LOGICGATE

Third-Party Risk:

Driving Cross-Functional Alignment Across the Vendor Lifecycle

TABLE OF CONTENTS

2 Introduction

2 Third-Party Risk: A First-Priority Concern
5 What are the Types of Third-Party Risk?
7 Who is Responsible for Third-Party Risk?

8 Current State of Third-Party Affairs

8 Risk Assessments
11 What to Assess Against
13 Tools
15 Common Mistakes
16 What are the Consequences?

17 The Way Forward

18 The Risk-Based Approach
19 Ongoing Assessments
21 Third-Party Security by Design
24 Centralization

26 Where LogicGate Can Take Your Organization

Today, **20–50%** of large organizations' total workforce is outsourced, according to estimates.

INTRODUCTION

THIRD PARTY RISK: A FIRST-PRIORITY CONCERN

From suppliers to software to human resources, businesses increasingly don't go it alone.

In recent years, we have witnessed the proliferation of the extended enterprise—companies relying on a network of third-party vendors to provide them with organizational value and competitive advantage. While outsourcing of some form has always existed, globalization and the Internet have caused the use of third-party vendors to increase exponentially. Whereas companies used to only rely on third parties for a few, non-core functions, today they're increasingly outsourcing critical functions to find cost savings and efficiencies.

The strict brick-and-mortar business is long gone. Physical buildings and conventional employees no longer define organizations—layers of relationships go beyond these walls to include suppliers, vendors, outsourcers, service providers, contractors, subcontractors, consultants, temporary workers, agents, brokers, intermediaries, and many more. Even for the old-guard organizations that have weathered the tides, the modern organization is a tentacular mess of relationships and interactions that flow beyond traditional business boundaries. Complexity grows exponentially as these interconnected relationships, processes, and systems proliferate and embed themselves in the organization's processes over time. Today, 20–50% of large organizations' total workforce is outsourced, according to estimates (source: *WSJ*).

Risk and compliance challenges no longer stop at traditional organizational boundaries.

Given this new reality, organizations are faced with a growing awareness that they stand in the shoes of their third parties. Risk and compliance challenges no longer stop at traditional organizational boundaries. Establishing the wrong business relationships—or allowing current ones to sour through poor management—can force an organization to confront extreme reputational and existential threats. Thus, third-party problems are the organization's problems, directly impacting brand and reputation while increasing exposure to risk and compliance matters. When questions of business practice, ethics, safety, quality, human rights, corruption, security, and the environment arise, the organization is held accountable, and it must ensure that third-party partners behave appropriately.

The biggest challenge for organizations is to provide the appropriate oversight of these third parties. While interconnectivity can help to establish a more dynamic and collaborative working relationship, it also exposes organizations to a host of risks—including damage to reputation, compliance status, and even cyberattacks. Just as firms were often slow to move on from perimeter-based defenses and tackle threats to their mobile workforce, the majority of companies are struggling to keep track of their network of third parties and the risks they may be introducing.

Third parties have become preferred vectors for cyberattacks.

Cybercriminals routinely target suppliers and partners in order to exploit connections to larger, more valuable targets. Given the expanding partner networks, the attack surface that they can target is rapidly expanding as well—from principle systems to connected devices, supply chains, and more. In fact, third parties have become preferred vectors for cyberattacks (source: Ponemon Institute).

If your company employs third parties, then the responsibility falls to you and your employees to manage the risk they bring. But how do you go about designing and implementing your third-party risk management program for maximum effectiveness?

We'll dive deeper in this eBook. But first, let's take a look at what Third-Party Risk is.

TARGETING TARGET

Target can attest to the importance of network security when companies build interconnected networks with suppliers and vendors. In its high-profile third-party data breach incident, a refrigeration vendor was hacked and allowed malware to spread through the network and access POS system information. This could have been prevented through simple network segmentation, which would have then prevented the hackers from connecting their systems to the critical parts of Target's networks. Instead, hackers were able to steal over 40 million credit cards from nearly 2,000 Target stores.

Risks typically fall into one of five categories based on impact to the principle business.

WHAT ARE THE TYPES OF THIRD PARTY RISK?

The risks that may arise from an institution's use of third parties are numerous and diverse. Some of the risks are related to the underlying activity itself, similar to the risks faced by an institution directly conducting the activity. Other potential risks arise from—or are heightened by—the involvement of a third party. Failure to manage these risks can expose an institution to regulatory action, financial loss, litigation, and reputational damage, and may even impair its ability to establish new, or service existing, customer relationships.

While the risk landscape is constantly evolving and new threats are ever on the rise, risks typically fall into one of five categories based on impact to the principle business.

Financial Risk: Risk that a third party could damage financial performance. For instance, the company could fall short of revenue goals after a supplier provides a faulty component, impairing sales.

Reputational Risk: The risk arising from negative public opinion created by a third party. Dissatisfied customers, inappropriate interactions, poor recommendations, security breaches, and legal violations are all examples that could harm a company's reputation and standing.

Regulatory/Compliance Risk: Risk that a third party will impact compliance with laws, rules, or regulations, or from noncompliance with internal policies or procedures. For example, if a supplier violates labor or environmental laws, the principle organization can still be found liable and face fines.

Operational Risk: Risk that a third party could cause loss from disrupted business operations. Examples include a software vendor being hacked, leaving a company with a downed system, or a supplier being impacted by a natural disaster.

