Gartner Market Guide

for

Third-Party Risk Management Technology Solutions (TPRM)

5 May 2025- ID G00784981- 28 min read

By Antonia Donaldson, Luke Ellery, and 7 more

Legal, compliance, risk and procurement leaders can use this research to identify technology solutions and risk domains for managing and mitigating third-party risk. TPRM platforms offer versatile capabilities that support supply chain, IT, cybersecurity, procurement, legal and compliance functions.

Contents

Overview

Key Findings

- Organizations utilize multiple technology platforms to address third-party risk domains because no single solution supports all use cases or domains.
- Organizations often use two or more technology solutions with third-party risk management (TPRM) capabilities, which multiple business functions leverage. These functions include enterprise risk, legal, compliance, sourcing, procurement, supply chain, vendor management, IT, cybersecurity and other stakeholders.
- Many TPRM technology providers continue to invest in integrated cross-functional risk-management capabilities, allowing clients and customers to manage their third-party risk domains across multiple business functions and numerous stakeholders.

Recommendations

Organizations considering third-party risk management technology solutions should:

- Review the current TPRM tools and data sources and engage relevant stakeholders with TPRM responsibilities to perform a gap analysis by comparing existing TPRM capabilities with holistic requirements. Define clear roles and responsibilities for TPRM, develop a TPRM governance framework, and consider the TPRM life cycle to identify core third-party risk domains and potential dependencies.
- Identify potential technology solutions to address priority risk domains and any preidentified gaps in the current TPRM program. Carefully evaluate the capabilities of the TPRM platforms covered in this market guide.
- Develop a TPRM strategic roadmap that includes a timeline, roles and responsibilities, implementation considerations, use cases, and technology investment. Create a shortlist of TPRM platforms to engage, and evaluate vendor capabilities, vendor concentration risk, scalability, and ease of integration with existing IT systems.

Market Definition

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.

Market Description

The TPRM technology market is a complex array of solutions servicing many business functions across an enterprise. This Market Guide categorizes TPRM solution providers into TPRM technology platforms and tools, and includes risk-domain-specific data and insights (see Note 1).

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. There are notable differences in the scope of risk domain coverage; 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 vary and should be carefully evaluated by buyers.

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 (see Table 1).

NOTE: Gartner does not provide detailed coverage of vendors in specific risk domain submarkets, and they are not covered in this Market Guide.

Table 1: Third-Party Risk Domains and Definitions

Risk Domain	Definition
Bribery and corruption	The risk of individuals or organizations engaging in unethical or illegal activities, such as offering or accepting bribes, to gain an unfair advantage. This includes the risk of third parties engaging in bribery or corruption when conducting business.
Business continuity	The evaluation of business resilience to disruptions, including disaster recovery and business continuity plans.
Business governance	The risk of business failure, fines or financial loss due to various financial risks such as credit downgrades, insolvency, inadequate financial controls, accounting irregularities, money laundering, lack of compliance with regulations, fraud, money laundering, terrorist financing or bankruptcy.
Capacity	The inability to deliver required products, services or personnel due to production or resource constraints.
Concentration	The risk associated with using third parties located or operating in a specific geographic area, or relying on services from the same subcontractor or fourth party. It also refers to the volume of work provided by a specific vendor or service provider.
Environmental, social and governance (ESG)	Metrics and principles used to assess enterprise nonfinancial performance data aimed at meeting disclosure requirements and complying with legislation and regulations across ESG focus areas such as carbon, environmental impact, labor relations, modern slavery, human rights, sustainability and ethical sourcing.
Geographic or geopolitical	Risks associated with services or products fulfilled outside the client's home country or region, including geopolitical risks, climate or natural disasters, currency fluctuations,

