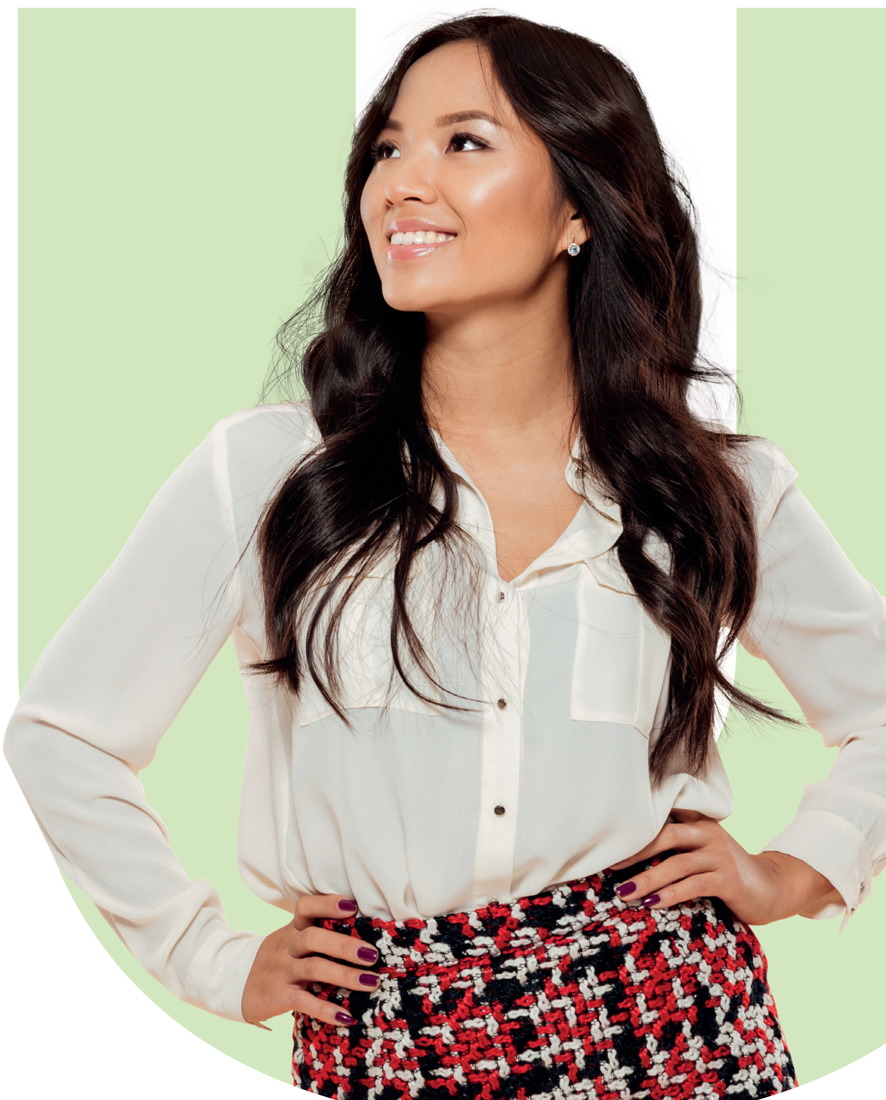
UNIT4
In business for people

Procurement's new imperative

DRIVING VALUE WITH STRATEGIC
THIRD-PARTY RISK MANAGEMENT



Build a digitalization strategy that maximizes the benefits of outsourcing Relationships and minimizes third-party risk

Despite the advantages of outsourcing, unmanaged risks can undercut your organization's goals and objectives. Intelligent digital tools improve your organization's risk position, business outcomes, and supplier relationships.

This paper will help sourcing, procurement, and finance leaders understand why traditional approaches to third-party risk management need to evolve and the role digitalization plays in mitigating risks associated with outsourcing partners. It outlines the general concepts of a third-party risk management framework and how it can help avoid costly errors, protect your organization, and improve business outcomes.

The value proposition for third-party risk management

Top performing procurement teams create outsourcing partnerships that deliver value beyond cost savings. Procurement's insight into the supplier ecosystem makes it uniquely suited to enhance the organization's brand value, minimize exposure to volatility and risk, and boost competitive advantage.