Strategic Risk: Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals. The use of a third party to perform critical functions can expose an institution to strategic risk.

INDUSTRY EXAMPLES

Financial Services

Regulatory scrutiny stemming from the 2008 financial crisis now reaches beyond banks to the companies that supply them. The Consumer Financial Protection Bureau (CFPB) and other regulators hold financial institutions responsible for not only their own actions, but for those of their vendors and suppliers. In recent months, Capital One, Discover Card, and American Express have paid a total of $525 million to settle complaints of deceptive selling and predatory behavior by their third-party suppliers. This new regulatory thrust poses a big challenge for financial institutions, which typically have more than 20,000 suppliers (source: McKinsey).

Healthcare

Hospitals and healthcare systems rely on hundreds of vendors every day to perform critical functions. These services can include hospitality, transportation, security, IT, transcription, laundry, patient care, and waste removal—to name but a few. In a highly regulated market such as healthcare, these relationships can pose big risks.

WHO IS RESPONSIBLE FOR THIRD-PARTY RISK?

Historically, third party relationships (and the risks that exist within them) have been the province of procurement departments. The process went something like this: Procurement would identify potential savings from outsourcing, the legal department would draft a contract, and that would be that—few would bother following up on the relationship. Thankfully, most large organizations have recognized that this doesn't cut it any more. The responsibility has extended from Procurement and Legal to functions like IT Security, Compliance, frontline business managers, and more. Everyone should play their part in managing the risks.

In practice, a company's third party network is typically managed by an executive in the procurement department, with input from IT Security. This might be a Vendor Risk Manager, who reports to a Chief Information Security Officer (CISO) or VP of Information Security. The program should also involve Compliance officers and the legal team. It's imperative that these groups work together to keep the company's overall Third-Party Risk in check.

While these departments may handle the day-to-day aspects of a company's third party ecosystem, sound Third-Party Risk Management principles need to start at the top: the C-suite and board of directors. This is where the culture of proper Third Party Risk Management begins. An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships—to the same extent as if the activity were handled within the institution.

BY THE NUMBERS

Modern organizations rely on vast and intricate networks of third-party suppliers and partners for essential operations. While the idea of suppliers is not new, the network of connections has become far denser and more complex. Not only are firms relying on a greater number of third-parties, but these suppliers are more often entrusted with access to sensitive data and mission critical systems.

583 average number of third parties with which companies share sensitive and confidential data

59% of companies have experienced a data breach caused by one of their suppliers or third parties

34% of companies keep a comprehensive inventory of their third parties

69% blame a lack of centralized control for their inability to keep track of third parties

16% of companies say they effectively manage third-party risks

SOURCE: PONEMON INSTITUTE

The risk assessment is fundamental to the initial decision of whether or not to enter into a third-party relationship.

CURRENT STATE OF THIRD-PARTY AFFAIRS

In Chapter One, we showed how difficult it can be for companies to manage the complex web of relationships they have with their third-party vendors, as well as consequences that can occur when things go awry.

In this chapter, we'll explore how companies typically manage their vendors. These include industry best practices—as well as some bad habits that are easy to fall into.

RISK ASSESSMENTS

A key objective of any third-party risk management process is to determine the highest-risk third-party relationships and then put activities in place to mitigate these risks to a tolerable level. The first piece of that objective—determining the highest-risk third-party relationships—is accomplished through something called a risk assessment. The risk assessment is fundamental to the initial decision of whether or not to enter into a third-party relationship. These activities should also be repeated periodically in order to monitor and assess the third party relationship on an ongoing basis—something we'll explore in a later chapter.

A number of key stakeholders should participate.

First, the relationship must be substantiated and backed by strategic business needs. It is key for management to develop a thorough understanding of what the proposed relationship will accomplish for the institution, and why the use of a third party is in its best interests. Thus, the first step in the risk assessment process should be to ensure that the proposed relationship is consistent with the institution's overall business strategy.

Next, management should analyze the benefits, costs, legal aspects, and potential risks associated with the third party under consideration. A number of key stakeholders should participate in this step, particularly those business owners responsible for managing the relationship after Procurement's execution of the agreement. Certain aspects of the risk assessment phase may also require input from internal auditors, compliance officers, technology officers, and legal counsel.

The assessment phase should also identify key performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing success of the relationship. Some of those include processes for the following:

Issue Reporting and Resolution: Even the most successful business relationships encounter bumps in the road. Companies need a process for capturing the issues that arise in third-party relationships. Issue reporting processes may be internal and done by employees and management, by the third parties themselves, or through external sources such as customer complaints.

Performance Monitoring: Performance monitoring processes should monitor the health of the relationship, satisfaction of service-level agreements, and value the relationship is providing.

Risk Monitoring: Risk monitoring processes identify and evaluate potential risks relevant to each third party relationship throughout their lifecycle in the organization.

Compliance Monitoring: The processes in place to monitor relationships for ongoing conformance to compliance requirements.

Audits and Inspections: The processes in place to exercise right-to-audit clauses and perform onsite inspections of third-party premises and facilities.

The assessment framework should be understood throughout the organization and used uniformly.

WHAT TO ASSESS AGAINST?

For an assessment to be worthwhile, it needs to begin from a commonly understood baseline—or framework— to determine whether the Third-Party Risk Management Program is accomplishing its key objectives. Organizations will have different objectives for the program, so it's natural that they will employ different measurement frameworks as well. What matters is that it's understood throughout the organization and used uniformly.

