NAVEX GLOBAL®

The 7 Step Guide to
THIRD PARTY RISK MANAGEMENT

The Case for Effective Third Party Risk Management

Two companies face the same challenge: a major disruption in their supply chain. The first company is caught flat-footed and spends the next 18 hours juggling suppliers and working the phones to apologize to customers for their late shipments. The second company got an early heads up from its online monitoring service that a key supplier was struggling. The risk manager interpreted the increased risk to operations and immediately alerted management. The second company proactively and successfully shifted to a previously identified alternate supplier per their business resiliency plan. As a result, customers received their shipments on time and without any knowledge of what happened behind the scenes.

Which of the two companies is more adaptive to dynamic changes in supplier operations? The latter, of course. The former, though, tells the story of a great many organizations. The first company's lack of foresight and planning was on full display during a disruption in their supply chain. This behavior is also likely present in their day-to-day operations that are mostly manual management processes, such as spreadsheets and email, which are inefficient and difficult to scale.

If an effective and efficient operation is the ultimate goal, why aren't more companies instituting better business practices with respect to their third parties and vendor risk management? The reason: it's easier said than done. It takes planning, due diligence, business integration, monitoring and more to create an effective third party risk management program. Most programs are ineffective due to a deficiency in one of three areas: effective starting point, an understanding of the organization's risk appetite or an efficient process.

In this e-book, we'll put you on the path toward effective third party risk management with plenty of guidance and resources. At the end, you'll have a clearer understanding of how to build your own third party risk management program.

Contents

1 Planning

The planning phase for third party risk management starts with your organization and the primary activities needed to serve customers and drive profits. Activities like logistics, operations, marketing/sales and service entail processes and requirements to do what they do.

Would it make business sense to outsource an activity to a third party? In answering that question, determine if it's an activity better managed internally or outsourced. What are the requirements for conducting the activity? Could a third party meet those requirements? Is it outsourceable or is it too internalized?

The shift from cost to value

According to Deloitte, "The drivers for third party engagement are progressively shifting from a focus on cost to a focus on value, reflecting organizational recognition of the strategic opportunity that third parties can create for them." [1]

[1] Deloitte

Laying the Groundwork

The organization's value-producing activities should determine the need for third parties. Here are the steps you should go through:

Assess business requirements

Identify the needs within processes to determine if it warrants a third party.

Get context

Identify the impacts of the business process to all parties involved in the process. Understanding this context helps ensure the business needs are met.

Identify inherent risk

Determine the inherent risks of performing the business activity. It's risks that exist without controls. Knowing inherent risk is helpful in quantifying risk.

Internal cost and value analysis

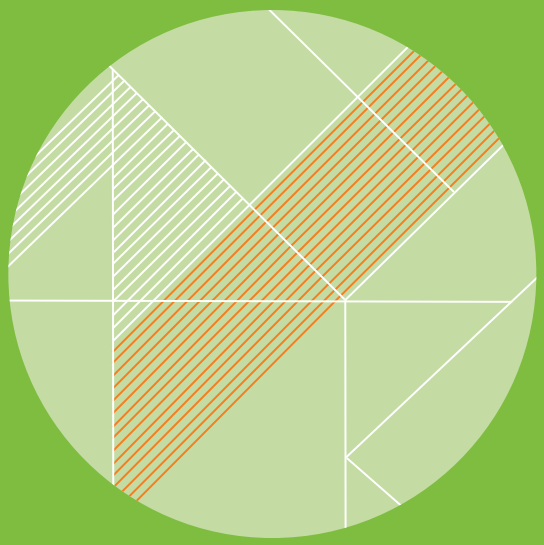
Conduct a cost-benefit analysis of the activity. It's instrumental in determining if the activity should be performed internally or outsourced and will help identify the evaluation factors when retaining a third party.

Control identification

Think back to the inherent risks you determined. Now identify controls that can manage risk more effectively. Are there controls that should be added to better manage inherent risks?

