ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

WHERE TPRM MEETS AI: Balancing Risk and Reward

in partnership with GAN Integrity

GAN INTEGRITY

Table of Contents

GAN INTEGRITY

Introduction

In our hyper-global, instant-access, always-on business environment, third-party risk management (TPRM) for organizations everywhere has grown exponentially in size and complexity. The sheer volume of vendors, deeper supply chain scrutiny, and evolving regulations make it increasingly difficult for manual processes alone to keep pace.

Heightened attention to issues such as human trafficking, trade compliance, environmental liability, and resultant reputational risk has raised expectations for robust third-party risk management. Additionally, we are seeing increasingly complex regulatory responses in critical areas such as data privacy, cybersecurity, artificial intelligence and supply chain due diligence. This evolving landscape requires companies to achieve an unprecedented level of third-party risk management (TPRM) maturity.

This report explores the growing challenges of third-party risk management and rising due diligence expectations, along with how technology—particularly artificial intelligence (AI) - can help ethics and compliance teams build stronger TPRM programs by automating critical functions. It also addresses the risks introduced by AI and provides benchmarks and guidance on integrating AI governance into TPRM practices.

GAN INTEGRITY

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

PART ONE

EXPANDING THIRD-PARTY RISK UNIVERSE

in partnership with GAN Integrity

The Expanding Third-Party Risk Universe

CASE IN POINT

According to Deloitte's 2023 global TPRM survey, most programs now manage nearly 20 different risk areas. Cyber and information security risk is the most prevalent, followed by geopolitical risk, business continuity, and data privacy.

The original focus of third-party risk management (TPRM) was compliance, particularly anti-corruption laws such as the Foreign Corrupt Practices Act (FCPA). However, TPRM has always included other critical areas like anti-money laundering, financial stability, business continuity, and operational resilience. As businesses and supply chains have grown more complex, TPRM has broadened to encompass risks related to environmental, social, and governance (ESG), human rights, data privacy, and cyber threats. The expansion of compliance risks, blurred boundaries between risk categories, and evolving functions within organizations have contributed to a more fragmented and complex TPRM landscape.

Other significant categories include concentration risk, regulatory risk, contract risk, anti-bribery and anti-corruption (ABAC), quality risk, environmental risk, reputational risk, and subcontractor risk. Notably, modern slavery and climate risk, while increasingly critical, are often managed separately or inadequately despite stringent regulations.

Regulations impacting TPRM are not only proliferating but also overlapping, creating a complex, intertwined risk landscape. Compliance risk is no longer the sole focus; financial, operational, and strategic risks are equally important. Fragmented TPRM functions across compliance, procurement, legal, IT, and business continuity often result in silos, inefficiencies, and gaps.

The challenge is clear: **Compliance cannot operate in isolation**. Organizations must integrate their various risk management functions under a unified framework to prevent gaps, eliminate redundancies, and enhance resilience against a broad spectrum of third-party risks.

THE EXPANDING THIRD-PARTY RISK UNIVERSE

Managing Risk at Scale

The sheer volume of supply chain partners is a significant challenge for third-party risk management (TPRM) today. Multinational companies often work with thousands of third parties - and even more fourth- and fifth-party relationships. Gartner's Third Party Risk Management Benchmarking Report 2023 underscores this complexity: 58% of companies reported an increase in their number of third parties from 2019 to 2022, and 46% noted growth in their fourth and fifth-party relationships.

Alarmingly, nearly half of Gartner's respondents also reported a 17-point increase in high-risk third parties - those whose vulnerabilities pose serious threats to operations, reputation, or financial stability. These high-risk relationships demand greater scrutiny and more robust risk mitigation strategies.

This trend shows no signs of slowing. A 2024 TPRM survey by Mastercard subsidiary RiskRecon found that the number of TPRM programs managing at least 250 vendors doubled between 2020 and 2023.

Part of this expansion reflects growing supply chains, but it also stems from organizations' increasing reliance on their internal teams to manage complex risk landscapes. With procurement, ethics, and compliance teams stretched thin, efficiently assessing, clearing red flags, monitoring compliance, and regularly re-evaluating risks across a vast network of suppliers presents a formidable challenge.

Managing risk at scale requires streamlined processes and tools to ensure visibility, consistency, and agility across third-party relationships. As companies expand their vendor networks to build resilience, they must also implement scalable TPRM frameworks to keep pace with mounting oversight demands.