Below are a few common categories of frameworks a company might choose.

Security Frameworks: Several independent bodies publish frameworks for companies to follow in order to be certified as secure by the body's standards. Two of the most recognizable cybersecurity frameworks are those published by the International Organization for Standardization, or ISO, and the National Institute for Standards and Technology, or NIST. Both frameworks offer standards, guidelines, and best practices to manage cybersecurity-related risk.

Regulatory Frameworks: Regulatory frameworks are sets of guidelines and best practices created due to the need to comply with different government mandates. Organizations must follow these guidelines in order to perform different business activities without running afoul of the law—such as issuing stock, doing business with government agencies, or operating a public utility. One common regulatory framework that affects third-party data is the European Union's General Data Protection Regulation, or GDPR. The 2018 law holds companies accountable for the personal data they retain concerning any citizen in the European Union—employees, customers, and third-party business partners included.

Policy Frameworks: Policy frameworks are typically created by the company for internal governance and are designed to provide guidance for all business units and functions. While unique to the company that created it (and even different divisions or geographies), a robust policy framework should include an overarching third-party risk management strategy, minimum standards for control, policies and procedures for different functions, and legal considerations.

Industry Frameworks: Many industries have their own sets of recommendations for proper Third-Party Risk Management. These are usually highly specific to the type of business being conducted in that industry, and published by professional associations or other governing bodies to establish a common language and understanding that can be used across the industry. In the healthcare industry, for example, the Health Insurance Portability and Accountability Act—better known as HIPAA—governs the protection and exchange of patient health and medical information.

Many different tools exist to help managers stay on top of their third-party risk programs.

TOOLS

Many different tools exist to help managers stay on top of their Third-Party Risk Programs. With different levels of ease and effectiveness, each approach gives managers the power to track and monitor data, facilitate workflow within and across business units, and monitor the company's overall risk profile. As the tools progress upwards on the sophistication scale, additional capabilities such as data analytics, centralization of risk exposures, and workflow automations may also be layered in.

Documents, Spreadsheets, and Email: Manual spreadsheet and document-centric processes are by far the most prevalent, despite their obvious shortfalls. These approaches are prone to failure as they bury the organization in mountains of data that is difficult to maintain, aggregate, and report on. The organization ends up spending more time in data management and reconciliation, as opposed to active risk monitoring and remediation.

Point Solutions: Point solutions are tools used to solve one particular problem without regard to related issues. While very common, they pose problems of their own. Often, point solutions are deployed for very specific risk and regulatory issues—creating a wide array of solutions that do very similar things but for different purposes, introducing a high degree of redundancy with little communication between resources.

Enterprise Resource Planning Solutions: A number of solutions exist in the ERP space, offering robust capabilities in the areas of contract management, transactions, and financial analytics. They are often weak when extended to third-party risk management, however.

Enterprise GRC Platforms: Many of the leading enterprise GRC platforms have third-party (or vendor) risk management modules. However, these solutions often have a predominant focus on risk and compliance and do not always have a complete view of performance management of third parties.

Third Party Management Platforms: These are solutions that are built specifically for third party management and often have the broadest array of features to support the breadth of third party management processes. They are good at incorporating both the business performance of third parties as well as risk and compliance considerations.

COMMON MISTAKES

Lack of Common Standards: Third-party risk management practices are bound to vary significantly across industries. Some of this is due to organizational differences, but there is a broader problem caused by the absence of commonly observed best practices. For example, the composition of teams conducting due diligence and onboarding varies enormously from firm to firm.

Lack of Centralization: Many firms manage third-party risk case-by-case or with numerous systems, policies, and frameworks. While this addresses most of what is expected of a third-party risk program, it does not provide a comprehensive, consistent framework that can be monitored and analyzed from one point of view. Thus, firms risk failing to capture the full lifecycle and range of third-party relationships, which may create inefficiencies, blind spots, and inconsistencies.

Not Incorporating All Stakeholders: Too often, the departments (often procurement) involved at the beginning of a third-party relationship are different than those who must manage it going forward. This creates the potential for gaps in oversight and communication—easily remedied by including all relevant personnel from the get-go.

Inconsistent Assessments: Most companies recognize the importance of doing risk assessments at the outset of a relationship, but the energy to stick with them at regular intervals can wane over time. Competing priorities and the uneventful nature of successful relationships often combine to push ongoing assessments lower on the list of a manager's long to-do list.

Considering Risk Management Too Late: It happens at every company: a division will create a great-looking business case and get approvals, only to then discover that there are issues with sourcing some of the vendors. Entire projects can be derailed because third-party risk management was not considered at the outset.

WHAT ARE THE CONSEQUENCES?

