



Third-Party Trust Intelligence

Reimagining TPRM
with AI Agents



What it is:

A solution to strengthen Third-Party Risk Management across the lifecycle

Third-Party Risk Managers



Enterprise Risk Leaders



Information Security Risk Teams



Address fragmented third-party oversight through a digitally enabled lifecycle.

Why it matters

Third-party exposure and regulatory expectations are increasing, while many programmes remain fragmented across ownership, data, and technology.

Limited ecosystem visibility, point-in-time assessments and inconsistent execution slow decisions and obscure concentration, subcontractor and ongoing performance risks. Connected lifecycle oversight helps organisations apply proportionate controls and identify adverse changes earlier.

What it does:

Strengthen Oversight Across Third-Party Relationships

Gain a connected view of third-party risk

so they can identify critical dependencies, concentration exposure and changes in risk posture.

Prioritise and accelerate risk activities

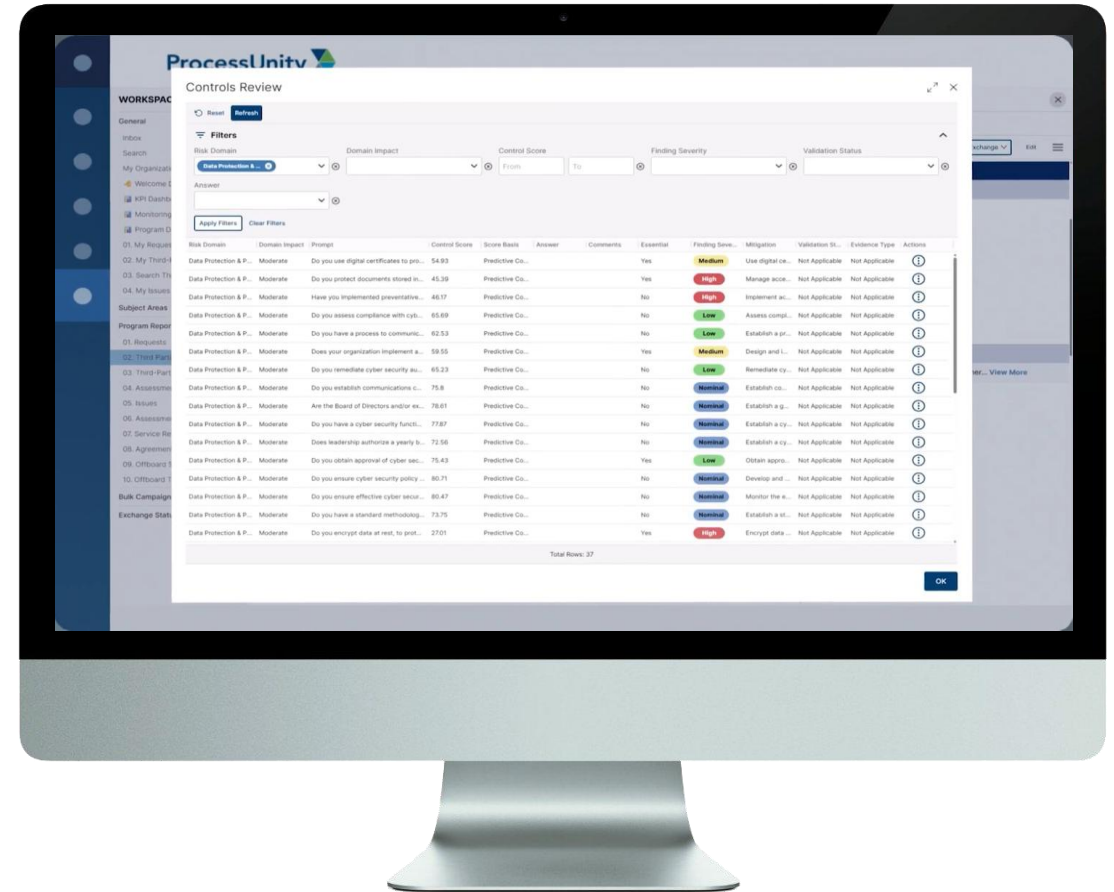
so they can focus resources on higher-risk relationships while reducing manual assessment effort.

