New York, U.S., with a majority of customers in North America, followed by Europe. Diligent serves clients in an array of verticals; its top three include financial services, manufacturing, and energy and utilities. Diligent's three primary third-party risk domains include cybersecurity risk, business and operational risk, and compliance and regulatory risk.

Its TPRM product is 3rdRisk. Innovative features include AI-native detection of third-party risks, continuous monitoring and enhanced due diligence reports. Diligent expects to amplify adaptive TPRM workflows across the entire third-party life cycle.

Strengths

- **Customer experience:** Diligent maintains a formal annual customer advisory board for its risk and compliance portfolio, and hosts a specific TPRM user conference. TPRM customers are actively involved in design partner programs, offering structured feedback loops and ensuring customer-driven prioritization of TPRM capabilities.

- **Vertical/industry strategy:** Diligent offers its customers a diverse set of industry-specific TPRM customizations and extensions. This range covers core risk areas such as sanctions, politically exposed persons (PEPs), adverse media, the Digital Operational Resilience Act (DORA), third-party risk classification and regulatory scans/reporting.

Cautions

- **Marketing execution:** Diligent's TPRM-specific marketing strategy has historically lacked clarity due to its GRC-first platform focus. While the acquisition of 3rdRisk in January 2026 signals an intent to expand into new verticals in Europe and North America, the effectiveness of this shift remains unproven.

- **Global support:** Following the acquisition of 3rdRisk, most dedicated TPRM staff are based in The Netherlands. Diligent may focus on change management and integration priorities. As Diligent scales its TPRM product resources, responsiveness outside of Europe may lag.

GAN Integrity

GAN Integrity is a Challenger in this Magic Quadrant. It is a private company headquartered in New York, New York, U.S., with a majority of customers in North America, followed by Europe and the Asia/Pacific region. GAN Integrity serves clients in an array of verticals; its top three include mining and extraction, manufacturing, and healthcare and life sciences. GAN Integrity's three primary third-party risk domains include antibribery and anticorruption risk, ESG and modern slavery risk, and trade compliance risk.

Its TPRM product is Third-Party Risk Management. An innovative feature is its native ability to surface deep risks covering several domains with real-time screening against global watchlists. GAN Integrity expects to enhance ESG features, amplify partner network mapping and deploy more AI risk screening of third parties.

Strengths

- **Market understanding:** GAN Integrity responds to assurance leaders' demand for efficient due diligence with Integrity Enrich. This open-source solution rivals other due diligence providers by rapidly revealing third-party ownership, risks and interdependencies.
- **Solution breadth:** GAN Integrity's compliance-focused tools cover diverse assurance and risk management use cases. Its architecture connects data points to identify risks, linking internally reported conflicts of interest with third parties for added risk detection and mitigation.

Cautions

- **Vertical/industry strategy:** GAN Integrity offers a highly configurable TPRM workflow engine; however, its delivery model offers only a public cloud, and it does not offer industry-specific configurations or add-ons. Buyers in highly regulated industries should evaluate the product delivery model.
- **AI integration:** Many of GAN Integrity's AI capabilities currently lag behind peers. Buyers seeking significant efficiency gains through advanced analytics, risk quantification, content generation or automated control development may find the tool limiting.

LogicGate

LogicGate is a Challenger in this Magic Quadrant. It is a private company headquartered in Chicago, Illinois, U.S., with a majority of customers in North America, followed by Europe. LogicGate serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and retail and e-commerce. LogicGate's three primary third-party risk domains include cyber risk, AI management and governance risk, and privacy risk.

Its TPRM product is Third-Party Risk Management Solution. An innovative feature is Spark AI, which accelerates processes such as third-party onboarding and questionnaire response review. LogicGate expects to amplify continuous third-party risk monitoring, automate population of third-party findings and enhance record linking.

Strengths

- **Innovation:** LogicGate's pragmatic approach to innovation prioritizes high-impact use cases. Its solution addresses common TPRM pain points, such as duplicative records, manual data entry, questionnaire development and program ROI calculation.