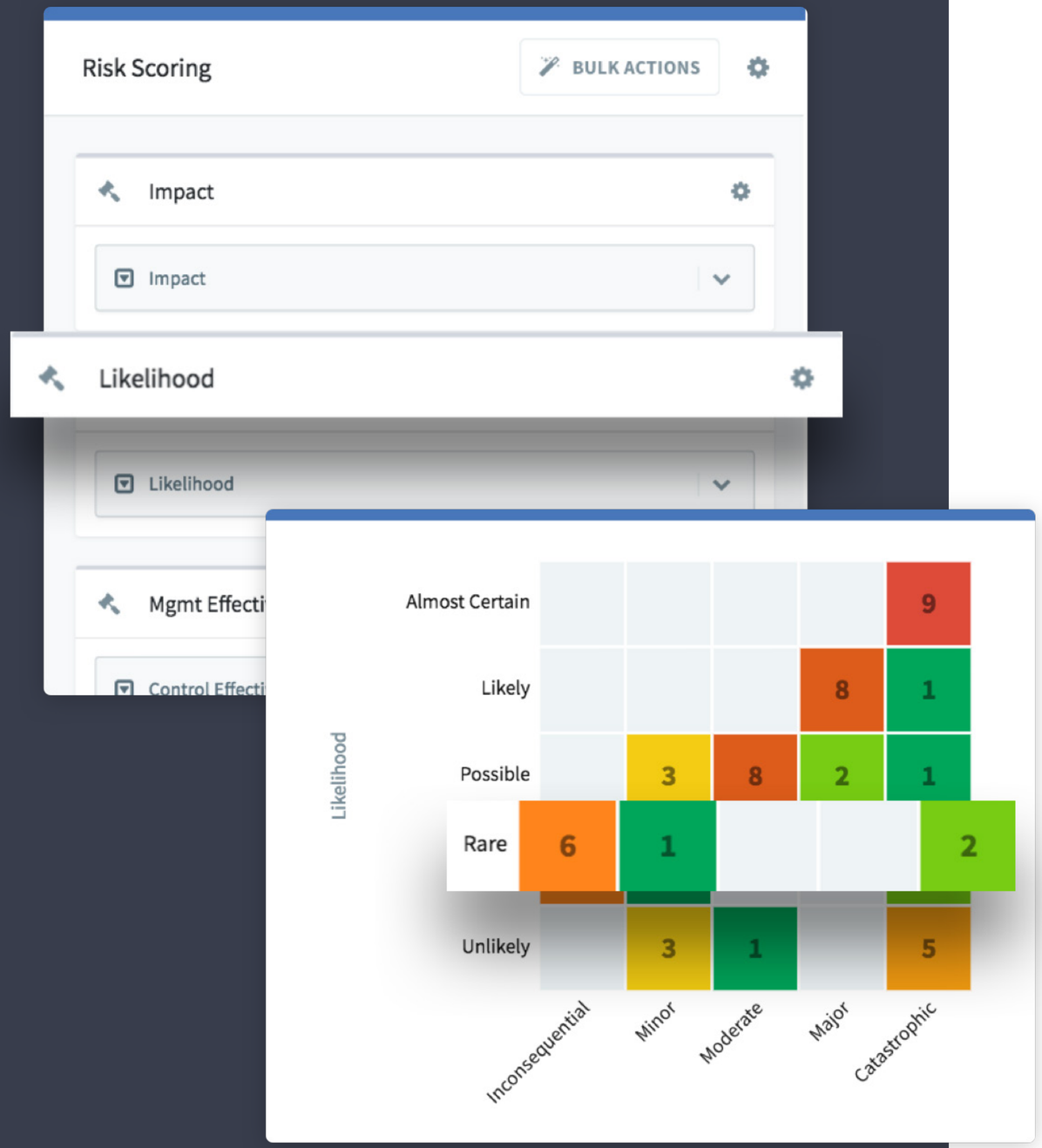
The consequences for the above mistakes can range from simple inefficiencies to catastrophic outcomes. At the benign end of the spectrum, poor third-party risk management can complicate approval processes or undermine sales. This often happens when the different stakeholders are operating from different playbooks and entering the process at different times. As an example, Procurement may source, vet, and onboard a vendor before ever engaging with IT Security—who subsequently discovers a major red flag with the vendor's data-security practices. Thus procurement wasted a great deal of time, money, and energy with the third party, when they could have engaged IT Security much earlier in the process and uncovered the issue from the start. Many companies have been stuck with bad contracts because their different departments aren't in sync with the overall Third Party Management process.

More dire consequences can occur when the third party's poor information security standards aren't discovered at all. This can happen due to oversight at the beginning of the process, or when the third party's security slips over the life of the contract and the lapse goes unseen. Either of these scenarios serve to increase a company's overall risk exposure while senior management remains in the dark. It happens at companies of every size and maturity level, and opens the door to data breaches like the kind that affected Target from Chapter 1.

THE WAY FORWARD

In Chapter 2, we described the issues companies confront when implementing and executing a Third-Party Risk Management program. Among these were a lack of standards, inconsistencies, and poor engagement across departments. These issues can be remedied by better communication and internal alignment—straightforward ideas that become complicated in practice. Still, they serve as useful goals when seeking improvement in the company's strategy vis-a-vis its network of third party relationships.

In Chapter 3, we'll offer some recommendations for how companies can chart a new course for their management of third parties, and some benchmarks against which they can measure their retooled program.



