Deloitte.

In association with **OneTrust**

MANAGING THIRD-PARTY RISK

PROACTIVELY WITH DATA INTELLIGENCE

Organizations increasingly rely on third parties to drive innovation and deliver on core objectives. As the number and complexity of these third-party relationships grow, so does the challenge of managing risk in an environment marked by rapid change. Traditional third-party risk management (TPRM) models, which often rely on periodic assessments, struggle to keep up with new and increased threats and expectations.

To help address this challenge, many organizations are transforming TPRM with data intelligence by moving programs toward near real-time awareness and proactive decision-making. As reliance on third parties increases, organizations are asking: How can we stay ahead of evolving risks and still realize value from these critical relationships?

What follows is a clear, five-step path to modernizing TPRM—grounded in practical choices, priority use cases, and the operating discipline needed to sustain results.

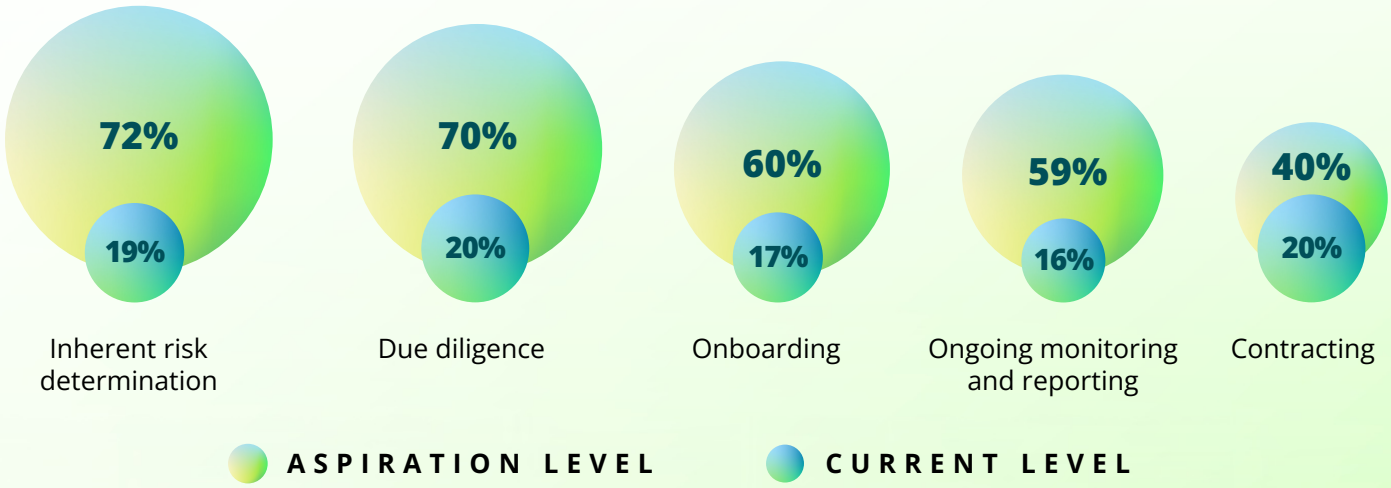
STEP 1

UNDERSTAND CURRENT MARKET TRENDS

Many organizations recognize that modernizing their TPRM practice is no longer optional. The accelerating pace of business, digital transformation, and broader supply chain interconnectivity have exposed gaps in legacy risk frameworks. Greater efficiency and integration are now critical, spurring investment in artificial intelligence (AI) and data intelligence capabilities to help teams sense risk earlier and respond faster.