Residual risk and risk appetite

After controls are factored in, the risks remaining are residual risks associated with a process or activity. Are these residual risks acceptable? It depends on your organization's risk appetite. If it's unacceptable to your company's risk appetite, you may need to consider more controls.



How Effective Organizations Plan

Effective organizations see third party risk as a business risk. For them, planning is about a careful review of what drives profitability and customer satisfaction. By examining processes and activities as steps and requirements, it's easier to see where third parties do or do not fit in.

Below are three common questions effective organizations ask during the planning phase:

1. What process will the outsourced activity support?
2. What departments are involved in the process? This includes departments in preceding and subsequent processes.
3. If the process were not completed, how would it impact the preceding and subsequent departments?

For more questions, download the **Third Party Risk Management Workbook.**

2 Due Diligence

All third parties present a risk to an organization. Depending on the data they handle and the service they provide, stakes can be high. It emphasizes due diligence and appropriately vetting each third party before signing an agreement.

When you conduct due diligence, you'll turn your attention to the pool of third party candidates. Everything you do will help answer, "How can we ensure we retain the best fit third party and remain at an acceptable amount of risk?"

Get started by evaluating third parties on their ability to perform the duties requested. Your checklist should include your requirements, as well as any pertinent information about the third party. Take precautions and don't get too enamored with what's said or promised. Conduct your due diligence.

Varying degrees of due diligence

The Office of the Comptroller of the Currency (OCC), a government agency that ensures a safe and sound US banking system and a leader in risk management guidance, sees due diligence with third parties in varying degrees. "The degree of due diligence should be commensurate with the level of risk and complexity of the third party relationship." [2]

[2] OCC Bulletin 2013-29. October 30, 2013

Properly evaluating third parties

Only your business can determine how much risk to accept and how deep to go on due diligence. With third parties, you should consider the following:

Mapping third party capabilities to needs

Mapping third party capabilities to needs point by point helps clarify which third parties meet your business requirements.

Assessing identified control capabilities

You've already identified and documented controls. Here, we'll assess the controls to determine the third party capability to meet your business requirements.

Assessing costs and value

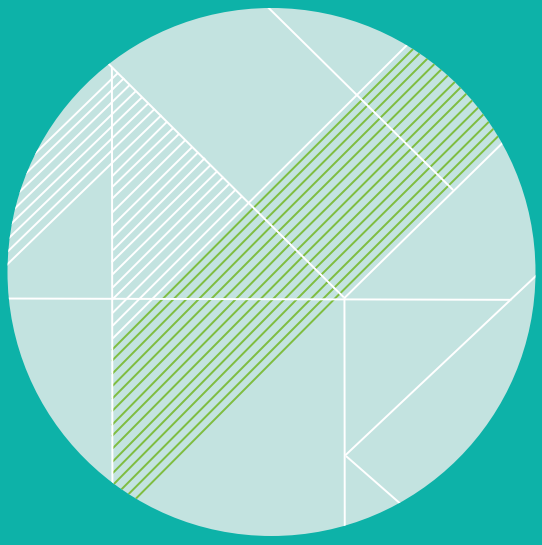
Previously, you conducted a cost-benefit analysis of the activity. Now you'll factor in costs and value for potential third parties who may assume that activity.

Identifying responsibilities

In any company/third party relationship, there are key roles on both sides. Use RACI (responsible, accountable, consulted, and informed) charts to document the matrix of responsibilities. If there are multiple steps and roles, use multiple RACI charts.

External information

Use relevant external information sources as part of your due diligence process, including online searches, background and credit checks, and information security monitoring systems.



How Effective Organizations Perform Due Diligence

Effective organizations rely on a cross-functional team to conduct due diligence of potential third parties. They gather evidence and record findings that are accessible and reportable at any time. The effective organization optimizes its level of due diligence based on the third party relationship and the level of risk it poses. Making smart business decisions is easier for effective organizations because they have the right data at their fingertips.

Below are three common questions effective organizations ask during the due diligence phase:

1. What are the capabilities of the third party as they relate to the activity requirements?
2. What gaps exist between capabilities and requirements?
3. Are there workarounds for these gaps?