Risk Domain	Definition
	legal or regulatory issues, resource availability (including human capital), or infrastructure-related risks.
Privacy and data processing and management	The risk of unauthorized access, misuse or loss of personal or sensitive data, including Personally Identifiable Information (PII), that the company stores, collects, or processes as a "data processor." This may involve potential violations related to the management of personal data, such as location, collection, processing, access, retention, return and destruction. Compliance with the General Data Protection Regulation (GDPR) is an example.
Regulatory compliance	Government or industry-body-mandated obligations and requirements that third parties must comply with, including monitoring and reporting obligations. This includes accessibility, conflict materials or minerals, the Bank Secrecy Act (BSA) anti-money laundering (AML), know your supplier (KYS), know your customer (KYC), U.S. Securities and Exchange Commission (SEC) disclosure and reporting requirements, and other regulatory or legal obligations.
Security or cybersecurity	The risk of malicious cyberattacks or threats. It examines the physical and cyber technologies and processes that protect digital or information assets against malicious attacks or threats, and the responses to these events to minimize harm.

Source: Gartner (May 2025)

Different types of third parties pose varied risks to an organization, with each department assessing these risks from its own perspective. For example, the legal department focuses on risks related to sanctions, litigation and bribery. According to Gartner, different functions prioritize different risk domains, which requires specialized support for detailed third-party risk analysis and management. For instance, IT sourcing, procurement and vendor management (IT SPVM) may prioritize concerns about business continuity, business governance and concentration risk.

A single third-party risk management platform may not adequately address the diverse requirements of all functions and roles within a large organization. Consequently, many organizations opt to use two or more TPRM technology tools to effectively meet their workflow needs and address various risk domains.

Supply chain — Supplier risk management focuses primarily on the direct relationships and dependencies between an organization and its suppliers, whereas TPRM encompasses an extensive array of external entities. Supply chain risk management targets direct procurement and the ongoing management of suppliers used to create finished goods and services sold to customers. It also aims to enhance buyer resilience by avoiding, absorbing and recovering from supply chain disruptions. These teams assess and monitor various risk domains, including supply chain disruptions, suppliers' financial stability, cyber monitoring, capability and performance. For more information about setting up a supplier risk management program, see Ignition Guide to Supplier Risk Management.

Information technology — IT pertains to IT vendors and other third parties who may access or control data, information, or assets. Consequently, there is a strong focus on cybersecurity, privacy, business continuity and new regulatory requirements (including disclosures).

Legal and compliance — Legal and compliance covers third-party risk primarily from a compliance perspective. They typically work with other organizational leaders across relevant risk domains. They emphasize bribery and corruption, trade compliance, sanctions, regulatory compliance, material risk related to business continuity and third-party events impacting corporate reputation.

For more background on setting up a TPRM program as a risk leader, see How to Build and Scale a Third-Party Risk Management Program.

Market Direction

Following persistent cyberattacks, trade compliance complexity, a challenging geopolitical landscape and continued pressure to meet new regulatory requirements, regulators and boards are increasingly interested in how third-party risk is effectively managed. Organizations are now looking to build and expand their TPRM programs by exploring technology and tools that help scale and automate workflows and enable collaborative risk management.

Organizations seek technology platforms and tools that facilitate holistic management of third-party risk throughout the third-party life cycle, from onboarding to offboarding. The best platforms for TPRM will manage enterprise risk by supporting a third-party risk evaluation process, including risk criteria, risk ranking and risk tiers, while providing a clear workflow, escalation and approval process. These vendor solutions will also streamline third-party risk management across the entire relationship life cycle, not just during initial due diligence and onboarding.

Many vendors are incorporating machine learning and AI to support automated assessment and analysis, and refine future recommendations and impact analysis with appropriate disclosures and human review. Gartner believes this approach will be a competitive differentiator, as TPRM is both data and labor intensive.

Gartner frequently addresses client concerns involving third parties across the following risk domains:

- Bribery and corruption
- Business continuity
- Business governance
- Capacity
- Concentration
- Sustainability or environment, social and governance (ESG)
- Geopolitical or geographic
- Privacy and data processing and management

- Regulations and regulatory compliance
- Security or cybersecurity
- Trade compliance and sanctions

Market Analysis

TPRM solutions will ideally 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.

