



**Build risk awareness
and resilience with our
managed third-party risk
management services**

Build risk awareness and resilience with our managed third-party risk management services

In an increasingly connected business environment, organisations are reliant on third party vendors to perform operations effectively and efficiently. TPRM helps organisations manage third-party risk and ensure that such third parties align with regulatory standards, security protocols and contractual obligations thereby safeguarding sensitive data and preserving customer and stakeholder trust.


As the digital landscape evolves, and regulations become more stringent, TPRM not only protects against immediate threats but also positions organizations to maintain resilience in an ever changing business landscape.

From uncertainty to unparalleled

At KPMG in Singapore, our experienced managed services professionals harness critical insights and market-leading tech to empower you on your cyber security journey with managed TPRM services tailored to your business needs and risk appetite.




Top TPRM challenges faced by organisations




Increased regulatory expectations

- **More accountability**
Greater compliance fulfilment, wider scope on outsourcing, third parties and cloud service providers
- **Integration challenge**
Understanding how does this link to digital operational resilience and Enterprise Risk Management (ERM)
- **Senior Management accountabilities**
Clearly identifying the roles and responsibilities of senior managers in ensuring compliance




Inadequate risk management

- **Risk of fines and sanctions**
Penalties from regulators and reputational damage as a result of non-compliance or breaches
- **Decisions not risk-based**
Inability of processes to be agile and adaptive
- **No single view**
Lack of clear overview of third-party risk
- **Ineffective and incomplete monitoring**
Failure to identify risks outside of risk appetite




Complex cross-organisational processes

- **Poor user interface**
Unsatisfactory end-user and supplier experience
- **Time consuming checks**
Risk assessments taking too long with inefficient processes
- **Disjointed strategy**
Existing processes not unified and do not meet business and regulatory expectations
- **No real-time risk monitoring**
Lack of continuous monitoring and point-in-time approach
- **Lack of resources**
Limited resource availability and capability
- **No clear channels of communication**
Ineffective coordination between various teams



Complex operating models

- **Decentralised models**
bring inconsistency in risk-making decisions and overall oversight
- **No risk ownership**
Unclear risk ownership and framework outmoded
- **Multiple risk domains to manage**
Evolving range of risk domains – e.g., Environmental, Social & Governance (ESG)
- **Generic solution and strategy**
A one-size-fits-all approach without risk-based or intelligence-led insights
- **Increasing risks**
Lack of capability to manage high volume of risks













Tech and data

- **Lack of automation**
and reliance on overly manual processes
- **No clear overview**
Lack of single source of truth due to disparity in data systems
- **Inefficient use of data**
Lack of data-driven insight with industry utilities and data feeds not being leveraged
- **Lack of alignment and integration**
with procurement, risk, and business functions

Mismanagement of these key areas can result in a lack of:

-  Speed
-  Flexibility
-  Visibility
-  Consistency
-  Depth
-  Insight
-  Engagement
-  Transparency
-  Traceability

Address third party risk through our managed TPRM services

	Transform	Execute	
Design	<p> Development and upliftment of client's third-party risk management framework covering:</p> <ul style="list-style-type: none"> • Maturity assessment • Building TPRM Target Operating Model (TOM) • Regulatory gap assessment 	<p> Service risk profiling – Inherent risk assessment for potential third-party arrangements. Periodic review of third-party arrangements to assess any change in inherent risk profile</p>	<p> Continuous risk monitoring – Monitoring third party threat intelligence to take informed action with respect to a third party arrangement</p>
Automate	<p> End to end implementation services for Commercial Off The Shelf (COTS) products (ServiceNow, Archer, OneTrust and MetricStream) and KPMG TPRM platforms (KaVACH, DSIP)</p> <ul style="list-style-type: none"> • Automated dashboards and reports for management consumption 	<p> Third party risk and control assessments – Self assessment, remote assessment, onsite assessment. These assessments are further divided based on third party lifecycle stage (onboarding, ongoing monitoring or termination) and depth of assessment (design/ implementation/ operating effectiveness check, response/ evidence/ walkthroughs based assessments)</p>	<p> Issue management – Track / monitor and review sustainable remediation for third party issues</p>
		<p> Thematic assessments – Ad-hoc assessments conducted for identified set of third parties and focused on specific risk areas (e.g., impacts assessment for log4j attack)</p>	<p> Leverage utility platform assessments – Review third party risk assessment results provided by utility platforms</p>
			<p> Contract compliance review – Information security review of third-party contracts</p>
			<p> Leveraging external data feeds – Leverage external sources to determine third party risk posture for specific risk groups without the need for intensive manual assessments.</p>

Sustain, transform and evolve your TPRM capabilities with us

Sectors

Our diverse range of clientele include organisations across the business landscape.

- ▶ Financial Services - 20+
- ▶ Technology, Media and Telecom - 10+
- ▶ Energy & Natural Resources, Consumer and Retail, Industrial Manufacturing and Life Sciences - 10+

Accelerators

Various accelerators to support different phases of your TPRM strategy.