For more questions, download the **Third Party Risk Management Workbook.**

3 Contract Negotiation

The centerpiece of the third party relationship is the agreement, a contract that documents the three R's: requirements, responsibilities, and ramifications for both the company and third party. That keeps it simple and straightforward.

Negotiate the contract right, and you're set up for success or a smoother landing if the relationship fails. Get it wrong, and a myriad of risks may become incidents.

That's why it's critical to use contract language to bring authority to requirements. Unless it's stated clearly and explicitly, you can't expect the third party to follow them and meet requirements. For guidance, revisit due diligence where responsibilities were identified. Finally, keep in mind that contracting isn't something that's written and filed away. It's a living, breathing agreement that can be revisited at any time for any reason. Take the time and effort to get the contract right and make sure the organization is getting the right value.

Contract renewal tip

It's renewal time for the third party contract. If the contract stipulated renewal terms, this is the time to review them. If the organization depends on the third party, don't delay. A contract lapse might grant negotiating power to the third party that proves costly to the organization.

Ensuring Success

What follows are suggested inclusions for standard contract terms with third parties:

Contract for performance - Spell out the metrics used to judge performance in the contract. Make certain that contract negotiators know the value provided by the third party and the business need. Knowing the desired value, requirements and context make contract negotiators more effective.

Define your audit process - Often overlooked, defining and documenting the audit process helps prevent issues later. Document how, how often and the escalation process. Knowing an audit is coming is far better than having one sprung on you.

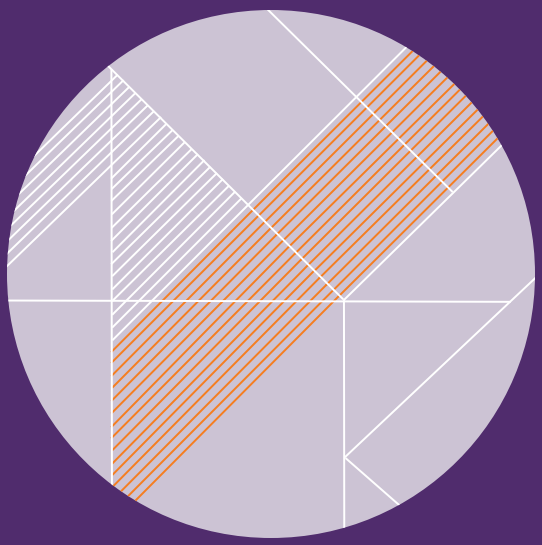
Service Level Agreements (SLA) - Service level agreements, better known as SLAs, are the typical name given to third party contracts that stipulate requirements. Since such agreements detail services provided, the name and acronym fit.

Roles and responsibilities in writing - You've used RACI charts to develop a responsibility matrix. Now during the contract stage, you'll record these roles and their responsibilities. Roles are preferable to names that often change.

Onboarding/testing/business resiliency/business continuity - Stipulating onboarding, business operations and emergency preparation in the contract creates welcomed expectations for the third party. The third party expects and values onboarding that helps them get up to speed on how the company operates. Also, the third party knows their role in business continuity, business resiliency and crisis events.

Data ownership/retention/destruction/purpose - Data privacy is serious business. Who owns the data? How long will data be retained? How will the data be destroyed or repurposed? At contract termination, how will data be handled? All aspects related to data should be stipulated in the contract.

Insurance - Insurance is helpful for the what-ifs, but only if coverage, roles and responsibilities are identified. Nothing is worse than a big loss and thinking the other party carried insurance.



How Effective Organizations Manage Third Party Contracts

For effective organizations, third party agreements aren't one and done. These agreements are active and working throughout the third party lifecycle and are stored in a central location for easy access. If there's a performance issue, they review against the contract and its performance requirements. If necessary, a review process can bring together stakeholders with defined steps for mitigation or remediation. Effective organizations are also proactive at contract renewal. They know a contract lapse could result in higher pricing from the third party.