Organizations worldwide are facing intense pressure to meet new and evolving regulatory requirements related to third- and fourth-party risk. Regulators and stakeholders are increasingly interested in how organizations effectively manage their third-party risk activities.

This Market Guide covers two types of TPRM technology solutions:

Third-Party Risk Management Technology Platforms and Tools

These software platforms assess, monitor, report and remediate third-party risks, typically providing workflow automation and a system of record for third-party risk management. They integrate with risk-domain-specific data and insight solutions, assisting organizations in analyzing and monitoring third-party risks. However, integration capabilities vary widely, affecting ease of configuration and depth of integration into platforms — some may require costly development or programming.

Workflow automation, supplemented by AI, is an emerging capability among many vendors in the TPRM technology space. Innovations distinguishing TPRM vendors leveraging AI and generative AI (GenAI) may include:

- Predictive analytics to support risk-based decisions
- Natural language processing (NLP) to evaluate survey responses or third-party-provided documents (such as International Organization for Standardization [ISO] or Service Organization Control [SOC] documents)
- Nth-party relationship mapping
- Graphing technology to identify fourth and Nth-party threats or related risks

Notably, some tools better address specific buyer needs than others. Some TPRM technology tools are purpose-built for specific risk domains, such as cybersecurity or finance. Organizations should assess their TPRM program's maturity alongside other considerations, such as industry, geography, integration and regulatory pressures. Large enterprises often deploy multiple TPRM technology tools to effectively address third-party risk.

Risk-Domain-Specific Data and Insights

These data subscriptions provide specific risk insights into particular domains. Organizations increasingly integrate this data into their third-party risk management tools to assist with initial assessments and ongoing monitoring, alerts and escalation. Some solutions integrate data from other third-party sources to offer comprehensive insights, with many beginning to leverage AI to autonomously search for and update data in their repositories.

NOTE: Gartner does not provide detailed coverage of vendors in these risk-domain-specific submarkets.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

List of Representative Vendors

The following is an alphabetical list of the 78 participating TPRM technology vendors covered in this Market Guide (see Table 2).

See the companion document, Tool: Vendor Identification for Third-Party Risk Management Solutions, which covers geographic location, risk domains and solution types.

Table 2: Vendors With Capabilities in TPRM Technology

Company Name	Product Differentiation (Self-Reported)
3rdRisk	3rdRisk is a European platform designed for third-party risk management, addressing all risk domains and frameworks such as DORA, NIS2 and CSDDD. It features a custom-branded user interface, gamification and AI, and can be launched in just a few days using best-practice blueprints. Additionally, it integrates seamlessly with over 40 data sources.
6clicks	6clicks employs a hub-and-spoke architecture, allowing for centralized oversight at the hub (enterprise or government) while maintaining autonomy at each spoke (such as country, state, subsidiary or department). Its AI continuously reassesses third parties across these spokes to meet varying risk and regulatory requirements.
A2SECURE	Riskblade analyzes perimeter and SaaS configuration risks, assesses vendors through compliance questionnaires, and ensures alignment with standards, such as NIS2, DORA, SOC2 and ISO. Its threat intelligence module identifies compromised accounts and incidents that may impact you and your third parties.
Achilles	The platform of Achilles operates globally, covering over 140 countries and addressing all suppliers, risks and geographies. It provides proactive, real-time, continuous risk monitoring with 100% data validation. Achilles achieves high supplier engagement with an over 80% response rate, fosters supplier

