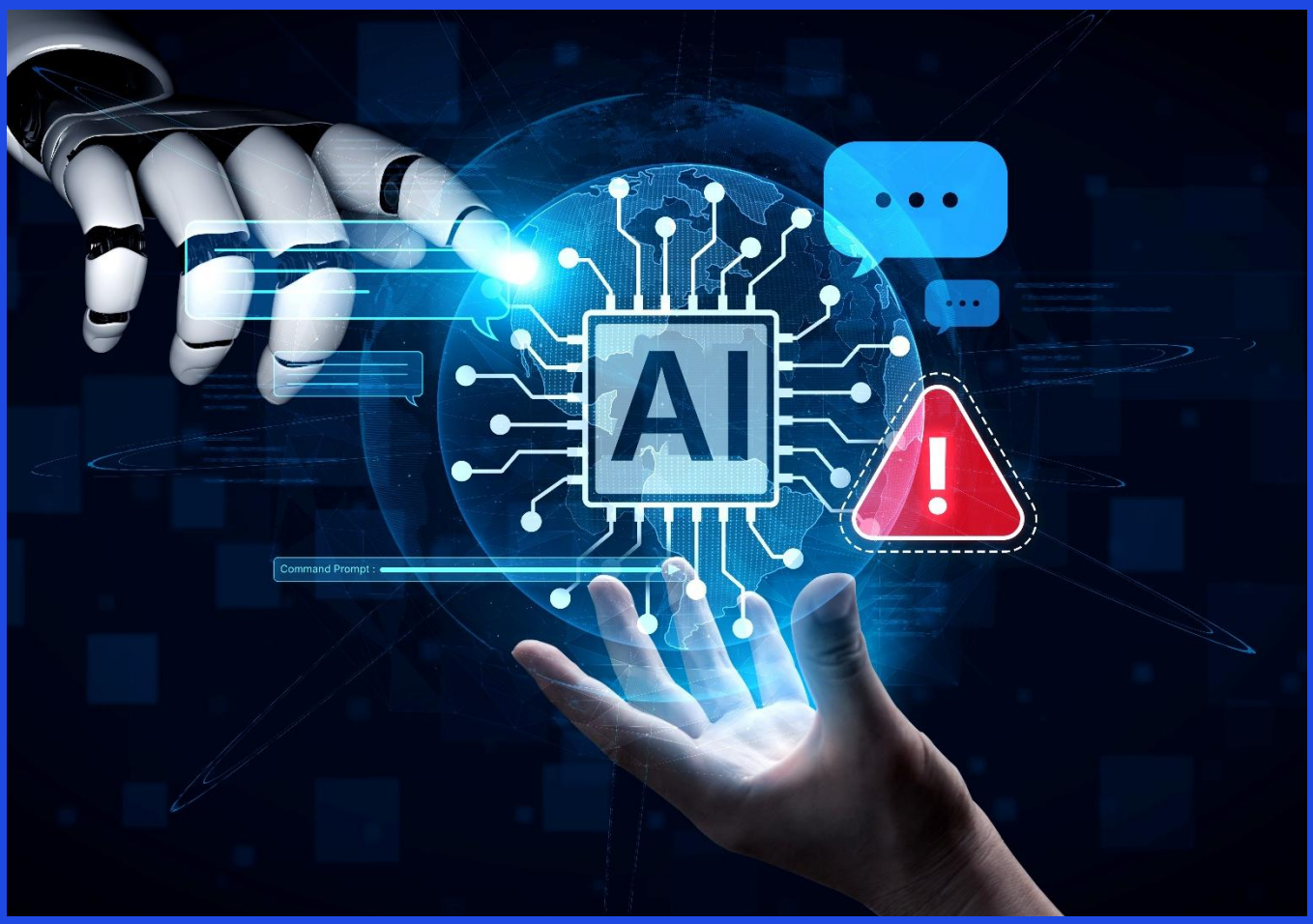
Bridging gaps and building guardrails with artificial intelligence in third-party risk management



November 2025

kpmg.com/in

KPMG. Make the Difference.