- **Deployment:** LogicGate enables focused, small-to large-scale TPRM deployments without requiring adoption of the full GRC suite. Its no-code configuration allows quick adjustments after go-live, making the platform easy to maintain and operate for nontechnical users.

Cautions

- **Sales execution:** LogicGate is intentionally shifting its sales focus from midmarket verticals to large enterprises. This may introduce complexity or changes to LogicGate's pricing structure.

- **Product:** LogicGate lacks native deep due diligence capability and offers only a limited selection of preconfigured connectors via its one-click marketplace. Assurance teams with limited IT resources may need to rely more heavily on prebuilt connectors.

LogicManager

LogicManager is a Niche Player in this Magic Quadrant. It is a private company headquartered in Boston, Massachusetts, U.S., with a majority of customers in North America, followed by Europe. LogicManager serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and manufacturing. LogicManager's three primary third-party risk domains include operational resilience and business continuity risk, cybersecurity and data protection risk, and financial risk.

Its TPRM product is LogicManager. An innovative feature is its ability to address operational resilience and business continuity risk by linking critical vendors to core business processes and recovery objectives. LogicManager expects to enhance fourth-party visibility and amplify TPRM workflow efficiency.

Strengths

- **Vertical/industry strategy:** LogicManager delivers embedded industry-aligned libraries, frameworks and workflows that streamline implementation in regulated sectors. Its industry-specific content expedites deployment and supports core TPRM functionality.

- **Market understanding:** LogicManager targets ERM, legal and compliance leaders responsible for governance, regulatory outcomes and contract exposure. Its cross-assurance design connects third-party workflows such as contracting and third-party oversight.

Cautions

- **Innovation roadmap:** LogicManager's pace of product innovation remains unclear. For example, its limited AI applications and lack of dedicated AI development resources may be a concern for buyers seeking advanced capabilities.

- **Geographic reach:** With more than 90% of revenue derived from North America, LogicManager's geographic reach is limited. Global support is minimal and English-only. Organizations with operations across multiple countries may encounter language barriers.

MetricStream

MetricStream is a Challenger in this Magic Quadrant. It is a private company headquartered in San Jose, California, U.S., with a majority of customers in North America, followed by Europe and the Middle East. MetricStream serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and energy. MetricStream's three primary third-party risk domains include cybersecurity risk, reputational risk and business continuity risk.

Its TPRM product is MetricStream Third-Party Risk Management. An innovative feature is its AI-driven risk classification, risk scoring and red flag identification. MetricStream expects to continue enhancing its product with investments in automated risk quantification, agentic workflows and scenario modeling.

Strengths

- **Regulatory industry expertise:** MetricStream supports complex global TPRM operations and sovereignty with robust capabilities that are configurable in its base product. It streamlines risk data, workflow design and governance, making it well-suited for highly regulated sectors like financial services, banking, and healthcare and life sciences.

- **Product:** MetricStream offers deep configurability and advanced features, including enhanced insights, predictive risk analytics and automated summarization. This addresses market demand for improved risk detection, decision quality and efficiency.

Cautions

- **User experience:** While MetricStream is transitioning to a React-based UI, customer feedback indicates the UI and overall user experience lack intuitiveness and modern design. Improvements are in progress, but Gartner client inquiries suggest the platform does not yet meet users' expectations for ease of use.

- **Implementation:** MetricStream's implementation can be complex and time-consuming. Deployments often require significant resources and extended timelines. Buyers seeking a dedicated, stand-alone TPRM tool may experience challenging deployments, particularly for large-scale or customized implementations.

NAVEX

NAVEX is a Niche Player in this Magic Quadrant. It is a private company headquartered in Lake Oswego, Oregon, U.S., with a majority of customers in North America, followed by Europe. NAVEX serves clients in an array of verticals; its top three include healthcare and life sciences, financial services, and manufacturing. NAVEX's three primary third-party risk domains include regulatory and compliance risk, reputational risk, and operational and business continuity risk.

