MITRATECH

Vendor & Third-Party Risk Management: Key Concerns & Proven Solutions

What are the challenges presented by ESG, vendor risk, and complex supply chains? And what are some solutions?

By Henry Umney

Table of Contents

Introduction: Are Your Vendors and Suppliers Putting You at Risk?

1 Managing Vendor Risk in a Platform-driven World

2 The Importance of Fourth-Party Vendor Tracking

3 ESG Risk Management & TPRM

4 Using VRM Technology to Mitigate Vendor Risk

About Mitratech

Introduction: Are Your Vendors and Suppliers Putting You at Risk?

Vendor Risk Management (VRM) is a process for managing and assuring that the third-party vendors and services your company is utilizing do not create negative impacts on your performance or operations.

A VRM program is designed to assist you in managing and monitoring vendors for potential risks, and must be methodical and organized to be effective. But, due to the ever-changing nature of business in today's financial markets, cost control and efficiency in supply chains are a *must.*

Ask yourself these questions right now:

Are my vendors and suppliers in compliance with all applicable regulations? Is my company safe from any risk created by any of my vendors?

The fact is, not many companies can answer these questions with a confident "*yes!*"

If your company *doesn't* have some sort of vendor compliance policy already in place, it could open itself up to unforeseen costs generated by non-compliance.

These costs can stem from late deliveries, improper shipments, hidden costs, and other unauthorized fees associated with existing products and services. Not to mention the fact that some regulations will not only penalize a vendor for violations like data privacy breaches, but *also* their client who initiated the work in the first place.

In this document, we'll explore several key areas of concern for risk managers, such as vendor diversity, data breaches, and the growing need for Environment, Social, and Governance (ESG) policies and practices. Within each of them, we'll lay out best practices for mitigating potential risk and maintaining compliance, even in a business landscape that seems to consistently create more complex compliance hurdles.

01 Managing Vendor Risk in a Platform-driven World

Managing your vendor network and supply chain used to be easier. You knew who all your suppliers were, you could visit their sites, and you knew them as individuals you'd worked with for many years.

More importantly, they *knew* you. Vendors understood the specifications you gave them; they visited your site to see how you would use their products and services. Maybe some of their employees spent much of their working week at your sites and offices, helping you make the best use of their services.

That's all changed.

You and your suppliers work in a **platform-driven world.** This transition from a process-driven world to a platform-led world was explored by Peter Bendor-Samuel, CEO of Everest Group, who pointed to the new risks global supply chains have faced:

One area of evolving risk is the supply chain. Recently, for example, the devastating outbreak of COVID-19 in India highlighted the concentration risk that many companies had for third-party services in this market.[1]

Intense competition drives the need for constant innovation, whether it's in the form of new product functionality or delivering new cost efficiencies. This pressure increasingly means spreading the talent net much further and more widely than in the past to get access to value-add capabilities at a competitive price.

Open technology standards mean that technology platforms are increasingly the primary entry point for working with suppliers, whether they supply services or physical products. It can mean your primary access, relationship, and order processing are conducted mainly through a company website or even a 'Gig Economy' market site. Human contact may be minimal.

Platform-based purchasing of goods and services, especially over long distances, may mean you are less likely to go on-site to meet a vendor. You certainly won't see how their supply chain works daily and fully understand how they subcontract.

Intense competition drives the need for constant innovation, whether it's in the form of new product functionality or delivering new cost efficiencies.

[1]Bendor-Samuel, Peter. "Managing Risks in Third-Party Services Is Changing." Forbes. Forbes Magazine, July 19, 2021. https://www.forbes.com/sites/peterbendorsamuel/2021/07/19/managing-risks-in-third-party-services-is-changing/?sh=6a9ce52d66b1.

Platform-based purchasing provides enormous operational flexibility and presents organizations with a choice. They need to decide whether to stick with an existing supplier's proven reliability or access a network of new suppliers quickly and easily using a range of platforms.

What are the risks?

While a platform-led supply chain model offers excellent flexibility, it does not come without risk. To address this, many companies may use a mixed approach that features working with their traditional vendors and employing others via their platforms to fill in any gaps that emerge. This can offer the best of both worlds.