- ▶ RegoDB – Database of global outsourcing regulations
- ▶ Control inventories
- ▶ Risk Tiering and Scoring template
- ▶ Ongoing monitoring approach
- ▶ Risk exception and acceptance handling
- ▶ Performance, Control & Risk metrics

Technology

Technology enablers help achieve your TPRM objectives in a time efficient manner.

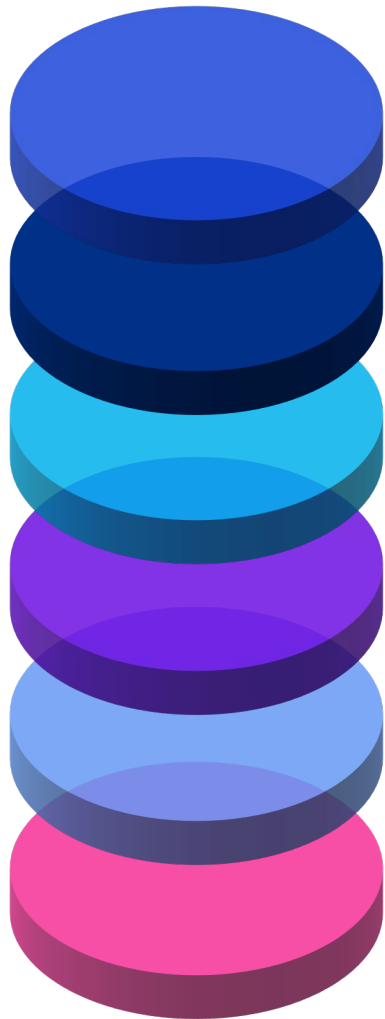
- ▶ KPMG Vendor Assessment and Compliance Hub (KaVACH) – SaaS based process automation platform
- ▶ Digital Risk Signals Insights Platform (DSIP) – Risk intel platform for outside in assessment of third parties
- ▶ TPRM Bot – Automated tool for centralised screening

Emerging areas

Expertise in emerging areas across the TPRM landscape

- ▶ Cloud Security Risk Management within TPRM
- ▶ Third-party Continuous Cyber Risk Monitoring
- ▶ Software Supply Chain Security Risk
- ▶ AI/ML powered platforms to automate third party risk assessments
- ▶ Fourth-Party Risk

Develop a third party risk management program aligned with your strategic objectives



01

Strong, compliant and consistent framework across the enterprise

02

Risk-based and robust screening, due diligence and monitoring

03

Reduced onboarding cycle times and program costs with optimised and streamlined processes

04

Quick ramp-up and ramp-down to support fluctuation in third party volumes

05

Pay per use model for third party risk assessments

06

Predictable, standardised and consistent service experience to suit business needs

Client feedback

“ KPMG has been a trusted partner in the transformation of our Third-Party Risk Management Program for more than two years. Their expertise guidance, insights, and support have been integral to the maturity and success of our program. ”

- Global US based software technology company

“ As always, it has been pleasure working with you. I have found the engagement to be incredibly organized and efficient, when delays did arise you demonstrated empathy and understanding. I and the wider team also appreciate the efforts that you put into reducing the controls through historical evidence mapping. ”

- Global Swiss investment bank and financial services company



“ We have been working with KPMG’s third-party risk management consultants for over two years and decided it was time to take our program to the next level. We needed industry expertise to help to uplift our manual end-to-end TPRM process. KPMG gave us the best TPRM expert and ServiceNow architects, Not only were they knowledgeable, but they were also extremely patient as we worked through some internal issues. Their partnership has proven valuable several times over. ”

- Global US-based retail company

Inspiring stakeholder trust with KPMG managed services

- ▶ Business transformation can pave the way for sustained advantage. But transformation is more than a destination — it is a continuous journey. How can you evolve your business while keeping up with everchanging goals?
- ▶ KPMG Managed Services can help you realise your dreams. We combine advanced tech with functional sector expertise to handle knowledge-intensive processes across your enterprise — both on a subscription and a as-a-service basis. In addition to maximising your costs, we can help deliver other outcomes like resilience, customer retention, stakeholder trust and an added competitive edge. Let us help you operationalise your growth ambitions as you can accelerate your transformation journey amid disruptions and risks.

Connect with us

- ▶ Shape a future-ready cyber security strategy to scale new frontiers of tomorrow. Connect with us today to transform your organisation.



Contact us

Reach out to learn how we can support you on your cyber security compliance journey.

Wong Loke Yeow

Partner

Cyber,
Advisory

KPMG in Singapore

T: +65 6213 3053

E: lokeyeowwong@kpmg.com.sg

Wendy Lim

Partner

Cyber,
Advisory

KPMG in Singapore

T: +65 6411 8263

E: wlim@kpmg.com.sg

kpmg.com.sg



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 endeavor 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 trademarks used under license by the independent member firms of the KPMG global organization.

© 2023 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.

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