Its TPRM product is NAVEX One. An innovative feature is its ability to apply business rules to automate workflow tasks, such as scoring and routing. NAVEX expects to continue to invest in advanced regulatory change management functionality in risk areas such as sanctions, trade and antibribery, and anticorruption laws.

Strengths

- **Customer experience:** NAVEX offers a diverse selection of products that cover a wide range of compliance and TPRM use cases. This enables assurance leaders to source multiple capabilities from a single vendor and enhances end-user experience.

- **Market understanding:** NAVEX has positioned its brand as a solution purpose-built for compliance and assurance leaders, rather than as an IT or privacy-centric tool. It offers deep compliance-related expertise and is a specialized provider capable of supporting multiple compliance use cases.

Cautions

- **Overall viability:** In 2025, NAVEX appointed a new CEO and was majority acquired by a Goldman Sachs-led consortium. NAVEX did not share its growth trajectory, profitability, or client retention data with Gartner; therefore, we are unable to verify its financial outlook, growth prospects or market position.

- **AI integration:** While NAVEX provides an assurance-focused, risk-oriented platform, its AI capabilities lag behind industry leaders. The platform is limited in areas such as autofill, advanced analytics, risk quantification, content generation and automated control development.

OneTrust

OneTrust is a Leader in this Magic Quadrant. It is a private company headquartered in Atlanta, Georgia, U.S., with a majority of customers in North America, followed by Europe and the Asia/Pacific region. OneTrust serves clients in an array of verticals; its top three include technology, manufacturing, and healthcare and life sciences. OneTrust's three primary risk domains include privacy, compliance and regulatory risk, and AI data risk.

Its TPRM product is OneTrust Third-Party Management. An innovative feature is its AI-assisted document scanning, ingestion and extraction to prepopulate third-party assessments. OneTrust expects to release new product functionality that enhances visibility into supply chain dependencies and identifies concentration and continuity risks.

Strengths

- **Product:** OneTrust offers a sophisticated and highly configurable onboarding process with automated due diligence questions and customized templates. It provides risk screening and ongoing monitoring for privacy and regulatory compliance, using data integration from complementary products such as Risk Exchange and Dow Jones.

- **AI innovation:** OneTrust's optional AI agents allow document ingestion and assessment response, automated onboarding, screening, risk tiering, and autogenerated risk reports. This allows customers to ask questions about the platform and compliance.

Cautions

- **Marketing execution:** OneTrust targets IT leaders for coverage of cybersecurity, privacy and data protection and is shifting from a module-based to a persona-led sales approach focused on GRC and TPRM workflows. Its IT governance, risk and compliance (ITGRC) emphasis has limited product relevance for assurance buyers. Its focus has historically been on third-party risk domains such as privacy and data protection.

- **Implementation support:** OneTrust has a limited number of employees dedicated to TPRM product implementation and integration. It relies heavily on consulting and implementation partners that are primarily located in North America.

Onspring

Onspring is a Niche Player in this Magic Quadrant. It is a private company headquartered in Overland Park, Kansas, U.S., with a majority of customers in North America. Onspring serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and insurance. Onspring's three primary third-party risk domains include cybersecurity risk, compliance risk and operational risk.

Its TPRM product is Onspring Third-Party Risk Management. An innovative feature is AI-driven third-party risk identification, which offers smart suggestions for risk response throughout the TPRM life cycle of a business relationship.

Onspring declined requests for supplemental information or to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Product strategy:** Onspring provides a no-code configurable TPRM platform that enables easy implementation without outside resources. Its AI-driven document ingestion and out-of-the-box real-time reporting support straightforward workflows and custom assessments.

- **Implementation:** Onspring offers centralized customer service from its headquarters location in North America. Clients report faster-than-average implementation timelines and high levels of customer satisfaction.

