WHITEPAPER

10 key insights to boost your third-party risk initiatives

# Third-party risk management

trustalliance compliance solutions x 3rdRISK

Third-party risk management

# The guide for the next generation risk and compliance professionals

**Want to know more?**

# Table of content

# COLLABORATE

At 3rdRisk, we believe **connecting** and **collaborating** are the first steps toward change. That's why our **platform** and **technology** revolves entirely around that.

# Introduction

**This whitepaper is a guide for risk and compliance professionals who are interested in or need to understand how to manage risks that come from working with other organisations.**

**Even if you are not doing much with this now, this topic will become more important in the future for compliance professionals, as this whitepaper will explain.**

In today's interconnected business landscape, no organisation works alone. Organisations often depend on other organisations for products, services, or support. This could be anything from getting parts from a supplier to using software from a tech company. But when we rely on these outside companies, known as third parties, risks are involved.

What if these organisations run into problems? They cannot deliver what you need on time, or they have a security issue with their software. These problems can affect your organisation too. That is where third-party risk management (TPRM) comes in. It is all about understanding and taking appropriate measures to mitigate these risks.

This whitepaper will look at ten essential considerations about TPRM – we refer to them as insights. We will discuss why TPRM is necessary, what risks exist, and how to deal effectively and efficiently.

We aim to make TPRM easier to understand, provide different perspectives on how you could look at it and give you valuable tips on bringing it into practice in your organisation. The tone of voice is informal and direct. We avoid technical jargon or explain it as much as possible.

As organisations grow and the world changes, managing third-party risks becomes more important. This whitepaper will help you see why it is vital and how staying on top of TPRM can make your organisation more sustainable, secure and compliant.

Let's dive in and explore these ten insights that will help you manage third-party risks better.


**Dave van Gulik**
Director, Trust Alliance
dave.van.gulik@trustalliance.com

**Bram Ketting**
CEO & Co-founder
3rdRisk

# What is third-party risk management?

**We refer to it as ‘TPRM’**

# What is TPRM?

TPRM is the process where you act out on risks **before** they exist and harm your organisation.

**TPRM is about dealing with risks that stem from working with other organisations and people not part of your organisation.**

**These other organisations might be suppliers who provide you with goods and services or partners you work with.**

Think of it like this: When your organisation works with another organisation, you share information, rely on their (ICT) services, and sometimes connect your systems. Suppose the other organisation is facing problems, like a data breach or a human rights violation, or they cannot deliver what you need on time. In that case, it can affect your organisation too. That is a risk.

**Third-parties** *are all external parties you do business with or have formal involvement with. So these are all your vendors, suppliers, service providers, business partners, joint ventures, alliances, distributors, resellers, agents, contractors, and many more.*

**Managing third-party risks** *is what we call third-party risk management. A specialised risk profession that is completely dedicated risks and compliance requirements that are associated with third-party relations.*

TPRM is the process where you act out on risks before they exist and harm your organisation. It involves checking how reliable, secure and sustainable other organisations are, ensuring they follow the same rules and standards as your organisation. It consists of reducing the impact as much as possible if something goes wrong.

It is like being careful and preparing ahead when you know there might be risks. By doing TPRM, your organisation can work well with other parties while keeping your organisation compliant with internal and external requirements.

# How to start with TPRM?

Let's explore how to start with third-party risk management.
To manage risks effectively, there are seven steps to follow.

## 1. Establish capability

**First, the governance needs to be put in place. Decide who will be in charge of third-party risk management.**

A person who sets out a plan for what your company wants to achieve with third-party risk management, decides what kind of risks to look at, and assigns people responsible for further establishing the capability. This person thinks about how to operate (locally in each office or centrally from one place), makes operational procedures, and chooses a tool to help do it well and efficiently.

## 2. Define requirements

**Decide what internal and external requirements need to be included.**

There are two types: the rules organizations make for themselves, like policies and standards, and the rules that come from outside, like regulations or industry standards.

## 3. Create an inventory of third-parties

**Make a list of all third parties you work with and the contracts you have with them.**

Some organisations might already have this list from their buying or procurement teams. Others might need to create it from scratch. It is important to know who in our organisation is in charge of each third party and contract, as they typically hold the most knowledge about the goods or services provided by the third-party.