Below are three common questions effective organizations ask during the contract negotiation phase:

1. Does the value of the contract exceed the value of the activity?
2. Does the contract include the controls identified to manage risk? Make sure you include business continuity risks.
3. Are audit requirements defined in the contract?

For more questions, download the **Third Party Risk Management Workbook.**

4 Business Integration

The true test of a third party relationship is in how well the vendor integrates with your business. Third parties are an extension of your company, and the services they provide are critical in enabling your company to serve customers and reach its goals. In this section, we will turn our attention from the third party to the company, and its role in engaging the third party.

What's centrally important about business integration is conveying business context. Context is defined as the circumstances that form the setting for an event, statement, or idea, and in terms it can be fully understood and assessed.

For example, you need to communicate not only requirements but also the context of those requirements. Context gives insight on company policies and procedures, even organizational idiosyncrasies, enabling the third party to customize their offering to the company. Along with context, communication helps ensure both company and third party understand each other's position and viewpoints.

Create a star third party

After planning, due diligence and contracting, you've made your choice of third party. Business integration is about ensuring the third party is a valued partner, not just another vendor.

Business integration

How well your third parties integrate with your business greatly determines success. Here are steps you should explore and implement.

Onboarding

You'll want to offer or require onboarding procedures for new third parties, so they get up to speed quickly. Sharing internal knowledge and policies during the onboarding process helps ensure the third party exhibits that conduct. Onboarding is typically done by the same business people that performed the planning phase. They know the way things should be done.

Attestation

Attestations are a way to confirm the third party acknowledges they received the information and are aware of their obligations.

Process mapping

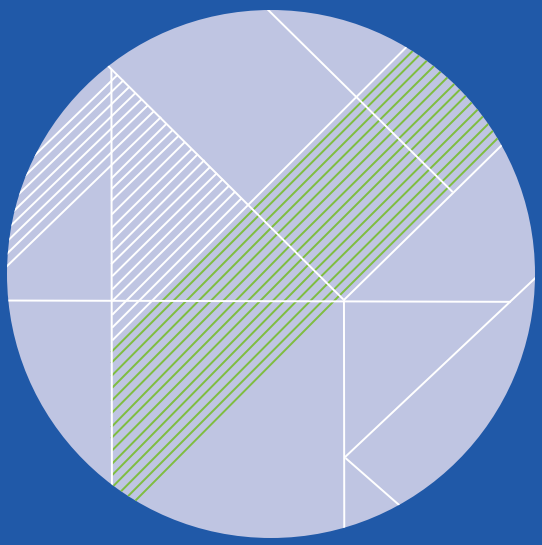
We previously mapped third party capabilities to our needs. Now map the processes and the steps the third party will perform. In essence, process mapping is how the business and the third party will tactically work together.

Deliverable schedules/SLAs

Bring detail and clarity to the third party deliverable schedule that's part of the service-level agreement (SLA). What was once articulated in planning is now the actual delivery schedule.

Business resiliency/continuity planning and testing

Here, the third party performs the business resiliency/continuity planning and testing activities outlined in the contract. It's not just in the event of a disaster. It's an ongoing responsibility, and the third party's role is vital depending on the outsourced service.



How Effective Organizations Manage Business Integration

Effective organizations know the success of a third party relationship isn't just in planning, due diligence and contracting. Success is also dependent on the third party understanding and adhering to the company's processes, procedures and standards. It's best practice for ensuring a seamless program that runs optimally and in compliance with the business context.

Below are three common questions effective organizations ask during the business integration phase:

1. Has the third party agreed to all applicable policies and procedures? Is this documented?
2. Do the business and the third-party have a clear understanding of process responsibilities?
3. Have the business and the third-party defined, planned and tested business outage scenarios?

For more questions, download the **Third Party Risk Management Workbook.**

5

Ongoing Monitoring & Analysis

Ongoing monitoring and analysis help ensure the partnership between the company and the third party is a good fit during the entire life of the contract. A third party relationship is like any working relationship where it pays to be on the same page. Ongoing monitoring helps with this while also providing assurance.