Cautions

- **Global reach:** While Onspring is an established player in the North American TPRM marketplace, it does not have a robust global footprint outside of the U.S. and Canada.

Organizations with broad global operations or those based outside North America with sovereignty requirements may require services and support this vendor does not offer.

- **Product positioning:** Onspring's top buying personas include managers of risk and procurement. Its product strategy highlights a consolidated, integrated GRC and TPRM solution. Few customers are buying Onspring as a stand-alone TPRM tool.

Optro

Optro, formerly AuditBoard, is a Leader in this Magic Quadrant. It is a private company headquartered in Wilmington, Delaware, U.S., with a majority of customers in North America, followed by Europe and the Asia/Pacific region. Optro serves clients in an array of verticals; its top three include financial services, manufacturing and technology. Optro's three primary third-party risk domains include regulatory risk, privacy risk and cybersecurity risk.

Its TPRM product is Third-Party Risk Management Solution. An innovative feature is its ability to scale and integrate TPRM across audit, risk and compliance for improved risk visibility. Optro expects to enhance data feeds and composite third-party scoring to enable cross-domain risk intelligence.

Strengths

- **Market understanding:** Optro's TPRM product is practitioner-led and resonates strongly with legal, risk, compliance and audit professionals. This offers customers the opportunity to configure the solution to address multiple third-party risk domains and meet the needs of a variety of assurance stakeholders.

- **Innovation:** Optro has invested heavily in the user experience and developed an intuitive TPRM product interface with a deep set of onboarding and training resources. This results in faster-than-average implementation, and clients report high levels of satisfaction.

Cautions

- **Overall viability:** TPRM is a relatively recent addition to the Optro portfolio and is still gaining traction. The vendor did not share the growth and installed TPRM customer base for the prior two years with Gartner; therefore, we are unable to verify its market traction in the TPRM segment.

- **Operations:** Optro does not have dedicated full-time employees assigned exclusively to its TPRM product, as it leverages a broader GRC platform strategy. This may impact specialized support and product development for customers seeking focused TPRM expertise.

ProcessUnity

ProcessUnity is a Challenger in this Magic Quadrant. It is a private company headquartered in Concord, Massachusetts, U.S., with a majority of customers in North America, followed by Europe. ProcessUnity serves clients in an array of verticals; its top three include financial services, IT, and healthcare and life sciences. ProcessUnity's three primary third-party risk domains include cybersecurity risk, financial risk and regulatory risk.

ProcessUnity's TPRM product is the ProcessUnity TPRM Platform. An innovative feature is its data-first approach. It integrates external threat intelligence with internal control data, and its deep data integration ensures that information from procurement, GRC, CRM and contract life cycle management (CLM) systems is normalized, contextualized and actionable throughout the third-party life cycle.

Strengths

- **Product:** ProcessUnity provides automated and interactive due diligence workflows by leveraging AI features such as document evaluation and assessment in response to third-party questionnaires. Customers can also integrate their own AI tools to evaluate third-party data.

- **Customer experience:** ProcessUnity takes a customer-driven approach to developing its roadmap. It hosts three annual in-person customer conferences globally, organizes in-person customer summits and runs virtual advisory board meetings.

Cautions

- **Buyer alignment:** While ProcessUnity has non-IT assurance clients, it is primarily aligned to IT-focused roles such as CISOs, CIOs and chief procurement officers. Assurance leaders assessing risks holistically across non-IT risk domains to support enterprise risk and compliance use cases may find the product less tailored to their traditional assurance needs.

- **Vertical/industry strategy:** ProcessUnity does not offer out-of-the-box industry-specific configurations or add-ons, although it does target verticals such as financial services and healthcare. Its add-ons for German Supply Chain Act, DORA and Australian Prudential Regulation Authority (APRA) may require configuration to satisfy the requirements of highly regulated industries.