As the broker for the organization's third-party relationships, procurement plays a critical role in value creation through intelligent risk mitigation. The benefits are even more robust when there is strategic alignment with finance, human resources, and IT. These comprise a large swath of outsourced functions.

Whether your organization's contracts are with a handful or hundreds of third-party suppliers, your risk management strategy needs to go beyond questionnaire-based assessments, especially if third parties have access to sensitive data. Your vendor selection process needs a technology component that helps you identify, assess, mitigate, and continuously monitor risks.

Outsourcing reaches a tipping point

For years, the benefits of outsourcing outweighed the risks, but with the complex and interconnected nature of today's supply chains, the risks are more severe and catastrophic. Financially speaking, a third-party incident can **cost companies up to $1 billion** and negatively impact share prices by 10%.

The best way to mitigate third-party risk is with intelligent tools that utilize robotic process automation (RPA), artificial intelligence (AI), and machine learning. Digitalization gives unprecedented visibility into supplier networks, including financial information, certifications, reputation, and even visibility beyond Tier 1 suppliers, allowing more granular visibility into Tier 2 and Tier 3 suppliers.

Today, organizations must go beyond treating third-party risk on a case-by-case basis. Automation and intelligent tools reduce human error. They also create a unified framework of policies and procedures to support data-based decisions.

51%

of businesses have suffered a data breach caused by a third party

Source: Poneman Institute

The origins of third-party risk management

Third-party risk management (TPRM) as a discipline originated from the heavily regulated financial sector. The Office of the Comptroller of the Currency (OCC), an independent bureau of the U.S. Department of the Treasury, defines a third-party relationship as any business arrangement between the enterprise and another entity, by contract or otherwise.

Within procurement, TPRM focuses on identifying and reducing risk related to the use of outsourced suppliers, vendors, partners, contractors, and service providers. It encompasses supply chain risk management, vendor risk management, and supplier risk management.

If you can identify and monitor these risks during the upstream sourcing process, then you can mitigate the risks throughout the lifecycle of the relationship.

It is important to note that TPRM is not just a burdensome requirement for regulated industries. It is a golden-egg opportunity to create value beyond cost savings that maximizes the benefits of outsourcing. A robust TPRM program protects enterprise operations, reputation, profits, and increases business resilience when a disruption happens.

Procurement's role in risk management

The COVID-19 pandemic was the catalyst for many companies to accelerate their digital transformation and supplier strategies. As businesses continue to adapt, procurement's involvement in risk management has even stronger implications to maintain business continuity.

Procurement's objectives have moved far beyond cost control, with operational efficiency now considered a top business priority among CPOs. Procurement plays a primary role in strategically aligning company values and goals to manage the supply chain.

Top 3 CPO priorities

78%
Driving operational efficiency

76.4%
Reducing costs

76.1%
Digital transformation

Source: 2021 Global CPO Survey

As companies turn to procurement to mitigate supply chain risk and maintain business continuity, a key component of this strategy is outsourcing.

Business process outsourcing (BPO), a sub-category of outsourcing in which specific business processes are outsourced, is a popular strategy to reduce costs. BPO is often used for functions such as human resources, IT, payroll and accounting, and call center operations.