Maintain consistent lifecycle oversight

so they can support governance, regulatory reporting and informed decisions from onboarding through offboarding

Benefits

- Focus resources on the third parties that matter most.
- Identify emerging risks and critical dependencies earlier.
- Support informed decisions with greater consistency and confidence.



How it does it: Demo

Input

The organisation provides third-party records, risk information, contracts, assessments and supporting evidence.

Action

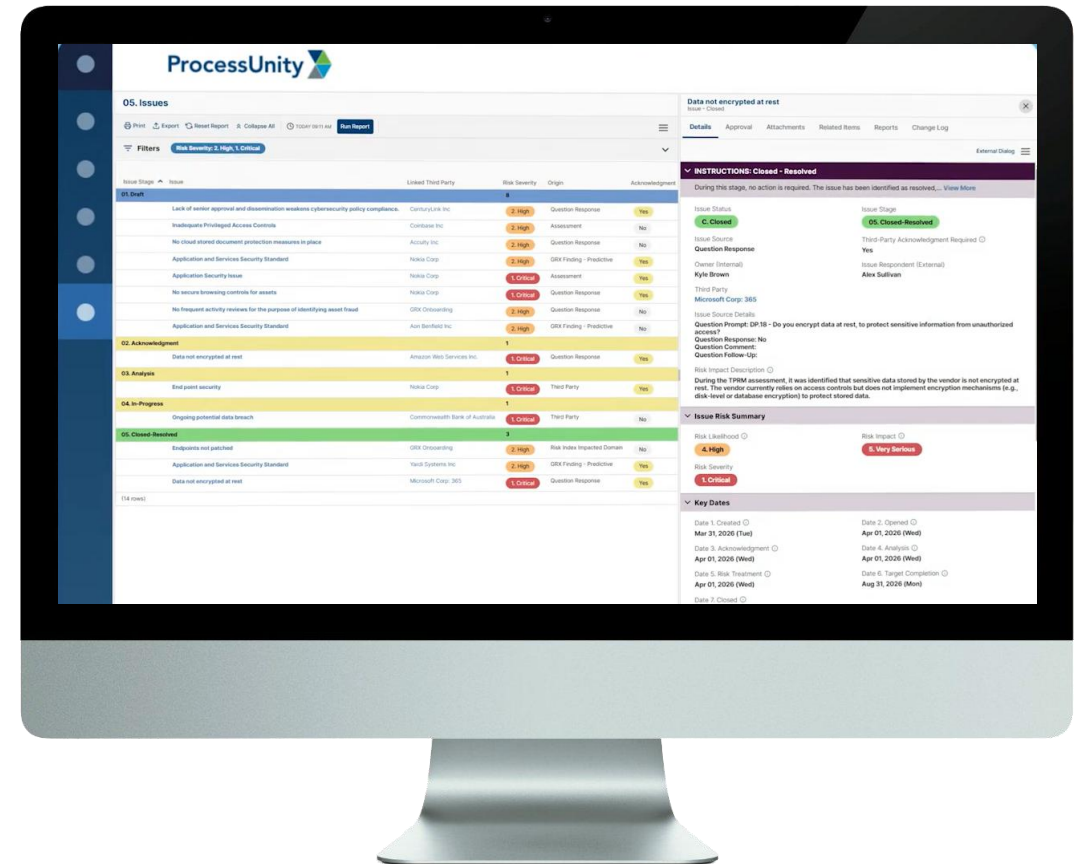
The solution applies risk-based workflows, monitoring, automation and AI across the third-party lifecycle, while practitioners retain oversight of consequential decisions.

Output

Users receive a connected inventory, risk assessments, evidence-backed insights, monitoring alerts and management reporting.