Organisations today face increasing pressure to manage third-party risks with greater speed, precision, and accountability. This perspective explores how artificial intelligence (AI)[1] is being applied across the third-party risk management (TPRM) in its entire lifecycle, the challenges involved in its integration, and the importance of combining AI with human intelligence to deliver targeted, actionable insights. While AI enhances decision-making and operational efficiency, but human judgement is essential for interpreting context, managing exceptions, and making ethically sound decisions. The future of TPRM lies in a collaborative model where AI enhances decision-making and humans provide strategic oversight and responsibility.

AI is revolutionising how organisations govern third-party relationships, elevating oversight from periodic reviews to continuous, intelligent risk governance. As supply chains grow more complex and regulatory scrutiny penetrates deeper, the ability to monitor, predict, and respond across vast third-party ecosystems is becoming a key marker of organisational resilience. Our research shows that AI is no longer a support function; it is fast becoming the strategic core of enterprise risk management.[2]

According to KPMG International's 2025 AI quarterly pulse survey, 56 per cent of Chief Experience Officer (CXOs) believe AI could reshape their business within a year, rising to **67 per cent** in two years. The KPMG in India's 2025 CEO outlook survey shows that **57 per cent** of Indian Chief Executive Officers (CEOs) and **69 per cent** globally plan to allocate 10–20 per cent of their budgets to AI in the next 12 months. Moreover, a strong majority, ***73 per cent in India*** *and* ***67 per cent globally***, expect to see ***returns on AI investments within one to three years***, reflecting growing confidence in AI's near-term business impact.

Despite growing confidence in AI's potential, one critical question remains, 'how is it fundamentally reshaping the nature of third-party risk?' Let's delve into how third-party risk is being redefined in the age of AI.

The changing face of third-party risk[3]

Third-party risk has evolved far beyond those identified during traditional due diligence at the time of onboarding a third party. In today's hyper-connected business landscape, organisations are increasingly exposed to ***risks stemming from global supply chains which make them*** interdependent, often cascading across departments and geographies. We regularly see compliance and procurement functions dealing with the following:

- **Compliance risk**: Compliance risk refers to the threat of legal or regulatory penalties due to non-adherence to laws, standards, or contracts. It is heightened in sectors like finance, healthcare, and government, where oversight is strict. Third-party failures such as data breaches or labour violations can expose organisations to indirect non-compliance, especially under regulations like European Union's General Data Protection Regulation (GDPR). According to KPMG in Belgium's 2024 KPMG Global chief ethics and compliance officer survey[4], ***84 per cent expect the focus on compliance to increase due to rising regulatory expectations and scrutiny in the next two years.***

1. For the purpose of this document, AI includes Generative AI (Gen AI) and associated technologies.
2. The AI outlook - KPMG Assurance and Consulting Services LLP, September 2025; Global CEOs double down on AI & talent drive despite economic challenges - KPMG International Limited, October 2025; KPMG 2025 global CEO outlook - KPMG International Limited, October 2025; Understanding AI in third-party risk management: 3 organizational use cases - Forbes Technology Council, September 2024; Leveraging AI to transform third-party risk management in 2025 - SAFE Securities, Inc, August 2025; KPMG 2025 India CEO outlook - KPMG Assurance and Consulting Services LLP, October 2025
3. Highlights from the State of third-party risk management 2025 Survey - Venminder Experts, February 2025; Regulatory & ESG compliance in third party risk for 2025 - Third Party Risk Institute Ltd., 2025; The future of third-party risk management: seven key predictions for 2025 - Cyber Defense Media Group, April 2025; Threat-informed TPRM: A new standard for supply chain security - BitSight Technologies Inc, October 2025; Third-party risk management (TPRM): A complete guide - BlueVoyant LLC, November 2025; Third-party risk management - Diligent Corporation, July 2025; KPMG 2025 India CEO outlook - KPMG Assurance and Consulting Services LLP, October 2025; Assessing third-party ESG risks - Risk and Insurance Management Society, Inc, April 2023
4. KPMG Global chief ethics and compliance officer survey, KPMG International Limited, January 2024