At the same time, the market reality is a familiar one: ambition is high, maturity is not. *Deloitte's Global TPRM 2025 survey* of 300+ leaders found 93% reporting low maturity in AI-enabled TPRM, even as organizations aim to adopt intelligent automation and manage both the opportunities and risks of AI across third-party ecosystems.[1]

Specifically, organizations aim to increase use of intelligent automation to enhance TPRM efficiency and outcomes in the following areas:



[1] Deloitte Global, Assessing AI's impact on Third-Party Rish Management (TPRM); Global third-party risk management flash survey 2025, p.14

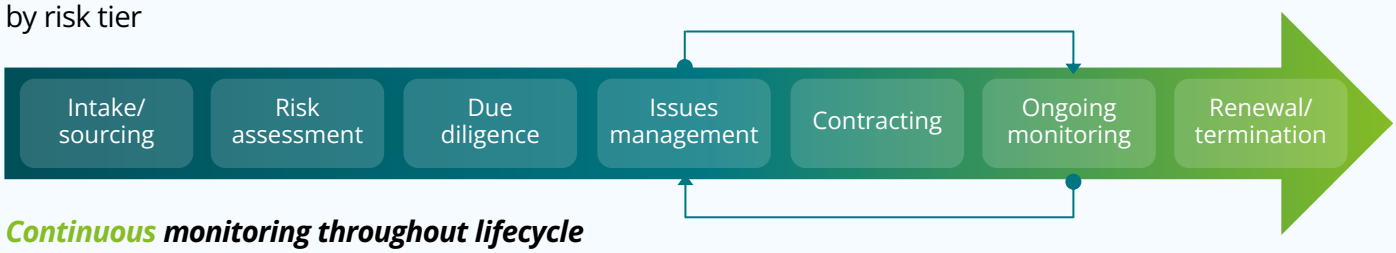
STEP 2

START NOW AND ESTABLISH CONTINUOUS VIGILANCE

Traditional TPRM programs use periodic and point-in-time assessments, often missing emerging risks. Transformation calls for an integrated and proactive approach for continuous insight into third-party risk.

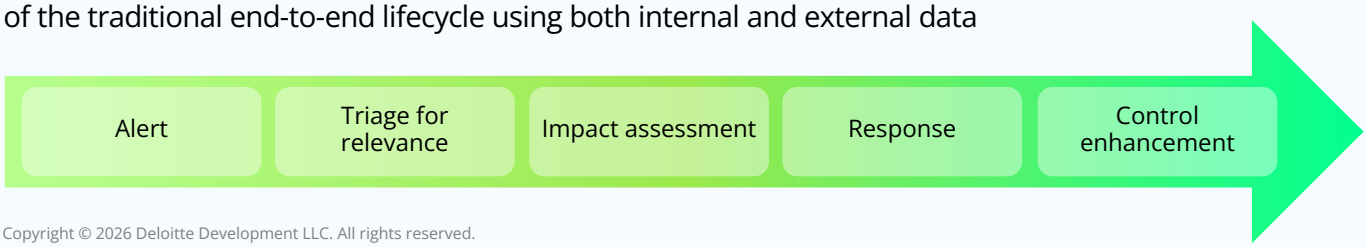
***Traditional* end-to-end lifecycle**

Evaluates third-party control effectiveness, relative to the service being delivered, on a cadence dictated by risk tier



***Continuous* monitoring throughout lifecycle**

Continuously monitors and evaluates third-party control effectiveness and emerging risks at any phase of the traditional end-to-end lifecycle using both internal and external data



Proactive TPRM programs are evolving to complement existing linear paths to the traditional end-to-end lifecycle and periodic reviews with continuous, data-fueled vigilance at each phase. This modern vision typically includes four capability shifts:

EMBED CONTINUOUS MONITORING THROUGHOUT THE LIFECYCLE

Tools across major risk domains can provide near real-time alerts on risks, threats, and events. Leading teams define alert thresholds to filter what matters, pair signals with playbooks, and often start with a pilot/proof of concept before scaling.

LEVERAGE AI-POWERED RISK MANAGEMENT TO AUGMENT HUMAN DECISION-MAKING

Many organizations already use automated workflow and data intelligence to run their TPRM program. AI agents can assist with risk rating, template creation, and semi-autonomous tasks such as routing and issue triage. These capabilities, which will be released soon within the OneTrust platform, can help workers identify and respond earlier to critical issues.