With ongoing monitoring and analysis, you can be on the lookout for third party violations in agreements, trends that can hurt goals, and risks or threats that could impact your organization. Discovered early with monitoring, poor performance can be addressed, and issues can be resolved before they become incidents. Feedback keeps decision-makers in the loop.

Third-party risk monitoring services

Business changes overnight. That's why it's wise to continuously monitor third parties, especially for information security and financial health. Several technologies offer third party risk monitoring, including RiskRate, SecurityScorecard, RiskRecon, RapidRatings and BitSight.

Trust but verify

Here are seven things to keep in mind with ongoing monitoring and analysis:

Flexible, risk-based scheduling - Determine the required assessment frequency based on the inherent risks of the business activity. Strive for flexibility to ensure compliance and lessen frustration with assessments.

Control monitoring - Monitor controls and remain on alert for controls that become ineffective or fail. Review SLAs and reports for control adherence.

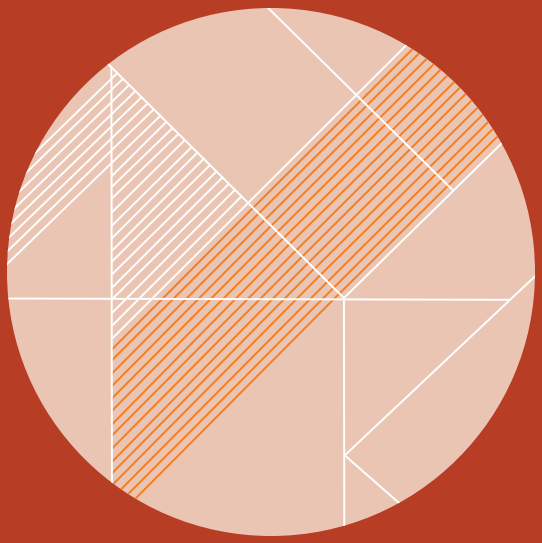
Assessments - Assessments help ensure controls are being adhered to and monitored appropriately. Many organizations rely on assessments like Shared Assessments' **SIG and SIG Lite** and the Cloud Security Alliance's **CAIQ assessment** for cloud providers to assess commonly required controls.

Reports and documents - Vendor reports such as SOC II can simplify the control adherence process.

Third-party intelligence - Third party intelligence provides independent, unbiased inputs to your program and help validate your risk management processes. Several technology providers offer scorecards reflecting the daily risk of third parties. If a third party is hit with a cyberattack, rocked by a news story, or stunned by its stock price swoon, you're first to hear about it.

Issues management - Issues can be a regular occurrence with third parties. What matters is having a process for documenting and resolving issues. Organizations that fail to implement an issue management process run the risk of issues rapidly growing into major headaches.

Analysis - Third party performed activities can mean different things to different parts of an organization. In Analysis, you'll turn data into messages that reflect the context gathered when your journey began.



How Effective Organizations Monitor and Analyze

Effective organizations manage third-party risk by working closely with the business and the third party. Ongoing monitoring and analysis perform a critical role. Risk managers can keep leadership engaged with status updates, trends, and metrics. Effective organizations also leverage technology to streamline the assessment process making real-time reporting possible.

Below are three common questions effective organizations ask during the ongoing monitoring and analysis phase:

1. Do you have the right KPIs in place to monitor controls?
2. Do you have the right KPI thresholds in place to measure risk?
3. Are there standardized reports from the vendor that can help you manage controls? (SOC II reports, SIG from Shared Assessments, etc.)

For more questions, download the **Third Party Risk Management Workbook.**

6 Business Continuity & Termination

Your business has goals and plans to achieve them. Even when challenges present themselves, you know the goal and what is at stake. That's where business resiliency comes in. It's your organization's ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and overall brand equity.

It's not always a major disruption that interferes with operations. It's often the small hiccup that slows the company down and hurts margins. Whether leadership realizes it or not, third parties are critical to a business's resiliency, to keep you going full bore toward your goals.