- **Reputational risk**: Reputational risk is a key concern in TPRM, where external lapses can reflect poorly on the organisation. Environment, health and safety (EHS) failures such as environmental violations, unsafe workplaces, or poor health practices can trigger public backlash and regulatory scrutiny. These risks undermine stakeholder trust and expose the organisation to compliance consequences. According to 'KPMG Middle East's 2025 report on 'Critical considerations in third-party risk management'[5], a survey conducted by KPMG found that ***73 per cent of respondents confirmed that inefficiencies in their TPRM program exposed them to reputational risk***.
- **Environmental, social and governance (ESG) integration:** ESG factors are key indicators in TPRM, bringing vulnerabilities. Environmental risks such as climate impact can disrupt operations; social risks such as labour violations may destabilise supply chains; and governance risks like fraud or corruption threaten financial integrity and reputation. Together, these factors demand proactive oversight. According to KPMG US' 2023 ESG risk practices article[6], organisations are responsible for the accuracy and governance of ESG data from their vendors, as regulators demand consistency and reliability. ***Poor third-party oversight can lead to reporting errors, compliance failures, and regulatory penalties.***
- **Security threats**: Security risks are key concerns in TPRM, as weak vendor security can lead to data breaches and operational disruptions. Threat actors may exploit software flaws, insert malicious code, or tamper with physical components, compromising entire supply chains. Such incidents expose sensitive data and damage organisational trust and resilience. According to 'KPMG Middle East's 2025 report on 'Critical considerations in third-party risk management'[7], a study by Cyentia Institute and Security Scorecard found that ***98 per cent of organisations have a relationship with at least one third-party that has experienced a breach in the last two years***.

Unlocking potential of AI across the third-party risk spectrum[8]

TPRM is an essential pillar of enterprise risk management, enabling organisations to systematically identify, assess, and mitigate risks associated with external vendors, suppliers, and partners. It plays a critical role in helping ensure regulatory compliance, safeguarding reputation, and maintaining operational continuity by addressing exposures across key domains such as cybersecurity, EHS, financial stability, and legal obligations.

AI is transforming TPRM by ***automating assessments, enhancing threat analysis, and streamlining oversight***. However, as organisations and third parties increasingly adopt AI, new risks emerge around the security of AI use cases and the reliability of AI-generated deliverables. This growing adoption expands the risk surface and prompts tighter scrutiny. KPMG in India's outlook on AI in TPRM aligns with a SMART approach:

5. Critical considerations in third-party risk management - KPMG International Limited, July 2025
6. KPMG ESG risk practices – KPMG LLP, January 2023
7. Critical considerations in third-party risk management - KPMG International Limited, July 2025
8. Third-party AI risk: A holistic approach to vendor assessment - Onetrust LLC, February 2024; How does AI factor into ESG? - Enhesa Group, August 2025; 69% of CEOs to allocate over 10% of budgets to AI over the next 12 months - Finextra Research Limited, October 2025; CEOs prioritize geopolitics, ESG, and digital in KPMG's latest outlook - The Financial Analyst, October 2025; ESG in the age of AI - KPMG Assurance and Consulting Services LLP, August 2024; How AI is poised to reshape compliance functions - KPMG International Limited, July 2025; Ai In The Compliance Industry Statistics - Wifi Talents, June 2025; 2024 Sustainability Organisation Survey - KPMG LLP, February 2024; How to use AI for contract review and compliance in 2025 - Nucamp Inc, August 2025; AI-based contract management guide 2024 - Contractpod Technologies Ltd, March 2024; The Strategic Role of AI in Governance, Risk and Compliance (GRC) – Technostrong Group Inc, April 2024; Automating the future: AI-driven vulnerability management and the rise of autonomous solutions - Vicarius Ltd, September 2025; 33+ AI statistics in cybersecurity for 2025 - All about AI, November 2025; Decoding the EU AI act - KPMG LLP, 2024; KPMG report – Where will AI/gen AI regulations go? - KPMG LLP, August 2023; Third-party risk management in the AI Era: Evolving models and practices | Blog - Everest Global Inc, July 2025; KPMG 2025 India CEO outlook - KPMG Assurance and Consulting Services LLP, October 2025; KPMG 2025 Global CEO outlook - KPMG International Limited, October 2025; 2024 ACC's chief legal officers survey - Association of Corporate Counsel, January 2024

SMART: AI across the third-party risk spectrum

S **Sustainability and ESG:** AI is reshaping ESG ***by improving data accuracy, emissions tracking, and supply chain transparency***, while also introducing ***risks such as energy use and algorithmic bias***. The current ESG frameworks often overlook AI's impact, prompting a push for '***sustainability by design' and stronger governance***. Responsible AI helps align innovation with ESG goals and strengthens visibility across multi-tier supply chains.