## 4. Prioritise third-parties

**Decide which of these third parties is most important to your organisation and give each one a risk score.**

This helps you to decide which third parties you need to assess first and most thoroughly.

# HOW TO START WITH TPRM?

## 5. Perform assessments

**Assess these third parties. You can do this in different ways, like asking them to fill out a questionnaire, doing audits, or using information from other sources.**

You can use standard questionnaires or make your own based on well-known guidelines like ISO or NIST. Determine when to do these checks, e.g., before you sign contracts, when you renew one, after something big happens, regularly, or all the time. Or depending on how risky they are and if they are in the scope of the internal and external requirements.

## 6. Remediate risks

**Ensure all these assessments are completed, look at what they tell you, and report this to the right people in your organisation.**

If you find too high risks, take steps to mitigate them and bring them back to appropriate levels. This process must be documented and shared with relevant stakeholders about their role and responsibilities in remediating third-party risks.

## 7. Continuously monitor

**Finally, managing risks is a collaborative exercise.**

You need to keep an eye on your third-party landscape constantly, making sure it stays compliant and monitoring for evolving risks. Especially for high-risk third parties, you want to be notified promptly about issues that could impact your organization. It allows you to take action and reduce the impact timely. Therefore, you must define how to monitor your third-party landscape continuously.

# TPRM and the third-party lifecycle

Managing third-party risks involves several stages in the third-party lifecycle. Here's how TPRM plays a role in each of these stages.

Did you know that **3rdRisk** is Europe's leading cloud platform for third-party risk and compliance operations?

## Initiation

Create an initial risk profile for the potential third party. This profile helps you to understand how critical they might be to your business. It guides you to the subsequent phases, helping you decide the depth and type of assessments needed for them.

## Third-party selection

Gather external data about the third party and have them complete a self-assessment. This helps you to understand their operations and the risks they might bring.

## Contracting

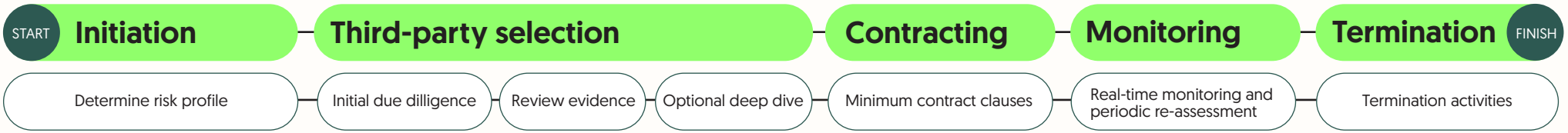
When we are ready to formalize the relationship, TPRM ensures that the contract includes the correct clauses. It also includes agreements on risks that need fixing and deadlines for these to be sorted.

## Monitoring

This is an ongoing stage where you keep an eye on the third party. You may use a mix of monitoring for adverse news and other data feeds, depending on the risks in play. Depending on how important the third party is, you might reassess them periodically, like sending out another self-assessment after one or two years.

## Termination

If the relationship ends, TPRM allows you to run a thorough checklist to ensure all contract agreements are met. It creates a smooth and compliant conclusion to the partnership.



# Why is this white-paper important?

In today's business world, it is becoming increasingly important to understand the risks that come from working with other organisations. Take regulatory initiatives like the Network and Information Security Directive (NIS-2), the Corporate Sustainability Reporting Directive (CSRD), the Digital Operational Resilience Act (DORA), the Corporate Sustainability Due Diligence Directive (CSDDD) and Deforestation frameworks as an example.

All these initiatives have in common that they require many organisations – from large corporates to small and medium enterprises – to thoroughly assess their entire supply chain and mitigate third-party risks. As a result, more compliance professionals are faced with this issue.

CLICK HERE **6 Reasons why you need third-party risk management**

# START WORKING SMART

Thanks to the 3rdRisk platform, we have been able to further professionalise our supplier risk management process, now have a better overview, and can allocate our time more efficiently.

