NAVEX®

A NAVEX **One**® Definitive Guide

Definitive Guide to Third-Party Risk Management

- How to successfully mitigate your organization's third-party risk

Contents

Overview

The Definitive Guide to Third-Party Risk Management is a comprehensive resource full of insight, advice, and examples to help organizations recognize and address all aspects of third-party risk.

A strong third-party risk management program helps your organization make smart choices when it comes to engaging with business partners. It will also protect your organization from the risks that third parties can present.

This definitive guide is divided into three main sections: **PLAN, IMPLEMENT,** and **MEASURE**. In these sections, you'll find the information and tools you need to develop a risk-based strategy, define third-party risk, and identify areas in which you should improve your program's effectiveness.

Introduction

Why is third-party risk management important?

The business landscape continues to be an ever-changing environment, particularly when it comes to managing third-party risk. As business needs change, global regulations develop, and new trends emerge, how does your organization identify and address the risks posed by your third parties? Simply put, if you don't have a robust program in place, your organization faces significant risk.

Reducing third-party risk should be a cornerstone of your GRC program. Below are some of the factors to consider when addressing third-party risk.

Growing reliance on third parties

The number of vendors, suppliers and other agents organizations engage with continues to grow – and so do the risks they represent. Organizations increasingly rely on third parties for critical operations – but outsourcing these responsibilities poses a myriad of risks and managing them appropriately should be a top priority for leadership.

Increased globalization

As markets expand and competition intensifies, increasing globalization is inevitable. For many organizations competing in new markets means working closely with third parties.

Increased enforcement

Over the past few years, the global landscape has changed and as a result, global regulators have put a heavier focus on third-party risk. The U.S. Department of Justice (DOJ) and the Securities and Exchange

Commission (SEC) made the Foreign Corrupt Practices Act (FCPA) enforcement a top priority, and the U.S. and other global regulators increased sanction enforcement. Further, there is a growing trend of global regulations to protect human rights in the supply chain, notably laid out in the German Supply Chain Act and EU Supply Chain Directive.

Rise in cyberattacks

All organizations, from small businesses to large enterprises, are facing an increase in the frequency, sophistication, and impact of cyberattacks. Relatedly, bad actors continually refine and update their efforts to compromise systems, network, and information – taken together, this makes cybersecurity a moving target.

As new technologies continue to be introduced into the market and adopted by organizations to streamline business operations, the degree to which your data is shared can grow exponentially. Increasingly complex technology stacks across all business verticals, plus the use of personal data demands a robust program to understand who has access to your organization's data and how they handle this information.

The risks are real

As we often see in the news, lapses in leadership around managing third parties have damaged organizations by exposing them to massive fines and penalties. Even if the financial penalty can be managed, the reputational impact can have far-reaching and long-lasting consequences for many years.

Third-party risk management is a top concern for leaders across the organization, including Compliance, Information Security, Legal, Procurement, and more, but many organizations are still coming to terms with how best to manage their third parties to limit risk and develop programs based on operational risk assessments.

Compliance

Information Security

Legal

Procurement

Benefits of a strong third-party risk management program

Managing third-party risk can make a big difference in how well your organization can identify, manage, and limit the liability a third party can represent. Your third party's risk is your risk – and you should have confidence in your program's ability to minimize the risk for your organization.

Having a strong third-party risk management program – including onboarding, screening, testing controls,

investigations, and risk mitigation of third-party relationships across the enterprise – helps your organization in several ways:

Avoid fines, regulatory enforcement action and legal costs

A strong third-party risk management program helps your organization avoid legal action and fines, and it may also reduce penalties and mitigate regulatory action if an incident occurs.

Promote your organization's culture

The FCPA advises that organizations must demonstrate they are promoting a culture of ethical and responsible behavior, both internally and with third parties. A clear pathway to accomplish this is through requiring third parties to understand and abide by your code of conduct, attend your third-party compliance training, and attest to your policies through a policy management solution.

Produce a more accurate picture of risk

A comprehensive third-party risk management program provides holistic data on where the organization is most exposed to risk and where it is well-protected. This insight is not only helpful in making training, policy and hiring decisions, but can also point to where immediate action may be needed and resources should be allocated.