However you choose to balance these two approaches, third-party risk management **is an important consideration.** Platform-based relationships typically mean working with new suppliers in potentially new areas of the world or new sectors – whether for you directly or in the deeper 4th and 5th levels of your supply chain. As a result, new and unfamiliar risks may emerge too, especially in the increasingly important area of Environmental, Social, and Governance (ESG) compliance.

Here, issues around modern slavery, bribery, climate change, legal risk, compliance risk, and security risk can each conspire to create a range of operational, commercial, legal, or reputational headaches for your company. This jibes with what we've heard in discussions with

Platform-based relationships typically mean working with new suppliers in potentially new areas of the world or new sectors.

customers working with their supply chain to find that competitive edge or capability that fills a gap in their business process.

The need for visibility and transparency

The key to effective TPRM is visibility and transparency. You need to proactively monitor your vendor network and supply chain for potential and emerging risks based on the service or products they provide, their location, and the nature of the vendor network and supply chains *they* rely on to deliver their service to you.

Some of these risks can include:

- **Business continuity risk,** if a site cannot be accessed, or goods delivered.
- **Commercial risk**, where a supplier might be acquired or go bankrupt, putting their ability to supply you at risk.
- **Concentration risk,** where a single service provider – for example, in cloud computing services – can impact multiple companies in your supply chain, making a recovery from an incident incredibly challenging.
- **ESG risk** of violating regulations, industry policies or societal expectations.

The ideal approach is to monitor, in-depth and proactively, your vendor network and supply chain so that issues that emerge can be addressed swiftly. Issues you identify early can be fixed with less disruption to the business and the relationship, compared to those allowed to develop and potentially fester.

This in-depth monitoring is supported by having **well-documented risk profiles** of the organizations that make up the supply chain. This forms the basis of the alerting systems that allow issues that emerge to be flagged in a risk dashboard. News events, business announcements, or issues raised by employees can be captured and consolidated to provide near-real-time monitoring of the risks within a supply chain. These issues can also be escalated into an enterprise GRC platform if necessary.

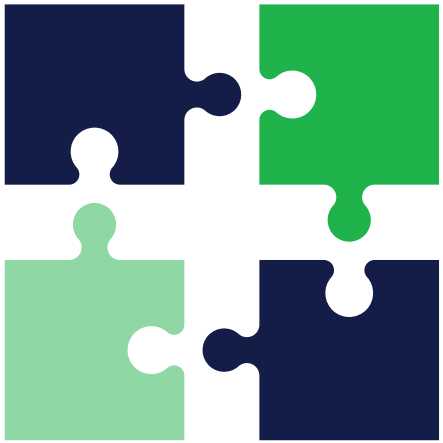
02 The Importance of Fourth-Party Vendor Tracking

We've alluded to the fact that your vendors have their own vendor networks, so what about fourth-party (or even fifth-party) risk? Particularly when it comes to protecting your corporate or customer data?

A fourth party is a subcontractor to your vendor. The effectiveness of your vendor and the risk to you increasingly depends on them, as your vendors outsource and subcontract critical activities.

Fourth-party vendors go by a lot of names, including "providers" and "strategic partners", and can provide a variety of data-intensive services like bill pay, mobile banking, core processing, legal, or others.

Organizations are so interconnected today that it's critical to make sure your vendors aren't leaving your data or critical processes vulnerable through *their* use of vendors. The trouble is, you might not be sure where to begin to sufficiently monitor fourth parties.



So, what do you need to know about fourth-party vendors to track them and reduce this outside risk to your organization?

Understanding risks at a deeper level

Without direct contract with fourth-party vendors, getting access to information they may have and knowing what data or business information of yours they have access to can be complicated. Sharing information with a party not bound by confidentiality agreements and other legal requirements is *not* advisable, so you need to understand:

- **Who they are in relation to you,** so you can consider the potential cost of managing these relationships when comparing prices and risk.
- **What critical products and services they provide** to your vendor.
- **What due diligence has been done** by your vendors - that includes everything from financials to test results, cybersecurity, and business continuity planning.