**Farida Fouad**, Head of Legal and Privacy Officer, de Bijenkorf

**Visit the client case:**

CLICK HERE

Insight #1

# Organisations face increased third-party risks

# 1. Organisations face increased third-party risks

Organisations have always worked together, but some things have changed over the last decades, and this changes the risks that come with working with other organisations.

### More third parties, more complexity

Organisations today often have more suppliers than they used to. Whether they are trying to reach new markets or need different kinds of products and services, with more third parties, it takes more work to keep track of everything, leading to a higher risk.

> An average organisation works these days with thousands of different third-parties. According to Deloitte, 60% of organisations are now working with more than 1000 third parties. [1]

### Globalisation of supply chains

Many organisations rely on suppliers from all over the world. While this is good for finding the best products and prices, it also means dealing with risks like political changes, natural disasters, or transport problems in different countries. For example, a storm in one part of the world can delay shipments, causing problems for businesses far away.

**Case:** Evergreen Suez Canal blockage (2021).
A colossal cargo ship became lodged in the Suez Canal, a pivotal global shipping route. This led to substantial trade interruptions, affecting countless ships and highlighting the fragility of global supply chains to unforeseen blockages.

### Outsourcing of critical processes

It is common for organisations to outsource some of their critical tasks to other organisations. For example, their customer service or IT system-management. But, when you outsource

crucial tasks, you also rely more on other organisations which can introduce new and more significant risks.

## Cybersecurity threats

The cyber-attack risk increases as organisations and their third parties use more technology. A breach at a supplier's end can lead to severe problems for your organisation, like data leaks or system shutdowns. For instance, a hacker attacking a supplier could also access your organisation's information.

**Case:**
JBS Foods ransomware attack (2021). One of the largest global meat processors, JBS Foods, experienced a ransomware attack that forced shutdowns across Australia and North America, disrupting the worldwide meat supply chain.

## Regulatory changes

Laws and regulations around the world are changing all the time. If a third party does not keep up with these changes, it can cause legal issues for your organisation. This is especially true for Environment, Social, and Governance (ESG)-regulations and data protection rules.

## Reputation risks

Suppose a third party is involved in bad practices, like not treating workers well or harming the environment. In that case, it can hurt your organisations reputation. Customers today care a lot about how products are made and where they come from.

## Some figures

- Cyber incidents: 41% of the organisations that suffered a material incident in the past 12 months say it was caused by a third party. [3]
- Data breaches: 49% of organisations have experienced a data breach caused by a third-party vendor in the last 12 months. [3]
- 39% of organisations expressed that a primary factor in improving security frameworks is vendor support issues. [3]
- 61% of organisations aren't confident that their third parties would notify them if they had a data breach involving your organization's sensitive and confidential information.[3]
- 50% of organisations don't monitor third parties accessing sensitive and confidential information. [3]

[1] Deloitte (2023). The rising importance of third-party risk management.
[2] World Economic Forum (2024). Global Cybersecurity Outlook 2024.
[3] Ponemon Institute (2022)

Insight #2

# Risk and compliance today falls short

# 2. Risk and compliance today falls short

Let's discuss the challenges many organisations face in managing risks stemming from third-party collaborations. It is getting increasingly complex – and not just because the number of third-party relationships is increasing. Here's why.

### One-dimensional focus

Many risk teams spend most of their time and resources on what's happening inside their company, like their systems and processes. But it is probably equally important to know what processes and assets your third parties work with that you are managing. For some organizations, the percentage of assets and processes managed by third parties can be bigger than what their own organisation handles.

### Teams working in siloes

Teams in organisations often work separately - in siloes. For example, security teams might assess a part of the third-party landscape, but could be unaware of sustainability and legal teams doing the same. When different teams do not work together, getting a full picture of the risks posed by third-party collaborations is hard. Plus, there is no standard way of doing things or even talking about these risks, which makes it harder for everyone within the organisation to understand each other and work together effectively.