Promote continuity

Disruptions in third-party relationships can be detrimental to the continuity of business practices. Third-party failures can result in legal action, operational standstills, or regulatory actions that require significant resources to resolve. In the worst cases, third-party failures can even threaten the viability of your own organization.

Protect the organization's reputation

As we see in many high-profile cases, a single third-party failure can deeply affect the organization's relationship with its clients and customers. Ensure your organization will thrive for many years to come by prioritizing vetted third parties.

One size does not fit all

Many program leaders worry that they don't know where to start on a third-party risk management program. But the good news is that organizations do not need legions of personnel or unlimited budgets to meet program best practices.

A risk-based approach to third-party risk management involves aligning your third-party risk profile with your organizational risk profile and building a program that optimizes both.

Almost every organization has some elements of an effective third-party risk management program. In the next sections, we provide recommendations and templates for identifying what you already have, determining what you need to address your gaps, and implement the right strategy for your organization.

Plan

Define your goals and create a strategy

Whether your organization engages with a handful of local consulting firms or thousands of manufacturers around the world, those engagements are relevant to your organization – and their failure would affect your organization's ability to function. The third-party landscape is expansive, often with complexities that can surprise even the most sophisticated organizations and leadership.

This section explains how to set up a standard process for third-party risk management – from initial identification of third parties, to onboarding, risk screening, identification, and continuous monitoring.

Building the business case for your third-party risk management program

Answer the following questions to help determine how much of an impact a purpose-built third-party risk management program would have on your business.

Needs assessment calculator

How valuable is a mature third-party risk management program to your business?	YES / NO
Our business would face significant impacts if we did not identify risks and analyze them in a timely and effective manner	
A third-party failure would drastically impact our business financially and reduce the ability to provide core products and services	
Our organization experiences challenges in ensuring and/or reporting that our third parties meet applicable regulations and compliance requirements	
Our industry has frequently changing regulations and compliance standards that require continuous monitoring and control testing	
How would you assess your existing third-party risk management program today?	
Our business units are siloed, resulting in independent risk assessments and an inability to integrate to our GRC program	
We do not have a structured approach for onboarding third parties	
We do not have a standard process for screening third parties	
Our program does not have a central location to view risks from our third-party landscape	
Our program does not have any technology to help gather, connect, and contextualize data throughout our business	
We have limited or ill-defined workflows to manage, monitor, and analyze our known risks and findings	
We have limited visibility into current and future risks, and primarily rely on a reactionary risk and compliance procedure	
How would you assess your third-party risk management process?	
We spend too much time on administrative tasks, such as gathering information for onboarding and communicating risks	
We are pressured to pull resources from other areas of the business to complete TPRM activities	
We don't have an automated process for gathering risk and compliance information	
We experience frequent business challenges due to unidentified and unmitigated risks within our business	
Total number of 'Yes' responses:	

Number of 'Yes' responses	<5	5 - 7	8 - 10	>10
Need Level	**Low**	**Moderate**	**Moderate High**	**High**
Investment Recommendation	Not Recommended	Selectively Invest	Invest	Immediately Invest

Critical components to include in planning

A unified approach

There are likely multiple areas of your business that engage with and manage third-party relationships. Because of this, it is critical that all key stakeholders, including those on the front lines of engaging with third parties, are aligned to use the same third-party management system. A siloed approach greatly increases an organization's exposure to risk. For example, your procurement department could be unaware of pertinent information uncovered by your compliance department related to a third party.

A key component for ensuring program consistency is a distributed automated system. To support this, full buy-in from senior executives and the board of directors is necessary. Your organization's leadership should regularly communicate about the third-party risk management program, making clear to everyone in the organization that relationships with third parties should be reviewed to identify and mitigate any associated risks to the business.

Adequate resources

Everyone deals with capacity, resources, and budget constraints. Beyond the time and cost involved in the initial onboarding of third parties, there are additional costs to keep in mind as you set up your program. Consider the operational and business costs related to:

- The frequency of ongoing monitoring, which is determined by your risk profile and your third-party risk profile
- The number of third parties to monitor – and which ones you need to monitor more often than others and why

- Your contingency plans for when a third party fails – how to disengage and limit repercussions or operational disruptions
- To what level you'd need to disengage. Would it require full disassociation or partial? Would it have an impact on all business units or only those directly affected?
- The specific assurances you need to reengage with a failed third party and how long the reengagement process would take
- Your expected costs in terms of lost productivity, downtime, open time of the relationship, and reengagement or finding a replacement vendor when a failure occurs
- Effective, automated solutions that save on resources (including full-time employees), increase productivity and drive down operational costs

Appropriate translations and outreach

Many high-risk third parties reside in emerging markets where English is not the native language. In many cases, third parties find the scrutiny of third-party risk management to be both high stakes and confusing – especially when the information being communicated is not in the third party's local language.