This understanding will help you anticipate risks that may reside at a deeper level, such as how your data may need to be shared and possibly even stored in vendors' systems where you do not have a direct contract.

Organizations are so interconnected today that it's critical to make sure your vendors aren't leaving your data or critical processes vulnerable through *their* use of vendors.

Limiting fourth-party vendor risk

Even relatively small service providers can cause major disruptions or outages to the companies that rely on them. Your organization isn't just responsible for what your vendor does, but also for the activities of its own vendors — especially in the eyes of your customers. The more critical these fourth-party vendors are to your vendor, the greater **the costs and risks.**

There are, however, ways to limit fourth-party vendor risk. When considering vendors:

- Routinely ask your third-party vendors for a list of their critical vendors.
- Request that your third-party vendors keep you apprised of any changes or concerns with fourth-party vendors.
- Require your advance approval of changes.
- Review your third party's policies around oversight of their outsourced services.
- Read vendors' SSAE 18 control audits, looking for mention of third parties.

03 ESG Risk Management & TPRM

There are few initiatives currently afoot in a heavily regulated sector like banking that don't feature **Environmental, Social, and Governance (ESG)** credentials, either to engage investors and customers or deliver the ESG risk management capabilities that banks now require.

These initiatives will embrace various business areas, including business process change, product development, investment management, and market positioning.

The widespread use of 'ESG' may inspire fatigue for some of us. That said? There's little doubt that issues around climate change, sustainability, or modern slavery, among others, are now hot-button issues for many people in a way they weren't just a decade or so ago.

ESG offers **investment and growth opportunities for some** and provides **a source of risk and challenge for others.** Wherever you stand, ESG needs to be embraced, and for financial services firms in particular, this inevitably leads to thoughts around ESG risk management.

ESG meets TPRM

ESG is a vast topic, but in working with financial institutions, it's clear that third-party risk management (TPRM) is a significant aspect of ESG for many banks. Banks have complex value chains and make extensive use of sophisticated technology and data capabilities from suppliers worldwide.

While providing scope for innovation, scalability, and business efficiencies, a bank's extensive supply chain can be a source of **an array of issues** beyond the purely practical problems of trying to work with multiple business partners in different time zones. Numerous social, commercial, contractual, operational, and compliance risks need to be identified, managed, and mitigated if an institution is to capture the total value of these commercial relationships.

Companies will have risk management systems and processes to address many of these risks. Still, the complex, interrelated and global nature of ESG risk means that many institutions need risk management tools and frameworks to manage their ESG risk specifically.

NOTE: Vendor Risk Management (VRM) and Third-Party Risk Management (TPRM) differ, in that many companies partner or otherwise work with third parties who are not selling them a product or service.

A framework for ESG risk management

KPMG has proposed an ESG risk management framework that covers all aspects of ESG risk management, including business strategy, product development, governance, capital charging, product distribution, regulatory & stakeholder reporting, and ESG data management.

As you might expect, this framework covers the traditional risk competencies, including governance, strategy, risk measurement and identification, reporting, and disclosure. It recognizes the need to have a defined ESG risk management profile to manage the ESG risk itself and inform other risk areas that it can impact, including operational risk, compliance risk, risk capitalization, and others.

From a TPRM perspective, it emphasizes *specific* risks, including human rights, climate risk, corruption, structural risk, legal risk, compliance risk, and data protection risks, as potentially significant issues in the supply chain.

Pursuing an optimal solution

These risks are already broadly recognized and well understood. The challenges for a bank or other business involve somehow fully capturing and defining these risk profiles, together with consolidating the data, metrics, and documentation used to monitor them. The aim is to proactively monitor

the status of their key suppliers that support the banks directly and their 4th and 5th-level suppliers.

Given the expectations from stakeholders, regulators, and customers to embrace the emerging opportunities surrounding ESG, there's a premium on delivering TPRM capabilities quickly and efficiently. In the U.K., the Bank of England's Prudential Regulation Authority (PRA) has been in the forefront of regulating this with its SS2/21 Supervisory Statement, which details the operational resilience aspects of TPRM.

The KPMG model will help institutions shape their response to managing the ESG risks, including any TPRM risks.