Riskonnect

Riskonnect is a Challenger in this Magic Quadrant. It is a private company headquartered in Atlanta, Georgia, U.S., with a majority of customers in North America, followed by Europe and the Asia/Pacific region. Riskonnect serves clients in an array of verticals; its top three include financial services, manufacturing and retail. Riskonnect's three primary third-party risk domains include operational resilience risk, cybersecurity and privacy risk, and regulatory risk.

Its TPRM product is Riskonnect Third-Party Risk Management software. An innovative feature is its embedded AI, allowing customers to rapidly generate third-party risk intelligence information and related reports. Riskonnect expects to add more features to streamline the third-party due diligence process.

Strengths

- **Overall viability:** Relative to the majority of vendors in this Magic Quadrant, Riskonnect has a proportionately smaller base of TPRM customers. Yet, it achieved 70% growth in its customer base last year, indicating a robust growth trajectory.

- **Product:** Riskonnect has core onboarding workflows, industry-specific assessments and broad risk coverage. It integrates with cyber risk intelligence and supports assurance-related risk domains, such as sanctions, ESG compliance and regulatory screening.

Cautions

- **Platform:** While customers do not need to be Salesforce CRM customers to use Riskonnect Third-Party Risk Management software, it is linked to the Salesforce platform; some CRM fields may not be compatible with end-user needs. Salesforce serves as the underlying technical foundation, but there is no integration requirement. Buyers should evaluate product architecture and platform dependencies.

- **Customer experience:** Riskonnect's emphasis is on GRC, connected enterprise risk and unified risk management. This may limit alignment with customers seeking a stand-alone, specialized TPRM workflow solution or assurance buyers seeking core third-party risk utility.

SAI360

SAI360 is a Visionary in this Magic Quadrant. It is a private company headquartered in Chicago, Illinois, U.S., with a majority of customers in North America, followed by Europe. SAI360 serves clients in an array of verticals; its top three include financial services, healthcare and life sciences, and manufacturing. SAI360's three primary third-party risk domains include compliance and regulatory risk, antibribery and anticorruption risk, and privacy and data processing risk.

Its TPRM product is SAI360's Third-Party & Vendor Risk Management software. An innovative feature is its customizable workspaces that allow customers to arrange TPRM workflow elements, such as assigned tasks, assessments, and data visualization. SAI360 expects to continue enhancing its vendor risk dashboards and advanced risk management capabilities for third-party suppliers, vendors and partners.

Strengths

- **Market understanding:** SAI360 focuses on assurance leaders, with TPRM functionality aligned to its core GRC product and integrated regulatory risk intelligence. Its investment in risk assessments tied to changing regulations may benefit organizations seeking robust compliance and privacy coverage.

- **Sales strategy:** SAI360 targets chief risk officers, chief compliance officers and heads of internal audit, positioning TPRM as part of overall risk governance rather than a stand-alone function. It intends to expand its geographic footprint, promoting adoption among highly regulated industries.

Cautions

- **Overall viability:** SAI360 did not share information pertaining to its TPRM customer base or profitability with Gartner; therefore, we are unable to verify its financial outlook, growth prospects or market position.

- **Customer experience:** SAI360 does not maintain either a customer advisory board or conduct TPRM-specific user conferences. As a result, TPRM customers have fewer opportunities for TPRM product input and training, especially those not using the GRC solution.

Inclusion and Exclusion Criteria

Inclusion Criteria

The inclusion criteria are the specific attributes that a provider must have to be included in this Magic Quadrant:

- Offer a generally available proprietary software product available for a minimum of 12 months prior to December 2025 that meets Gartner's Market Definition, enabling third-party life cycle risk management for those risk domains managed by assurance leaders.
- Solution must be sold to and adopted by assurance leaders who lead legal, enterprise risk, compliance and/or audit functions.
- Demonstrate the following essential features: identify third-party risk; analyze third-party risk; manage and escalate third-party risk; monitor third parties; and offer third-party analytics, including risk dashboards, mapping and metrics.
- Demonstrate required TPRM capabilities without requiring the mandatory adoption or integration of other vendor-specific enterprise business applications that may reside on the same platform layer, for customers to realize significant value from the TPRM product itself.
- Gartner client relevance, as determined by analyst expertise and guided by public and proprietary information.

