

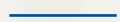


Third party risk management

Managing supplier risk



KPMG International



home.kpmg

Organizations are increasingly reliant on third party suppliers to deliver business-critical products and services to their clients and customers. They are also finding that failures by third parties can significantly impact their ability to operate effectively and tarnish their societal trust and reputation. Both can have significant downstream operational delivery, quality and cost implications, and potentially upstream growth impacts. While value and risk have been openly discussed as part of the procurement agenda, COVID-19 and the global pandemic have highlighted that more needs to be done given the connected supply chains in which we operate within globally. Organizations are beginning to address the concerns around these issues, but it is evident that they should develop a clear strategy for the selection, approval and management of third parties. As there are a myriad of stakeholders involved, from the business as well as the procurement and risk functions, developing and implementing this strategy can continue to be highly challenging.

Supplier risk, which has been a key emergent focus for organizations through the pandemic, is only one element of the end-to-end supplier lifecycle management, the other two being contract management and supplier relationship management. Candidly, without all three lenses, you or your organization may not have a holistic view across your entire supply base, be they material, moderate or those found in the tail. The aggregation of your entire supplier ecosystem creates the goods or services you provide to your customer.



Throughout this [document/film/release/website], “we,” “KPMG,” “us” and “our” refers to the global organization or to one or more of the member firms of KPMG International Limited (“KPMG International”), each of which is a separate legal entity.

Through KPMG member firms' extensive work with originations across the world, a number of key challenges have been identified that exist across third party and supplier risk management. These range from supplier concentration all the way through to ongoing management and governance and are explored below.

Supplier concentration risk:

Across sectors, there is an increase in supplier concentration, which raises dependency and competition concerns. With the move towards digital transformation and cloud implementation, this connected and concentration risk has accelerated and will continue to do so.



Third party governance:

Increased regulatory focus, and the financial and reputational impacts of getting it wrong, have required organizations to have better third party risk management processes in place, given that documentation and accountabilities invariably continue to be insufficient and unclear.



Supplier risk assessments:

Supplier risk assessments are often performed in silos and on a reactionary basis, with limited depth, lack of subject matter expert input, and can often result in the insights from the risk assessments not being used to inform sourcing strategies and future decision-making.



Third party supplier management:

Third party supplier management is talked about, but usually lacks sufficient capacity and capability to be an effective process due to a lack of engagement with subject matter experts to support effective supplier oversight.













COVID-19 impacts:

COVID-19 has not only amplified the impact of third party and supply chain disruption but has also challenged the ability of global organizations to plan and execute key third party risk management components, such as onsite assessments. Some specific examples from a COVID-19 perspective include:

- business continuity and resiliency risk
- IT and cyber risk
- key person risk
- inadequate service provider monitoring, and
- fourth-party risks.



So, let's explore this further by looking at each critical element that creates the overall supplier risk picture. What are the real risks to the organization? Well, in short there are several categories or domains, which are typically either not addressed or else spread across the organization from an accountability perspective. Some may reside within the procurement function, while others may sit within risk management teams, the wider business or at times have no home at all and slip between the cracks. Below are several domains that need to be considered within your organization as part of your end-to-end supplier lifecycle review.