Interactive poll not supported

View online version

THE EXPANDING THIRD-PARTY RISK UNIVERSE

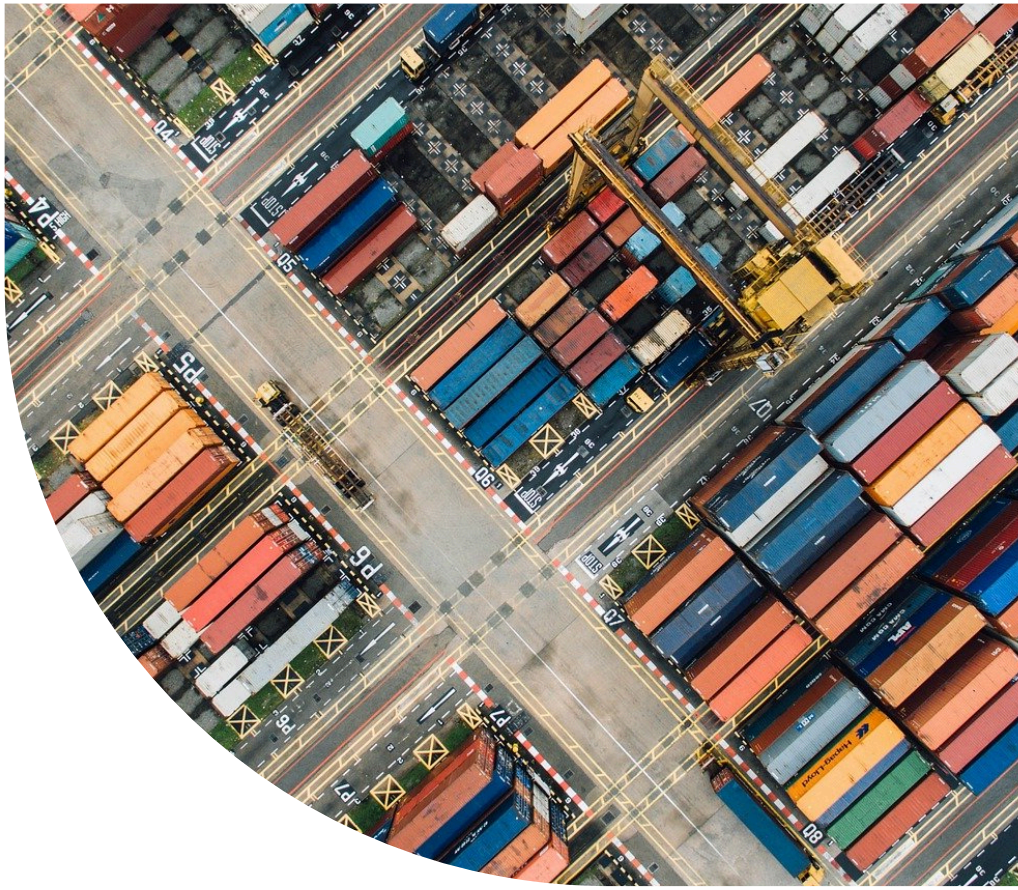
Enter the EU

Given an already large risk universe across an expansive and expanding third party population, recent regulatory schemes have focused on specific risk areas by requiring deeper and more detailed disclosures.

In 2024, the European Commission enacted the Corporate Sustainability Due Diligence Directive, a new standard that requires businesses operating in the European Union to establish, fund, and maintain the framework and processes to identify and address potential and actual "adverse human rights and environmental impacts" within their own operations, those of their subsidiaries, and those of their business partners within their value chains.

This standard has since been simplified by the European Commission's Omnibus Package, which refocuses due diligence primarily on direct suppliers. But the best practices bar has already been raised in the eyes of organizations and their stakeholders.

While this was intended to address human rights risk and environmental sustainability issues, as organizations develop these required capabilities, they will also be able to address other risks deep within their supply chain, such as reputational risk, trade compliance issues, and more. Beyond what this law mandates, the bar for best practices has also been raised by it.



We can expect that like the GDPR influence on global privacy regulations, the EU will be setting the standard for supply chain due diligence not only across a range of risk areas, but also deeper into parties beyond immediate business partners. But worth noting, is that unlike the GDPR, this is currently enacted as a directive, which opens the door for increased complexities as independent member EU member states codify the directive into country specific regulations.

THE EXPANDING THIRD-PARTY RISK UNIVERSE

Data Overload & Budget Constraints

In order to meet due diligence and monitoring requirements, organizations find themselves subscribing to a growing number of data feeds that include (but are hardly limited to) global watchlists, sanctions, adverse media, ESG databases, financial health ratings, cyber-security ratings and more. All of this increases the volume of TPRM data to review by an order of magnitude at a time when program funding and headcount are not keeping pace—despite regulatory guidance such as 2024's U.S. Department of Justice Evaluation of Corporate Compliance Programs (ECCP) update, which clearly expects companies to adequately resource their E&C functions.

According to Ethisphere's 2025 World's Most Ethical Companies benchmarking data, companies ranging from 25,000-50,000 employees have, on average, almost 84 ethics and compliance full-time equivalents. E&C teams, long familiar with making the case for adequate levels of resourcing, are intimately familiar with the challenge of adding headcount, which explains figures from EY's *2023 Global Third-Party Risk Management Survey*, which states that 42% of organizations plan to integrate automation to better manage reporting, and 63% of the plan to integrate external data providers and automation to better manage their inherent risk assessments by 2025 or 2026.

The truth is the adjudication of results and significant numbers of false positives make TPRM a resource-intensive process at a time when flat or even modestly increasing compliance budgets are hard-pressed to manage the data deluge.