Exclusion Criteria

- Resellers of TPRM solutions, including data aggregators or third-party providers, even if their solution meets the Market Definition.
- Vendors that primarily sell related software technologies or tools, such as regulatory intelligence, third-party cybersecurity risk management solutions (TPCRM), supply chain management, procurement and/or purchasing systems, business continuity management (BCM) tools, or operational technology (OT) tools, independent of an

offering that addresses third-party life cycle management including the following: risk identification, assessment, mitigation, monitoring and reporting for core risk domains managed by legal, compliance and risk leaders.

- Vendors with TPRM product offerings that are predominantly centered on specialized business functions such as supply chain, procurement, cybersecurity, data analytics, regulatory intelligence, and environmental, health and safety (EHS).
- Vendors that specialize in a particular industry such as healthcare or hospitality.
- Vendors for which a majority of their client base is primarily attributed to any single one of the following business functions:
  - Procurement and sourcing leaders (CPOs)
  - IT leaders (CIOs, CTOs)
  - Infosec/cybersecurity leaders (CISOs)
  - Supply chain leaders
  - Data privacy leaders (DPOs)
  - Chief data and analytics officers (CDAOs)

Evaluation Criteria

Ability to Execute

Vendors were evaluated based on their Ability to Execute by assessing how well their products, services and operations enable assurance leaders (legal, risk, compliance, audit) to effectively manage third-party risk across the enterprise.

The evaluation criteria for Product or Service and Customer Experience have High weightings. The Product or Service criterion evaluates the capabilities, features and overall quality of the core goods and services that serve the defined market. Customer Experience evaluates the degree to which a vendor’s products, services and programs enable customers to achieve their desired results.

The criterion for Operations receives a Medium weighting, evaluating the organization's ability to meet its goals and commitments.

Overall Viability, Sales Execution/Pricing and Marketing Execution receive Low weightings. While these criteria assess important factors like overall financial health, sales strategy and brand messaging, they are secondary to the core functionality and user experience required by assurance leaders.

Finally, Market Responsiveness/Record is not rated. By assigning a zero weight to this criterion, the assessment focuses the analysis more heavily on items that are truly differentiating for current TPRM buyers and personas.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Low
Sales Execution/Pricing	Low
Market Responsiveness/Record	NotRated
Marketing Execution	Low
Customer Experience	High
Operations	Medium

Source: Gartner (April 2026)

Completeness of Vision

Gartner evaluates vendors on their Completeness of Vision by assessing their ability to understand current market trends, articulate a clear direction and innovate to meet the future needs of assurance leaders managing third-party risk.

The evaluation criteria for Market Understanding and Offering (Product) Strategy have High weightings. Market Understanding evaluates a vendor's ability to grasp current and future customer needs and translate them into a clear vision for the evolving TPRM market. Offering (Product) Strategy assesses the vendor's approach to product development, looking for scalable, highly differentiated solutions that focus on assurance-centric risk domains, advanced data analytics and embedded AI tools.

The criterion for Innovation receives a Medium weighting, evaluating the vendor's product roadmap, customer-centric support strategies and overall marshaling of resources for competitive advantage.

Sales Strategy, Vertical/Industry Strategy, and Geographic Strategy receive Low weightings. While these criteria assess important factors like sales network effectiveness, industry-specific configurations and geographic reach, they are secondary to the foundational product vision and market understanding required to support assurance leaders.