M **Monitoring regulatory compliance:** Global regulations are evolving rapidly, and this complexity makes manual compliance tracking nearly impossible. AI is transforming regulatory compliance by enabling real-time monitoring of legal updates, automating documentation, and forecasting regulatory shifts. AI reduces audit errors and costs by streamlining compliance evaluations.

A **Automated contract intelligence:** AI streamlines contract management by enforcing compliance and identifying risks early. It rapidly analyses large volumes of vendor data with precision. This enhances efficiency and uncovers patterns often missed manually.

R **Risk detection in cybersecurity and data privacy**: AI is redefining cyber and data security by delivering faster, smarter, and more scalable threat detection, vulnerability management, and compliance capabilities.

T **Third-party mapping and workflow automation:** AI improves visibility across extended third-party networks, supporting better oversight and supply chain resilience. It streamlines workflows by generating risk-based questionnaires, auto-filling responses, and analysing vendor data efficiently to enhance consistency in screening.

Did you know?

- *According to the KPMG International's 2025 Global CEO Outlook,* ***65 per cent of CEOs have fully embedded sustainability into their business*** *and believe it is critical to their long-term success. Further, according to KPMG in India's 2025 CEO outlook, nearly* ***77 per cent CEOs in India*** *in alignment with* ***78 per cent CEOs globally*** *consider AI instrumental in* ***reducing emissions and enhancing energy efficiency****.*
- According to KPMG US's 2024 Sustainability Organisation Survey, **58 per cent** of organisations plan to **improve ESG data collection with AI**.
- According to the **Association of Corporate Council (ACC)'s 2024 chief legal officers report**, **45 per cent of Chief Legal Officers (CLOs)** plan to invest in new technology solutions to enhance operational efficiency.
- According to all about AI's 2025 article on AI statistics, AI-powered systems detect hidden threats with ***up to 80 per cent accuracy and predict future attacks with 66 per cent reliability.***
- According to KPMG in India's 2025 CEO outlook, CEOs in India and globally are leveraging AI primarily to enhance decision-making and data analysis, with **23 per cent in India** and **19 per cent globally** citing these as one of potential benefits. Beyond analytics, AI is also seen as a strategic enabler for **improving efficiency**, **automating routine tasks, detecting fraud,** and **strengthening cyber resilience**.
- According to KPMG International's 2025 Global CEO outlook, **34 per cent of CEOs** are prioritising **AI integration into operations and workflows** as a key investment driver.

The world is recognising: current and emerging AI regulations[9]

AI is being regulated across the globe, with authorities issuing or finalising frameworks that emphasise restrictions, responsible development, and approval protocols. Below is given a glimpse of AI regulations, around the world:

Canada

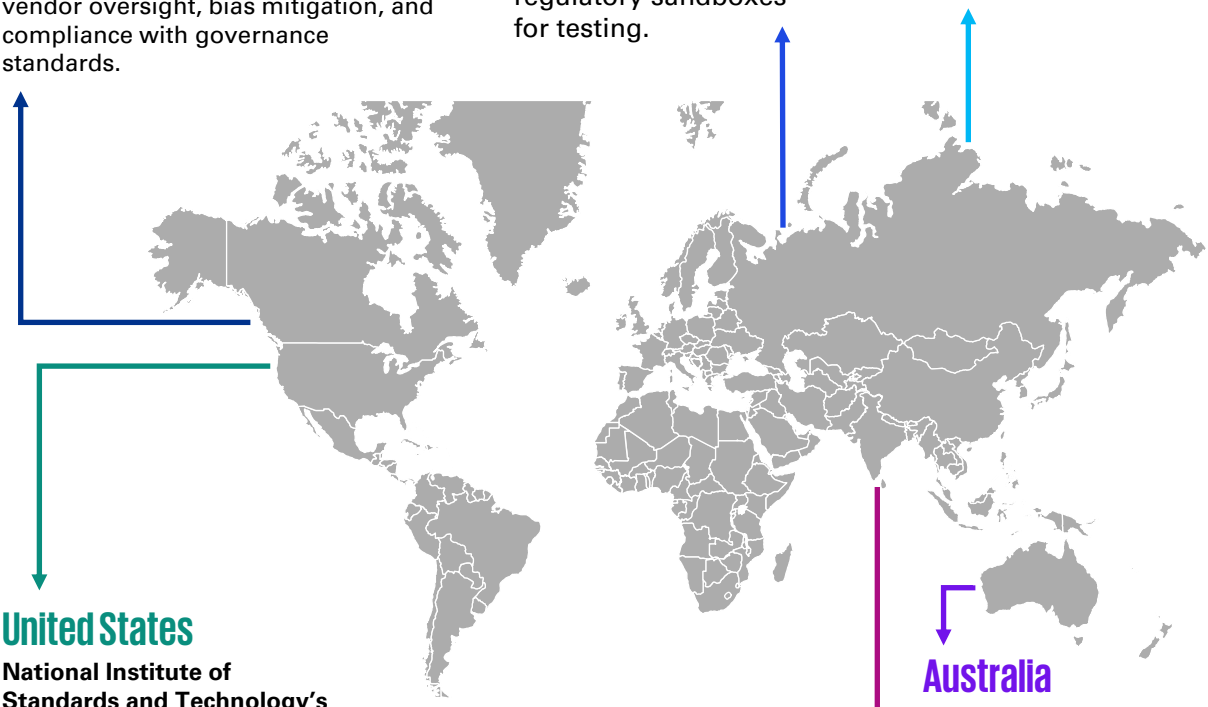
Canada's **Artificial Intelligence and Data Act** (AIDA), introduced in 2022 under Bill C-27, aims to regulate high-impact AI systems with principles like transparency, fairness, and accountability. It requires organisations to ensure ethical AI use, vendor oversight, bias mitigation, and compliance with governance standards.

United Kingdom

The **UK's AI regulation bill** proposes an AI authority and governance principles, transparency, accountability, safety, fairness, and inclusivity, along with regulatory sandboxes for testing.

European Union (EU)

The **EU AI Act 2024** is one of the first comprehensive law regulating AI, categorising systems by risk level, **unacceptable, high, limited, and minimal**, with strict requirements for high-risk applications. It applies to both EU and non-EU entities impacting EU.



United States

National Institute of Standards and Technology's (NIST) AI Risk Management Framework (2023) offers voluntary guidance for trustworthy AI, supported by a resource center and global alignment efforts. Its generative AI profile (2024) provides targeted risk management strategies for generative AI systems.

India

In 2023, Ministry of Electronics and Information Technology (MeitY) **proposed a voluntary ethical AI framework, while the Reserve Bank of India (RBI) introduced** AI governance guidance under its 2025 risk standards. Expert committees and the Bureau of Indian Standards are drafting national norms for responsible, secure AI development and deployment.

Australia

Australia's **Voluntary AI Safety Standard (2024)** outlines ten guardrails for ethical AI use, focusing on governance, risk, data oversight, and transparency. Though non-binding, it guides businesses in responsibly deploying third-party AI systems and sets the stage for future regulation.

According to the **KPMG US's** 2023 generative AI survey, ***77 per cent of the business leaders cited the uncertain and evolving regulatory landscape*** as a top barrier to implementing generative AI. However, this concern is not slowing down the AI adoption - ***83 per cent plan to increase investments in generative AI*** by 50 per cent or more in 6-12 months.

