Deloitte.

Reimagining modern third-party risk management (TPRM)

Rapid tech evolution and new business needs are driving a reimagination of the TPRM function. In pursuit of efficiency gains, organizations are prioritizing artificial intelligence (AI) investments in components of their TPRM programs.

The future of TPRM is being shaped by the integration of advanced technologies, particularly AI. Organizations are prioritizing AI-enabled solutions in TPRM—such as smart alerts for risk prioritization, dynamic risk assessments, and predictive analytics dashboards—with the intention of improving compliance, risk management, loss avoidance, and supply chain efficiency, including effective integration with legacy systems.

These innovations can also introduce challenges such as heightened data privacy concerns, new cyber risks, and the potential for bias and ethical issues. Addressing these challenges will be critical as organizations aim to realize the potential benefits of AI-enabled TPRM.

Current map of the TPRM function and underlying life cycle, services, and processes

A blueprint for an AI-powered future: This model represents the TPRM function, along with the foundational services and processes that form the baseline for reimagining and transitioning to an AI-driven approach. It illustrates how people, processes, and technology are integrated within the TPRM function. The legend below identifies the new and evolved AI-enhanced services.

TPRM life cycle

Evaluate and select	Pre-contract due diligence	Contract and onboarding	Ongoing monitoring	Renew or terminate
• Identify need and define qualification requirements • Source and shortlist third parties • Complete pre-screen and service/product request • Complete inherent risk questionnaire (IRQ) and due diligence applicability matrix • Select and/or move to due diligence	• Identify and assess third parties using risk data sources • Conduct targeted due diligence and control assessments • Document findings, recommend actions, including risk acceptance • Map and align security controls to the TPRM framework	• Negotiate contract terms • Draft risk clauses and include auto-generated ones based on risks profile • Obtain approvals and execute agreement • Initiate onboarding and establish performance metrics	• Track performance metrics • Segment third parties and monitor risks • Continuously monitor third-party risks using external data • Conduct periodic assessments and ongoing monitoring • Manage issues, risk mitigation, and risk acceptance	• Notify third-party • Cease service access • Retrieve assets/data • Finalize documentation and checklists • Conduct exit strategy and review

TPRM program management

Policies and standards	Risk domains (cyber, privacy, AI, etc.)	Cross-functional alignment (GRC[1], S2P[2], CLM[3])	Training and awareness	Risk culture
Governance and oversight	Quality assurance and integrity	Program management office	Reporting KRIs[4], KPIs[5] and aggregate metrics	Performance management

TPRM technology management

Platform integration and architecture	Configuration and change management	Platform maintenance and optimization	Dashboards and analytics	Data quality, management and security	User experience management	Compliance and audit support

LEGEND

- **TPRM-specific AI uplift (partial + SME input**
- **Deloitte Ascend™ for Cyber (primarily applies to broader tech and program management)**
- **Partial AI uplift and SME input**
- **TPRM core capabilities (tech vendors AI uplift)**

1. Governance, risk & compliance, 2. Source to pay, 3. Contract life cycle management, 4. Key risk indicator, 5. Key performance indicator

Connect to accelerate

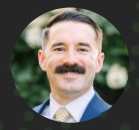
Contact our leaders to dive deeper into the blueprint and reimagine what's possible for your organization.

Mark Nicholson
Principal
Cyber AI GTM Leader
Deloitte & Touche LLP
manicholson@deloitte.com

Naresh Persaud
Principal
AI Transform Leader
Deloitte & Touche LLP
napersaud@deloitte.com

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

Ali Ziaee
Managing Director
TPRM Leader
Deloitte & Touche LLP
aziaee@deloitte.com



Steve Ruzzini
Senior Manager
Cyber AI GTM
Activation Lead
Deloitte & Touche LLP
sruzzini@deloitte.com