Interactive poll not supported

View online version

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

PART TWO

AI AS A DRIVER OF EFFICIENCY

in partnership with GAN Integrity

GAN INTEGRITY

AI as a Driver of Efficiency

In a recent McKinsey survey, 78 percent of respondents say their organizations use AI in at least one business function, up from 72 percent in early 2024 and 55 percent a year earlier. In many use cases, this includes automating tasks such as data analysis, screening, and policy management support. In areas such as supply chain and third-party risk management, survey respondents report cost savings as high as 20% more.

The reality is that the technology delivers massive efficiency benefits. Manual teams cannot systematically review tens of thousands of suppliers in real time. Nor can they identify emerging red flags such as negative news or changes in beneficial ownership faster than a machine. This creates use cases such as:

- **Automated Due Diligence:** AI-driven background checks can scan large volumes of adverse media and watchlists to identify potential risks.
- **Contextual Risk Assessments:** AI creating bespoke risk assessments and pre-populated questionnaires.
- **Continuous Monitoring:** Machine learning models can assign dynamic risk scores, alerting compliance when significant changes occur.
- **Pattern Detection:** Identify anomalies in invoicing or contractual relationships that may signal fraud or corruption.

E&C teams are no exception to this, already forming strategies for how to leverage AI to increase program efficiency, and also developing AI policies to provide guardrails for the use of this nascent technology as well as to manage the risks it presents itself.

The allure of AI also applies to other areas of risk management, which in various Roundtables and Working Groups hosted by the Business Ethics Leadership Alliance point out that programs are looking for scalable solutions that unify pre-existing hodgepodges of systems and technologies, drive efficiency, and perhaps unify efforts in ethics and compliance with work in other departments across the enterprise.

Creative Use Cases for AI in TPRM

- Automated Due Diligence
- Contextual Risk Assessments
- Continuous Monitoring
- Pattern Detection

Interactive poll not supported

View online version

TERMS DEFINED

Automated Due Diligence: AI-driven background checks scan large volumes of adverse media and watchlists to identify potential risks.

Contextual Risk Assessments: AI creating bespoke risk assessments and pre-populated questionnaires.

Continuous Monitoring: Machine learning models assign dynamic risk scores, alerting compliance when significant changes occur.

Pattern Detection: Identify anomalies in invoicing or contractual relationships that may signal fraud or corruption.

Automated Document Review: AI scans contracts, financials, and compliance reports for red flags and anomalies

AI-Driven Contract Analysis: Machine learning to detect risky clauses, deviations from standard terms, or hidden obligations

Decision Support: AI provides risk experts with machine-learning-based recommendations. (e.g. to approve or deny a third party.)

Automated Triage & Risk Scoring: AI-based classification and prioritization of third parties, helping teams focus on the highest-risk entities first

AI-Driven Ownership & Relationship Mapping: AI supported graph analytics to uncover complex ownership structures, beneficial owners (UBOs), and hidden relationships.

AI AS A DRIVER OF EFFICIENCY

Prioritizing AI Use Cases

AI should be deployed with purpose - solving real compliance challenges rather than adopting technology for its own sake. To maximize effectiveness, companies should:

- **Identify Compliance Pain Points:** Clearly define the specific regulatory, ethical, or operational issues AI will address before deploying solutions.
- **Solve Practical Problems:** Focus AI efforts on enhancing compliance efficiency and accuracy, not adding unnecessary complexity.
- **Enhance, Don't Replace:** AI should support human decision-making, not replace it. Effective AI complements expertise with enhanced data processing capabilities.

Success depends heavily on building a clear, well-defined use case for AI.

High-Impact vs. Feasible:

Start by applying AI to straightforward, high-impact tasks like adverse media checks and sanctions screening - data-intensive processes that are ideal for automation. Once these foundational capabilities are established, gradually expand into more sophisticated applications such as predictive risk modeling and transactional analysis. The success of AI deployments relies heavily on data quality. Incomplete, outdated, or inaccurate data will undermine AI's ability to generate reliable insights.

Implementation Roadmap:

Break down your AI integrations into discrete segments with their own time horizons and KPIs.

- Phase 1: Integrate AI with existing TPRM tools for screening and due diligence.
- Phase 2: Expand to continuous risk monitoring and pattern detection.
- Phase 3: Orchestrate a holistic approach that merges data from procurement, finance, E&C, and InfoSec.

A phased approach allows companies to demonstrate early wins, refine their strategy, and scale AI solutions effectively.

AI AS A DRIVER OF EFFICIENCY

The Power of AI in Streamlining Due Diligence

AI offers powerful efficiencies in due diligence, allowing organizations to accelerate screening processes, reduce false positives, and enhance overall accuracy. By automating labor-intensive tasks, AI enables compliance teams to focus on high-risk findings instead of wading through irrelevant data.

AI-Enabled Screening Efficiencies

For example Integrity Essential™ - GAN Integrity's AI-powered risk screening solution, has been found to:

- **Reduce false positives by 77%.** AI screening and consolidated results, reduce irrelevant alerts, cutting down manual review efforts and increasing accuracy.
- **Support 50% faster onboarding:** Automated screening processes accelerate due diligence, enabling more rapid vendor onboarding.

