Moody's Analytics

TRANSFORMING RISK & COMPLIANCE

Creating a world where risk is understood, so decisions can be made with confidence

The rising tide of third-party risk management

Surfacing risks to safeguard reputations

MOODYS.COM/KYC

SECTION ONE

About the research

CONTEXT & OBJECTIVES

In an increasingly globalized and interconnected world, supply chains have grown in complexity. It's an accelerating trend that poses significant risks to organizations globally. In today's volatile operating environment, supplier performance is harder to gauge, inflation harder to contain, and disruption across the world harder to predict. Challenges can emerge anywhere, from geopolitics to natural disasters, pandemics and the digital sphere. Beyond pure business continuity, corporates face growing reputational risks as the focus on environmental, social and governance (ESG) issues moves up corporate agendas.

Firms are having to be much more cautious, moving from a 'Just in Time' approach to supply chains, where being streamlined was king, to a 'Just in Case' model that anticipates disruption, builds slack into inventories, and accepts a level of redundancy as part of doing business.

For corporates, having a better understanding of the risks in your supply chain is of increasing importance, with a growing demand for best-in-class Third-Party Risk Management (TPRM) and Supplier Due Diligence tools.

We conducted primary research with a view to exploring attitudes towards TPRM within a range of target audiences and regions, exploring the following questions:

- What is people's understanding and awareness of TPRM?
- How do they approach TPRM and Supplier Due Diligence today?
- What are the challenges companies face when onboarding and managing suppliers?
- What does best practice look like and what steps are taken to mitigate risk?
- What are corporate customers' attitudes towards TPRM, openness towards solutions and perceptions of the benefits of improved monitoring?

METHOD

We worked with an independent research consultancy, Context Consulting, to design and conduct the study. The research is based on in-depth interviews with senior third-party risk management experts within 41 multinational organizations.

SAMPLE

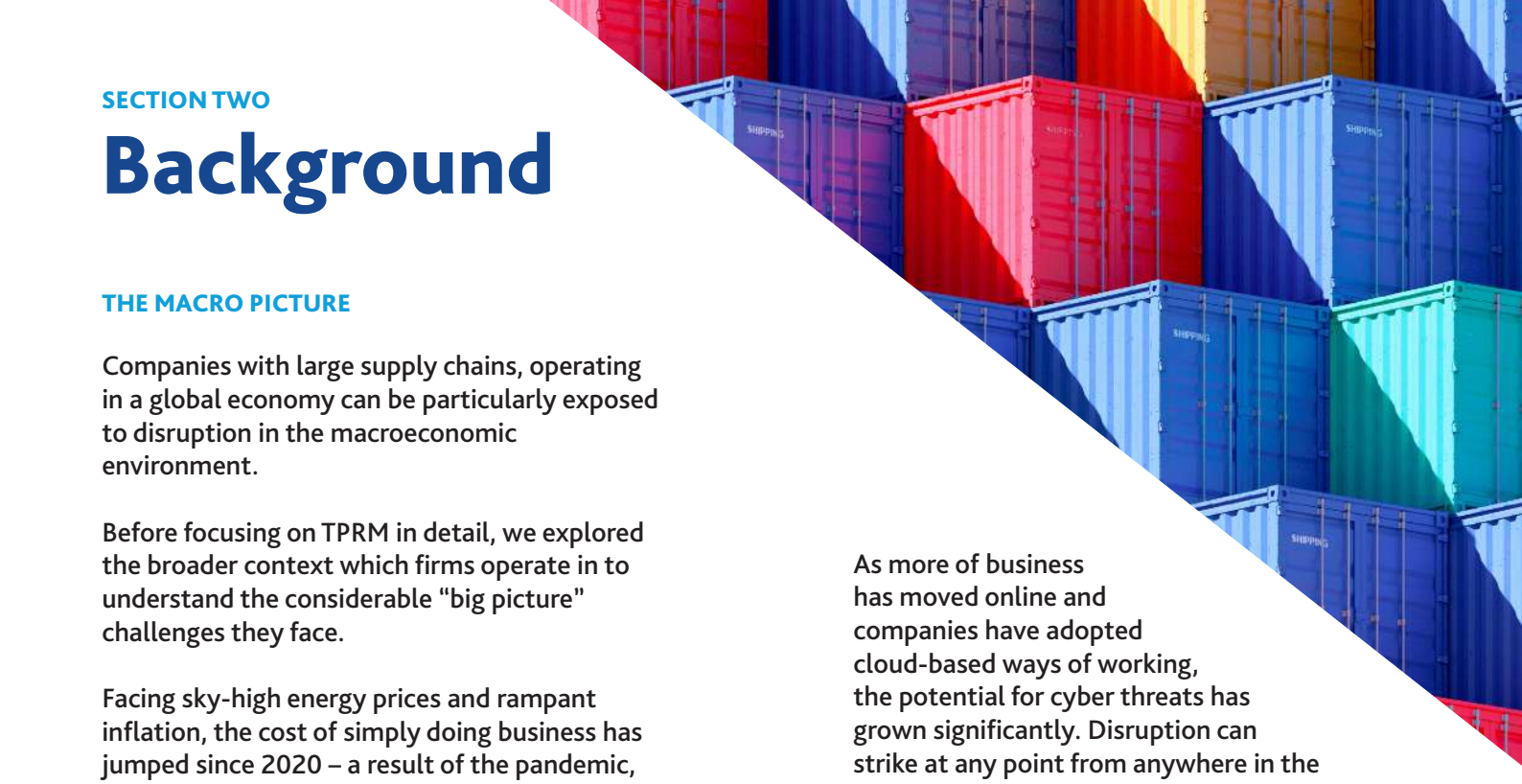
The study was global in its scope, with interviews spanning Europe, North America, and APAC. We interviewed people in a wide range of roles that deal with suppliers day-to-day, across a breadth of sectors:

ROLE	TOTAL
Compliance	16
Risk management	12
Procurement	10
Supply chain	3
TOTAL	41

SECTORS	TOTAL
Industrial	15
Pharma & Health	8
Finance & Insurance	7
Tech & Telco	6
Energy & Utilities	5
TOTAL	41

SECTION TWO

Background



THE MACRO PICTURE

Companies with large supply chains, operating in a global economy can be particularly exposed to disruption in the macroeconomic environment.

Before focusing on TPRM in detail, we explored the broader context which firms operate in to understand the considerable "big picture" challenges they face.

Facing sky-high energy prices and rampant inflation, the cost of simply doing business has jumped since 2020 – a result of the pandemic, conflict, and supply chain dislocation among other factors. Coupled with sluggish demand, slow growth, and tightening liquidity, respondents noted a growing list of economic headwinds at every level of business.

Russia's invasion of Ukraine, rising US-China tensions and uncertainty in Taiwan – political instability around the world threatens business continuity, access to resources, the normal functioning of supply chains, and companies' traditional routes to markets.

While the worst of the pandemic is over, its impacts continue to be felt. China only recently relaxed lockdown measures, major production backlogs persist, demand remains unpredictable, and businesses face ongoing supply chain instability.

With the growing focus on sustainability, carbon reduction, human rights, and corporate responsibility, businesses in every sector are adapting how they work and their core focus.

As digital innovation accelerates, businesses must continually transform to keep pace with progress and meet changing customer demands. Finding new routes to market, innovating to grow their top line, cutting costs to become leaner, and adopting new technologies like AI – digital transformation is now a priority.

As more of business has moved online and companies have adopted cloud-based ways of working, the potential for cyber threats has grown significantly. Disruption can strike at any point from anywhere in the world. Companies must build resilience and be able to recover fast when problems arise.