THE RISK-BASED APPROACH

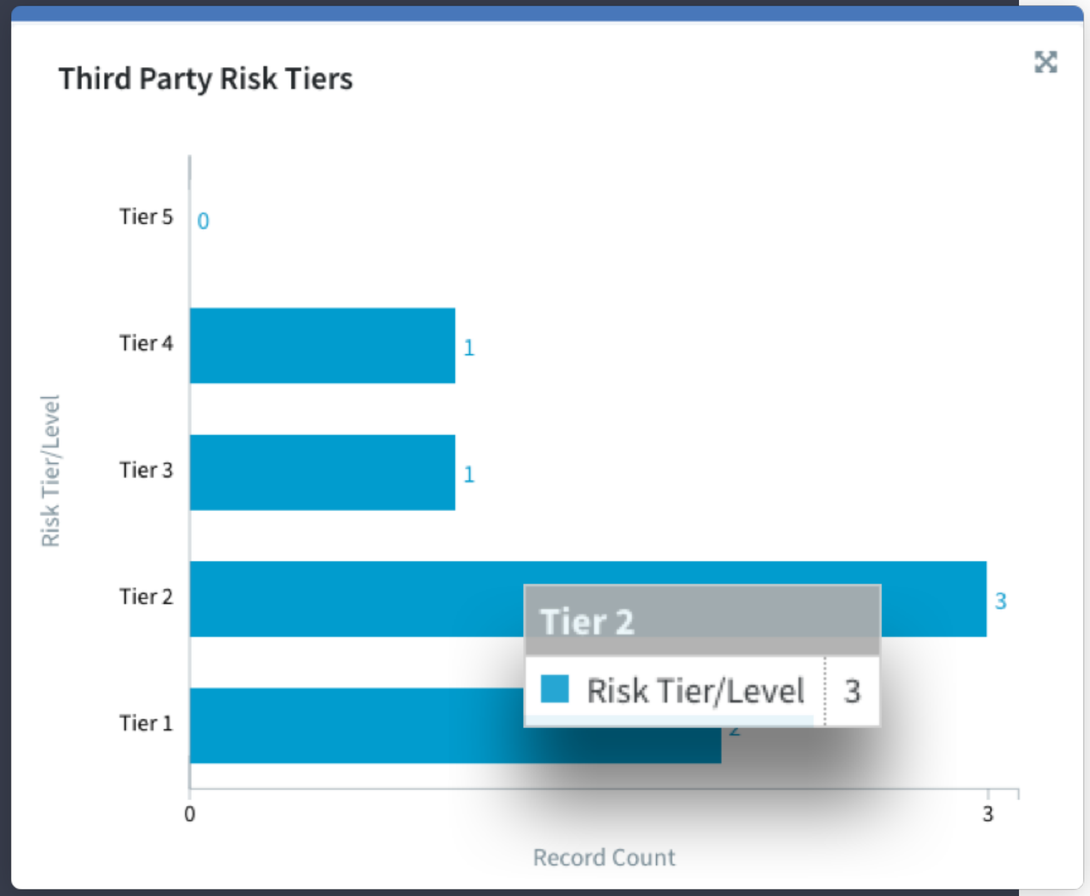
With a complete inventory of third parties and their relative risks in hand, the firm can categorize its supplier relationships based on the level of risk to organizational objectives. Even a simple system of "high," "medium," or "low" risk categories can be useful. An effective segmentation helps the firm efficiently allocate resources.

Firms often use two approaches to assign their third parties to risk tiers:

- In the **score-based** approach, the firm conducts due diligence across all dimensions, and uses the results to develop a composite risk score. While very thorough, the approach can be onerous and resource-intensive for many organizations.

- In the **rules-based** approach, the firm defines some rules or criteria tied to breakpoints to streamline the assignment to a risk category. The approach entails only the risk assessment and due diligence activities needed, making it faster than the score-based approach.

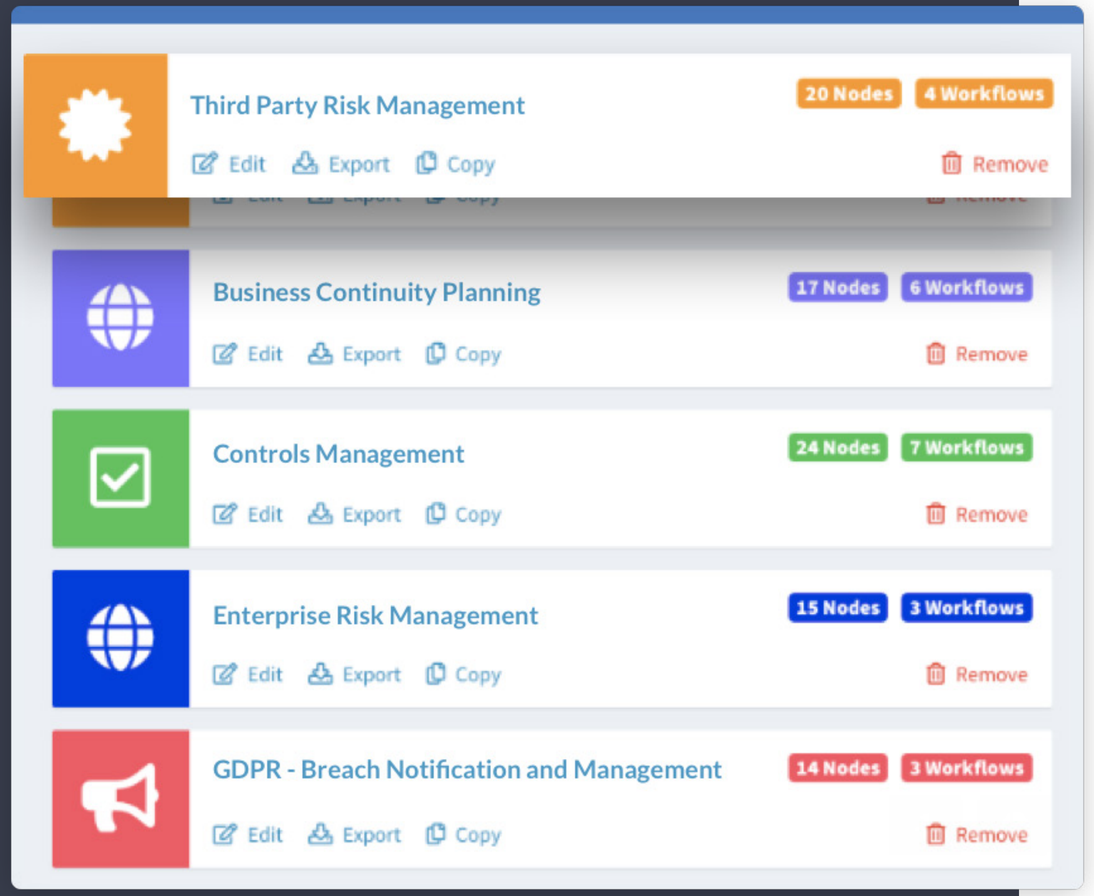
Managers should identify the risk categories deemed critical to the organization and then develop each category's weighting criteria—which will inform requirements like assessment and touchpoint frequencies. For each third party, a cross-functional team should then score the risks based on impact and likelihood so that the third parties can be categorized into tiers and prioritized. Once all third parties are scored and subsequently tiered, managers can develop risk mitigation plans and allocate resources to focus on the higher-risk third parties.