Company Name	Product Differentiation (Self-Reported)
	improvement, offers flexible pricing and customizes solutions to meet client needs, backed by its experience and expertise.
Allgress	Risk Suite, which includes exception management, a register and risk assessment, automates risk evaluations and streamlines compliance. Key differentiators include AI-powered onboarding, automatic assessments and reviews, AI-driven policy and certification reviews, continuous and fourth-party monitoring, incident and news alerts, and recommended approval or denial actions.
apexanalytix	Private Agentic AI automatically detects and resolves risks according to the client's priorities, policies and tolerance levels. It evaluates every supplier, applying appropriate assessments and resolutions based on the supplier segment, relevant regulations and potential impact on client outcomes.
APROVALL	APROVALL leads in Europe's third-party governance, risk and compliance (TPGRC). It offers free, seamless onboarding, standardized and mutualized data collection capabilities, and a robust AI-enabled IdP. APROVALL currently assesses and monitors over 450,000 third parties across more than 153 countries.
Aravo	Aravo's solution is highly configurable, catering to customers' needs for both simple and complex TPRM programs, accommodating rapidly changing scopes, and addressing expanding regulatory scrutiny. Our extensive risk domain expertise allows us to deliver the solutions customers demand and adapt them as needs evolve.
Archer	Archer TPRM offers comprehensive life cycle support for vendor management, including risk, engagement, contract assessment, metrics, reporting and oversight processes, as part of an overall enterprise solution for GRC.
Atlas Systems	ComplyScore seamlessly integrates platforms and services to streamline third-party life cycle management. Its intelligent automation optimizes vendor tiering, risk scoring and control assessments — boosting efficiency, reducing manual effort and enhancing risk mitigation.
AuditBoard	AuditBoard provides best-in-class user experiences for internal and external collaborators, enterprise-grade interoperability, and GRC-trained AuditBoard AI, driving risk owner accountability and intelligent automation like no other TPRM solution on the market.
Aujas Cybersecurity	Aujas Cybersecurity offers TPRM services, including managing and hosting TPRM Desks, conducting vendor on-site and off-site audits, and following up with vendors to resolve noncompliance issues. Aujas focuses solely on TPRM services and does not offer a TPRM product.
Avetta	Avetta aims to fundamentally transform supply chain dynamics. It enables and verifies ongoing safety, environmental, social and financial performance, helping hiring companies build a strong and diverse contractor base globally.
Bitsight	Bitsight TPRM provides a comprehensive solution with continuous, data-driven cyber-risk insights and automated vendor assessments. It facilitates real-time monitoring, risk prioritization, remediation and workflow automation, empowering organizations to manage risk effectively using trusted security analytics and intelligence.

Company Name	Product Differentiation (Self-Reported)
Black Kite	Black Kite offers top-tier data and threat intelligence that is transparent, accurate and aligned with industry standards such as MITRE and FAIR. Instead of relying on survey-based assessments, Black Kite continuously monitors to provide actionable insights, such as ransomware exposure and event notifications.
BlueVoyant	BlueVoyant's proprietary approach helps clients enumerate, prioritize and remediate risks in their supply chains. Its expert-staffed ROC validates risk findings and collaborates with clients and their third parties to actively remediate cyber exposure and achieve measurable risk reduction.
Board of Cyber	Board of Cyber's two products enable clients to streamline their TPRM programs. With Security Rating, clients can seamlessly assess their suppliers' cybersecurity posture, build third-party risk dashboards and share precise cybersecurity remediation plans.
Censinet	Censinet RiskOps is the only TPRM exchange purpose-built exclusively for the healthcare industry.
Certa	Certa's "Third Party OS" powers a comprehensive solution, offering a full spectrum of risk with modular deployment. It is agile, easy to update, and automated with built-in rules and AI. Certa AI agents handle repetitive tasks, allowing humans to focus on high-value work.
Coupa	Coupa proactively reduces risk across N-tier relationships and multiple risk domains by integrating third-party risk into company spend management processes. It enhances decision making through community-powered signals and data from over 3,000 customers.
CybelAngel	CybelAngel uses an outside-in approach to third-party exposure monitoring, scanning the internet daily to uncover document-level data leaks, brand exposures, dark web chatter and vulnerable assets of any supplier, whether third- or nth-party to any organization.
Cyberint	Cyberint provides continuous monitoring of vendors, partners and suppliers, along with comprehensive cyber-risk evaluations that incorporate deep and dark web intelligence, as well as other data points and assessments. Cyberint issues real-time alerts if a third party experiences a major cyber incident or breach.
CyberSaint	The CyberStrong Platform supports use cases such as TPRM, control monitoring and risk quantification. Unlike static tools, it offers real-time gap analysis, maps compliance across frameworks, and correlates internal and external risk domains. Users can organize, sort, and filter assets and vendors, managing risk holistically.
Dataminr	Powered by over 50 proprietary LLMs, Dataminr's solution delivers the earliest actionable insights to detect external risks. Its multimodal AI integrates terabytes of data (text, image, video, audio, sensor and more than 150 languages) for accurate real-time risk detection. ReGenAI (Predictive+Generative AI) describes rapidly evolving events with dynamic updates.
Diligent	Diligent's Third-Party Risk Management solution stands out with AI-powered and integrated due diligence services, customizable risk models and seamless access to screening, monitoring and beneficial ownership data. It