As someone involved in third party risk management, your role is pivotal. You're on duty with determining the risk of third party business disruption like data breaches, geopolitical strife, and executive departures, or any number of small things that could interfere with operations. All need addressing in your assessments, audits, and ongoing monitoring. You will also want to address this during contract evaluation time to determine if continuation or termination of the relationship is warranted.

Just cause for third-party termination

A leader in third party risk management, **Shared Assessments,** outlines four established standards for termination of third parties: The business relationship is no longer necessary or appropriate; there has been an irreparable violation of contract terms; either the organization or third party has a better arrangement/opportunity; or the third party violates a regulation or industry standard.[3] Knowing the four standards for termination, you can be on alert for them.

[3] Shared Assessments

Acting in the best interests of the company

There are a few features of a mature third party risk management program that can contribute to your efforts and business resiliency.

Business interruption support

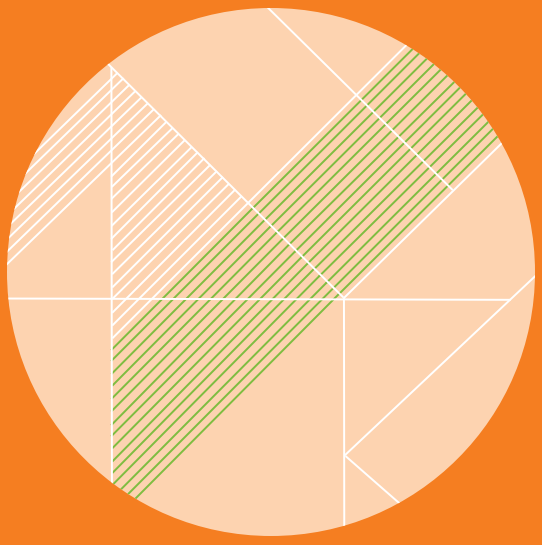
Business continuity management (BCM) helps address risks of business interruption. Knowing the critical role your third party plays in operations, it's essential to have them on board with the BCM plan. You need their support in planning, testing and actions if a disruption occurs.

Termination risk and alternatives

Your company should have a game plan in the works before terminating a third party. Is the plan to bring the activity in-house? Shift it to a different third party? Maybe the contract should be renegotiated, or the company should acquire the third party. It's up to the risk professionals to supply the information and rationale, so higher-ups can make better decisions.

Retrieving/disposing assets

When things with a third party don't go as planned, companies need to have a plan for what happens to assets like data, tools and space. Should they be retrieved or disposed of? The plan for assets after termination should be considered in the contracting stage and, if applicable, included in the contract.



How Effective Organizations Manage Business Continuity and Termination

Effective organizations see business continuity and termination contributing to third party risk management. They value business continuity planning with third parties and the third party's participation in testing and crisis response. If a third party requires termination, there's a plan for it. For effective organizations, resiliency is the result of smart planning, whether it calls for a new performance requirement, contract renegotiation, or contract termination.

Below are three common questions effective organizations ask during the business continuity and termination phase:

1. Do your business continuity plans require third parties?
2. Are you testing your plans with your third parties?
3. Are your third parties contractually obligated to help with business outages?

For more questions, download the **Third Party Risk Management Workbook.**

7 Toolsets

Technology holds the promise of streamlining and automating processes. You can accomplish more, scale with demand, and maintain accuracy—all because a technology solution delivered efficiency to your third party risk management program. That's only possible if it fits your processes and is set up correctly for your team's needs. If it all works, you made it. For that to happen, you need a lot of things to go right. That's what this section is all about.

Many organizations rely on office tools like spreadsheets to manage third parties. Spreadsheets can be manageable with a handful of third parties. But, if you're managing dozens, hundreds or thousands of third parties, paper and spreadsheets are inefficient and cumbersome. Technology solutions designed for third party risk management offer rich capabilities and efficiencies. To illustrate, the right solution can enable you to manage the entire third party lifecycle more efficiently—from planning and due diligence to contracting, monitoring, and reporting. It also streamlines assessments, aids collaboration, and ensures third party data contributes to an enterprise view of risk.