ONGOING ASSESSMENTS

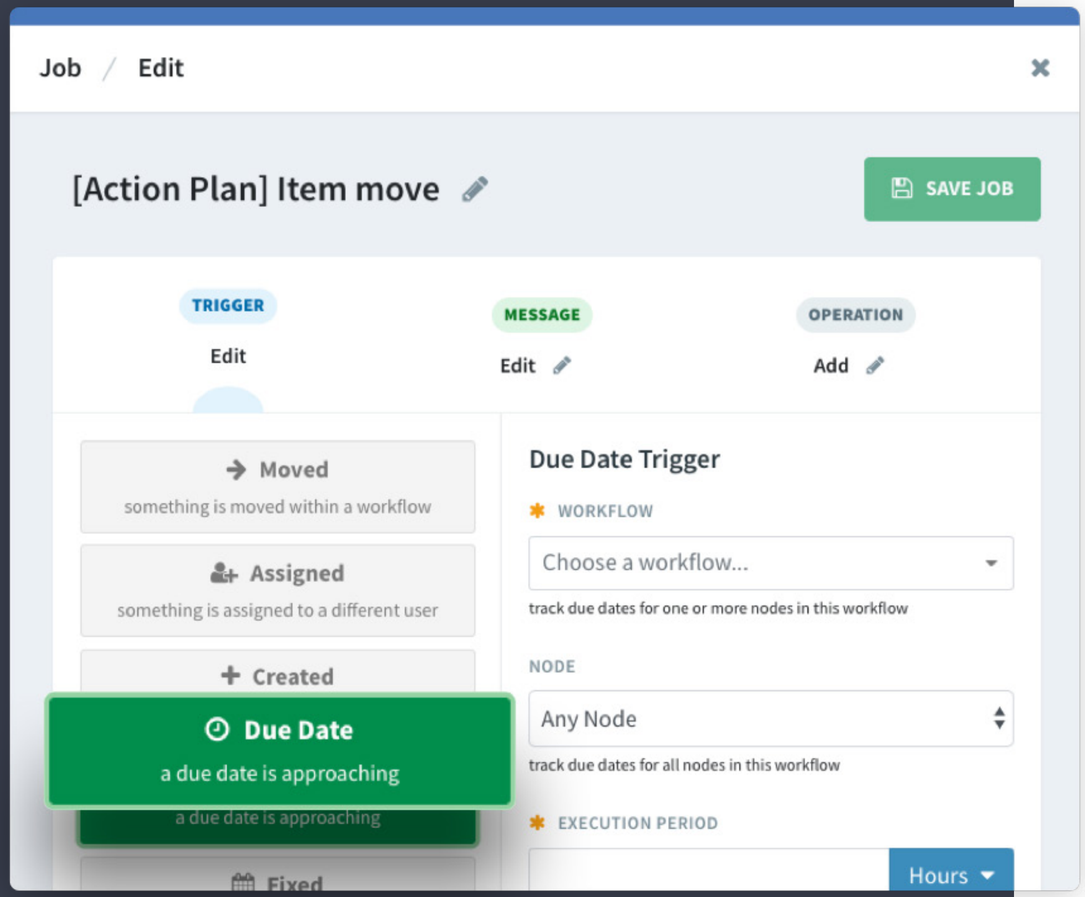
Third-party risk must be monitored throughout the relationship lifecycle, not just at the onboarding stage. Considering how rapidly threats can emerge and evolve, the findings from one risk assessment can become outdated quickly—even in a matter of days. A company previously rated as secure can quickly become a liability.

Current third party assessment tools include audits and questionnaires—methods that are useful for intermittent snapshots of a company's risk profile. However, they have a major shortcoming: they fail to provide the continuous, evidence-based assessments companies need to understand their vendor risk over time. Ongoing monitoring should capture fluctuations in risk exposure after the third party has been onboarded, and limit the implications of potential failures in the due diligence process. It should also help to ensure third parties continue to fulfill the firm's needs and abide by contractual arrangements. Monitoring should be tailored to third-party risk profiles, including more frequent and thorough check-ins with high-risk entities and simple monitoring for less severe threats.