SUPPLIER RISK FOCUS

In addition to macro-level challenges, compliance teams face a number of pressures in their day-to-day activities.

Governments and lawmakers are stepping up regulations in relation to ESG concerns. From fashion and household goods to electronics and food production, companies in every sector need to improve traceability, transparency, and sustainability through their supply chains while addressing areas like human rights violations. Meeting these new standards presents complex legal, compliance, monitoring, and reporting demands.

While globalized supply chains have huge benefits for specialization and improved efficiency, they also create complexity for businesses. From logistical challenges such as the one highlighted by the Suez Canal incident or bottlenecks at strategic ports, to traceability of goods and performing supplier due diligence with counterparties on the other side of the world – tiered supply chains present a significant organizational challenge and risk to businesses.

With increased regulations and the growing complexity of supply chains, simply bringing on a new supplier can be an arduous undertaking, requiring detailed factory inspections and the implementation of new systems and monitoring procedures.

Overly manual and time-consuming for teams, the systems created to cope with supplier management in the past are quickly becoming unfit for purpose. The data needed for third-party due diligence and supplier risk management is often inadequate.

With new reporting demands and the need to measure areas like source of raw materials and carbon emissions across the supply chain, companies are needing to upgrade their technology to operate with confidence and efficiency in this new era.

NEWS TRAVELS FAST. BAD NEWS, FASTER.

Today, supply chain risks pervade businesses in every industry. From a cosmetics company using palm oil linked to deforestation, to a fashion retailer sourcing clothes made by forced labor, or an electronics company being connected to child labor in precious metals mining, as supply chains grow larger and more tiered, it becomes harder to identify and mitigate risks. Companies' reputations are on the line. And in this digital, interconnected world, bad news travels lightning-fast, making companies vulnerable.

SECTION THREE

Third-party risk management today

Facing a challenging business environment and a growing list of macro financial, geopolitical, technological, and reputational threats, it's unsurprising that businesses and compliance teams are eager to get to grips with risk management and due diligence. This is at a time when they also face the converging challenges of being asked to onboard more suppliers while struggling with outdated systems and data deficiencies.

The organizations we interviewed have highly complex supply chains, often dealing with tens of thousands of suppliers across more than 50 countries and with so many connections at different levels of business, third-party risk management is often the responsibility of many different people and can fall between gaps.

AGREEING ON TERMINOLOGY

One of the key barriers to understanding the risk, standardizing approaches, and coordinating activity is the sheer number of terms used to describe the same or similar processes.

From the well-established third-party risk management or supplier risk management to terms like vendor risk assessment, chain of trust, supplier due diligence and integrity checking, and many more, there are countless terms used to describe the discipline.

ONE SIZE DOESN'T FIT ALL

Naming is just the beginning of the issue of unification, with our interviews identifying fragmentation and variations in TPRM approach between almost everyone we spoke to. While every company had many people involved in TPRM, the number was not always defined, and we encountered everything from a handful of staff to hundreds.

With TPRM taking up just a part of many people's roles, it is often unclear where ultimate responsibility lies. We saw both highly centralized and totally decentralized operating models.

Even the term "decentralized" can mean different things to different companies. For example, it may refer to different levels of global, regional, or local focus. In some cases, teams are divided between onboarding and ongoing monitoring, or between strategic suppliers and regular suppliers who are more easily replaced or pose less of a critical risk. Outsourcing third-party risk management is also prevalent but approached by organizations in different ways.

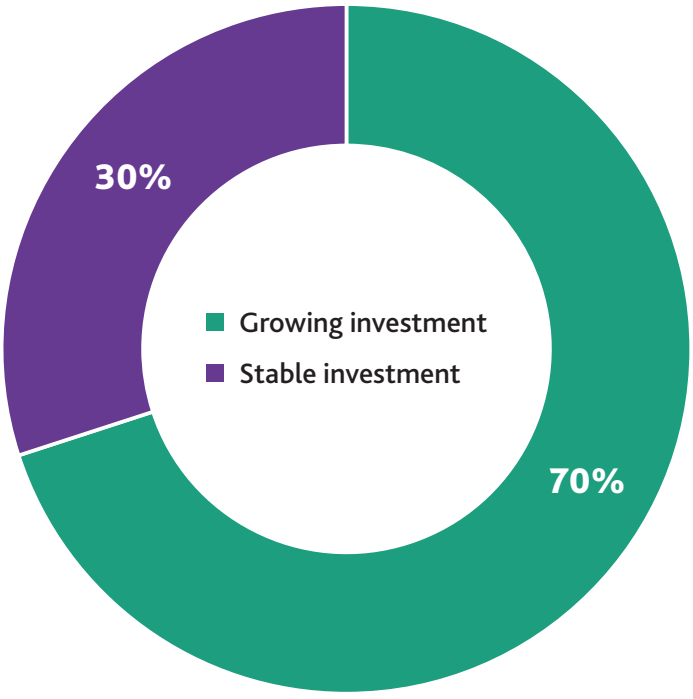
With some companies dealing with thousands of suppliers, responsibilities are often split across different teams – from procurement to compliance and risk management to supply chain functions. There's overlap in managing supplier risk, and with inadequate data and time-consuming manual effort, it can often fall through the cracks between teams. Depending on organizational structure, some entities see reporting into multiple C-suite executives, with the potential for duplication of effort or disagreement on priorities.

The upshot? There's no "one size fits all' approach. Complex entities, with complex supply chains require a nuanced approach. But what's clear is that firms without a clear structure in place – taking a fragmented approach to supplier risk across regions and business units – will find it difficult to know whether they have invested enough in third-party risk management. Finding the right balance requires careful strategic coordination.

STEPPING UP TPRM

Faced with continual disruption, growing global uncertainty and a recognition of current shortcomings, 7 in 10 firms report an increase in terms of focus on TPRM. They are building teams to handle increased workloads and investing in the tools and systems to meet growing supply chain complexity and evolving regulatory demands.

IS YOUR THIRD-PARTY RISK MANAGEMENT ACTIVITY GROWING OR DECLINING IN TERMS OF HEADCOUNT & BUDGETS?



It's definitely going up. You can no longer look at your direct suppliers, you've got to look at your supply chain and there's more topics coming into due diligence.

The budget is growing between 5 and 10% per year.

In the last three years we have definitely seen a budget increase and more staff, while the number of vendors has also gone up. There is a recognition that there is more work, and more people are required.

THE PUSH FOR STANDARDIZATION

Across the board, third-party risk management is growing in importance, with many companies around the world in the process of developing departments to improve it. It is increasingly being viewed as an important investment companies must make to protect themselves from financial, regulatory, and reputational risk.

This prioritization of TPRM is aligned with a push for centralization of processes and the standardization of procurement approaches, reporting, and risk management across companies.

With challenging new legislation emerging, like the SAPIN 2 in France and the German Supply Chain Due Diligence Act, UFLPA in the USA and the modern slavery act in Australia, pressures on companies to address third party risks are growing. These pressures are being met with increased investment to build TPRM departments, meet pressing risks, and transforming their organizations for the future.

> **Supplier risk management is growing and becoming increasingly structured, especially considering regulations that stem from three major and active countries: US (FCPA), France (Sapin II) and the UK (UKBA)**

MISSION CRITICAL

Each company is different, facing unique circumstances and challenges. The supply chain risks felt by one, won't necessarily translate to another. The extent to which TPRM is critical to a particular business is impacted by (at least) four key variables:

1 SENSITIVITY OF ACTIVITY

Companies operating in sensitive or consumer-facing fields, will have a business-critical need for effective TPRM.