The right technology setup can make staff dedicated to third party risk management more efficient. For example, a company complying with Dodd-Frank's requirement for conflict minerals in the supply chain faced adding 50 FTEs to manage the requirement using manual processes. A technology solution enabled the company's six-member compliance department to handle it without additional staffing or resources.

Fund your program

Showing a return on investment with your third party risk management program is essential to securing funding. **Download Third Party Risk Management: Estimating ROI from an IRM Platform.**

With so many toolsets to choose from, which one is right for your organization? For advice and guidance on toolsets and program maturity, **contact** our third party risk management experts.

The right tool for the task

Here's a rundown on the major toolsets for managing third party risk, along with pros and cons for each:

Manual options

Pros: They are readily available and familiar.

Cons: They have limited functionality, hard to collaborate, can't see connections, cost/time barrier, often called into question during audits.

Point solutions

Pros: They are designed specifically for third party risk management

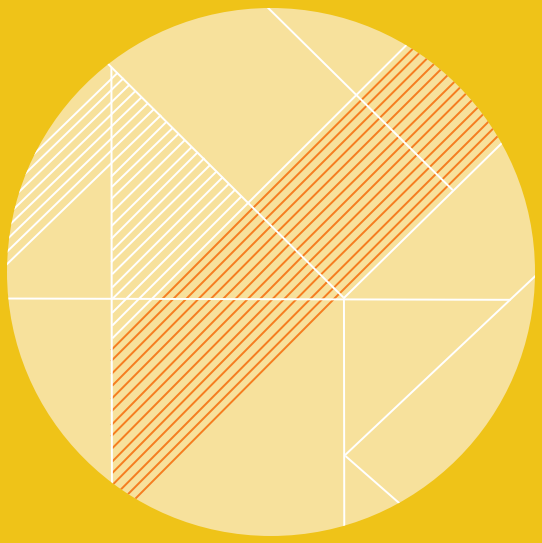
Cons: Point solutions often focus on a single department but fall short on integrating risk across the organization.

Integrated risk management platforms

Pros: They equip users to manage third party risk, as well as integrates third party data into an integrated risk management program that's effective, agile and efficient.

Cons: There are cost considerations, learning curves, and often require executive level support.

Only you can determine which approach fits best with your organization. A lot depends on your current business processes and the size and maturity of your program.



Track down technology

You need a toolset to build an effective third party risk management program, but which one is right for you? Before looking into third party risk management technology solutions, you need to understand your third-party risk program maturity and determine your company's needs.

Request our **Vendor Risk Management Benchmarking Assessment** to help you determine your program maturity and needs so you can find the toolset that's right for you.

The present and future of effective third party risk management

Current business trends toward outsourcing and adoption of digital processes create risks that were unimaginable a few years ago. Risks like access management, privacy concerns, corporate espionage, geopolitical and nefarious actions by nation-states create new challenges. For risk management programs, these new risk challenges are doubled, impacting your organization and your third parties.

Third party risk management is on the leading edge of globalization. You're an eyewitness to a supply chain stretching across lands and oceans. You're the first to know when a third party in another continent has an issue, thanks to ongoing monitoring. Your contacts and connections help ensure third parties do their part in helping the company succeed.

Your goal is to leverage third parties with an acceptable level of risk, so your organization can be as effective as possible. The results you seek are streamlined processes, agility and efficiencies that improve productivity and competitiveness. It's not just possible; it's probable with planning, due diligence, contracting, business integration, ongoing monitoring/analysis, business resiliency/ continuity, a committed team, a leader, and an investment in technology.

Take the first step today. The Lockpath Platform can help you on your journey.

Info@lockpath.com | 913.601.4800

NAVEX Global is the worldwide leader in integrated risk and compliance management software and services. Trusted by more than 14,500 customers, our solutions help organizations manage risk, address complex regulatory compliance requirements and foster an ethical, highly productive workplace culture. For more information, visit www.navexglobal.com