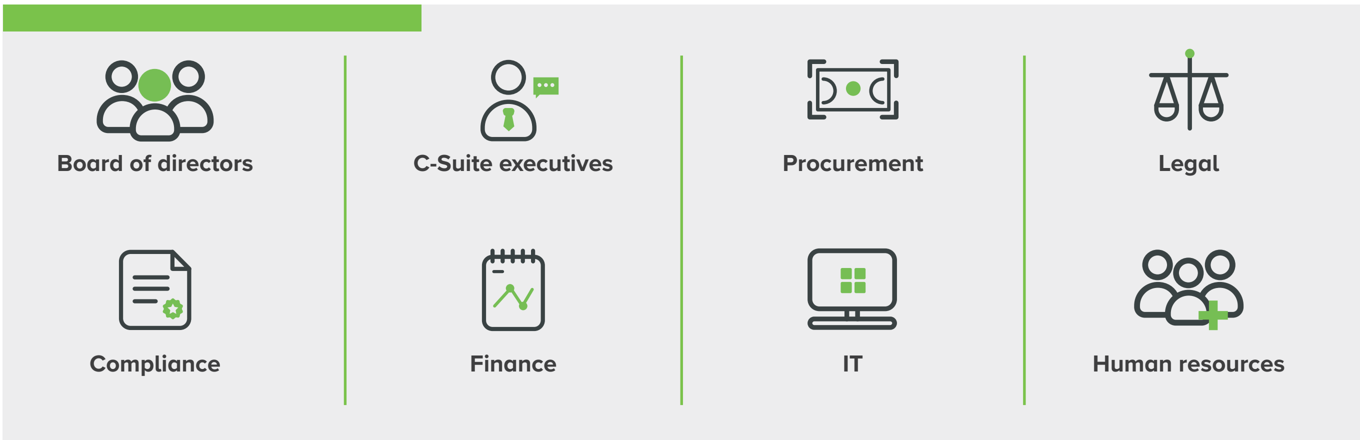
The expected growth in BPO means that internal stakeholders across the extended enterprise need to align on a risk strategy and framework when it comes to finding outsourcing partners.

The global BPO market size was valued at $232.32 billion in 2020.

It is expected to register a CAGR of 8.5% from 2021 to 2028.

Source: Statista Research Department, 2021.

TPRM key stakeholders



The process to qualify suppliers generally follows a baseline assessment: collect information on the third parties and determine a rating system to assess their risk to the business. Based on these data, you ensure that vendors meet the basic compliance requirements of the organization.

The problem with this kind of process is that it quickly becomes outdated when the market shifts.

The risks and rewards of third parties

McKinsey shows that companies that consistently collaborate with suppliers demonstrate higher growth, lower operating costs, and greater profitability than their industry peers.

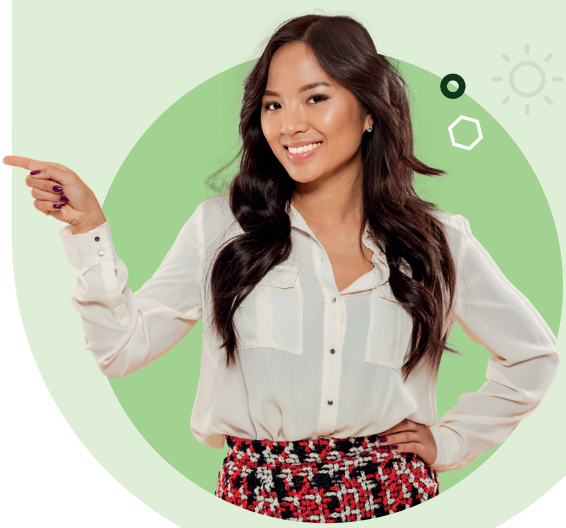
A collaborative approach with suppliers can lead to innovative new products, cost-cutting measures, or improved service levels, while at the same time mitigating risks and strengthening the supply chain.

But your third-party business partners also carry inherent risks. Some may be known, such as operating in an earthquake-prone location; or they may be unknown, like having questionable cybersecurity controls.

Visibility is key to managing risk

A risk-based approach to outsourcing requires visibility into supplier data, spend and contract terms to understand the different types of risks that third parties carry.

Using intelligent tools to identify risks helps your team quickly classify third parties based on their threat to the business and accurately assess third-party risk. From there, mitigation and remediation strategies can ensure that all identified threats are addressed.



60%

of organizations work with more than 1,000 third parties

Source: Gartner, 2019

We'll touch on the process to identify, assess, and mitigate third-party risk, but first, let's define some of the different types of risk posed by third parties.

Cyber risk accounted for just 1% of total risk in 2020. By 2021, it increased by nearly 150%.

Source: Riskmethods 2021 Risk Report

Cybersecurity risk

This is a kind of operational risk, but it's worth its own discussion point. The massive shift to remote work during the COVID-19 pandemic has led to an increase in cybercrimes. **Consider this 2021 report by HP among IT** decision-makers on the severity of cyber-attacks:

- 54% report an increase in phishing
- 56% report an increase in web browser-related infections
- 44% report compromised devices used to infect the wider business
- 45% report an increase in compromised printers used as an attack point

With the growing increase in cyber threats, it is more important than ever to monitor and assess every third party's cybersecurity protocols.