> 54% of organisations have insufficient visibility into the vulnerabilities of their supply chain. [1]

### Amount of work

There is much work involved in assessing and mitigating third-party risks. It can be overwhelming, especially if an organisation has to work with many third parties worldwide,

# Insight #2

each needing to adhere to many different regulatory frameworks. Keeping up with these varied regulations adds another layer of complexity to the already challenging task of managing these risks.

## Inadequate tools

The tools organisations use to manage these risks are not always good enough – that is fit for purpose. Many organisations still use basic tools like spreadsheets or rigid Governance, Risk and Control (GRC)-systems, which are not really designed for handling the processes involved with third-party risk management.

Spreadsheet efficiency
**decreases**
as the number of third parties
**increases.**

**TIP**

## No more spreadsheets

When dealing with more than 50 third parties, the use of spreadsheets can lead to challenges in data management and security. The efficiency of spreadsheets decreases as the number of third parties increases, leading to difficulties in data analysis and a higher risk of errors. Additionally, spreadsheets are not considered a secure method for sharing data with external parties. Moreover, they hinder good collaboration between different teams within the organisation as every team will likely have its own spreadsheet.

**TIP**

## Choose a smart TPRM-solution

GRC-systems are often rigid and not specifically designed for TPRM. Making these systems suitable for this purpose is time-consuming and expensive. Furthermore, as the workflows are not specifically designed for TPRM, using this technology still requires a relatively large amount of manual labour.

[1] World Economic Forucm (2024). Global Cybersecurity Outlook 2024.

Insight #3

# Compliance has an important role to play

# 3. The important role of compliance within TPRM

In managing third-party risk, compliance has one or more roles to play. Which roles can change depending on your organisation.

Suppose your organisation already has teams for managing operational risks and looking after sustainability. In that case, the compliance team might work differently.  But if no such teams exist, the compliance people might need to do more hands-on work.

Let's look at how compliance can have various roles in managing third-party risks depending on what your organisation is like.

### 1. Norms setter

Compliance defines the rules. They decide how the organisation should work with other organisations and set the requirements. In this role, compliance looks at laws, regulations and good practices, then use these to make internal policies and guidelines. Their job is to make sure the organisation knows the right way to do collaborate with third parites.

### 2. Risk assessor

This role is about 'hand-on' identifying, analysing, and responding to risks that are introduced by third-party collaborations. This could entail assessing how third-parties are handling data or if they follow environmental rules.

# Insight #3


## 3. Troubleshooter

The troubleshooter steps in when something goes wrong. If there is a problem like a data leak or a supplier not following the rules, they figure out what happened and how to fix it. They also work to stop the same problem from happening again in the future.

## 4. Change leader

This role leads the way when the organisation needs to change how it manages risks and compliance issues. If there are new regulations or if the organisation grows and faces new challenges, the change leader helps the organisation adapt. They make plans for new ways of doing things and guide the organisation through these changes.

## 5. Awareness creator

The awareness creator's job is to teach, inform and advise people in the organisation about risks and how to manage them. They make sure everyone understands the rules and why they are important. They also help people stay alert to any new risks or changes in the way the organisations need to work – independently or in collaboration with third parties.

Insight #4

# Regulatory obligations for third-party risk

# 4. Regulatory obligations for third-party due diligence are on the rise

Lately, there has been a big increase in the rules and regulations about assessing third-parties – that is third-party due diligence. This means many organisations have to be more careful about who they work with.

They also need to have measures in place to minimise the impact of third-party incidents. Let's explore some of these new regulatory frameworks.

## NIS-2

**Network and Information Security Directive**

This is a European directive that focuses on cybersecurity. It says that organisations that fall under the critical infrastructure need to make sure they put appropriate measures in place to manage cyber risks, including those stemming from third-party collaborations. At this moment, it is not yet known what those measures need to be, as the directive still has to be transposed to national legislation.

## DORA

**Digital Operational Resilience Act**

Also from Europe, DORA is about making sure organisations in the financial sector can handle technology issues without stopping their services. This includes measures for third-party ICT providers supporting critical or essential services within the organisation.

## CSRD

**Corporate Sustainability Reporting Directive**

This one is about organisations reporting on how they affect the environment and society. It means they also need to look at how their third-party partners are handling these topics.