Regulatory/ compliance risk		<ul style="list-style-type: none"> — Regulatory requirements — Theft/crime/dispute risk — Fraud, anti-bribery and corruptions/sanctions 	<ul style="list-style-type: none"> — Compliance with internal procedures and standards
Strategic risk		<ul style="list-style-type: none"> — Service delivery risk — Expansion/roll-out risk — Mergers and acquisitions 	<ul style="list-style-type: none"> — Alignment to outsourcing strategy — Intellectual property risk
Subcontractor risk		<ul style="list-style-type: none"> — Applicable across all risk areas 	
Concentration risk		<ul style="list-style-type: none"> — Supplier concentration across critical services — Industry concentration (including subcontractor) 	<ul style="list-style-type: none"> — Concentration of critical skills (i.e. tech support) — Geographic concentration — Reverse concentration
Technology/ cyber risk		<ul style="list-style-type: none"> — Information security — Cyber security — Data privacy/data protection 	
Country risk		<ul style="list-style-type: none"> — Geopolitical risk — Climate sustainability 	
Financial viability		<ul style="list-style-type: none"> — Financial risk from lending to a third party — Liquidity risk 	
Operational/supply chain risk		<ul style="list-style-type: none"> — Business continuity — Disaster recovery — Physical security — Operational resilience 	<ul style="list-style-type: none"> — Performance management (including SLAs) — Model risk — Human resources risks (conduct risk, etc.)
Reputational risk		<ul style="list-style-type: none"> — Negative news — Lawsuits (past and pending) — Brand of the third party 	<ul style="list-style-type: none"> — Key principals/owners of the third party — Workplace safety
Legal risk		<ul style="list-style-type: none"> — Jurisdiction of law — Terms and conditions of the contract 	

You may be familiar with many of the above domains and some may be new, but the question some may be asking is how exactly do they all fit in? Sadly, all too often we see the risk assessments or understanding of the risk profile being performed too late in the strategic sourcing process. Quite often, this activity is being conducted post-award, which can make it difficult to get the supplier to cooperate. Equally, when conducted post-award, what happens if you suddenly find out that your newly appointed vendor is in fact unsuitable, having several red flags that that will impact your operations, reputation or trust agenda? Of course, this assumes you ask the question. These assessments should be integrated early in the category planning and sourcing process, coupled with continuous monitoring (to be discussed later) to enhance effectiveness.

If we keep extending the discussion further, let's assume we've conducted the risk assessment. Now we need to do the all-important activity of making sure the supplier is complying with their obligations to mitigate the risks that have been identified — for example, given the global COVID-19 pandemic, many organizations had to enact their business continuity plans. Let's now consider that even though this was agreed to as part of the sourcing and negotiation phase, but was never established or monitored, where does that leave your organization? In addition, if it has been established, but never tested, is it adequate?

The key point here is to make sure the assessment and resulting outcomes are effective. If you undertake this as a box-ticking exercise, you can expect to be either be wrong or lucky, and gambling on risk with so much to lose from an operational, reputation and trust perspective may be a poorly considered approach.

What's next?

— **Third Party Risk Management (TPRM) is a strategic priority:**

Many businesses are dependent on third parties to deliver critical products and services to their clients and customers. At the same time, growing regulatory pressure — particularly in relation to privacy breaches and the loss of customer data, or to operational resilience — is putting third party relationships under additional scrutiny.

— **Organizations are inconsistent in their approach:** Businesses work with a wide variety of third parties worldwide, and each third party manages a subset of risks on the business's behalf. For good reason, businesses should understand each third party's ability to manage risks in line with expectations before deciding whether to engage that third party. Many organizations are not prepared for the complexity that comes with assessing multiple risks in a cohesive manner across business lines and regions. Holistic risk identification and assessment upfront in the onboarding process, as well as during the lifecycle of the contract, is crucial for organizations to have line of sight into the risk profile of their entire third party portfolio. Three-quarters (74 percent) of respondents admit that their organizations urgently need to make TPRM more consistent across the enterprise.

These assessments should be integrated early in the category planning and sourcing process, coupled with continuous monitoring (to be discussed later) to enhance effectiveness.

— **A risk-based approach is the number one ‘get right’ for TPRM programs:** Managing third party risk in today’s business environment is far from straightforward, and the scope of the program, along with the amount of coordination involved, causes some to feel overwhelmed. The situation is not helped by limitations in organizational resources and budget. Many businesses do not have the required capabilities in-house to manage all the third party risks they face. In our view, organizations can achieve both efficiency and effectiveness by taking a risk-based approach to assessing and monitoring third party products and services that present the highest risk to the organization.

— **Data and technology are improving TPRM teams’ performance:** Across industries and regions, respondents indicated that the sheer volume of third-party assessment activities has increased in recent years. At first, TPRM programs simply increased their headcount to complete a greater number of risk assessments. Today, organizations have the potential to innovate their approach in three areas:

- greater automation of the TPRM process internal workflow
- leveraging shared utility providers for due diligence questionnaires and responses, and
- moving away from point-in-time risk assessments to continuous controls monitoring.