Company Name	Product Differentiation (Self-Reported)
	enables a risk-based approach, automating workflows for efficiency and transparency.
Drata	Drata’s VRM product features SOC 2 and Vendor Questionnaire AI Summaries. Integrated with Drata’s GRC platform, VRM directly links vendor risks to internal risk registers and controls across any framework. SafeBase integration streamlines access to vendor Trust Centers for faster security reviews.
Dun & Bradstreet	Data Cloud tracks over 550 million public and private organizations, monitoring corporate linkages, ultimate beneficial ownership, and international data through WWN alliances. It includes proprietary data on credit, firmographics, TPRC, payment history and more. The D-U-N-S Number is widely recognized and associated with the Live Business Identity.
EGERIE	EGERIE specializes in cyber-risk management and offers third-party cyber-risk management capabilities. EGERIE Risk Manager focuses on risk and action plans, allowing users to model the effect of controls on risk posture. Users can query third parties through in-app forms.
Enlighta	Full life cycle TPRM suite for continuous risk monitoring — from vendor identification, selection, due diligence, risk management and onboarding all the way through postcontract compliance, performance, governance and offboarding.
Enthec	Enthec offers companies continuous, real-time alerts on data leaks from their third parties across the internet, the deep web, the dark web and social networks. Beyond simple scoring, it identifies specific vulnerabilities, enabling swift remediation and mitigation actions to effectively prevent potential attacks.
Exiger	Exiger efficiently manages every step of third-party processes, including onboarding, monitoring, management, engagement and offboarding. Its proprietary risk intelligence offers unparalleled breadth and depth, analyzing risk across multiple dimensions without relying on external sources, revealing hidden risks that others overlook.
Exostar	Exostar’s supplier management solution connects a vetted network of over 100,000 organizations worldwide. It integrates seamlessly with other applications, such as supplier collaboration and procure-to-pay, enhancing visibility and ensuring compliance with ITAR and CMMC standards for highly regulated industries.
Fortress	Fortress focuses on energy and national security supply chains, providing a comprehensive third-party risk management solution. It includes a platform, data, exchanges, services, assessment marketplace and automated workflows to prioritize and resolve risks.
Fortrex	Fortrex offers personalized services tailored to meet clients where they currently stand, partnering with them to advance their TPRM programs.
GAN Integrity	GAN Integrity assists enterprises in managing risk and compliance across extensive networks of third parties and suppliers. Our “Integrity Identity” feature facilitates risk screening, due diligence and in-depth risk analysis. It provides a broader risk perspective by integrating gifts, conflicts and incidents into a single platform.