Supplier financial risk

This kind of risk arises when a third party becomes financially unstable or insolvent. Worse, it can have a snowball effect on other suppliers in the supply chain, and the financial implications can be staggering. Even a minor supplier can cause millions of dollars in incurred costs.

The **2021 Risk Report**, which monitors over 740,000 risk objects including suppliers, locations, ports, company sites, and customer sites worldwide, notes that the financial stability of suppliers (the largest category of risk facing global supply chains) grew from 41% of total risk in December 2019 to nearly 52% in early 2020.

Reputational risk

Trust is often an organization's biggest asset. Reputational risk has to do with the public perception of your company and can be difficult to manage.

There are steps to mitigate reputational risk as it relates to the supply chain. Your suppliers' actions can tarnish the company's reputation, which is why it's essential to thoroughly research and assess a supplier's business practices, management structure, and relationships with its workers.

The third-party risk management lifecycle

Despite the advantages of outsourcing, numerous risks can undercut your organization's goals and objectives. Setting up standardized processes and procedures to monitor third-party risk will complement your existing supplier relationship management work.

The most important thing about TPRM is that it is an ongoing process, not a quarterly check-the-box exercise. A robust TPRM framework should include automated workflows to all stakeholders tasked with monitoring third-party risk.

The first step is to identify the third parties. Next, determine how to measure or score each third party's risk. Finally, map a process to report and act on the data, then use technology for continuous monitoring.

Let's dive into each step.

Identify third parties

You can't monitor third parties you don't know about. Working cross-functionally with internal stakeholders, compile a list of all current suppliers that support the business. If your company has an overwhelming number of suppliers, then at a minimum you should include the suppliers that support your core business functions.

Next, segment your supply base for attributes that align with business priorities. This will help you determine suppliers that are truly strategic and integral to your company's supply chains.

During the identification phase, it's also important to map your supply chain to understand logistical risks that third parties may face. How many tiers you map depends on the resources you have available. It could be as simple as identifying your major Tier 1 suppliers or you can go deeper into Tier 2 and Tier 3 suppliers.

For example, you'll want to know if your Tier 1 suppliers depend on components from Tier 2 or Tier 3 suppliers that may be in a geographic location prone to natural disasters or under the jurisdiction of a government that allows child labor.

A Supply Base Management (SBM) tool minimizes the time it takes to identify third parties, especially for Tier 2 and Tier 3 suppliers. With an SBM tool, you have a central repository of third-party information where suppliers can manage their own profiles and upload certifications, files, contracts, and other documentation. All of this can be easily exported into reports for faster data-based decision-making.

Once you understand some of the challenges your suppliers face, it's time to assess each third party's risk.

Assess third-party risks

Assess suppliers on the value they provide, not just the cost for their service or the volume of purchasing.

For example, suppose a third party has access to sensitive data, but overall comprises a small amount of spend. In that case, it's still important to include this supplier in the risk assessment to determine whether adequate controls are in place to prevent a data breach.

Many organizations utilize a risk scorecard to consistently assess third parties. They are also known as vendor scorecards or supplier scorecards. Scorecards are a living document that allows you to quantify the potential risks of a third party.

A high-risk vendor may have access to information like intellectual property or financial records, which poses high financial, compliance, operational, or even reputational damage.

Organizations categorize a third party's scorecard metrics to assess the risk of a vendor as high, medium, or low risk. You can also use a stoplight system: Red (high risk), yellow (medium risk), or green (low risk).

Scorecards help stakeholders analyze vendor performance to determine if it requires improvements and whether to reconsider the partnership. Supplier scorecards contain insight for other stakeholders, too. They help the strategic sourcing team with supplier relationship management. Used in conjunction with a spend analytics tool, scorecards help finance teams with forecasting and modeling.

Mitigate

The mitigation phase gives your TPRM framework teeth. After you identify and assess the third parties, plans to mitigate risks need to be mapped so they can be continuously monitored.

According to Gartner, more than 80% of legal and compliance leaders said that third-party risks were identified after initial onboarding and due diligence. This proves why risk assessments based only on questionnaires are not enough.