AI Deepsearch for Due Diligence

For example Integrity Enrich™ - GAN Integrity's AI-powered deep-search due diligence solution, has been found to reduce the volume of results requiring manual assessment by approximately 93%.

To put this in context, if the system initially flags 1,000 potentially relevant items, Integrity Enrich can narrow that list down to just 67 for human review.

With an average review time of 30 seconds per item, this process saves approximately 7.75 hours - transforming a full workday of manual review into just 35 minutes.

In these scenarios, AI streamlines efficiency, allowing teams to focus their expertise on critical risks rather than sifting through noise.

CASE IN POINT:

Digging Deeper, Faster

In addition to improving efficiency, Integrity Enrich™ surfaces hidden risks that traditional open-source searches often miss.

For instance one Fortune 50 company monitoring 20,000 third parties using AI deep-search capabilities, consistently uncovers risk signals that conventional risk intelligence databases fail to detect. This proactive approach helps them stay ahead of emerging threats, highlighting AI's ability to deliver better and faster risk detection.

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

PART THREE

AI AS A NEW RISK TO MANAGE

in partnership with GAN Integrity

GAN INTEGRITY

AI as a Risk to Manage

It is no small irony that the use of AI to manage risk creates its own risks to manage. The risks can be significant, including:

Data Privacy & Security

Carefully vet AI systems handling confidential or regulated data.

Regulatory Compliance

Emerging legislation (e.g., EU AI Act) could impose new liability on companies using AI-based tools.

Reputational Damage

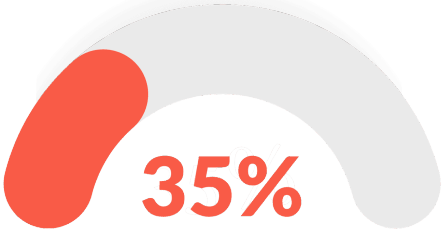
AI errors or biases (e.g., discriminatory lending algorithms, user bullying, or data hallucination) can undermine brand trust

Without a clear understanding of where and how AI is used, organizations face potential compliance, security, and ethical risks, including exposure to data privacy and intellectual property security violations and regulatory non-compliance. Cataloging use cases (both internal to the organization and within third-parties) is a must and with the speed of evolution in this space, is not a “one-and-done” proposition.

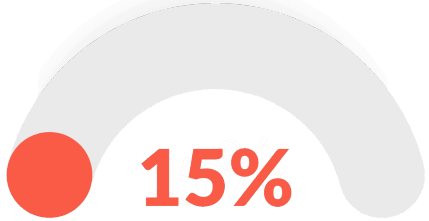
AI AS A RISK TO MANAGE

Lack of Visibility

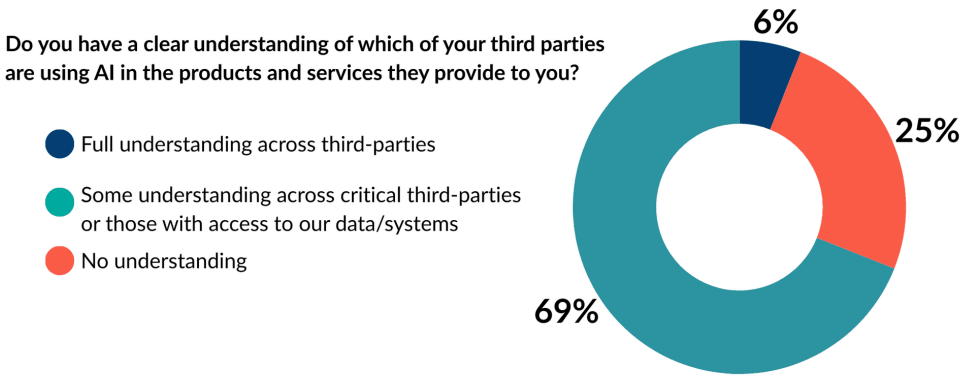
There is also the issue of a lack of visibility into and third party's use of AI. According to GAN Integrity survey data, only 6% of respondents have *full knowledge* of how their vendors leverage AI tools, while 25% have *no* visibility at all.



Include AI risk in third-party due diligence



Have AI provisions in third-party codes



Similarly, Ethisphere's own survey data shows that only 35% of organizations are including AI risk in their ethics and compliance third-party due diligence, and only 15% of organizations have provisions for Use of AI in their third-party code.

Like other technology solutions, there is always the risk of being lured by the promises of features that at the end of a long hard implementation, may not pay off in terms of efficiencies or improved quality. However, integrating AI into a TPRM program is very much emerging as the way to build a best-in-class program that can not only withstand the rigors of modern third-party risk, but place organizations ahead of their peers.

4 AI Risk Management Strategies

AI Governance Model

Define roles, responsibilities, and escalation protocols for AI-related breaches or bias incidents.