Providing notifications, instructions, and interview questions in the third party's local language can make the third party more comfortable with the process and help accurately answer important questions, such as "why is the process important?" and "how will our information be used?"

Third-party training

Organizations should consider, where appropriate, extending organization compliance training, especially on codes of conduct and policy attestation, to their various third parties. Decisions about when and in what form to offer training support should reflect the third-party's risk profile and the degree of risk in the relationship. A top-tier Governance, Risk, & Compliance (GRC) program offers customizable training for third parties and can easily be added to your ongoing compliance training.

Identify your third parties

The third-party landscape continues to expand in breadth and complexity for most organizations. As organizations look to grow, there is an abundance of third parties with deep expertise and broad capabilities that can extend the organization's ability to succeed. These days, many organizations are actively expanding their business capabilities through third-party engagements, with or without a risk-based third-party risk management program in place.

Your immediate supply chain and distribution channels represent direct relationships between your organization and the third party, yet it is increasingly common these days to see your direct third parties engaging on your behalf with outside specialty consultants, agents, and contractors with whom your organization has no direct relationship. When your third parties have a network of indirect third parties – sometimes called fourth parties — they need attention too.

Consider what types of third-party risk exist

There are several types of potential risks third parties can bring to your organization, which are summarized in the following categories:

Compliance The risk of an organization's potential exposure to legal penalties, financial forfeiture and material loss resulting from a failure to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

Financial risk The risk of losing money on an investment or business venture. Some more common and distinct financial risks include credit risk, liquidity risk and operational risk – these risks can result in the loss of capital to interested parties.

IT and cybersecurity risk The risk related to a loss of confidentiality, integrity, or availability of information, data, or information (or control) systems, and reflecting the potential adverse impacts to organizational operations.

Legal risk The risk that a third party will impact your organization's compliance with local legislation, regulation, or agreements.

Operational risk The risk that a third party will cause disruption to the business operations. This is generally managed through contractually bound service level agreements (SLAs).

Regulatory risk The risk that a change in laws and regulations will materially impact a security, business, sector or market.

Reputational risk Reputational damage is the loss of financial capital, social capital, and/or market share resulting from damage to a firm's reputation. This is often measured in lost revenue, increased operating expenses, capital or regulatory costs, or destruction of shareholder value.

Strategic risk The risk that your organization will fail to meet its business objectives because of a third-party failure.

Your third-party risk profile

After identifying your network of third parties, it is important to be forthright about the implications of these engagements for your organization's success. This means not only defining the depth and breadth of your third-party engagements, but also understanding the costs of your program's success or failure. It means defining measures of success and planning for all possible program limitations.

Evaluate your risks by defining the following:

1. The regulatory environment and industry your organization operates in
2. The number of third parties your organization engages with
3. The types of third parties you work with (suppliers, resellers, distributers, manufacturers, etc.) and where they are located
4. The number of third parties critical to your business operations
5. The products and services provided by each third party
6. What data is available to each third party

When assessing your position, consider the regulatory environment in which your organization and your third parties operate. Some industries are more regulated than others, and some third-party engagements draw more legal and regulatory attention. To best protect your third-party program and your organization, start by knowing the threats and opportunities present in the environment in which you operate.

The number of third parties with which your organization engages is one indicator of your level of risk. It can help you define your challenges – much more so than the size of your organization in terms of employees or revenue. In fact, the proportion of third parties to your organization's size is a clearer indication of your risk level than total numbers. For example, there are global manufacturing firms that facilitate manufacturing through large third-party networks while directly employing very few staff. Conversely, there are huge multinationals that work with very few third parties.