9. States are passing AI laws; what do they have in common? - Corporate Compliance Insights, May 2025; Consumer protections for artificial intelligence - Colorado General Assembly, 2024; Global AI regulations and their impact on third-party risk management - Mitratech Inc, April 2025; AI and Regulation Are Merging in India; and it's the right time to setup a clear ethical framework - The Indian Express [P] Limited, August 2025; Voluntary AI Safety Standard - Australian Government, September 2024; AI regulation in India: current state and future perspectives - Morgan, Lewis & Bockius LLP, January 2024; Where will AI/GenAI regulations go? - KPMG LLP, August 2023; AI risk management framework - National Institute of Standards and Technology, October 2025; 2023 KPMG generative AI survey - KPMG LLP, June 2023

AI in action across the TPRM lifecycle [10]

	TPRM lifecycle	AI-integration: use cases
1	**Data collection and questionnaire:** Gather initial third-party information through standardised forms and public data.	**Automated data extraction and questionnaire analysis**: AI pulls structured/ unstructured data from submissions, and flags missing or inconsistent responses.
2	**Inherent risk assessment:** Assess baseline risk based on factors such as nature of work, industry regulations, economic conditions, complexity of operations etc.	**AI-driven inherent risk evaluation**: AI generates bespoke risk profiles and auto-classifies third parties based on inherent risk factors.
3	**Due diligence:** Deep dive into third-party background, financials, ownership, adverse media, legal and compliance screening.	**Mapping complex ownership and hidden relationships:** Utilising AI-driven analytics to map intricate ownership networks, identify ultimate beneficial owners (UBOs), detect risks associated with third parties, and uncover concealed relationships.
4	**Financial and compliance review:** Assess financial health and regulatory adherence to identify potential red flags.	**AI-Driven Compliance Document Analysis:** AI automates the review of key documents like contracts, financial statements and other reports to detect compliance risks, anomalies, unauthorised subcontractors and potential fraud.
5	**Contracting:** Finalise agreements with risk-mitigating clauses and compliance terms.	**Clause-level risk detection**: Machine learning reviews contractual language to highlight deviations and unusual clauses from standard terms and ensure compliance with policies.
6	**On-going monitoring:** Continuous monitoring of high-risk third parties through external sources to detect emerging risks.	**Real-time monitoring and pattern detection:** Continuously monitor third parties to generate alerts when adverse information, reputational issues, or compliance concerns arise.
7	**Continuation/offboarding:** Reassess third-party relationships to determine whether to continue engagement or initiate a structured exit.	**AI-supported risk mitigation:** Evaluates performance trends, emerging risks, and compliance posture to support continuation decisions or prioritise high-risk entities for offboarding through dynamic scoring and automated triage.

10. The New Triad of AI Governance: Privacy, Cybersecurity, and Legal - Isaca, March 2025; Ethical and regulatory challenges in AI-driven cybersecurity - daily security review, August 2025; Integrating ESG and AI: a comprehensive responsible AI assessment framework - Springer Nature Limited, June 2025; Critical considerations in third-party risk management - KPMG International Limited, July 2025; What is Third Party Risk Management (TPRM)? - Veza Technologies Inc, July 2025; 2023 KPMG generative AI survey - KPMG LLP, July 2023; 9 emerging use cases for AI in TPRM - Corporate Compliance Insights, May 2025; Intelligence-Led Third-Party Risk Management: What It Means and Why It Matters - Gan Integrity Inc, July 2025; AI in third party risk management - SafetyCulture, September 2025

Navigating AI integration challenges in TPRM?[11]

While AI is undeniably transforming the risk management by driving efficiency, scalability, and deeper insights across phases, its integration is not without challenges. Some of the key challenges includes:

Data protection and security considerations: Safeguarding sensitive third-party data from breaches and unauthorised access is critical in AI environments, especially given the volume and sensitivity of information processed.

Data quality and availability: AI models require accurate, complete, and unbiased data. Inconsistent or missing data can lead to flawed risk assessments and unreliable insights.

Integration challenges and skill gaps: Many organisations face difficulties integrating advanced AI solutions with existing infrastructure and manual workflows, which may not be designed to support automation or intelligent analytics. These challenges are further compounded by technical skill gaps, limiting the effective deployment and utilisation of AI technologies.

Regulatory and ethical compliance: Organisations must navigate evolving legal frameworks such as GDPR, the EU AI Act, and India's Digital Personal Data Protection Act (DPDPA), 2023, helping ensure that AI usage aligns with ethical standards and data protection laws.

Cost Considerations in AI Implementation: Deploying AI solutions often demands significant investment in technology, infrastructure, and skilled personnel, which can be a barrier for many organisations.