2 NUMBER OF SUPPLIERS

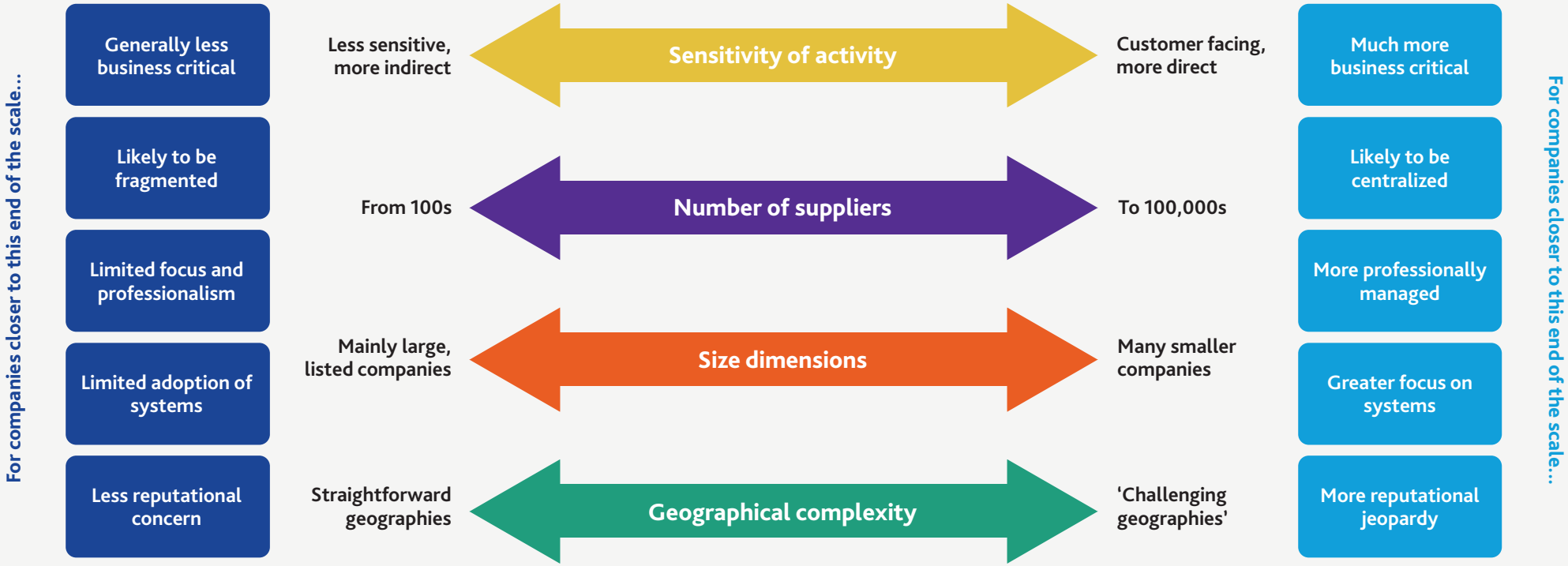
Where companies have fewer suppliers, TPRM is likely to be fragmented and handled locally, with limited professionalism. As supplier numbers grow, the process needs to become more professionally managed.

3 SIZE DIMENSIONS

Counterintuitively perhaps, companies that have a greater proportion of smaller, unlisted or privately-owned suppliers face greater risks, as there tends to be less reliable data about such companies.

4 GEOGRAPHIC COMPLEXITY

Reputation concern grows for organizations as they move into more complex and challenging geographies, with a limited availability of reliable data on third parties.



Moody's Analytics

SECTION FOUR

TPRM approaches and challenges

Given the unique set of circumstances and challenges each company faces, it's important that firms bring nuance to risk management.

Considering the following supplier risk use cases and asking the right questions about them can help firms develop an effective approach, tailored to their business:

COMPANY PROFILE

Can we verify and enhance the information given by the supplier, including company ownership details?

FINANCIAL & OPERATING PERFORMANCE

What does a supplier's financial health predict about their near-term performance?

RESILIENCE

Which of our critical suppliers are at risk of deteriorating performance for quality, cost, and delivery times?

REGULATORY & COMPLIANCE

What is a supplier's risk-level for key compliance areas?

REPUTATIONAL

What significant risks are created for my company by supplier scandals or misdeeds?

ESG & SUSTAINABILITY

How do my important suppliers score on ESG?

CYBERSECURITY

What is the cybersecurity risk of my key suppliers?

BUILDING THE CASE

By asking our sample corporates to evaluate these different use cases, we learned valuable lessons.

There is no one-size approach. Company and supplier context must always be considered to evaluate supplier risk in each case. And sector is a key factor in determining which use case is is most appropriate. For example, cyber risks are more prevalent for telcos, and ESG risks feature highly across FMCG brands.

There is fragmentation of TPRM subcategories across firms, making it hard to collaborate and focus efforts to tackle issues. As a result, companies are increasingly trying to centralize operations.

At the same time, categories overlap, and different business units need to cover multiple common areas, making it hard to categorize precisely or assign responsibility. A more holistic approach to TPRM with centralized oversight is needed.

Risk use cases are at different stages of maturity. Some have been around for years, are well understood, and easy to manage. Others, like ESG and cyber risk, are still developing and thinking around them needs to mature. In complex systems, building compliance, understanding, and efficiency takes time for companies to adapt.

As a result, compliance teams are finding gaps in their coverage as they are asked to look at more use cases. They are increasingly looking for end-to-end solutions to cover their supplier risk end-to-end.

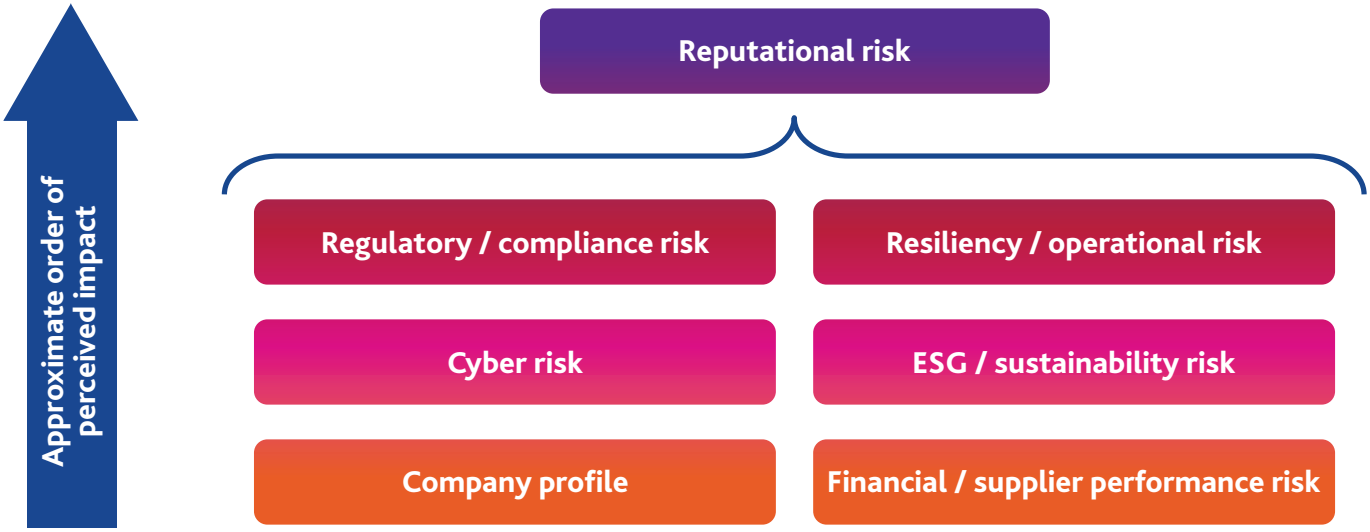
NOT ALL SUPPLIERS ARE CREATED EQUAL

As we've seen, there's no one size fits all answer to third-party risk management. Many dynamic factors feed into the risk rating of any given counterparty, and this changes over time. From the size of spend and frequency of transactions with a supplier, to the length of a contract, their previous records on sanctions, geographic location, or the access they require to systems and customer data – these are just some of the 12 variables we identified that can drive supplier risk ratings.