Impact

Teams can make faster, better-supported decisions and maintain consistent oversight throughout each third-party relationship.



Explore stronger third-party risk oversight

Discover how connected data, automated workflows and continuous monitoring can strengthen control across your third-party lifecycle.

Consider a discussion if your organisation is:

- Preparing for expanded MAS third-party risk expectations
- Improving visibility across third and fourth-party dependencies
- Reducing manual effort across assessments and ongoing monitoring

Speak to us on how you can strengthen your third-party risk lifecycle.



Girish Nair

Manager, Cyber
KPMG in Singapore

girishnair2@kpmg.com.sg

KPMG's Offerings: Four service families that cover the whole lifecycle

			
TPRM Strategy & Transformation	TPRM Execution	TPRM Assurance	TPRM Managed Services
<ul style="list-style-type: none">• Assess TPRM maturity and identify gaps against MAS and other Outsourcing and Technology Risk Management expectations.• Design risk-based policies, standards and governance frameworks for managing third-party risk.• Develop target operating models, accountability structures and oversight mechanisms across the third party lifecycle.• Establish supplier risk tiering, assessment methodologies and risk acceptance criteria.• Define transformation roadmaps to strengthen regulatory readiness and programme effectiveness.	<ul style="list-style-type: none">• Establish and maintain comprehensive third-party inventories to improve third party visibility and risk coverage.• Perform inherent risk assessments and due diligence reviews across key risk domains.• Conduct critical third party and dependency assessments to identify resilience and concentration risks.• Review contractual arrangements against organisational requirements and regulatory obligations.• Support planning and issue management to address identified control and compliance gaps.	<ul style="list-style-type: none">• Assess the design and operating effectiveness of TPRM controls across the third party lifecycle.• Perform independent reviews of governance, oversight and compliance with regulatory expectations.• Evaluate supplier monitoring, risk reporting and escalation processes.• Conduct third party assurance reviews to validate the management of material third-party risks.• Test business continuity, resilience and exit management capabilities for critical third-party arrangements.	<ul style="list-style-type: none">• Operate day-to-day TPRM activities including supplier onboarding, assessments and ongoing oversight.• Perform continuous monitoring and periodic reassessments to maintain an up-to-date view of third party risk.• Manage remediation, incident response, escalation and action tracking.• Support governance forums through risk reporting, management information and regulatory reporting inputs.• Maintain ongoing oversight of third-party risks to support compliance and informed decision-making.

Technology and digital enablement across all service families

Delivery Approach: To Support MAS TPRM Readiness

01 MAS TPRM READINESS ASSESSMENT

3 - 4 WEEKS

KEY ACTIVITIES

Evidence review Review the framework, policies, register, contracts, due diligence files and monitoring evidence.

Requirements mapping Map proposed MAS requirements to existing processes

Gap validation Provide a set of activities in the form of a roadmap to address gaps in the current process along with dependencies (indicative budget, resources, technology)

ILLUSTRATIVE DELIVERABLES

- Obligations/control matrix
- Readiness assessment and gap report
- Risk-ranked remediation backlog
- Implementation plan and board briefing

02 TPRM FRAMEWORK & GOVERNANCE DESIGN

4 - 6 WEEKS

KEY ACTIVITIES

Framework development Draft the strategy, framework, policy and standards for FI review and approval.

Risk methodology Define risk appetite, materiality, risk tiers and proportionate lifecycle requirements.

Operating model Identify and suggest the proposed operating model for executing the set of activities.

ILLUSTRATIVE DELIVERABLES

- Draft framework, policy and standards
- Materiality and risk-tiering method
- Lifecycle control library and RACI
- Board and management reporting templates

03 THIRD-PARTY REGISTER & ASSESSMENT PREPARATION

8 - 12 WEEKS

KEY ACTIVITIES

Register remediation Reconcile source records into a complete MAS-aligned register with data quality controls.