AI-Specific TP Codes and Contractual Clauses

Only **15%** of organizations currently include *AI usage* clauses in their third-party codes. Introduce AI-specific clauses in contracts (e.g., requirement to advise if systems or services use AI)

Human Oversight

Even the best AI systems need human review for nuance. Train staff to spot *algorithmic anomalies* and interpret complex risk alerts.

Continuous Improvement

Regularly update AI models and TPRM policies to reflect *changing regulations* (e.g., potential EU AI Act). Also, auditing AI processes ensures they remain aligned with evolving standards and best practices.

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

PART FOUR

BUILDING A BEST-IN-CLASS TPRM PROGRAM

in partnership with GAN Integrity

GAN INTEGRITY

BUILDING A BEST-IN-CLASS TPRM PROGRAM

Governance & Ownership

Governance and policy form the bedrock of an effective TPRM program. They define the organization's risk appetite, set accountability, and guide all external engagements.

By establishing documented policies and clear oversight structures, businesses ensure consistent standards, transparent decision-making, and cohesive conflict resolution methods.

Regular policy reviews allow for adaptation to changing regulations and technologies, minimizing non-compliance risks.

Strong governance aligns TPRM with enterprise objectives, embedding a proactive risk culture across departments. Ultimately, well-defined governance streamlines processes, fosters accountability, and sets the tone for the entire TPRM lifecycle.

Among the 2025 World's Most Ethical Companies honorees:

90% have a significant role in the end-to-end third-party risk management process.

95% maintain a documented policy for vendor management.

15% incorporate AI-specific clauses, such as a Use of Ai provision in their third-party code.

How AI May Help

Automated Policy Management: AI tools can monitor regulatory changes, compare them to existing policies, and suggest updates, streamlining compliance and reducing manual effort.

AI Governance Consideration

Ensure your TPRM policies require third parties to disclose if their products or services use AI, specify related controls, and provide evidence of their AI governance practices to maintain accountability and compliance.

BUILDING A BEST-IN-CLASS TPRM PROGRAM

Cross-Functional Collaboration

Effective TPRM requires breaking down silos between compliance, procurement, legal, risk, cybersecurity, and business units.

A centralized governance framework defines roles- for example, procurement owns vendor onboarding, compliance conducts due diligence, and IT assesses cyber risks.

Collaboration tools (e.g., shared dashboards) ensure visibility into vendor risks across teams. Accountability is enforced through clear escalation paths; for instance, high-risk vendors may require C-suite approval.

Training programs educate employees on red flags (e.g., suspicious invoicing) and reporting mechanisms.

How Technology May Help

- **Centralized Risk Intelligence:** Dashboards aggregate inputs from procurement, compliance, and IT to create a unified risk view, enabling faster, more informed decision-making.
- **Automated Workflows:** Machine learning can route risk alerts or approvals to the right stakeholders based on vendor criticality, or risk type streamlining processes and enforcing accountability.
- **Anomaly Detection:** AI algorithms can scan financial and operational data for unusual patterns (e.g., suspicious invoicing or vendor behavior), flagging potential issues early for cross-functional teams.

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

PART FIVE

FIVE PILLARS FOR TPRM SUCCESS

in partnership with GAN Integrity

FIVE PILLARS FOR TPRM SUCCESS

Comprehensive Third-Party Inventory

Maintaining a complete, centralized inventory of all third-party relationships is crucial for visibility and control. This repository details each vendor's services, contact points, contract terms, and associated systems. By mapping every supplier or service provider, organizations ensure they don't overlook hidden or rogue engagements.

Why It Matters

If you don't know who your third parties are, you can't effectively identify and manage their risks. Without an accurate inventory, risk assessments become inconsistent, and potential vulnerabilities may go unaddressed.

Industry Note

Many organizations find it challenging to keep their vendor lists updated, especially as various business units independently engage suppliers. This challenge is compounded by the rise in SaaS and freemium applications that employees may adopt without formal oversight.

How AI May Help

- **Automated Discovery:** AI-driven network scans can identify unregistered connections or data flows with third parties.
- **Data Consolidation:** Machine learning can reconcile disparate vendor records from multiple systems, such as accounts payable, ERP systems, and GRC systems into a single, unified profile.

AI Governance Caution

- **Data Accuracy:** Automated discovery can yield false positives; periodic human review is critical to confirm legitimate vendor relationships.
- **Privacy Compliance:** Any system that collects vendor data must adhere to data protection requirements (e.g., GDPR).

FIVE PILLARS FOR TPRM SUCCESS

Risk Identification & Assessment

The second pillar of TPRM is accurately identifying and assessing third-party risks before onboarding and throughout the engagement. Standardized questionnaires capture key details - such as cybersecurity measures, financial stability, and compliance posture - to guide risk scoring and segmentation. Vendors are classified as low, medium, or high risk, with scrutiny scaled accordingly. High-risk vendors, particularly in corruption-prone regions or industries, may require enhanced due diligence, site visits, or ongoing audits.

Why It Matters

A risk-based approach ensures resources are allocated effectively, focusing on the vendors and scenarios with the highest stakes.