How suppliers perform against these criteria will drive the risk category they are assigned, from low to medium, high or critical risk. Firms need to evaluate risk on a case-by-case basis. By reviewing each suppliers' performance against these use cases they can determine the level of risk a supplier presents and evaluate whether they have the tools and capabilities in place to manage it effectively.

REPUTATION AT STAKE

While each use case is highly relevant for companies to assess risk overall, they can vary in impact from company to company and sector to sector. Reviewing how a supplier performs against the combination of use cases is important, with different use cases creating different impacts.



Understanding supplier profiles and financial stability is relatively easy to achieve and broadly relevant to all suppliers. Risks can be understood and minimized here more easily.

Cyber and ESG risks are quickly growing in importance and can create bigger problems for companies where they are highly exposed, impacting some organizations more than others. However, these risks tend to be more narrowly relevant across the supplier base.

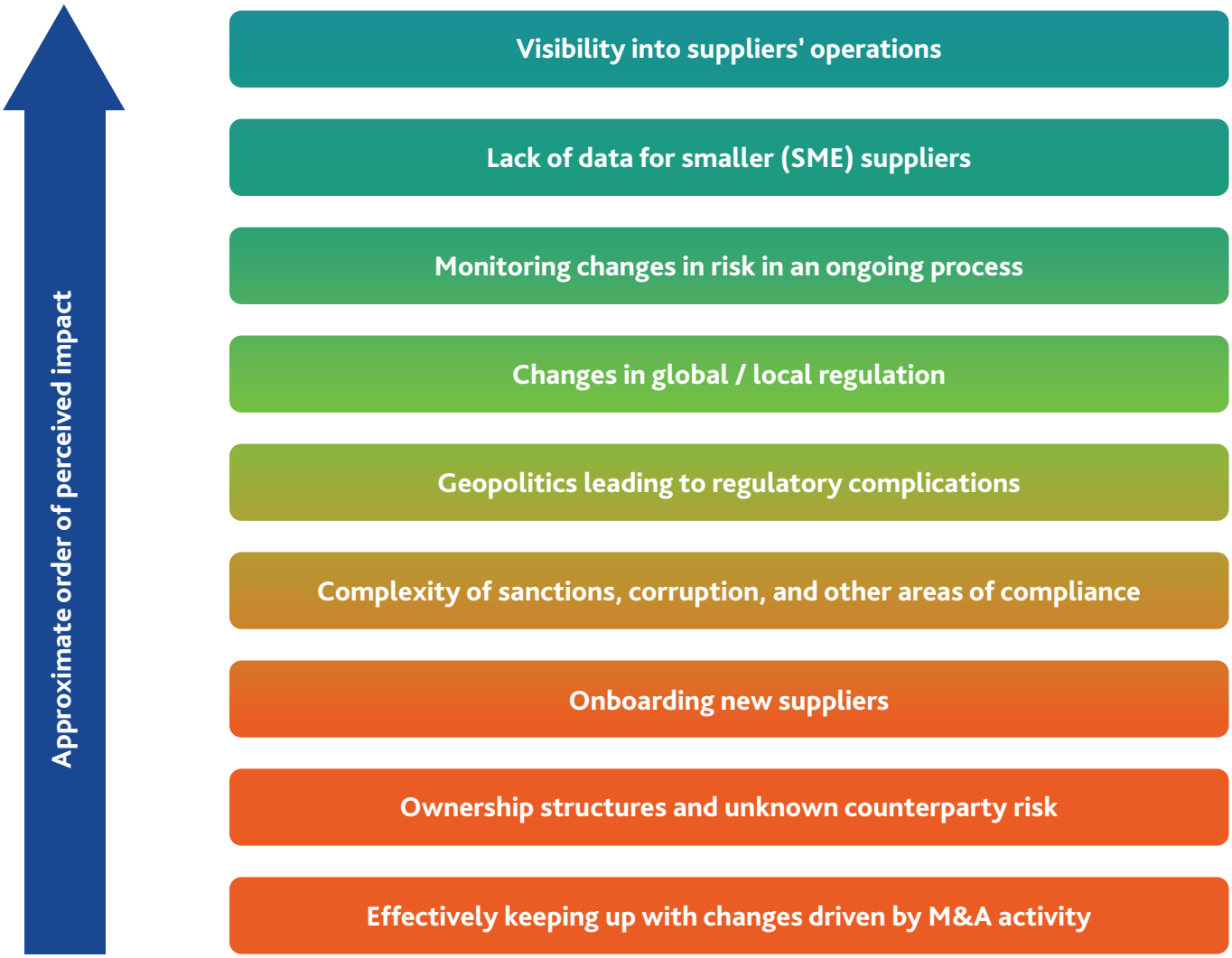
Regulatory and operational risks are massively important across the board, with far-reaching implications for businesses when things go wrong.

Ultimately, everything ladders up to reputational risk. In a world where information is at everyone's fingertips, issues at any level can hurt a brand. When any use case goes wrong, it has the potential to damage reputations and limit people's willingness to deal with a company or buy from it in future.

> **Reputation takes years to build and a second to destroy.**

CHALLENGES MONITORING SUPPLIER RISK

Across complex and global supply chains, companies will naturally run into a number of different issues when trying to manage third-party risk. Visibility into a supplier's operations is the single biggest TPRM challenge, but lack of information on small and medium sized enterprises (SMEs), geopolitics, and sanctions are all up there as big issues.



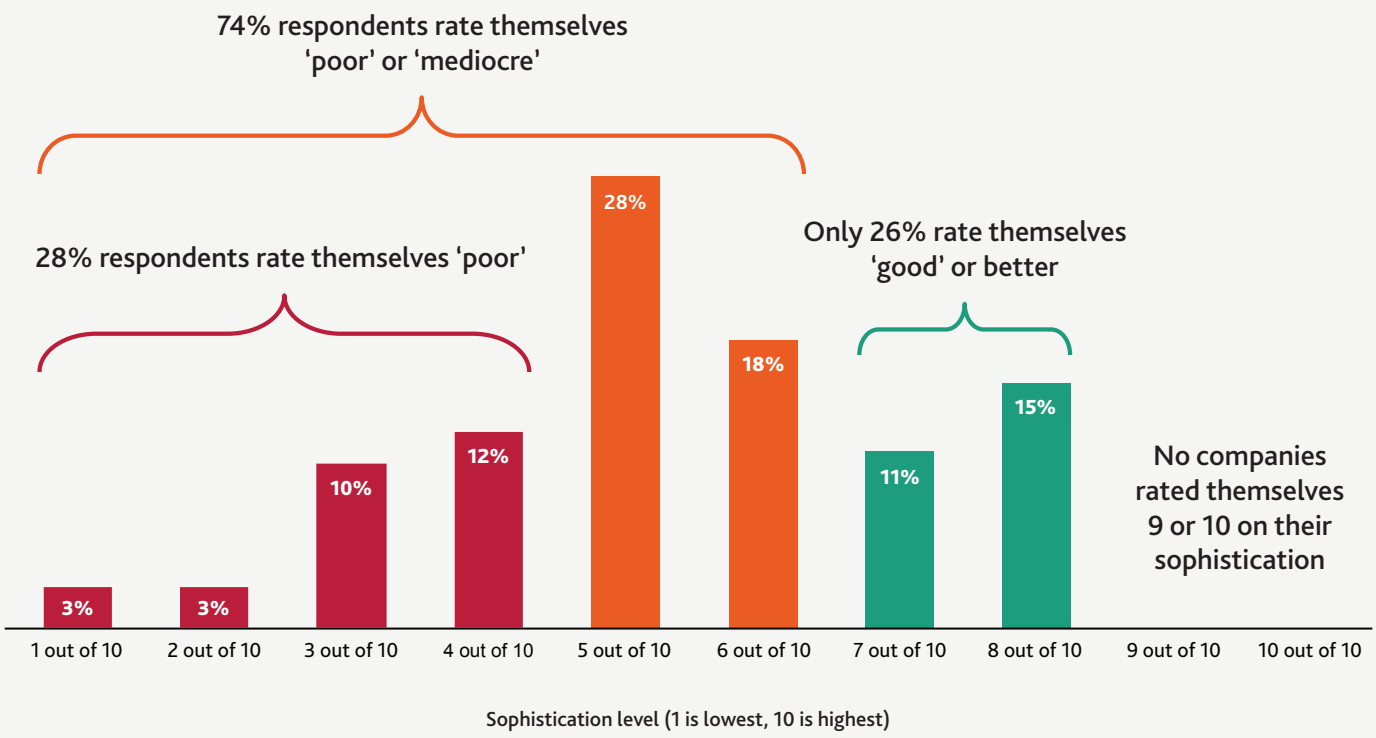
The real challenge comes when factors are combined. If a change in sanctions or global regulations is met with geopolitical instability, a supplier who was low risk can quickly become a headache for compliance teams. Understanding the interplay of factors and viewing them as dynamic, fast-changing challenges is key to successful TPRM.