Company Name	Product Differentiation (Self-Reported)
Graphite Connect	Graphite Connect streamlines third-party risk management with a network-based model, enabling suppliers to update risk and compliance data once and share it instantly with all buyers. It offers automated risk assessments, AI data validations, over 6,000 industry-standard questions and remediation plans.
HICX	HICX integrates high-quality data, workflows, and AI through a mature, enterprise-grade, no-code process orchestration platform, leading in supplier domain expertise, master data excellence, and human-centric design. HICX uniquely combines all these capabilities.
HITRUST	HITRUST delivers effective and efficient cybersecurity assurances for TPRM, which has been proven to identify and mitigate risks. It offers five threat-adaptive, customizable security assessments, including AI, and three trust levels ranging from self-attested to certified, available with managed services and ServiceNow integration.
IBM	The solution distinguishes itself with comprehensive TPRM capabilities, featuring robust AI-driven insights, automated workflows, and customizable reporting. Its rich questionnaire functionality allows organizations to dynamically assess and monitor risks across their third-party ecosystems.
interos.ai	interos.ai, a true AI-SaaS solution, provides continuous real-time risk insights with the i-Score, a dynamic risk rating that encompasses financial, cyber, ESG, geopolitical, catastrophic and restriction risks to prevent disruptions, protect revenue and build resilience.
ISS-Corporate	ISS-Corporate's "Cyber Score" is forward looking and empirically derived through supervised machine learning analytics, trained on real cyber incidents. It benefits from rigorous cyber attribution management, supporting continuous monitoring, weekly score refreshes and customizable risk tuning.
Ivalua	Experience seamless "Source-to-Pay" integration without compromising between a best-of-breed ecosystem and an integrated suite. Maintain a single source of truth for supplier information with no-code/low-code flexibility to stay agile.
S&P Global Know Your Third Party (KY3P)	S&P Global delivers high-quality data across multiple risk domains through a TPRM life cycle platform. With seamless integration, end-to-end managed services and global expertise, it provides actionable insights that enhance risk assessment, streamline workflows and drive efficiency.
LogicGate	Risk Cloud streamlines TPRM with automated assessments, AI-powered remediation, and continuous monitoring. Its no-code platform integrates seamlessly with cybersecurity tools, ensuring real-time visibility, regulatory compliance and proactive risk mitigation across dynamic vendor ecosystems.
LSEG (Risk Intelligence)	With a global reach, London Stock Exchange Group (LSEG) boasts risk and compliance experts in 158 jurisdictions, speaking over 70 languages. Built on a heritage of quality, integrity and trust, LSEG's industry-leading solutions scale to accommodate any risk-based workflow.
MetricStream	Utilize prebuilt industry-specific templates and workflows to simplify end-to-end third and fourth-party risk management. AI-powered autonomous risk identification, assessments and action plan recommendations integrate

Company Name	Product Differentiation (Self-Reported)
	seamlessly with business continuity, enterprise risk and compliance for resilience.
Mirato	Mirato reduces manual work. Mirato's AI streamlines assessments using an organization's risk framework, while the Mirato Questionnaire Killer preanswers due diligence questionnaires. Both solutions cut manual effort, helping organizations reduce time, cost and effort by 60%.
Mitratech	The Mitratech Prevalent TPRM solution leverages AI to assess, monitor and remediate third-party risks from onboarding to offboarding. The solution combines a large library of security, operational and compliance assessments with native continuous monitoring backed by in-house managed services.
NAVEX	Begin with prescribed program outlines, templates, and workflows featuring 15 personas, 7 dashboards, and 60 reports. Establish a program foundation using policy templates and in-house third-party risk screening and monitoring. Implement quickly with broad integration capabilities.
Ncontracts	Ncontracts distinguishes itself with a fully integrated GRC suite that connects vendor management to broader risk and compliance functions. Its knowledge as a service model provides expert-driven insights, automation and regulatory intelligence, enabling proactive risk management and operational resilience.
NQC	SUPPLIERASSURANCE facilitates compliance-ready due diligence by identifying, assessing and mitigating supply chain risks. Through predictive mapping, nonintrusive surveillance, supplier engagement, evidence verification and corrective actions, it supports compliance with UFLPA, EUDR, CSRD and more.
OneTrust	OneTrust Third-Party Management uses a data-enabled, risk-led assessment approach to identify and mitigate risks, continuously monitor changes in risk posture, and ensure compliance with legal and regulatory standards, building a resilient, secure and scalable third-party ecosystem.
Onlayer	Onlayer uniquely combines vendor and merchant risk intelligence with AI-driven deep web monitoring, continuous compliance automation and transaction laundering detection. Unlike traditional TPRM solutions, it provides real-time fraud signals and behavioral risk insights for banks and PayFacs.
Onspring	Manage third-party risk holistically through risk evaluation processes, including ongoing monitoring, response workflows and automated actions throughout the life cycle of third-party engagement, beyond the initial review, with an engagement-focused workflow.
Panorays	Single solution for TP(C)RM processes; Panorays offers supply chain discovery, context-based nth-level visibility and inherent risk tiering. It also includes cyber and IT risk assessment based on customer risk policies, integrating dynamic questionnaires, continuous attack surface monitoring, threat detection, remediation and collaboration.
Phinity Risk Solutions	The TPRM product of Phinity Risk Solutions stands out for ease of use, fast implementation, automation and deep integrations. It streamlines risk assessments, automates workflows and enhances third-party risk visibility.