Assessment design Classify material arrangements and build risk assessment and due diligence requirements. Conduct pilot risk assessments for sample third party arrangements.

Contract remediation Review key clauses and track control, contract and exception gaps to closure.

ILLUSTRATIVE DELIVERABLES

- Updated third-party register
- Dependency and concentration map
- Risk and due diligence toolkit
- Clause library and remediation tracker
- Completed assessment reports for sample third-party arrangements

04 MONITORING, INCIDENT RESPONSE & EXIT TESTING

6 - 10 WEEKS

KEY ACTIVITIES

Ongoing oversight Define KPIs/KRIs, evidence needs, oversight cadence and reassessment triggers.

Incident response Establish notification requirements, response roles, escalation and action tracking.

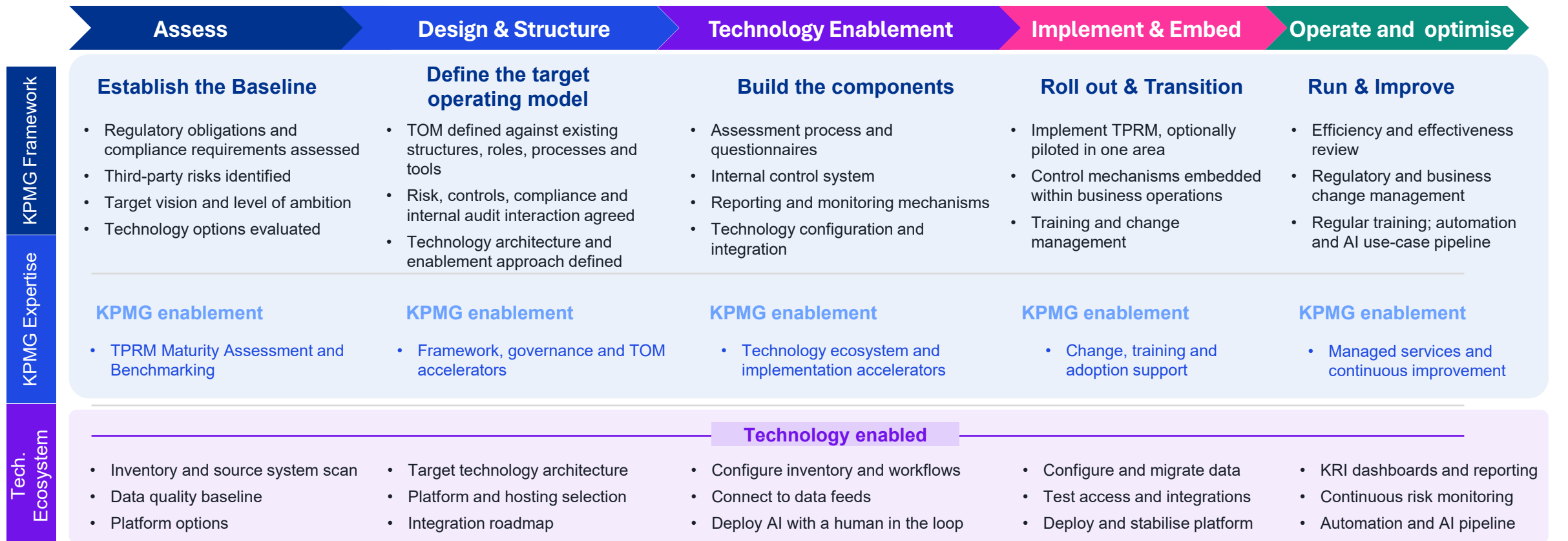
Resilience testing Run disruption and exit exercises; document residual risk and management actions.

ILLUSTRATIVE DELIVERABLES

- Oversight and reporting pack
- Assurance and reassessment plan
- Incident response and escalation playbook
- Continuity and exit test materials

Target Operating Model

KPMG framework + KPMG expertise + technology ecosystem = Digital TPRM



Digitally enabled TPRM





KPMG Services Pte. Ltd.

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

General disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public