TPRM SOPHISTICATION LEVELS VARY WIDELY

With supplier risk being more established in some companies and industries, it's natural that TPRM functions are more sophisticated in some areas than others. We asked respondents to evaluate their company's sophistication level in terms of third-party risk management – on a scale from 1 to 10, with 10 being fully digital / automated.

There is clearly room to improve sophistication – with 3 in 4 rating themselves poor or mediocre.

HOW DO YOU RATE YOUR FIRM'S SOPHISTICATION LEVEL IN SUPPLIER / THIRD-PARTY RISK MANAGEMENT?

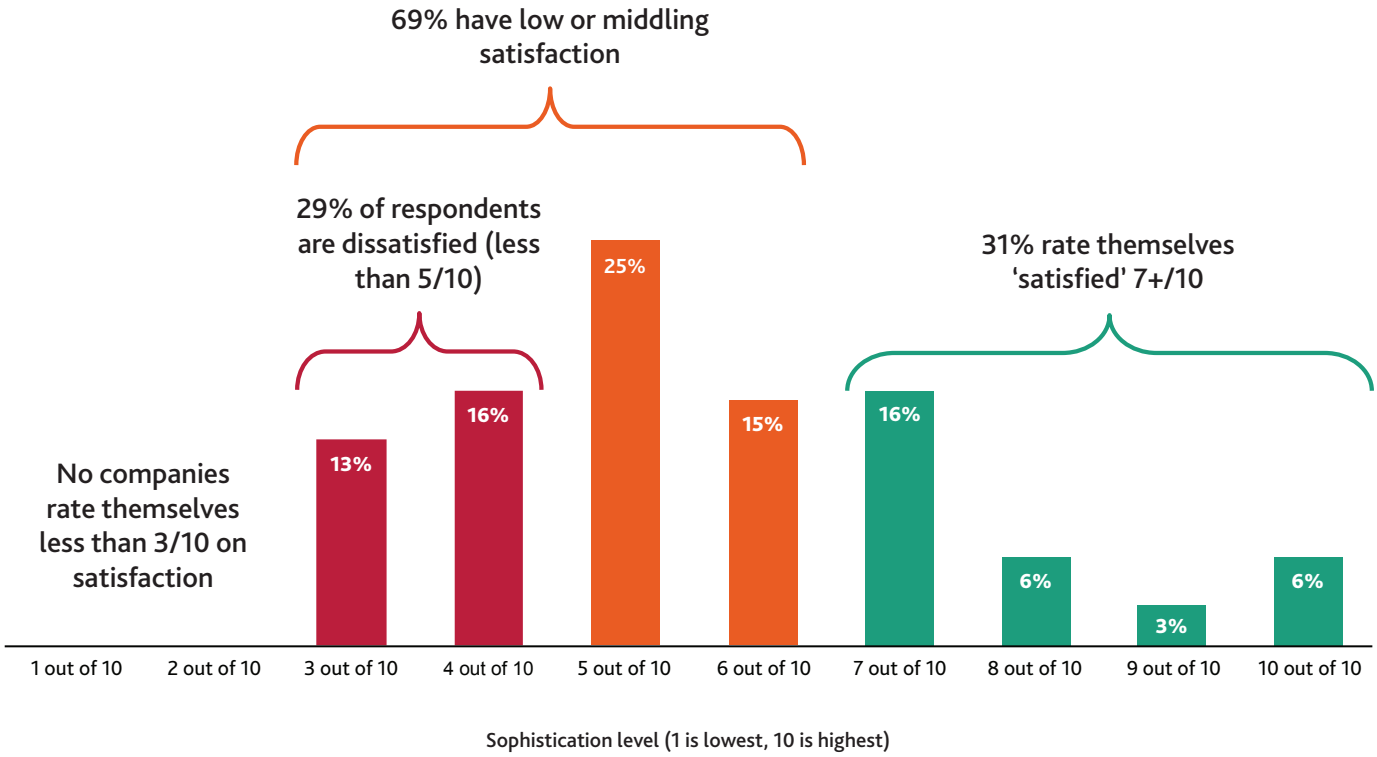


FIRMS ALSO HAVE DIFFERENT LEVELS OF SATISFACTION WITH VISIBILITY

We next asked respondents to evaluate on a 10-point scale how satisfied they are with their level of visibility into different risks across their supplier base, such as Anti-Bribery & Corruption and ESG.

At present, 7 in 10 firms have only low or middling satisfaction with the level of visibility they have into different risks across their supplier base.

HOW SATISFIED ARE YOU WITH THE LEVEL OF VISIBILITY YOU HAVE TODAY INTO DIFFERENT RISKS ACROSS YOUR SUPPLIER BASE?