Industry Note

Organizations increasingly use continuous, event-driven assessments- prompted by media reports or vendor changes - to keep risk profiles current. It's also vital to consider concentration risk, avoiding over-reliance on a single vendor or region.

How AI May Help

- **Contextual Risk Assessments:** AI creates bespoke risk assessment questionnaires and pre-populates with known data.
- **Contextual Risk Scoring:** Algorithms evaluate factors like vendor industry, country stability, assessment responses and known incidents to risk-score third parties

AI Governance Caution

- **Explainability:** Regulators and stakeholders often demand clarity on how AI models generate risk assessments.
- **Vendor Risk Assessment:** Identify third parties that may expose you to AI-related risks. Integrate questions to assess their AI risk posture effectively.

FIVE PILLARS FOR TPRM SUCCESS

Due Diligence & Onboarding

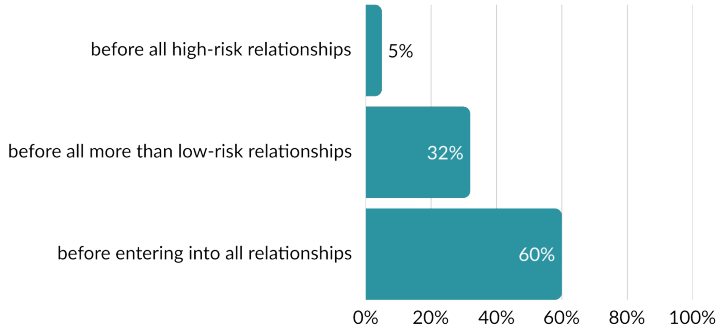
Due diligence and onboarding are critical pillars of a successful Third-Party Risk Management (TPRM) program, ensuring vendors meet compliance, ethical, and operational standards before formal engagement. According to Deloitte, effective due diligence is risk-based and tailored, scaling efforts according to the vendor's risk profile to maximize efficiency and minimize blind spots. Screening typically includes checks against sanctions lists, politically exposed persons (PEPs), adverse media, certifications, financial stability, and regulatory compliance.

Leading practices increasingly extend due diligence beyond direct suppliers to include subcontractors, addressing emerging ESG concerns such as modern slavery and environmental impacts.

Contracts are structured to define performance expectations, data protection requirements, and service-level standards, providing a clear framework for accountability and ongoing assessment.

Effective onboarding involves setting clear expectations and communication protocols from the outset, fostering transparency and collaboration.

2025 World's Most Ethical Companies honorees perform third-party due dilligence:



How AI Can Help

- **AI Screening:** Automates scans of public records, databases, and financial statements to quickly detect risks and inconsistencies.
- **AI Due Diligence:** Leverages deep search capabilities to compile thorough, narrative-driven reports from vast data sources, enhancing accuracy and speed.
- **NLP-based contract analytics** parse and compare proposed terms to risk policies, automatically flagging missing clauses and inconsistent performance benchmarks.

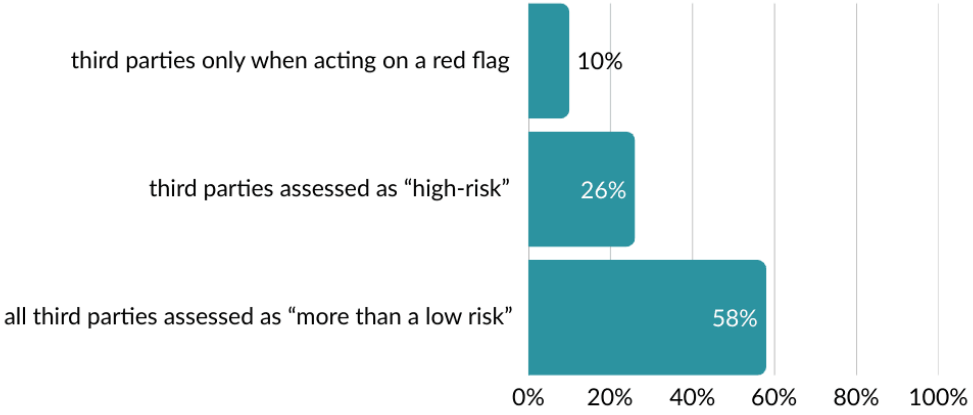
Continuous Monitoring & Oversight

Managing third-party risk is an ongoing effort. Continuous monitoring ensures that any changes in vendor risk profiles, service-level agreements, regulatory requirements, or cybersecurity alerts are identified promptly—allowing rapid, targeted corrective actions.

Why It Matters

Early detection of performance or compliance lapses prevents minor issues from escalating into major incidents, protecting both operational continuity and organizational reputation.

The 2025 World's Most Ethical Companies honorees routinely monitor:



Industry Note

Although many organizations traditionally rely on monthly or quarterly reporting cycles, technology advancements in data analytics and automation are making **near real-time monitoring** increasingly practical, enabling a more agile and proactive approach to third-party risk management.

How AI Can Help

- **Real-Time Alerts:** AI anomaly detection can quickly spot suspicious activity or sudden performance drops.
- **Predictive Trend Analysis:** Machine learning uses historical and external signals to forecast potential vendor issues.