ENHANCE PROGRAM EFFICIENCY WITH "DIGITAL CO-PILOT" EXPERIENCES

A practical early value area is enabling a more user-friendly interface for business/first-line users to interact with the risk program—routing communication and providing baseline information without requiring heavy navigation of a broader governance, risk, and compliance (GRC) platform. Automating document analysis/validation reduces manual effort, accelerates onboarding, and enables more granular profiling through dynamic assessments.

USE INTELLIGENT AUTOMATION TO SHIFT WORK FROM ADMINISTRATION TO DECISION

Automating intake, document validation, and dynamic risk scoring can help reduce human error and free risk teams to focus on strategic challenges. OneTrust will soon support additional capabilities for semi-autonomous agents, including issue logging, evidence management, and ongoing triage—functioning as staff augmentation, grounded in data intelligence.

STEP 3

ASSESS MATURITY TO BUILD A REALISTIC ROADMAP

Organizations differ widely in their maturity in data intelligence, proactive risk management, and AI adoption. At the same time, many are encountering practical barriers that can slow progress from interest to scaled adoption:

Unclear business case: Upfront cost concerns and limited visibility into return on investment (ROI) on AI investments.

Integration complexity: Difficulty integrating AI tools into legacy platforms and workflows.

Capability constraints: Limited internal expertise and capacity to build an AI strategy.

Governance concerns: Heightened security and privacy concerns drive more complex AI governance.

Understanding your current position is the foundation for setting clear goals and charting a realistic path forward—so you can identify the capabilities to build and sequence what matters most.

ENHANCE PROCESSES WITH AUTOMATED ACTIVITIES	SEAMLESS INTEGRATION OF AUTOMATED WORKFLOWS	AUGMENTING HUMAN ACTIVITY WITH AI AGENT	INNOVATION THROUGH AUTONOMOUS AGENTIC AI
• **Task automation** streamlines compliance, **reduces errors**, and accelerates TPRM cycles, **enabling rapid adaptation to changes** • Augment manual assessments with **data intelligence and risk ratings**	• **Modernize legacy processes** by adding **automation to the TPRM lifecycle** to stay current with regulatory and business changes • Use **conditional logic to relate** processes and manual risks	• Position AI agent as a **digital co-pilot, proactively** surfacing risks, recommending actions and **handling routine communications** with third parties • Automate the **creation of issues, corrective actions**, and recommendations • **Enable** risk professionals to focus on complex **analysis and strategies**	• **Enable semi-autonomous execution** of routine TPRM activities, such as continuous monitoring, real-time risk scoring, and relevant external data risk scans • **Advance TPRM maturity** by leveraging agentic AI that **learns** from outcomes, **enhances** processes, and **scales** across the enterprise • Monitor activities and processes with **real-time altering and actioning response plans**

As organizations mature and evolve, automation unlocks new horizons and empowers teams.

STEP 4

SELECT AND IMPLEMENT PRIORITY USE CASES ACROSS THE TPRM LIFECYCLE

Organizations and vendors continue to invest in proactive use cases and data insights. Near real-time, continuous risk, threat, and event intelligence can enable TPRM teams, business owners, and executives to make adaptive, risk-based decisions.

Use cases and data insights span across the TPRM lifecycle:

PRE-CONTRACT SCREENING

Prescreen third parties across priority domains, apply rules-based scoping to reduce time-to-market, and enable dynamic inherent risk as new signals emerge. Targeted innovative applications include:

Agent-assisted intake, prescreen, inherent risk questionnaire (IRQ), and profile creation

Agent-driven control assessments, evidence review, and data correlation

Agent-assisted issue management

ASSESSMENT EFFICIENCY

Improve scoping and deferral decisions, enable dynamic assessment and issue management, and challenge control assessment responses more consistently. Accelerate remediation by tailoring recommendations to business impact and internal indicators, and trigger re-assessment based on contractual terms and available data intelligence.

CONTINUOUS MONITORING

Expand scope and depth of coverage with continuous oversight, improve impact analysis, and strengthen incident response through always-on insights. Leverage supplier master data and segmentation to set and update risk/threat/event (RTE) triage thresholds and continuously scan internal and external sources to identify potential RTEs.