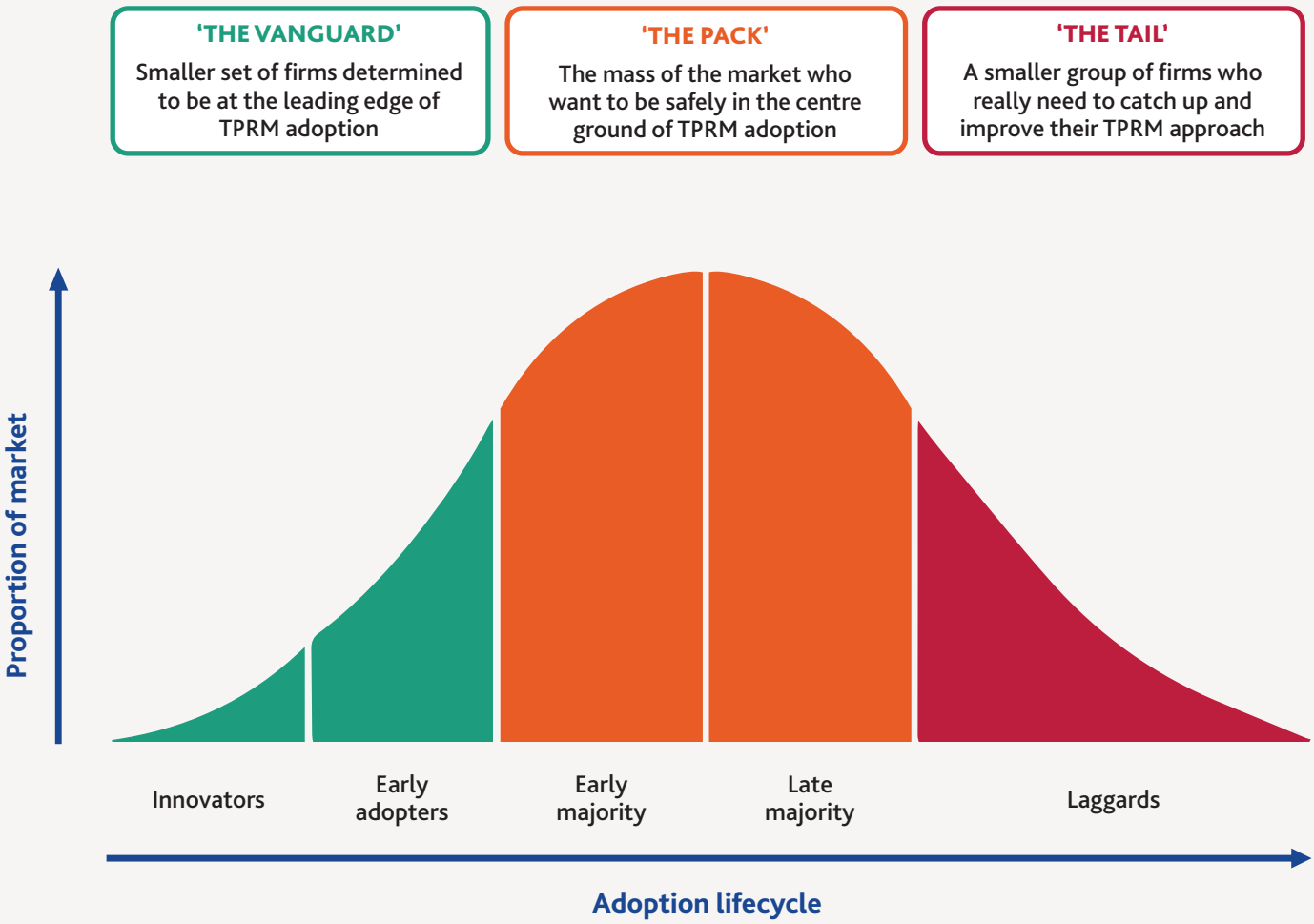
> **We need the tools to be able to run a proper third-party risk management program. The data is different across platforms and not all joined up. This makes reporting difficult when I'm missing key information on some of my suppliers.**

For too many companies, there is only limited visibility of supplier risks, which is driven by different factors. From the manual process of collecting and inputting relevant data to a lack of adequate tools to understand and tackle risks or taking a reactive approach to addressing problems as they arise – some companies are clearly behind the curve in terms of managing the complexities they face.

SECTION FIVE

Delivering competitive advantage

Throughout our sample, we observed a wide range of firms at different stages of maturity and sophistication. The most mature firms in the vanguard of TPRM are investing at appropriate levels, benefit from high levels of C-suite interest, and have a clear desire to protect their reputation.



For the majority of firms in the "pack", progress is underway. But challenges remain in making the business case for investment and justifying added costs, especially when the return on investment is tricky to quantify.

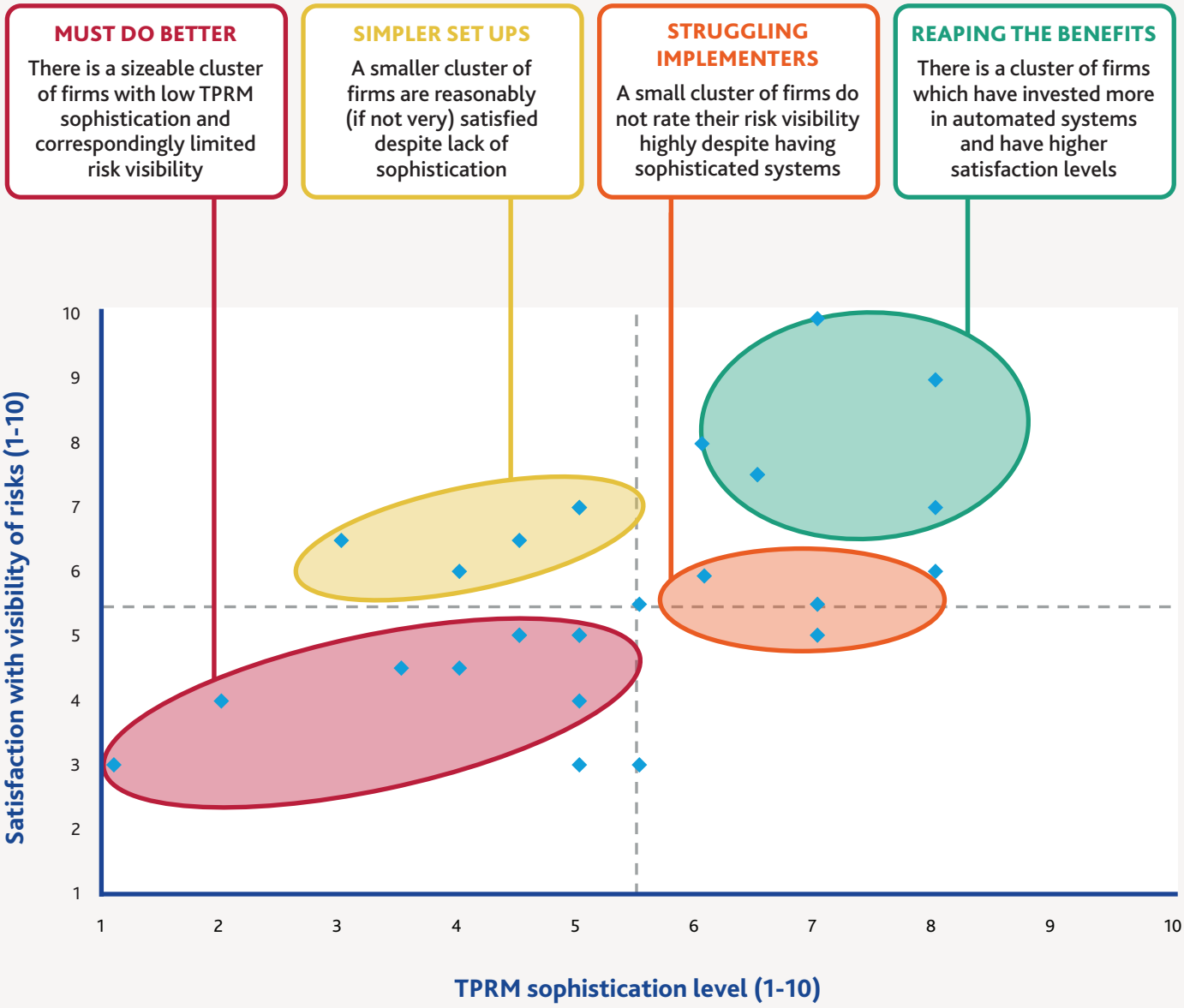
A smaller group of companies in the tail are playing catch up and need to radically improve their TPRM approach.

INVESTMENT PAYS OFF

One thing is clear - staying ahead of risks and investing in TPRM pays, helping companies at the vanguard create a competitive advantage.

There is a clear and positive correlation between investment in TPRM systems and satisfaction with the visibility of risks.