AI Governance Caution

- **Alert Fatigue:** Excessive automated alerts can desensitize teams, risking missed genuine threats.
- **Data Reliability:** AI results rely on accurate, timely data; errors can significantly skew outcomes.

FIVE PILLARS FOR TPRM SUCCESS

Issue Remediation & Continuous Improvement

Even robust TPRM programs can face incidents—ranging from data breaches to compliance lapses or reputational crises. A well-defined remediation process ensures swift containment, thorough root-cause analysis, and transparent stakeholder communication.

Why It Matters

Effective remediation protects customer trust, averts regulatory penalties, and reduces the risk of repeat incidents. Ongoing refinements help these programs mature and stay ahead of evolving threats.

Industry Note

Lessons learned during remediation should feed back into risk assessment criteria, onboarding protocols, and performance metrics, continually strengthening the overall TPRM strategy.

Maturing a third-party risk management (TPRM) program delivers tangible advantages across multiple dimensions:

1. **Stronger Regulatory Compliance**
2. **Enhanced Operational Resilience**
3. **Improved Vendor Performance and Accountability**
4. **Cost Efficiency and Resource Optimization**
5. **Reduced Reputational Risk**
6. **Data-Driven Decision-Making**
7. **Competitive Advantage**

How AI May Help

AI-driven root-cause analysis tools can rapidly sift through incident data—logs, user reports, system metrics—to pinpoint contributing factors and propose targeted remediation steps.

FIVE PILLARS FOR TPRM SUCCESS

Don’t neglect…offboarding

Offboarding third parties is a critical yet often overlooked aspect of a robust Third-Party Risk Management program. Proper offboarding ensures that once a vendor relationship ends, all associated risks are effectively mitigated, compliance obligations are fulfilled, and sensitive data is protected.

Neglecting offboarding can leave organizations exposed to data breaches, compliance violations, contractual disputes, and reputational damage.

Key Considerations for Offboarding

- **Data Security & Access Termination**
  Revoke vendor access, retrieve or destroy sensitive data, and ensure compliance with data privacy laws (e.g., GDPR, CCPA).
- **Contractual Compliance**
  Confirm all obligations are met, document termination compliance, and complete final checks to fulfill deliverables.
- **Knowledge Transfer & Continuity**
  Complete knowledge transfer, document lessons learned, and apply insights to future processes.
- **Record Keeping & Auditing**
  Maintain detailed records for compliance, archival, and future audits
- **Payment System Updated**
  Ensure vendors are promptly removed from payment systems to prevent unauthorized or erroneous payments after contract termination.

CONCLUSION:

Making TPRM Work Smarter

Managing third-party risk is more challenging than ever. With expanding supply chains, evolving regulations, and rising ESG expectations, the pressure is on for companies to keep pace. But the solution isn't just about working harder, or adding more headcount -it's about working smarter.

AI is proving to be a powerful tool in streamlining TPRM. It's cutting through mountains of data, reducing false positives, and speeding up onboarding and monitoring processes. Instead of drowning in noise, compliance teams can focus on what really matters- identifying genuine risks and taking action.

But AI alone isn't enough. It works best when it's part of a bigger strategy that connects compliance, procurement, IT, legal, and cybersecurity teams. It's about building a unified approach where everyone is aligned and working toward the same goals.

The key is using AI where it makes the most impact. That means automating repetitive tasks, surfacing hidden risks, and continuously monitoring vendors for changes that matter. And just as importantly, making sure governance is in place to keep everything fair, accurate, and transparent.

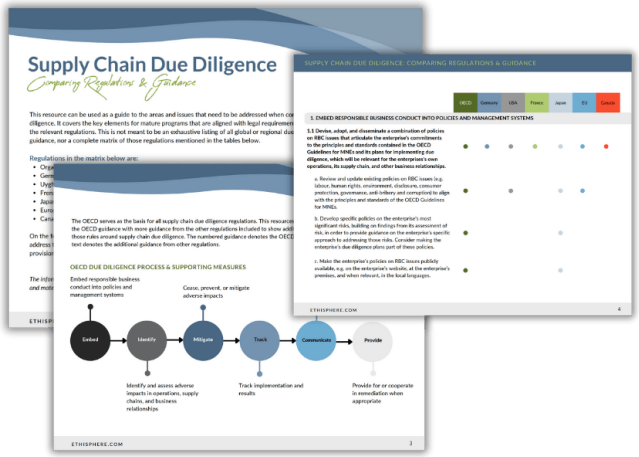
Ultimately, TPRM success comes down to blending AI's efficiency with human expertise. When done right, it transforms TPRM from a reactive process into a proactive advantage- giving companies the visibility, speed, and resilience they need to stay ahead of risks.