SUPPLY CHAIN TRANSPARENCY

Use 4th/5th (Nth)-party concentration insights to identify geographic and dependency risks and to surface ecosystem exposure to service disruptions.

PREDICTIVE RISK INDICATORS

Move from sensing to anticipating by combining proactive risk sensing and threat intelligence with internal third-party advisories and early warning indicators.

STEP 5

LEARN, ADAPT AND CREATE VALUE

MAKE VALUE DURABLE WITH A "SINGLE SOURCE OF TRUTH"

Organizations can unlock value by integrating TPRM with broader strategic goals and building unified data repositories—a "single source of truth" that gives decision-makers relevant, actionable insight with speed and confidence.

FOCUS ON THE OPERATIONAL "MUST-HAVES"

Key priorities typically include data quality, integration with existing systems, and managing privacy/cyber risks introduced by new technologies—supported by defined processes, smart tooling, and continuous learning as systems refine performance over time.

TREAT AI GOVERNANCE AS A CORE RISK DISCIPLINE

As AI becomes embedded into third-party activities and services, TPRM programs are updating vendor agreements to require disclosure around AI use, deploying AI detection tools, and incorporating AI-specific risk assessments. AI is increasingly treated as its own risk domain with tailored controls for bias, reliability, data privacy, and regulatory shifts (e.g., rising expectations under regulations such as the Digital Operational Resilience Act).

THREE TAKEAWAYS FOR LEADERS:

Be practical, value-driven, and consider both opportunities and risks from using AI

Make better, faster and proactive decisions using real-time insights and automation

Commit to continuous improvement: learn, adapt, and refine based on maturity and evolving priorities

HOW TO APPLY THESE TAKEAWAYS TO YOUR TPRM PROGRAM

NOW

- **Build an AI automation business case** including a roadmap and specific tactical goals
- If needed, perform a rapid assessment to **align priorities across relevant stakeholders**
- **Focus on low hanging fruits** such as piloting available external and internal risk ratings and insights into your lifecycle

NEXT

- **Articulate both current and future value** from your TPRM program including at the executive level
- **Communicate risk aggregation, risk escalation and incident management** as means to accelerate decisions and time to market
- In parallel, **begin designing and implementing longer term enhancements** such as process and tech transformation, change management, and optimization

LATER

- **Adapt and calibrate enhancements as well as** transformation from program redesign and pilot learnings
- **Continue to elevate TPRM to the executive level** as a core risk management and value add function

HOW DELOITTE AND ONETRUST CAN HELP

In today's complex risk environment, organizations are relying on third parties at unprecedented scale, accelerating innovation while increasing supply chain, data, and compliance exposure. OneTrust's AI-powered TPRM platform unifies data intelligence, supply chain visibility, threat intelligence, regulatory compliance, and risk management so teams can move faster with greater confidence.

Technology alone doesn't deliver outcomes: adoption, operating model, and execution do. Deloitte helps clients translate OneTrust capabilities into measurable risk reduction and business value end-to-end: from strategy and implementation through run-state support.

Deloitte is OneTrust's #1 system integrator (2024–2025), with deep experience aligning deployments to each organization's risk appetite, regulatory context, and operating realities. **We bring demonstrated accelerators, access to a global delivery team, and TPRM leading practices that include modern data intelligence and next-generation automation,** all supported by deep knowledge across Cyber, Compliance, and Data Privacy. We design scalable, audit-ready workflows that help organizations reduce manual effort, improve decision quality, and sustain performance through advisory and managed services.

Together, Deloitte and OneTrust help clients unify silos, enable data-driven decisioning, and operationalize efficient, resilient TPRM, supporting stronger performance and sustainable, value-added growth.

READY TO GET STARTED?

Suzanne Denton
Managing Director
Deloitte & Touche LLP
sudenton@deloitte.com

Nikolay Hristoskov
Specialist Leader
Deloitte & Touche LLP
nhristoskov@deloitte.com

Hannah Borreson
Manager
Deloitte & Touche LLP
hborreson@deloitte.com