## CSDDD

**Corporate Sustainability Due Diligence Directive**

CSDDD focuses on making organisations responsible for the environmental and social impact of their activities, including their entire supply chain.

## Deforestation Act

Aims to prevent supply chain contributions to deforestation, impacting procurement strategies for product sourcing.

## LkSG

**Lieferkettensorgfaltspflichtengesetz, in English German Supply Chain Act**

Applicable to all organisations operating in Germany, this regulation requires entities to assess human rights and environmental issues within the supply chain – so direct and indirect third-parties.

**Read more about TPRM regulations** CLICK HERE

Insight #5

# Collaboration among teams is key

# 5. TPRM is a multidisciplinary challenge – collaboration is key

Managing third-party risk requires different risk disciplines to look at the same supplier.

Collaboration among teams is essential as each team brings expertise and perspective, allowing for a thorough understanding of third-party risks.

Let's explore why having multiple risk disciplines working together is beneficial.

### Combining different expertise for full risk picture

Each risk team, like cybersecurity or legal, has its own area of expertise. By looking at the same supplier together, they can uncover a range of risks, from digital dangers to legal issues, providing a complete risk assessment.

### Identifying hidden risks

Different perspectives allow teams to spot risks that others might miss. For example, the finance team might approve a supplier based on their financial stability, but the IT team might find issues with their data security.

### Consistency in evaluation

Collaborative TPRM ensures that all teams use the same criteria and methods in evaluating suppliers. This consistency leads to more accurate and fair assessments.

### Effective risk mitigation strategies

Sharing insights among teams leads to better strategies for reducing risks. Teams can pool their knowledge to find the most effective ways to handle potential problems.

> Having multiple risk disciplines working together gives a **complete picture** of the risks involved in third-party relations.

### Efficiency gains

When an organisation has a streamlined, collaborative approach to third-party risk, it is easier for the third party to engage. They can provide their information once and know it is being reviewed comprehensively, rather than navigating requests from multiple disconnected teams. Also, for the organisation it is far more efficient: when teams collaborate, they avoid duplicating work and can streamline the assessment and follow-up process.

Insight #6

# A single pane of glass is essential

# 6. A single pane of glass is essential

In third-party risk management, it is helpful to have all relevant data about your third-party relations and associated risks in one place. This is what we call a ‘single pane of glass’.

It is like having one big window where you can see everything outside, rather than looking through lots of little windows.

Let’s see why this is so important.

### Everything in one view

Having a single pane of glass means all the information about risks, third-parties, and compliance requirements is in one system. You do not have to switch between different tools or documents. It makes it easier to get a clear picture of what’s going on.

### Saves time and effort

When everything is in one place, you save a lot of time. You do not have to spend hours gathering information from different sources – for instance using separate tooling for sending questionnaires to third parties, adverse media monitoring and screening. When you have a single pane of glass it is all right there for you, which makes working faster and more efficient.

### Improved decision making

With all the information in front of you in one view, you can make better decisions. You can see how changes in one area might affect another and understand the risks more clearly.

### Easier communication

It is easier to talk about third parties and their associated risks when everyone is looking at the same information. This way, teams can work better together and agree on what needs to be done.

### Rapid response to problems

If a problem, like a risk, suddenly worsens, you can see it right away with a single pane of glass. This means you can react quickly and take steps to fix the problem before it gets bigger.

In short, having a single pane of glass makes managing third-party risks much easier and more effective. It helps you see everything clearly, make good decisions, and react quickly to any issues.

Insight #7

# Ensure reporting and traceability

# 7. Regulators and supervisors expect reporting and traceability

It is not enough for many organisations to just manage risks from third-party collaborations; regulators and supervisors want to see proof of this. They expect organisations to report on how they manage these risks and to be able to trace back to how they handled them. Why is that important?


### Reporting to supervisors

More and more supervisory bodies such as the European Central Bank (ECB) or the Bundesamt fur Wirtschaft und Ausfuhrkontrolle (BAFA) in Germany want organisations to tell them how they are managing third-party risks. It is like an organisation showing its homework to prove it's doing things right.