Any risks identified among current suppliers should be flagged so that legal, compliance, and contract management teams can work together to renegotiate terms based on the new insights. Automated supplier onboarding ensures that any new third parties comply with updated standards.

Every third party does not need an individualized mitigation plan. Instead, your SBM tool can sort suppliers into groups based on risk threats, such as natural disasters, financial risk, cyber risks, etc.

This is also where procurement and finance can work together on forecasting. Can funds be allocated to an additional supplier in the event of a natural disaster? What are the financial implications of a Tier 1 supplier's insolvency? Working through these questions will provide your company with a competitive edge when a risk event arises.

Agile internal and external processes supported by intelligent tools that flag potential fraud and employee error help mitigate risk, catch costly missteps, and streamlines the entire process.

Strengthen third-party risk management framework

Third parties are increasingly important to business success, but comprehensive risk management isn't just for large enterprises. Digitalizing your strategic sourcing activities will help you find, evaluate, and select the best vendors that drive savings and increase value while managing risk.

Automation

Automated workflows are a critical component to manage remote teams, stakeholders, and suppliers so that steps in the risk management process are not missed. Team members must complete specific tasks, gain approvals, or acknowledge triggered alerts to progress in the workflow.

Additionally, automation makes it easier to align stakeholders, streamline communications, and expedite approvals so your team can focus on mission-critical tasks.

Supply chain diversification is a risk management strategy

The coronavirus pandemic exposed single sourcing as a unique national security threat when hospitals were unable to procure necessary personal protective equipment and ingredients to manufacture certain drugs.

Maintaining a global, diverse pool of suppliers helps companies absorb and recover more quickly from supply chain shocks. Introducing more suppliers into your business may increase some costs, but the benefits of being able to deliver products and materials outweigh those risks.

An SBM tool is a central repository that provides a strategic overview of supplier selection, compliance, and portfolio. It can reduce the time spent on supplier identification, onboarding, and profile scoring through automation of all supplier engagements.

The improved supplier competition and faster response times increases savings, requires fewer people involved in the process, and gives all suppliers equal opportunities.

Spend visibility

Visibility into your organization's spend patterns is critical to identify and manage third-party risk. AI and machine learning can gather spend data from various company systems into a single repository that is then cleansed, enriched, and classified to provide a holistic picture of both direct and indirect spend across categories, vendors, geographical spread, languages, and business units.

An enhanced spend analytics tool helps you identify areas where you may be overleveraged with a supplier. Real-time data helps you quickly diversify your spend and find opportunities for efficiency gains and risk reduction.

A single source of truth

Organizations large and small are forgoing daily trips to the office and embracing remote work. While risk management is everyone's job, everybody needs to work from the same data to make informed decisions. Having multiple systems, spreadsheets, and processes sucks up valuable time and resources.

The CEO, finance team, and category managers all need to work from a single source of truth. Manual, point-in-time data to assess spend and manage suppliers is an operational risk.

AI, RPA, and machine learning reduce risks associated with human errors, making teams more agile and better able to flex during a risk event.

An easier way to manage third-party risk

Monitoring third-party risk is a resource-intensive undertaking that requires continuous visibility into your supplier ecosystem.

Scanmarket's S2C platform helps optimize this process with built-in integration between Spend Analytics, Supplier Assessment, Supplier Identification, Sourcing, and Contract Management. It has been successfully integrated with all the market-leading P2P platforms.

Outsourcing is a strategic way for organizations to focus on core business processes and lower operational costs. Procurement can support enterprise stability and business continuity by taking a risk-based approach to outsourcing and supplier relationship management.

The adoption of modern digital tools will drastically improve business outcomes, make teams and suppliers more agile, and improve alignment with the goals of the business.

Scanmarket

Scanmarket is a source-to-contract software provider that develops advanced functionalities in an effortless design. Originating from the needs of the end user, Scanmarket's S2C solution is attuned to meet the needs of the procurement professional. We take ownership of customer success with experts at your fingertips to drive user adoption. Digitalize your upstream procurement functions with technology that is built to be used.

For more information go to:

unit4.com

UNIT4
In business for people

In business for people