Finally, Marketing Strategy and Business Model are not rated. By assigning a zero weight to these criteria, the evaluation focuses more heavily on the strategic product direction and innovation that directly impact TPRM capabilities for buyers.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	NotRated
Sales Strategy	Low
Offering (Product) Strategy	High

Evaluation Criteria	*Weighting*
Business Model	NotRated
Vertical/Industry Strategy	Low
Innovation	Medium

Source: Gartner (April 2026)

Quadrant Descriptions

Leaders

Leaders are in the strongest position to influence the market's growth and direction. They demonstrate a market-defining vision for how TPRM technology can help organizations support a holistic TPRM process, encompassing risk identification, assessment, mitigation, monitoring and reporting across multiple risk domains and assurance roles. Leaders are often the vendors that other providers measure themselves against.

Leaders in the TPRM technology market demonstrate strong execution and a comprehensive vision tailored specifically to the needs of assurance leaders. They offer robust, highly configurable platforms capable of managing a wide array of cross-functional risk domains.

Leaders combine advanced capabilities, such as AI-native risk detection and continuous monitoring, with exceptional customer experience and postimplementation support. While the market is still maturing, typical Leaders also possess a deep understanding of market trends and showcase a clear offering strategy that scales across multinational organizations and highly regulated industries.

Challengers

Challengers possess a strong Ability to Execute and maintain a solid operational track record, often supported by established risk and compliance experience and large installed customer bases. They deliver capable TPRM solutions with reliable core functionalities, such as centralized onboarding workflows, data connectors and automated due diligence.

However, Challengers typically lack the comprehensive market vision or targeted innovation seen in Leaders. In this market, a Challenger may trail in advanced AI integration, maintain a narrower geographic focus or lack deep, industry-specific configurations, which can restrict their ability to fully anticipate and address the evolving, specialized needs of enterprise assurance leaders.

Challengers have demonstrated the ability to meet customers' expectations in terms of functionality and customer experience. Challengers may have a good vision for TPRM technology, but may not have fully won over assurance leaders and other business stakeholders.

Visionaries

Visionaries demonstrate a strong understanding of where the TPRM market is heading and offer innovative strategies to address the complex oversight requirements of assurance leaders. They may pioneer advanced capabilities, such as integrated regulatory risk intelligence, dynamic risk assessments tied to changing regulations and customizable workspaces for data visualization.

Despite their forward-looking product strategies, Visionaries often trail in their overall Ability to Execute. Compared to Leaders and Challengers, they may have a smaller or less proven installed customer base or less robust customer experience programs, such as lacking dedicated customer advisory boards or comprehensive user conferences.

Visionaries are ahead of most competitors in terms of delivering innovative TPRM products and/or delivery models, and offer a solid product strategy. They may embody trends that are shaping, or will continue to shape, the TPRM technology market.

Niche Players

Niche Players provide practical, accessible TPRM functionalities that address core risk identification, assessment and monitoring needs. In this market, typical Niche Players cater well to midsize enterprises, first-time adopters or organizations seeking straightforward, limited-resource deployments. While they execute adequately within their specific areas of focus or within their primary regions, they generally lack the broader solution breadth, advanced AI capabilities and geographic reach necessary to support complex, cross-domain risk management for large, multinational organizations.

Niche Players may offer compelling TPRM solutions, but may lack some functional components and consistent positive customer experience and implementation. Niche Players can often offer the best solutions to meet the needs of particular organizations or specific assurance risk domains. However, they are typically not winning new business across multiple regions or verticals at the same pace as vendors in the other quadrants.

Context

The market for TPRM tools for assurance leaders is densely populated and in the early stages of maturity. As organizations realize that a siloed approach to third-party management is inadequate for addressing the full spectrum of risks, they are increasingly seeking integrated, cross-functional capabilities.

Furthermore, AI is an emerging competitive differentiator, enabling platforms to enhance usability, provide continuous third-party monitoring and generate actionable risk insights.