Company Name	Product Differentiation (Self-Reported)
	Our configurable frameworks and RPA engine ensure maximum efficiency and compliance.
ProcessBolt	ProcessBolt provides an accurate view of your supply chain security by integrating and correlating vendor assessment data with continuous attack surface monitoring and AI-driven document intelligence. ProcessBolt sources its own data to reduce false positives and provide real-time vulnerability detection.
ProcessUnity	ProcessUnity differentiates itself by meeting the unique needs of TPRM clients at every stage of market maturity. Our combination of workflow automation, data and artificial intelligence enables TPRM teams to extend their existing program resources to cover more of their portfolio.
Protecht	Protecht offers integration with ERM features for holistic risk visibility, resilience, BCM and cyber-risk features to understand and manage critical interdependencies and third-party impact on resilience and continuity. Its intuitive UI design aligns with the TPRM life cycle.
Risk Ledger	Risk Ledger offers a dynamic, network-based platform that connects suppliers in real time. Suppliers maintain one profile shared with connected clients, reducing redundant assessments and delivering clear visibility, proactive risk insights, and streamlined compliance to secure your supply chain.
RiskRecon	RiskRecon's platform boasts data accuracy certified to 99.1%, supported by a dedicated analyst team. It performs the majority of scans in-house using its proprietary vulnerability scanning algorithm. Experience a modern and simple user interface and user experience powered by actionable intelligence.
RiskXchange	RiskXchange stands out by offering a fully managed third-party risk service that combines expert-driven insights, AI-powered risk intelligence and compliance-focused solutions. It actively guides businesses in risk mitigation, ensuring seamless integration with procurement, security and compliance.
SAFE	SAFE TPRM empowers data-driven, risk-based decisions with continuous visibility and automation. Built on open standards such as FAIR-CAM and FAIR-MAM, it integrates threat intelligence, inside-out/outside-in monitoring, and automation to unify first- and third-party cyber risk, enhancing scalability and trust.
SaltyCloud	Isora GRC transforms questionnaires into scientific tools with scoring and benchmarking for precise vendor risk analysis. Its vendor inventory links assessments to vendors, while a risk register ensures teams can track, own and address risks efficiently — all within a user-friendly workflow.
Sayari	Sayari's approach, unlike traditional TPRM solutions, unifies best-in-class proprietary risk intelligence with AI-driven workflow automation. It delivers real-time insights, configurable risk scoring and automated remediation, ensuring scalability, compliance adaptability and seamless integration.
Seconize	Seconize's comprehensive TPRM includes external risk ratings for an outside-in view and questionnaires for an inside-out view. It offers customizable workflows for vendor onboarding, multiple levels of assessments,