SOPHISTICATION LEVEL VS. SATISFACTION RATING



More sophisticated players are reaping the benefit of investment by reducing exposure to risks, improving efficiencies through automation, and minimizing duplication of effort. Some firms continue to struggle despite investment in systems and others buck the trend by reporting high levels of satisfaction without sophistication. But the connection is clear – low TPRM sophistication leads to poor visibility of risks creating potential for greater negative impact when things go wrong.

INVESTMENT PAYS OFF

A combination of factors underpins any company's TPRM maturity. From C-suite buy-in to having centralized TPRM, taking a consistent approach across the business, and developing advanced, integrated tools that deliver a "balanced scorecard" of risks – much of what's needed to achieve maturity starts with senior management recognizing the problem and making the right decisions to embed a culture of effective risk management.

This enables teams to achieve the right visibility of risks throughout the relevant tiers of their supply chain to improve efficiency and ensure things don't get missed.

By asking the right questions, companies can benchmark their TPRM maturity, ensuring they balance risk management with business performance to develop confidence that their processes are safeguarding their reputation.

WEIGHING THE BENEFITS

From avoiding reputational damage to improving operational resilience, the benefits of effective TPRM are clear. But it's not just about preventing problems.

Having the right systems in place can help businesses run more efficiently. It smooths supplier onboarding processes and helps improve their performance. It builds resilience for companies operating in challenging global environments, helping them recover faster, clear regulatory hurdles, and protect their reputations.

Ultimately, minimizing supplier risks delivers a clear competitive advantage, enabling organizations to push further, win new contracts, grow their business, and move forward in an uncertain world.

> **Competitive advantage is hugely important: Our compliance with standards like Sapin II gives us an advantage over tender responses from regions where this legislation does not apply.**

SECTION SIX

Key takeaways

BUSINESSES FACE INCREASED SUPPLIER RISKS

With tiered global supply chains, ongoing uncertainty around the world, and new demands in areas like ESG, companies face increasing risks associated with their supply chains. From macro challenges like geopolitical instability, inflation, or cyber threats to specific supply risks like increasing regulations and issues around onboarding suppliers – companies are vulnerable to a host of issues that can hamper continuity, damage their reputation or create a catastrophic impact on performance.

RISK MANAGEMENT TODAY FALLS SHORT

Facing a growing list of threats, complex supply chains, and a demand to onboard more suppliers with old systems, businesses are feeling the increasing pressure of supplier risk. But in today's world, where businesses can have thousands of suppliers spread across the globe, the tools and systems available to meet these risks are not always fit for purpose.

Third-party risk management is often highly fragmented and the responsibility of many different teams in multiple locations, often with conflicting priorities. It's a problem exacerbated by the lack of standardization in approach and terminology used to describe the field.

DEMAND FOR PROGRESS

Given the increasing risks, better knowledge and understanding of TPRM and recognition that the current approach is inadequate, calls for improvements are growing.

70% of companies interviewed are investing to bolster their TPRM team and improve the systems used to manage risk. Across the world major companies are in the process of developing departments to improve TPRM to meet financial, regulatory, and reputational risks. But there's no "one size fits all" approach. Complex entities, with complex supply chains require a nuanced approach.

FIRMS NEED TOOLS TO OVERCOME CHALLENGES

Defining key TPRM use cases can help firms develop an effective approach tailored to their business. From reviewing a supplier's background and financial performance to understanding the regulatory, reputational, ESG, and cyber risks that each supplier poses can help companies identify weaknesses and build the business case for investment.

ALL SUPPLIERS ARE DIFFERENT

Understanding the specific risks of each counterparty is important. What may be true for one business might not apply to another. Dynamic factors feed into the risk rating of any given supplier, and they can change over time. From cyber and ESG risks to regulatory and operational challenges, companies must take a nuanced approach to understand risks posed by a supplier in the context of their business, sector, and geographical location. Ultimately, all other risks ladder up to create an impact on reputational risk.

COMPANIES ARE ALL AT DIFFERENT STAGES ON THEIR TPRM JOURNEY

From visibility into a supplier's operations to lack of information on SMEs, geopolitical instability, and sanctions, businesses face many challenges in monitoring supplier risk. And every firm is at a different stage in their journey.

There is clearly room to improve sophistication – with 3 in 4 rating themselves poor or mediocre in their TPRM capabilities. Satisfaction levels are equally poor, with 7 in 10 firms having low or middling satisfaction with the level of visibility they have into different risks across their supplier base.

INVESTMENT MATTERS

Firms have differing levels of maturity and sophistication, with those in the vanguard of progress investing more and experiencing higher levels of satisfaction with the visibility of risks throughout their supply chain.

They're able to automate more, work proactively to identify and mitigate risks before they become problems, which ultimately leads to a more efficient, secure, and higher performance business.

THE BUSINESS CASE IS CLEAR

To achieve effective TPRM it starts with recognizing the need and getting C-suite buy-in to invest in systems and processes. From having centralized TPRM to taking a consistent approach to risk, developing integrated tools and automating processes – businesses with advanced TPRM capabilities gain a competitive advantage over their peers, improving efficiency, building resilience, achieving regulatory compliance, and avoiding unnecessary costs.

Ultimately, effective TPRM protects businesses against reputational harm, helping win new business, and making progress against a backdrop of increased disruption and uncertainty.

SECTION SEVEN

Executive summary

Commentary from
Keith Berry, General Manager,
Moody's Analytics KYC

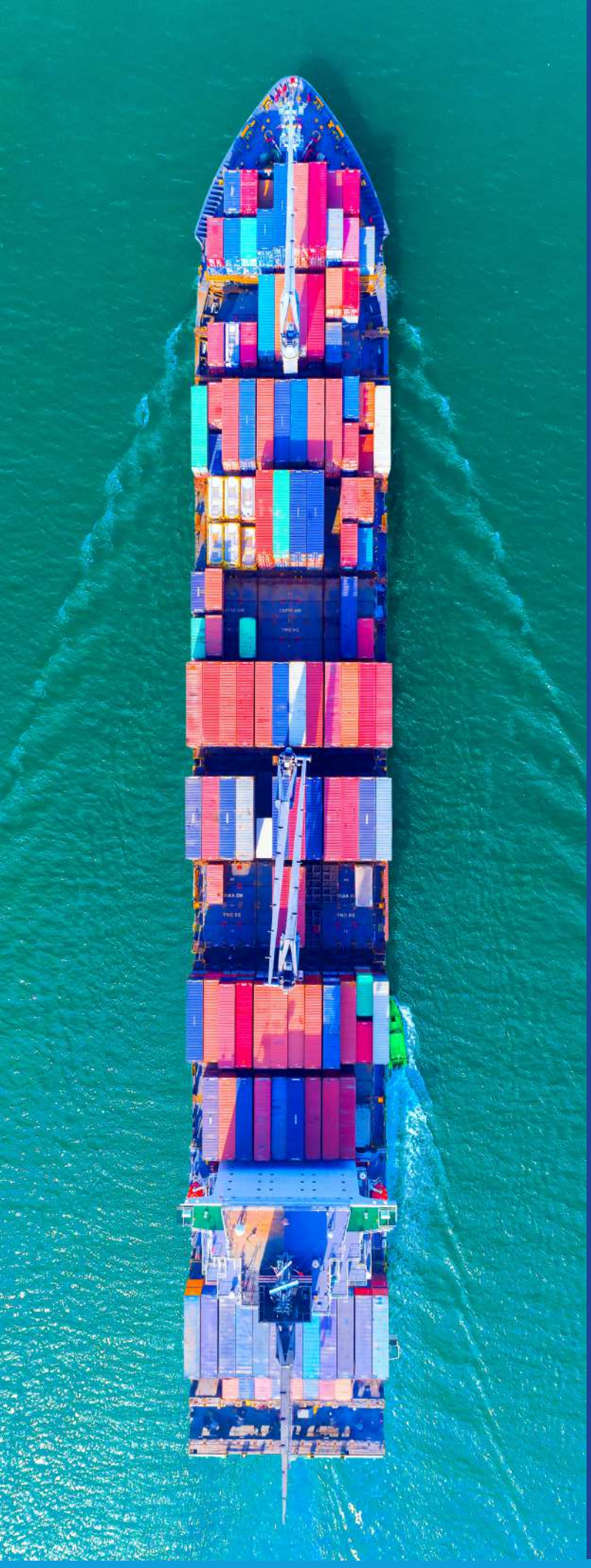
"There is an acute need for businesses to understand the risks posed by third-party providers. The drivers are clear: Geopolitical factors influencing who is sanctioned; existing regulation about money laundering, counter-terrorist financing, fraud and corruption; new regulations dictating greater supply chain due diligence; changing business ownership thresholds that dramatically alter how power and control are measured; and that's not to mention customer expectations that providers will choose to work with ethically sound partners.