Algorithmic complexity: The technical sophistication of AI algorithms can be challenging for non-specialist teams to understand, manage, and validate, potentially limiting adoption and trust.

According to the **KPMG US's** 2025 AI quarterly pulse survey, ***82 per cent of business leaders cite risk management including data privacy as the most significant challenge*** to their generative AI strategies, followed by concerns ***over the quality of organisational data (64 per cent)***. Additionally, ***66 per cent of organisations identify system complexity*** as the primary obstacle in ***training employees to effectively work with AI agents.***

11. AI in third party risk management - SafetyCulture, September 2025; KPMG Q1 2025 AI pulse survey - KPMG LLP, April 2025; AI in risk management: top benefits and challenges explained - TechTarget Inc, July 2025; 5 Ways AI is revolutionizing third-party risk management - NB Ventures Inc, March 2025

AI and human intelligence: a collaborative risk lens

As AI matures, it might shift organisations from reactive fixes to proactive and resilient strategies across sustainability, security, and compliance. However, human judgment remains essential for interpreting context, managing exceptions, and helping ensure ethical accountability. The future lies in a collaborative model where **AI enhances decision-making, while humans provide strategic insight and uphold responsibility.**[12]

While AI is transforming due diligence with speed and scale, it's human intelligence that ensures precision, context, and judgment. Here's how our experience proves that the best outcomes come from blending both.

Assessment area	AI intelligence: need of hour	Human intelligence: the accuracy filter	Our experience : a real-world catch
Data source complexity	• AI supports background review of third parties. • Extracts structured data such as registrations, activities, and key financials. • Extracts unstructured data like media reports. • Operates at scale to streamline data collection.	While AI enables faster aggregation, human intelligence remains critical to validate accuracy, interpret context, and identify subtle complexities that automation may overlook.	When a vendor publishes a sustainability report claiming full compliance with ethical labor standards, an AI system may classify it as low-risk based on structured data and keyword analysis. However, during manual review, signs of greenwashing were spotted including vague language and the absence of independent audits. These concerns were looked into further using local regulations, media reports, and contextual understanding to get a clearer picture.
Beneficial ownership analysis	• AI uses advanced data processing to analyse ownership structures. • Employs pattern recognition to identify relationships and control. • Applies predictive analytics to uncover beneficial ownership. • Enhances visibility into complex corporate hierarchies.	Ownership data often varies across sources due to differences in reporting standards, update cycles, or disclosure depth. AI can sometimes misinterpret intricate ownership patterns, misinterpret incomplete filings, or fail to reconcile conflicting data. That's where human intelligence becomes essential.	In one case, AI compiled shareholder data from public sources to fill gaps left by financial statements that didn't disclose parent company shareholding percentages. However, during manual review, it was found that the data should have been cross verified with the parent companies' annual reports.

12. KPMG 2025 India CEO outlook - KPMG Assurance and Consulting Services LLP, October 2025

Assessment area	AI intelligence: need of hour	Human intelligence: the accuracy filter	Our experience : a real-world catch
Reputational risk analysis	• AI-driven media ingestion automates data collection. • Analyses vast amounts of unstructured information. • Interprets content from diverse sources like news articles and regulatory databases.	Human intelligence brings essential context, judgment, and verification that AI alone can't offer. Analysts validate flagged content, correct misinterpretations, and filter out noise, outdated data, or speculative claims.	AI scanned public sources to identify reputational risks efficiently. In one case, it relied on outdated articles and missed recent developments. In another, it used speculative language that could have influenced the risk rating. These issues were resolved during human review, helping ensure the final output was accurate, current, and objective.
Litigation intelligence monitoring	• AI speeds up legal risk analysis. • Scans public records and litigation databases to flag potential exposure. • Enables scalable checks across jurisdictions. • Identifies legal matters that may impact compliance or risk ratings.	Data pertaining to litigations can be complex, fragmented, or outdated. AI may miss recent case updates, misinterpret legal terminology, or flag irrelevant proceedings. Human reviewers validate findings, interpret context, and ensure that only relevant, current, and accurately classified matters related to disputes or proceedings are considered.	AI was used to extract and summarize orders pertaining to lawsuits during compliance checks, aiding in the identification of cases across jurisdictions. However, it occasionally misinterpreted orders or classified cases ambiguously. These errors were resolved during human review, helping ensure accurate legal risk assessments.
Real-time exposure detection	• AI enables real-time monitoring of third parties. • Continuously scans for changes in legal, regulatory, sanctions, and media exposure. • Sends automated alerts to identify emerging risks early. • Reduces manual oversight. • Helps maintain compliance across large vendor networks.	AI may flag irrelevant updates or misinterpret context, especially across jurisdictions or industries. Human reviewers assess the materiality of alerts, verify relevance, and ensure that only meaningful developments impact third-party risk assessments.	AI monitored 40+ third-party entities for adverse media, sanctions, and regulatory risks - delivering real-time alerts and reducing manual effort. In one case, it flagged a target due to a full-name match with a sanctioned entity. Human review revealed the match was with a completely unrelated entity, having no connection to the third party under assessment, eliminating a false positive and helping ensure accurate risk evaluation.