As with other areas of VRM and TRPM, what's the key enabler for implementing this type of framework? A suitable **technology platform** that provides the efficiencies, scalability, and results that an institution needs to implement comprehensive TPRM.

The optimal **ESG risk management solution** will feature SaaS-based capabilities that allow for rapid deployment, both within a bank and within the companies that make up its 3rd, 4th, and 5th line supply chain. It should also feature a dashboard so that any issues – operational, political, commercial, et cetera – can be flagged early on, with proactive alerts.

Experience suggests that the earlier an ESG risk management issue is identified, the easier it is to address without harming the business or the relationship. Equally, the platform needs to be the repository of all the vendor risk documentation, contracts, and risk metrics, so staff can access them quickly when incidents develop.

04 Using VRM technology to mitigate vendor risk

So it's obvious that third- and fourth-party vendors and other entities have the potential to create significant vulnerabilities for your enterprise. But the need for vendor diversity and the complexities of today's vendor networks and supply chains means monitoring and mitigating all of the risks they present can be an **almost impossible task** using traditional means.

Technology rides to the rescue, however, since organizations can now utilize vendor risk management solutions that can help ensure they manage and monitor third-party vendors and their fourth-party providers.

As risks proliferate and regulators create more regulations, exposures increase. So you need to implement new measures to mitigate those risks. That includes managing your supplier ecosystem more stringently than before – because your vendors' failures might become *your* business disasters.

As risks proliferate and regulators create more regulations, exposures increase.

A solid vendor risk management system that offers a platform for vendor compliance will help you avoid disputes and unnecessary charges – and save you time.

Setting up effective vendor compliance

An effective VRM software solution offers a platform where you can create an oversight and policy compliance dashboard that's based on your current internal policies. This dashboard will show all of your vendors at a glance and if the internal policy requirements are met or outstanding. This means that for each vendor there will be a policy requirement matrix as part of the vendor relationship profile that will show all the policy requirements that are required for them based on their level of risk (critical to low risk) to your company.

For each vendor, you should be able to tell quickly if they are compliant or not for all aspects of your internal policy. The VRM solution should also be able to assign certain documents that are already in the system to meet the policy requirements.

Finding efficiencies in VRM

Communication is vital for vendor compliance. To make sure you have all the necessary documents and other data in place, you're going to have to work with a variety of customer service teams among all of your vendors.

Working with outside customer service support teams, it's important to be courteous and have a clear picture of the missing content when you talk with them. This will ensure that you are giving them all the information they need so they can provide you with the correct documentation to make them compliant as a vendor.

The best VRM solutions can remove some of that work for you, with dedicated due diligence teams that help you acquire the necessary SOC1/SOC2, financial, business continuity, insurance, and information security documents. They can also take the time to perform a compliance review.

Having a vendor risk management system that delivers comprehensive oversight and policy compliance will help ensure that you have a lasting relationship with your vendors. **The long-term goal** is to be able to monitor all of your vendors but to keep a closer eye on those who could pose a negative risk to your growing business.

Having a risk management platform that you can trust to help you keep track of your vendors will give you the peace of mind to continue to grow, and bring on new vendors over time.

Having a vendor risk management system that delivers comprehensive oversight and policy compliance will help ensure that you have a lasting relationship with your vendors.

About the **Author**

Henry Umney is the Managing Director of GRC Strategy at Mitratech and joined the company as part of the ClusterSeven acquisition in 2020. Henry joined ClusterSeven in 2006 and for over 10 years was responsible for the commercial operations of ClusterSeven, overseeing all global sales and client activity as well as partner engagements before being appointed CEO.

About **Mitratech**

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across their organization.

With Mitratech's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

Mitratech serves over 1,500 organizations worldwide, including 30% of the Fortune 500 and over 500,000 users in 160 countries.

For more info, visit: **www.mitratech.com**

MITRATECH

CONTACT US

info@mitratech.com
www.mitratech.com

Mitratech US
+1 (512) 382.7322

Mitratech EMEA
+44 (0) 1628.600.900

Mitratech AUS
+61 (0) 3.9521.7077