### Traceability of actions

Traceability means being able to show the steps you took to identify, assess, mitigate, and monitor third-party risks. If a problem happens, like a data breach, you need to be able to show what you did to try to prevent it and how you responded. It is like keeping a detailed diary of your actions so you can show it if someone asks.

# Insight #7

**Example of reporting requirement:**
The German Supply Chain Act (LkSG) places organisations that have their central administration, principal place of business, administrative headquarters, statutory seat or branch office in Germany under the obligation to respect human rights by implementing due diligence obligations.

The core elements of the due diligence requirements include the establishment of a risk management system to identify, assess and minimise the risks of human rights violations and damage to the environment.

The Act defines the necessary preventive and remedial measures, makes complaint procedures mandatory and requires regular reports. A specific requirement is regularly reporting to the BAFA, the German supervisor.

The reporting requirement include amongst others the risks identified during self-assessments and alerts from adverse news monitoring, number of affected individuals and the actions that have been taken.

## Building trust

Good reporting and traceability help build trust. They show that an organisation is serious about managing third-party risks and staying compliant. This can be important for customers, partners, and even investors.

## Staying compliant

Regulations such as the German Supply Chain Act and the CSRD expect organisations to report on supply chain risks on a regular basis.

## Continuous improvement

Reporting and traceability also help organisations make better decisions in the future. By looking back at what happened and how they handled it third-party rsisk, they can learn and improve their approach.

Insight #8

# Invest in fit-for-purpose automation

# 8. Fit-for-purpose automation keeps the workload limited

When managing third-party risk, using the right kind of automation can make your life as a compliance professionals much easier. Fit-for-purpose automation means using software tools that are just right for the job. Let's see why this kind of automation is so helpful in managing third-party risk and keeping the workload manageable.

### Speeding up repetitive tasks

There are lots of tasks in third-party risk management that are the same thing over and over, like checking information, chasing stakeholders within the organisation, sending out self-assessments or creating a standardised report. Automation tools can do these repetitive tasks much faster than people, which saves a lot of time.

### Reducing human error

When people do the same tasks many times, they might make mistakes, like entering wrong information, sending the wrong questionnaire or forgetting to follow-up. Automation helps reduce these kinds of errors because software follow the same steps every time.

### Focusing on important work

With automation handling the routine tasks, you can focus on more important things – like following up on the risks identified during the third-party due diligence process.

### Handling large amounts of data

Fit-for-purpose tools are really good at dealing with lots of data. They can quickly sort through information from many different suppliers and spot any risks or problems.

# Fit-for-purpose tools offer the ability to monitor third parties **in real-time**.

For instance, the usage of tooling allow you to identify concentration risks, that is risks that arise from the fact that many of the organisations that you are working with make use of the same limited number of third parties.

## Monitoring third parties in real-time

One of the biggest advantages of automation is the ability to monitor third parties in real-time – for instance by using adverse media monitoring services or leveraging security, financial credit or sustainability risk ratings. This means you can see and react to any changes or risks as they happen, keeping you always one step ahead. For instance, if you see the financial credit risk rating drop, you can timely terminate the payments to a third party.

## Analysing information

Automation can also assist in reviewing evidence provided by third parties. It can pre-analyse this information, highlighting areas that need your attention, and guiding you on where to focus your efforts.

## Making reporting easier

TPRM platforms can also help with reporting. They can automatically collect and organise the information you need to report to regulators, supervisors, management and other important stakeholders in your organisation.

Insight #9

# The business case for TPRM is strong

# 9. The business case for third-party risk management is strong

There are many good reasons why managing third-party risks makes sense for organisations.

Here is a look at some facts that show why TPRM is not just important, but a smart choice for organisations.

### Cost of data breaches

Data breaches can be very costly. Studies have shown that when these breaches involve third parties, the costs can be significantly higher compared to breaches caused internally.[•] This means investing in TPRM can save a lot of money by preventing such expensive incidents or reducing the impact of it.

### Reputation and trust

Customers trust organisations that are secure and responsible. A survey found that businesses suffering a major third-party breach often face a decline in customer trust and, consequently, a drop in revenue. Effective TPRM helps maintain customer trust and protects the company's reputation.