Conclusion: targeted intelligence for risk scenarios[13]

While AI and associated technologies are new and rapidly evolving, true value lies in applying them responsibly. It's not just about innovation; it's about embedding thoughtful controls at every stage to strengthen governance and risk posture. A well-structured responsible AI programme enables organisations to treat TPRM risks with the same rigor as other enterprise risks, helping ensure **trust, transparency, and resilience** in predictive analytics and decision-making.

AI is revolutionising TPRM. It is transforming traditional processes across the lifecycle, from onboarding to monitoring, into intelligent and automated workflows. It improves user **experience through simplified interfaces and reduced manual effort**. AI enhances risk understanding using predictive analytics and contextual data. It also enables full integration of risk areas such as cyber, compliance, and financial into a single, unified framework. Moreover, it drives **standardisation across functions**, promoting scalable and proactive risk governance. Embedding AI boosts **negotiation power**, and **strategic impact**, while reducing **cyber risk**. It also automates complex diligence like **contract analysis, privacy checks**, and **compliance reviews**, scanning vast data for **regulatory gaps and security flaws**. As AI integrates with enterprise risk frameworks, organisations can **reassess vendor risks in real time**, cut costs, and strengthen **cyber resilience**. According to KPMG Middle East's 2025 report on 'Critical considerations in third-party risk management',[14] **with AI-integration – 50 to 80 per cent of today's procurement tasks,** including many linked to vendor risk evaluations, **can be automated, streamlined, or shifted to self-service models**.

At KPMG in India, we understand that responsible AI involves navigating complex business, regulatory, and technical challenges. We are committed to helping clients put it into practice effectively. By combining deep industry expertise, advanced technology capabilities, and a strong partner ecosystem, we help leaders harness AI, **from data collection to continuous monitoring of third parties, with confidence and clarity**.

13. 5 Ways AI is revolutionizing third-party risk management - NB Ventures Inc, March 2025; Understanding AI in third-party risk management: 3 organizational use cases - Forbes Technology Council, September 2024; AI in third party risk management - SafetyCulture, September 2025; Critical considerations in third-party risk management - KPMG International Limited, July 2025; The TPRM lifecycle in 6 phase - Aravo Solutions Inc, January 2024
14. Critical considerations in third-party risk management - KPMG International Limited, July 2025

Contributors

Rahul Atreja

Director, Managed Services-CDD

Rachna Rawal

Manager, Managed Services-CDD

Arun Choudhary

Assistant Manager, Markets

Angeeta Baweja

Manager, Markets

KPMG in India contacts:

Akhilesh Tuteja
Head - Clients & Markets
E: atuteja@kpmg.com

Hemant Jhajhria
Partner – Head of Consulting
E: hemantj@kpmg.com

Manoj Kumar Vijai
Office Managing Partner and Head – Risk Advisory
E: mkumar@kpmg.com

Maneesha Garg
Partner and Head – Managed Services
Forensic, F&A, HR, Learning, Insight Led Sales, Digital Business Operations and Sourcing
E: maneesha@kpmg.com

Vipul Jain
Partner – Managed Services
Forensic
E: vipuljain@kpmg.com

Ummehaani
Partner – Managed Services
Forensic
E: ummehaani@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.