Assurance leaders should use this Magic Quadrant to evaluate the performance and strategic vision of leading TPRM technology tools and take the following actions:

- **Determine priority third-party risk domains:** Identify which specific third-party risk domains are key priorities for your organization.
- **Evaluate strategic alignment:** Identify the vendors that best align with your industry, your organization's near-term third-party risk management needs and your long-term technology roadmap, combined with your unique assurance operating model.
- **Assess required functionality and AI maturity:** Evaluate TPRM products to find those offering the specific use cases and features your organization requires, taking care to assess the relevance and maturity of their embedded AI capabilities.
- **Plan for integration:** Prepare for the TPRM technology implementation process, recognizing that replacing legacy systems with advanced TPRM solutions often requires additional data connectors, customization and integration with existing enterprise solutions.

Market Overview

The market for third-party risk management (TPRM) tools for assurance leaders remains crowded and competitive. It is fragmented and continues to be fueled by venture capital, private equity investment and periodic acquisitions. This Magic Quadrant is U.S.-centric because of the vendors included. They are all headquartered in North America; however, many of them have a global presence.

Demand for TPRM workflow solutions continues to accelerate, particularly among large enterprises in highly regulated industries such as financial services, oil and gas, healthcare, and manufacturing.

Market Evolution

The TPRM technology market is still in the early stages of maturity, with a crowded field of providers and no single solution that addresses all organizational requirements. Large enterprises may use two or more technology solutions with distinct TPRM capabilities that multiple business functions then leverage.

Organizations are finding that a siloed approach to third-party management across disparate functions doesn’t surface or address the spectrum of third-party risks adequately. As a result, assurance leaders may invest in integrated cross-functional third-party risk management capabilities, allowing them to manage assurance-led third-party risk domains across multiple business functions and numerous stakeholders.

Key Market Trends

AI is emerging as a competitive differentiator. In the TPRM technology marketplace, vendors are heavily investing in generative AI use cases. Over the past one to two years, GenAI has evolved from a nice-to-have feature to a key differentiator when it comes to thoughtful TPRM vendor selection.

AI capabilities in TPRM technology solutions vary widely. Those providers that leverage and deploy AI tools and chatbots as part of their systems will remain competitive. AI chatbots often improve the UI, allowing users to ask natural language questions and query the system’s third-party data repository. TPRM is data-intensive. As a result, those TPRM solutions that feature AI are often able to enhance usability, provide continuous third-party monitoring and generate actionable third-party risk insights. Buyers should carefully assess the relevance and maturity of embedded AI capabilities.

Integration and Implementation

Many TPRM vendors are aiming to make their platforms more intuitive and configurable. Select TPRM solutions claim they can offer rapid implementation, within three to six months; however, timelines are often longer and may require supplemental configuration, additional data connectors or customization.

Assurance Leaders Are Influencing TPRM Purchasing Decisions

Assurance leaders in large organizations seek intuitive and configurable workflow solutions capable of addressing multiple third-party risk domains. There is a continued focus on maturing TPRM governance, including greater clarity around roles and responsibilities tied to TPRM. In turn, this effort leads to requests for TPRM workflows that facilitate real-time cross-functional visibility into third-party risk. Many organizations are exploring the centralization of third-party roles and responsibilities, and they express a desire to move from siloed manual processes to automated risk identification, risk scoring, third-party risk mapping and visualization. Assurance leaders often seek to replace legacy systems with more advanced TPRM solutions that require customization, multiple data connectors and/or integration with existing enterprise solutions.

How to Use This Magic Quadrant

Assurance leaders should use this Magic Quadrant to evaluate the performance and strategic vision of leading TPRM technology tools. Identify the vendors that best align with your organization's immediate TPRM needs and long-term enterprise assurance strategy. Assurance leaders should also determine which third-party risk domains are key priorities and identify those TPRM products that offer the specific features and functionalities their organizations require.

This is the first version of the Magic Quadrant for Third-Party Risk Management Tools for Assurance Leaders and supplements the ***Market Guide for Third-Party Risk Management Technology Solutions****.*

⊕ Evaluation Criteria Definitions

Unlock more AI value

With unmatched, proprietary AI insights from Gartner

Explore the AI Hub ↗