Unfortunately, many companies recognize the value of ongoing re-assessments but fail to follow through. The reason behind this is simple: at most companies, assessments are a time-consuming and manual undertaking. Many managers also recognize that they are only equipped to take a snapshot of their third-party ecosystem, and elect to forgo it because the findings will become obsolete soon anyway.

Today's business landscape demands a much more dynamic approach to dealing with third-party risk. Implementing a third-party monitoring system that is able to alert the organization to new threats in real time will help to identify risks and enable the organization to work with their partner to address them before a serious incident occurs.



THIRD-PARTY SECURITY BY DESIGN

Security by Design—often styled SbD—is an approach to vendor management borrowed from the world of information security. In the IT context, security personnel formalize the design of their data infrastructure and automate security controls so that security exists throughout the development process. The Third Party context is similar: SbD makes security a chief concern of every part of the third-party lifecycle, from preliminary sourcing all the way to retirement of third party contracts. As a result, managers spend their time developing the system that governs the company's entire third-party ecosystem, as opposed to managing relationships and issues on a spot basis.

SbD is concerned with establishing standardized, repeatable, and automated processes so that security and assessment standards remain consistent across multiple third party relationships. Rather than retroactively enforcing security policies— and always being behind—SbD principles are part of the planning process from the beginning. Managers can check their third party contracts against pre-approved templates, and move the process along through the proper channels with efficiency. Managers no longer need to be consulted on each and every decision, which means less repetitive busy-work and more focus on real issues.

The entire process is designed for efficiency, collaboration, and completeness.

It also means getting each of the departmental stakeholders involved in the third party process as early as possible. No longer will procurement own the relationship and then hand the reins over to business unit managers after onboarding has concluded. Procurement, managers, legal, compliance, and security all play a role from start to finish. It presents an opportunity for security professionals to get what they have always dreamed of: introducing security earlier in the development process. It also ensures that the contractual process doesn't get mired in a gauntlet of sign offs and approvals—the entire process is designed for efficiency, collaboration, and completeness.

How can a company get started with SbD? Below are some key items to consider.

Define standards for selecting new vendors—and ensure each business unit plays a role in the creation of those standards. Keep the business units informed and engaged at all times by clearly outlining their roles in the development process. In addition, each relevant business unit should play a part in the delivery and upkeep of the final standards document.

Review the vendor list on a regular basis. With many companies now relying on hundreds or even thousands of partners and suppliers, prioritization is an essential first step to managing third-party risk. Firms should solidify the list of all connections and rank them based on factors such as security posture, importance, and the potential impact of a breach. Without a firm understanding of the current vendor ecosystem, design cannot take place.

Create a robust set of due diligence procedures, coupled with well-documented analyses. There should be a checklist of due diligence requirements that must be satisfied, and then double-checked to ensure conformity. Ensure that document collection is comprehensive and that the artifacts gathered are thoroughly analyzed by experienced subject matter experts (SMEs).

Use an initial vetting questionnaire with high-level, need-to-know security concerns early in the process. This shorter checklist will address the major questions of IT Security and Compliance, without slowing down the onboarding process. A more thorough assessment can be performed if needed once an initial risk rating has been determined based on the initial questionnaire.

Implement strong vendor contract management practices, and keep them up-to-date through accurate tracking of key dates and terms, lest an important renewal or termination date be missed.

Update all vendor documentation on a regular basis, including contracts and internal reports. The frequency of updates should be dictated by the degree of risk inherent in a particular division, product, or service. Repeatable processes will ensure this is completed routinely and efficiently, rather than forcing managers to start from scratch every time.

A third party program can’t be designed effectively if its constituent parts can’t be made to work together.

CENTRALIZATION

Third party management fails when it is managed as a system of parts that do not integrate and work as a collective whole. When the program is immature, this often involves information that is scattered in various parts of the company, redundant, and inaccessible. Recommended activities like continuous assessments and scoring are only possible when information is readily available and controlled from one central location. It’s also a foundational piece of Security by Design—a third party program can’t be designed effectively if its constituent parts can’t be made to work together.

A centralized third-party management program will be able to integrate information from across third-party management systems, ERPs, procurement solutions, and third party databases. This requires a robust and adaptable information architecture that can model the complexity of third party activities, which encapsulates a number of moving pieces. Within a centralized Third-Party Risk Management program, business users should have access to:

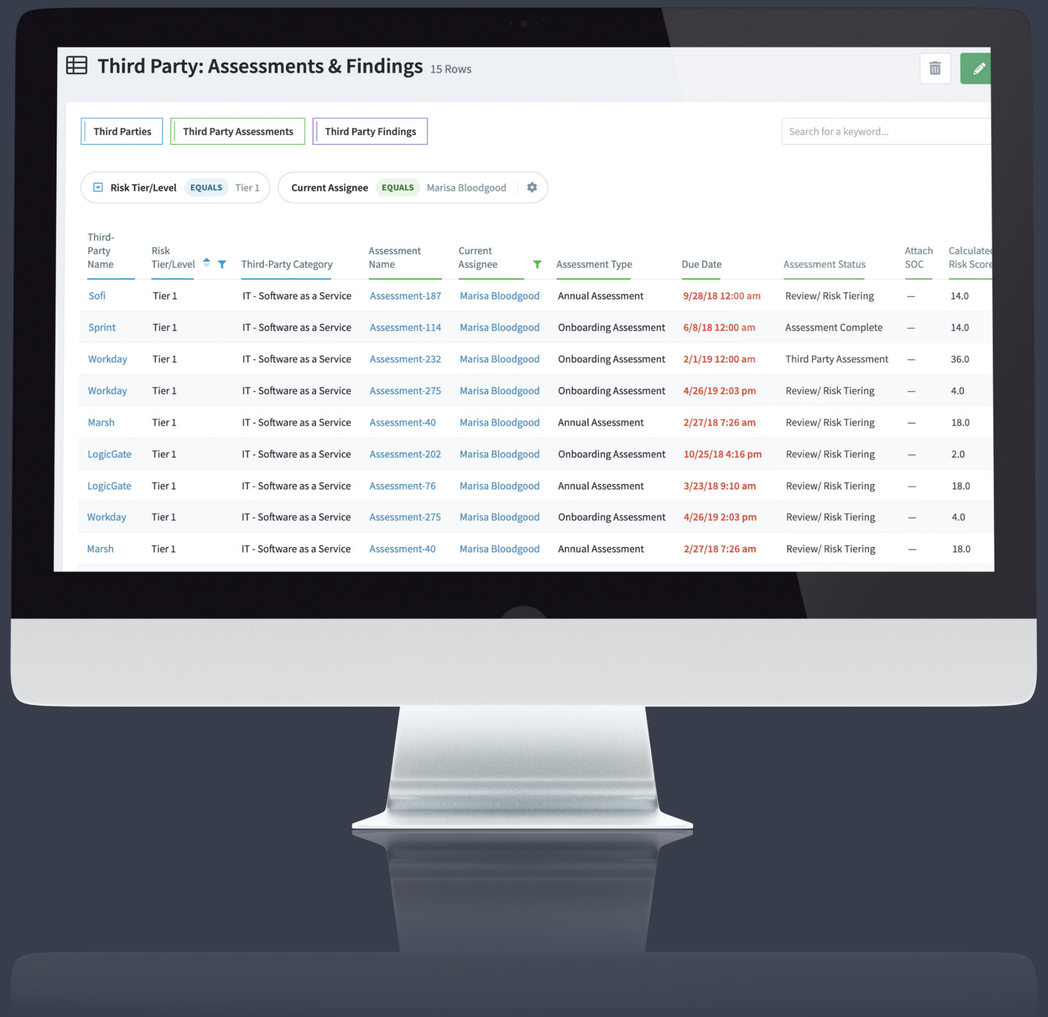
- **Master data records:** This includes data on the third party such as address, contact information, and bank/financial information
- **Third party compliance requirements:** Listing of compliance/regulatory requirements that are part of third party relationships
- **Third party risk and control libraries:** Risks and controls to be mapped back to third parties
- **Policies and procedures:** The defined policies and procedures that are part of third party relationships
- **Contracts:** The contract and all related documentation for the formation of the relationship
- **SLAs, KPIs, and KRIs:** Documentation and monitoring of service level agreements, key performance indicators, and key risk indicators for individual relationships as well as aggregate sets of relationships
- **Third party databases:** The information connections to third party databases used for screening and due diligence purposes such as sanction and watch lists, politically exposed person databases, as well as financial performance or legal proceedings
- **Transactions:** The data sets of transactions in the ERP environment that are payments, goods and services received, etc.
- **Forms:** The design and layout of information needed for third party forms and approvals
- **Communication:** Notifications to IT security, procurement for new vendor requests

WHERE LOGICGATE CAN TAKE YOUR ORGANIZATION

Make no mistake: the recommendations laid out in Chapter 3 are not quick fixes.

However your company currently handles its Third-Party Risk Management, performing ongoing assessments or implementing Security by Design principles are never easy. They require that managers first step back from their limited, day-to-day perspective and get a holistic view of the entire third party ecosystem. Managers must also carry the torch as internal champions of program reform, which usually entails convincing other departments that there's a better way forward. It can be a thankless task at times.

The right technology can help with the transition. A robust Third-Party Risk Management program helps companies verify third-party access and ensure that every stakeholder follows proper procedures. Timely and accurate certifications and attestations are small but effective steps to ensure appropriate parties follow the right protocols every time.



LogicGate's Third-Party Risk Management software is an agile solution that adapts and grows with your organization and its needs. Putting an automated system in place to manage your company's compliance standards can help significantly reduce the risk of fines and reputational damage. If it plays even a small part in preventing a data breach, the return is inestimable.

LogicGate can help your company solve its most critical Third-Party Risk Management needs:

- **Protect the integrity of your third-party relationships.** LogicGate helps your organization automate its vendor risk assessment program to ensure third-party relationships are protected from vulnerabilities. You'll build vendor risk management processes that are robust, repeatable, and flexible enough to grow with your business.

- **Create a central vendor management platform**, allowing for cross-functional collaboration among procurement, compliance, and risk, as well as tracking of assessment findings and remediation activities.

- **Customize your workflow** to include steps that match your organization's procurement or outsourcing process, including assessments and risk-scoring procedures.
- **Use conditional logic** to send the appropriate questions/questionnaires to vendors based on the type of service they provide, their risk level, geography, and other attributes.
- **Get started quickly** with LogicGate's best practice templates.

LOGICGATE