Company Name	Product Differentiation (Self-Reported)
	offboarding and vendor risk scoring, along with a virtual auditor using GenAI to autofill using SOC2.
Semantic Visions	By integrating data from multiple languages and sources, our platform helps organizations identify critical risk points, gain n-tier visibility with multitier supply chain mapping, and monitor geopolitical and environmental impacts, all with unparalleled scope and precision of data.
ServiceNow	ServiceNow delivers enterprisewide TPRM, integrating internal and external data with intelligent workflows, real-time insights, and scalable automation. Our user-centric experience reduces assessment fatigue, enhances efficiency and empowers leadership with a holistic, auditable third-party risk view.
Smart Global Governance	The TPRM module of Smart Global Governance automates 90% of third-party risk tasks, reducing manual effort. It integrates CRM, SRM and ERP, offers AI-driven risk scoring and real-time compliance tracking (GDPR, ISO 27001, DORA and NIS 2), and supports SaaS, on-premises and hybrid deployment.
SupplierGateway	SupplierGateway delivers unmatched speed to value, deep customization and automated supplier onboarding with transparent pricing. Seamless workflows and integrated risk monitoring provide a single platform for instant visibility into compliance, risk, economic impact and vendor management.
Supply Wisdom	Supply Wisdom's solution offers consolidated, continuous risk intelligence monitoring of companies, countries and cities across multiple risk categories throughout the entire supply and sourcing chain. Information is delivered through an interactive, multicategory, configurable dashboard, driven by AI and analysts.
SureCloud	SureCloud is differentiated by its intuitive UI for frictionless user adoption, accountless vendor access and no-code workflow. Leverage prebuilt workflows for vendor tiering, real-time risk insights and external assessments, enabling organizations to launch their programs within weeks.
Tenchi Security	Zanshin assesses and improves third parties' cybersecurity posture through automated, continuous, comprehensive, nonintrusive checks. It goes beyond external attack surface and threat intelligence checks, conducting inside-out tests on cloud (IaaS, PaaS, and SaaS) infrastructure and security solutions.
Trustwave	Trustwave optimizes the TPRM process by utilizing automation tools, AI and human analysts to be both cost-efficient and provide valuable, actionable insights.
UpGuard	UpGuard's vendor risk offers a complete TPCRM solution, centralizing visibility, insights and control. AI-powered workflows, automation, and daily scanning drive faster, dynamic risk decisions. With intuitive design, scalable deployment and simple packages, it reduces complexity while enhancing security.
Vanta	Vanta accelerates vendor security reviews with AI-powered analysis and automated evidence gathering through Vanta's network of Trust Centers. It provides customized risk scoring to meet organizations' unique business needs and integrates across their GRC programs for a complete view of cyber risk.

Company Name	Product Differentiation (Self-Reported)
VISO TRUST	Experience fast, AI-driven vendor risk intelligence without manual analysis. Our single-platform solution provides visibility, continuous monitoring of public data and inside-out assessments using audit reports. Every assessment undergoes expert review for accuracy, enabling teams to trust results and scale TPRM efficiently.
Whistic	Whistic's AI-First TPRM is integrated throughout the entire TPRM life cycle. It offers AI transparency with sources and explanations for all AI-generated output. Whistic's platform makes it easy to leverage multiple data sources, ensuring simple, straightforward implementations and is designed to integrate with GRC platforms.

Source: Gartner (May 2025)

Market Recommendations

- Build and scale the TPRM program by considering the entire TPRM life cycle. Ensure the TPRM platform facilitates the flow of third-party risk information across all relevant functions and users to maximize the organization's visibility of emerging third-party risks.
- Select a TPRM solution that is adaptable and scalable for both near-term and future program needs. When assessing TPRM technology options, ensure the organization has a "must have" list of capabilities prior to engaging with vendors.
- Evaluate the licensing options and consider both short-term and long-term implementation and integration requirements and APIs for the chosen TPRM solution provider, rather than solely focusing on cost.