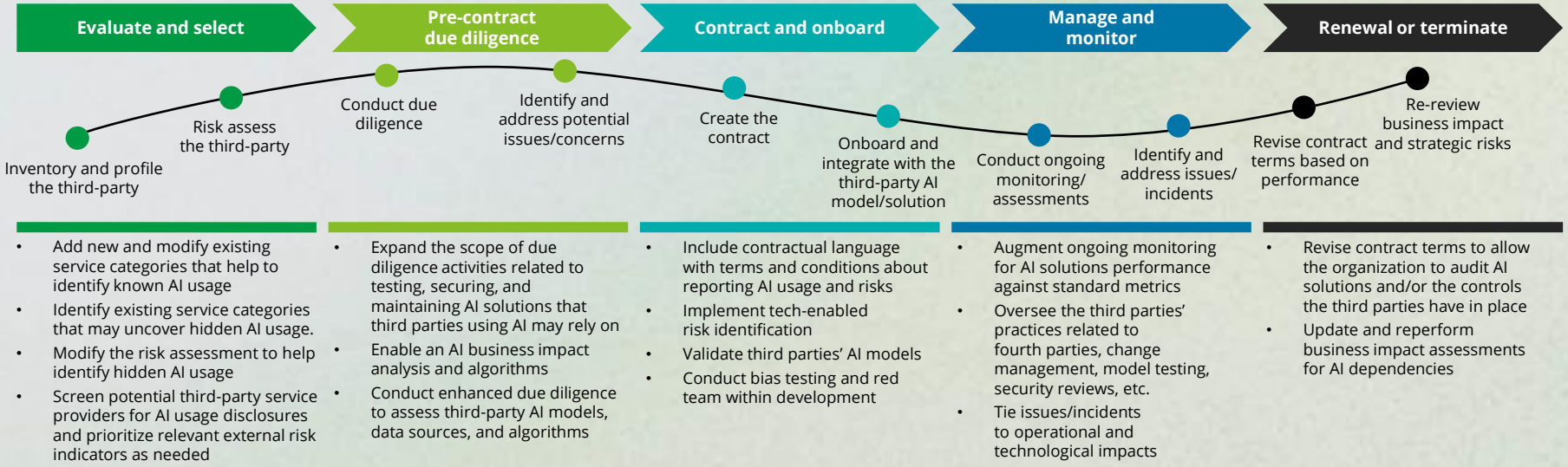
AI for TPRM: Functional uplifts to achieve greater efficiency

Explore how harnessing AI and smarter solutions can reduce manual effort and accelerate results across key functions.

Process/function	Uplift approach	Potential resulting impact
Evaluate and select	Agent-assisted vendor inventories onboarding, services categorization, risk assessment, using data to inform risk scores and future contracts	• Adequate information • Reduce errors and duplications
Pre-contract due diligence	AI-driven control assessments, evidence reviews, issue management and data correlation	• Near elimination of questionnaire-led assessment and improve accuracy via dynamic due diligence
Contract and onboard	AI-enabled contract generation based on inherent risk and control assessments, escalations based on deviations to contract requirements	• Reduce manual mapping and data entry from contracts
Ongoing monitoring	AI-guided continuous risk monitoring, performance management and response planning based on external and internal data	• Efficient and effective filtration through alerts • Relevant risk / threat / event (RTE) alerts
Renewal or termination	AI-guided renewal activities, coordination of termination and contingency plan activities	• Proficient termination process
Program and technology management	AI-enabled intelligent reporting, smart program helpdesk, data quality, role-based training	• Improve consistency/efficiency in reporting • Near elimination of manual requests/follow up

TPRM for AI: Managing risk across the third-party life cycle

Various activities across the third-party life cycle can be enhanced to better identify, assess, and manage both known and hidden AI usage.



Evaluate and select

- Add new and modify existing service categories that help to identify known AI usage
- Identify existing service categories that may uncover hidden AI usage.
- Modify the risk assessment to help identify hidden AI usage
- Screen potential third-party service providers for AI usage disclosures and prioritize relevant external risk indicators as needed

Pre-contract due diligence

- Expand the scope of due diligence activities related to testing, securing, and maintaining AI solutions that third parties using AI may rely on
- Enable an AI business impact analysis and algorithms
- Conduct enhanced due diligence to assess third-party AI models, data sources, and algorithms

Contract and onboard

- Include contractual language with terms and conditions about reporting AI usage and risks
- Implement tech-enabled risk identification
- Validate third parties' AI models
- Conduct bias testing and red team within development

Manage and monitor

- Augment ongoing monitoring for AI solutions performance against standard metrics
- Oversee the third parties' practices related to fourth parties, change management, model testing, security reviews, etc.
- Tie issues/incidents to operational and technological impacts

Renewal or terminate

- Revise contract terms to allow the organization to audit AI solutions and/or the controls the third parties have in place
- Update and reperform business impact assessments for AI dependencies

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for adetailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting. Copyright © 2025 Deloitte Development LLC. All rights reserved.