### Regulatory fines

Failing to manage third-party risks can lead to breaking laws, especially with data protection and privacy regulations like GDPR but also with upcoming frameworks like NIS-2 and the CSRD. The fines for these breaches can be in the millions, making TPRM a key strategy to avoid financial penalties.

### Operational disruptions

Problems with a third-party can lead to operational issues, like production delays or service interruptions. This not only costs money but can also harm an organisation's long-term ability to compete. Good TPRM helps avoid these disruptions.

> Investing in TPRM can save a lot of money by **preventing expensive incidents** or reducing the impact of it.

[•] Deloitte (2023). The rising importance of third-party risk management.

# Insight #9

## Market advantage

Companies with strong TPRM are often seen as more reliable partners. This can be a competitive advantage, opening doors to new business opportunities and partnerships that others might miss.

## Insurance premiums

Some businesses find that effective TPRM can lead to lower insurance premiums, as it reduces the risk profile of the company. This can be a direct financial saving.

## Smart business decision

In summary, the business case for third-party risk management is strong. Not only does it help prevent costly data breaches, maintain customer trust, and avoid regulatory fines, but it also ensures smoother operations and can even provide a competitive edge in the market. Investing in TPRM is not just a matter of security; it is a smart business decision.

**Example:**

There is a clear business case for fit-for-purpose TPRM tooling. TPRM platforms automate repetitive tasks and let you work much faster than old-fashioned spreadsheets. Based on customer analyses using the 3rdRisk platform, Deloitte found that:

using the **3rdRisk platform** instead of spreadsheets **saves 140 hours** (approximately six days) **for every 10 suppliers.** If you deal with **100 third parties,** you will **save** work equal to about **0.75** of a full-time employee's annual hours.

**Calculate your FTE savings →**

Insight #10

# You don’t have to do it all yourself

# 10. You don't have to do it all yourself – partnering pays off

In managing third-party risks, remember that you do not have to handle everything independently. Specialised consulting firms offer a wide range of services for managing third-party risk.

They can help you set up your own third-party risk management (TPRM) capability, or they can take care of everything for you.

They advise you on how to implement a capability and manage third-party risks or do all the operational work on your behalf, depending on your need.

**Schedule a conversation to get in contact with one of our managed service partners.**

CLICK HERE

### Making things easier

Outsourcing all your third-party risk management work can be helpful, especially if your organisation does not have the people or know-how to do it or if you prefer not to handle it yourself.

This approach is great if you need to check many other third parties quickly or if buying the right technology for doing third-party risk management well is too expensive for your organisation. By outsourcing, you can ensure everything is handled correctly without investing a lot in new resources or technology.

# Conclusion

**Key takeaways**

# Key takeaways

In this whitepaper, we have explored the crucial aspects of TPRM and why it is so important for organisations today. From understanding increased third-party risks and the evolving roles of compliance, to the rising regulatory obligations and the benefits of automation, it is clear that managing third-party risks is a multidimensional but manageable challenge.

Key takeaways include the importance of having a single, comprehensive view for monitoring third-party risks and compliance issues, the growing expectations from regulators for transparency and traceability, and the strong business case for effective TPRM.

We have also seen how partnering with specialised consulting firms can offer a range of benefits, from expertise and cost-effectiveness to agility and scalability.

Ultimately, TPRM is not just about protecting your organisation from external risks and compliance violations; it is about embracing an approach that enhances operational efficiency, compliance, and strategic decision-making. Whether you build your TPRM capabilities in-house or outsource them, the goal is to create a system that is responsive, efficient, and aligned with your organisation's objectives.

As we look to the future, it is clear that the world of TPRM is evolving rapidly. Staying ahead will require a commitment to continuous learning, adaptation, and collaboration.

By embracing these principles, businesses can turn the challenges of third-party risk into opportunities for growth, compliance and resilience.

# CONNECT

Do you want more information on how to get started with third-party risk management, or what tools are available to help you run your third-party risk and compliance operations more efficiënt and effective?

Plan a demo →

Visit Trustalliance.com