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

PEER RESOURCES

in partnership with GAN Integrity

Best Practices

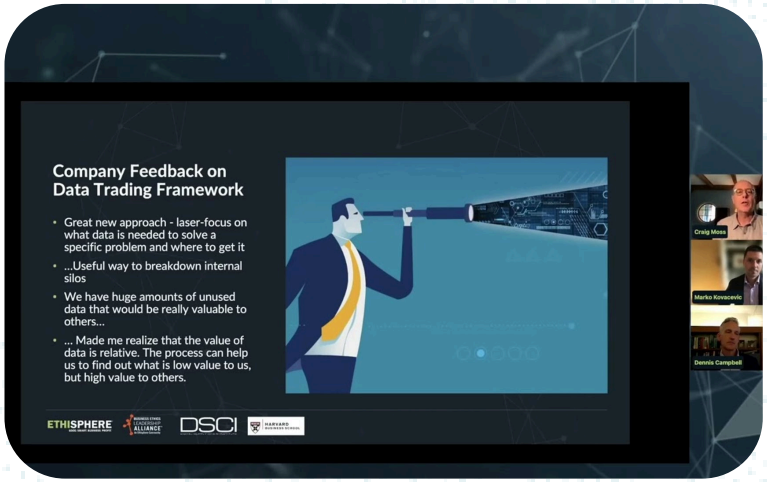


[Supply Chain Due Diligence: Regulations & Guidance Comparison Guide]

This resource can be used as a guide to the areas and issues that need to be addressed when conducting global or regional supply chain due diligence. It covers the key elements for mature programs that are aligned with legal requirements and includes a sample of the relevant regulations.

Strategic Data Trading: A New Approach to Reduce Third-Party Risk

Experts from Ethisphere, Harvard University, and the Digital Supply Chain Institute discuss the concept of data trading as a way to manage third-party risk.



PEER PRACTICES

Exclusive Insights: Program Examples

Save time and be more effective with BELA's support. Tap into our community, best practices, and time-saving resources to enhance your compliance efforts, level up your program, and reduce the burden on your internal teams. The BELA Member Hub is full of expert created templates and real examples of what works for Fortune 500 organizations globally.

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

REQUEST GUEST ACCESS

TTEC

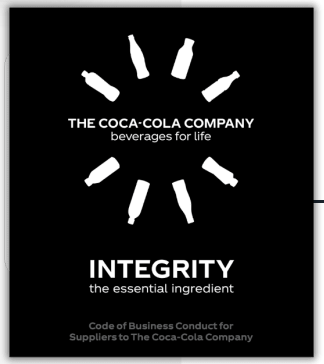
Supplier Code of Conduct

TTEC shares their Supplier Code of Conduct with the BELA Community. The Code establishes standards for their supply chain to ensure that they align with TTEC's values, policies, and applicable laws and regulations.

ADM

Supplier Expectations Principles

Archer Daniels Midland Company's suppliers are expected to do business fairly, ethically, and in compliance with all applicable laws and regulations at all times. Additionally, suppliers are expected to understand and abide by ADM's Supplier Expectation principles.



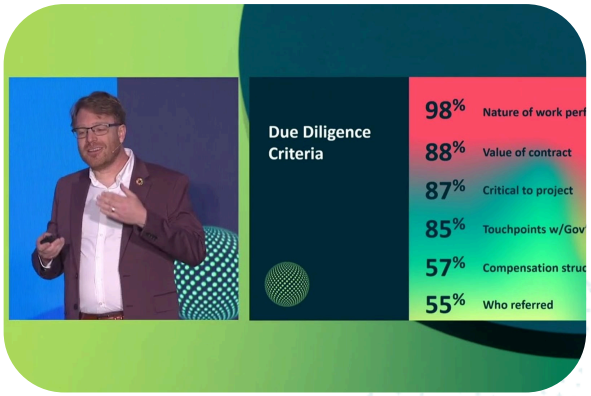
COCA-COLA

Code of Business Conduct for Suppliers

BELA member The Coca-Cola Company shares their Code of Business Conduct for suppliers.

Expert Insights from the Global Ethics Summit

Click on the image to play the session.



Ethisphere Driven Data: Third-Party Due Diligence

Rethinking Third-Party Due Diligence: Moving to a Coordinated Approach Across the Organization

Managing Multi-Level Third Party Relationships and Due Diligence Requirements in Emerging Markets

Ethisphere Solutions: Assessing and Building Maturity in Third Parties

Reports & White Papers

Comprehensive Guide to Third-Party Risk Management Mastery

This high-level document provides a helpful breakdown of the discrete elements of a successful third-party risk management system, including implementing a tiered, risk-based approach; establishing comprehensive due diligence processes; and embracing automation and AI (with appropriate governance in place).

An Introduction to Third-Party Risk Management

Just getting started on a TPRM roadmap? This primer offers helpful overviews of the TPRM process and its constituent sub-topics.

A Buyer's Guide to Third-Party Risk Management Software

This provides a concise but detailed breakdown of the key considerations for investing in AI as a part of your third-party risk management system, as well as use case and implementation road map descriptions.

AI Governance Under Pressure

This report explores how compliance leaders are ensuring AI governance keeps pace with the technology's rapid adoption.

TPRM

Need more resources?

ethisphere.com/resources
ganintegrity.com/resources