At present (on a global level), only about a quarter of businesses are using technologies to improve either the workflow automation or monitoring of third parties.

— **It’s time to sustainably scale the program:**

Organizations are integrating, streamlining and maturing their TPRM/Supply Risk programs to better understand where they are at risk of goods and service disruptions resulting from third party non-performance. Further, organizations are expanding risk identification,

assessment, and management to material and lower level suppliers. Many organizations have room for improvement across their entire operating model, inclusive of service delivery model, process, people, governance, data and technology. With that in mind, our analysis has helped us refine the steps that organizations should take to upgrade their TPRM programs. Many organizations are approaching the journey differently, however given the sensitivities, a “crawl,” “walk,” “run” approach is what most are favoring. The key point to raise here is that putting your head in the sand and thinking the problem will resolve itself can be flawed — it doesn’t matter where you start, but you should start.

So, the big question is where does that leave us? Our global research and local views confirm that organizations across all sectors and geographies are rightfully considering TPRM, inclusive of supplier management, to be a strategic priority. We see businesses being led by procurement and risk taking a proactive approach to TPRM/supplier risk, exploring how they can refine and expand their existing processes, and then streamline through technology enablement and innovation as part of their end-to-end supplier lifecycle programs.

That said, KPMG’s view also makes clear that, for many organizations, specifically those early on in the journey, including those that have not been regulated, TPRM and supplier risk remain a work in progress. As organizations adjust to global events and economic uncertainty, they may also find that their historical third party assessment information and control environment analysis needs to be updated to account for new risks and challenges. As a matter of urgency, organizations should improve the business resilience across critical customer/client services by accurately understanding the role third parties play in delivering these services and adjusting policies, controls and mitigation plans accordingly.

Unlock the potential in procurement

The majority of organizations and functions are aware that the future can require different and flexible operating models to keep pace with the changing landscape. Technology disruptors should naturally drive the automation of low-value tasks, moving the workforce to higher value activities such as category innovation. However, even these higher-value activities will likely require a high degree of cross-skilling to allow the workforce to flex based on current priorities. In other words, having category managers managing one category in an endless loop is expected to become rare.



Read more about what the future of procurement looks like at home.kpmg/futureofprocurement.

Introducing Powered Procurement

Choose to extend the role of procurement

Faced with empowered customers, emerging technologies, cyber threats, severe periodic disruption and a battle for skills, CPOs face important questions:

- How can procurement help unlock transformation?
- Can I be a better partner to my business
- How do I move away from a mix of models and processes?
- Can I drive value with richer spend analytics?
- What is the best way to make change happen smoothly?

Introducing Powered Procurement

Powered Enterprise | Procurement is an outcome-driven business transformation solution that combines deep procurement knowledge, proven delivery capability and leading technologies to drive sustainable change, rising performance and lasting value.

The Powered procurement solution provides an out of the box operating model for Source to Pay that helps clients transform their S2P process – accelerating delivery and enabling clients to maximize the value of their technology investment.

KPMG professionals understand the human factors involved in business transformation. We can help inspire and empower your people to embrace change, as you align your transformation with industry disruption.

A pre-configured cloud solution, embedded with years of KPMG leading practice and enhanced with automation, Powered Procurement can help you to quickly transform and derive value from your move to the cloud.

To find out more about Powered Enterprise | Procurement and the impact it can have on your business visit: home.kpmg/poweredprocurement.

Contacts



Peter Liddell
Global Head, Operations
Center of Excellence
T: +61 3 9288 5693
E: pliddell@kpmg.com.au



Chris Clements
Partner
KPMG Australia
T: +61 410 419 728
E: cclements1@kpmg.com.au

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/socialmedia



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.

©2021 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document/film/release/website, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve | Publication name: Third party risk management | Publication number: 137455-G | Publication date: July 2021