Many of these should be priorities for global brands and are articulated through this research. Businesses want to protect their reputations, maintain compliance, and look for competitive advantage in their third-party networks. It's a challenge we recognize.

What clearly emerges from the many factors to consider around third-party risk management (TPRM) can be distilled into three actionable areas.

ONE: UNIFICATION

The research has made clear that there are many different people and departments who consider themselves responsible for third-party risk management. With disbursed ownership and accountability comes additional risk. Organizations could benefit by thinking about unifying their approach to TPRM - leveraging people, processes, and technology. Operating unified processes based on risk policies, risk appetite, and the type of counter-party network needed for operational resilience. Technology to translate that process into an automated workflow that will support efficiency. People working to one standard, with access to one solution that holds an accurate view of risk.



TWO: VISIBILITY

We heard through the research that professionals working in TPRM are lacking visibility - visibility deep into the different tiers of their supply chain, and visibility into their suppliers' operations. A fragmented approach is not going to deliver visibility and maintaining a picture of risk will be harder. This opens up the way for reputational harm and financial penalties. With unification of people, processes, and technology focused on accessing and integrating real-time, global data about vendors, consultants, and suppliers comes greater clarity and visibility of risk. And understanding where high-risk cases exist enables organizations to make better risk-based decisions.

THREE: REPUTATION

As one respondent said, "reputation takes years to build and a second to destroy". It is a clear and primary concern for the organizations participating in this research to protect their reputations. For organizational pride; for good and ethical practice; for competitive advantage; and for future growth, the reasons for unifying an approach to TPRM and gaining visibility of risk are clear.

Certainly, this research has given myself and my team much to think about in terms of how we create the right strategies to support organizations to address TPRM and supplier due diligence. I look forward to having conversations with organizations managing complex counterparty networks to see how Moody's can support them to unify their approach to TPRM, gain visibility of risks, and protect their reputations.

I'd like to end by thanking everyone who took time out of their business schedules to participate in this study. We gained access to some awesome global brands, and the insight they provided is invaluable. Thanks also to Paul Nola and the team at Context Consulting for their work in carrying out the study and drawing up these findings."

Keith Berry

GET IN TOUCH

Contact information

AMERICAS
+1.212.553.1653
clientservices@moodys.com

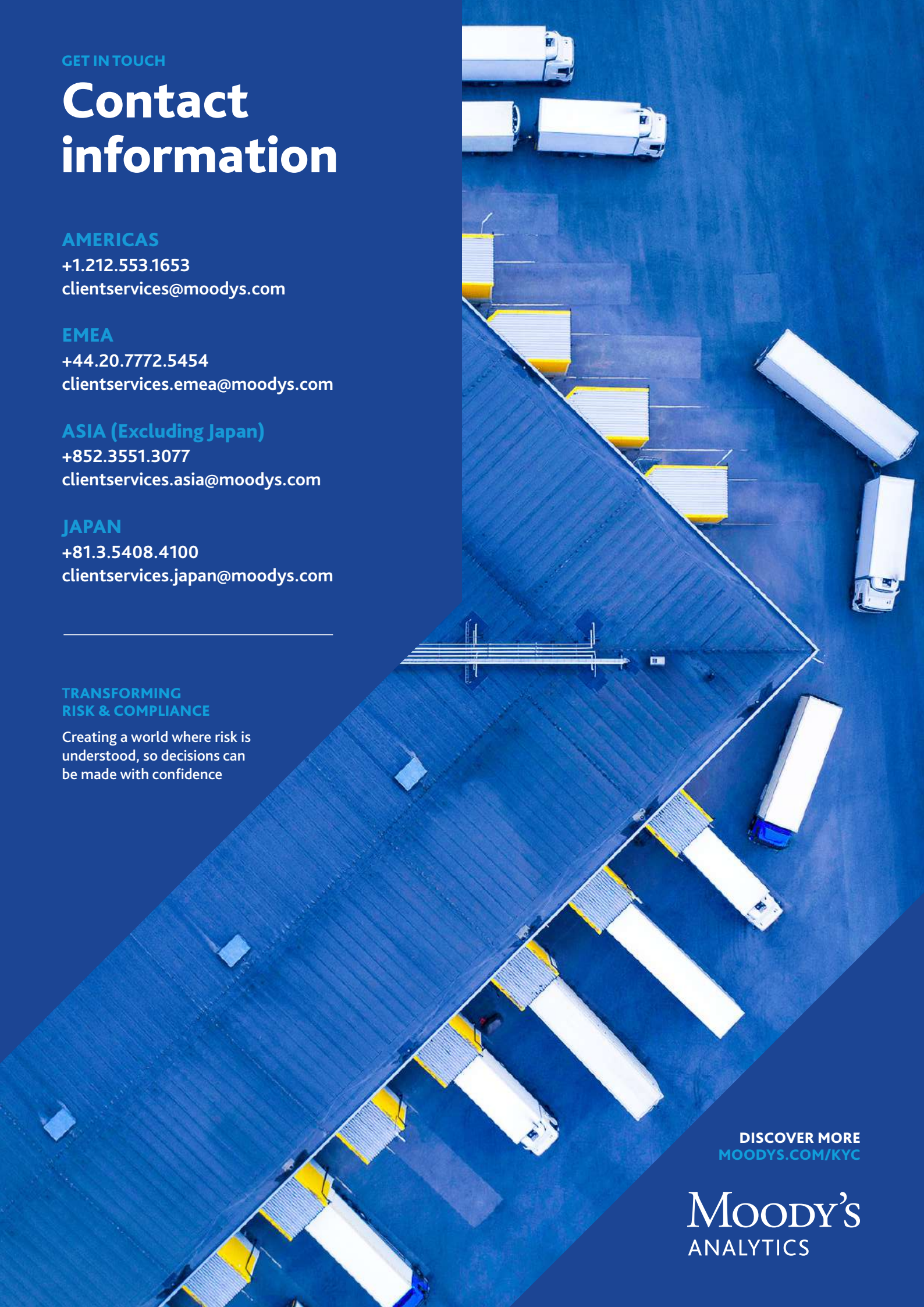
EMEA
+44.20.7772.5454
clientservices.emea@moodys.com

ASIA (Excluding Japan)
+852.3551.3077
clientservices.asia@moodys.com

JAPAN
+81.3.5408.4100
clientservices.japan@moodys.com

TRANSFORMING RISK & COMPLIANCE

Creating a world where risk is understood, so decisions can be made with confidence



DISCOVER MORE
MOODYS.COM/KYC

MOODY'S ANALYTICS