Part of your risk profile is defined by how deeply your third parties are integrated into your organization. When considering how many of your third parties are critical to your business performance, keep in mind how much of an impact it would make if you had to rapidly reduce or ramp up your engagement with a third party or a set of third parties, or to disengage from them entirely. While you can manage your organization's internal GRC program directly, you have less visibility into your third party's programs. Therefore, the capacity of a third-party failure to affect operational ability is a measurement of risk.

When reviewing the potential financial, operational, and reputational risks to your organization, keep in mind your organization's ability to adequately manage and mitigate third-party risk. In some cases, the risks of doing business with a third party outweigh the potential

benefits. Set the criteria for that decision well in advance or define a champion who has the authority to approve or veto borderline decisions.

The adage **trust but verify** is apt in terms of third-party risk. Use data, tools, and an active third-party risk management program to define your actual risk.

Define a third-party risk management process

Develop a consistent, structured process for assessing and assigning risk to each third party. While process consistency delivers efficiencies, a risk-based third-party risk management solution requires that you assess each third party based on your relevant risks and the distinct risks the third party represents.

Questions to ask include:

1. Which departments in the organization complete which tasks?
2. Are we duplicating efforts?
3. Which components require input from external third parties?
4. What approvals are required from whom and at what point in the process?

Identify elements that can be automated

Use technology to streamline processes

Reductions in complexity, time and associated costs resulting from streamlining processes can be significant. More importantly, automation forces you to set clearly defined standards. Enforcing adherence to those standards in turn helps organizations avoid bias and error. Common processes to consider automating for a strong third-party risk management program:

- **Onboard & Screen Third Parties**
  Streamline onboarding with a consistent process to collect all necessary third-party details and conduct initial screenings to understand the associated risks during the consideration phase of your business relationship
- **Gain a Deeper Understanding of Risks & Beneficial Owners**
  Uncover ultimate beneficial ownership to determine third-party ownership and conduct enhanced due diligence to further examine high risk third parties to make informed decisions
- **Monitor Third Parties Continuously**
  Monitor third parties throughout the course of business to receive real-time alerts as risk statuses change to understand the impact of risks and make informed decisions
- **Assess Third Party ESG Performance**
  Uncover third-party commitment to Environmental, Social, & Governance (ESG) practices to ensure your partners are aligned with your organization's values and standarrds
- **View All Risk With a Comprehensive Risk Score**
  Link third parties to policies, risks, and controls for a greater view of their risk to the business
- **Know How Third Parties Protect Their IT Risks**
  Ensure third parties take the proper security measures and meet your expextations when handling your data
- **Uncover Supply Chain Integrity & Plan for Interruptions**
  Track how third parties operate and establish business continuity processes to plan and prepare for potential business operations from third-party failures

Who should own your third-party risk management program?

Planning and implementing your third-party risk management program should be a collaborative and inclusive process, involving representation from various departments, including compliance, legal, human resources, internal audit, security, risk management, procurement, and IT. Stakeholders need to partner to ensure the program is implemented smoothly and that all departments get what they need from the program.

Implement

Manage your third-party risk management program

Implementing your organization's third-party risk management program should follow a continuous process of onboarding, screening, continuous monitoring, and lifecycle management. Alongside these activities, you should include ongoing communications with management and other key stakeholders about program processes, success, performance, and anticipated changes.

When you implement your plan, transparently communicate the expectations of your program to current and prospective third parties. Work closely with your third parties to educate them on your expectations, including your code of conduct, policies and processes, and behavior expectations. Doing this early protects you and the third party from conduct breaches and unnecessary risk throughout the life of the engagement.

Communicate the policy

One of the most critical aspects of managing your program is communicating a clear, written policy about third-party risk management. Make sure the third-party, procurement, and supply-chain policies clearly state your current third-party policy. Policies should be reviewed regularly, updated as necessary, and included in regular compliance training.

Mitigate risk

Many program initiation elements can be done in house before engaging with any third parties.

These initial steps may include defining and sharing objectives, structuring program parameters, identifying stakeholders and program champions, acquiring a budget, among other items. This initial program setup may last months before your first third-party onboarding and review can take place.

Particularly when organizations work within a complex third-party landscape and assurances on program efficacy are critical, stress-testing your processes and capabilities through a limited early-adopter program can help ensure program success and stakeholder confidence.

A structured program should guide third parties through a set sequence of events to ensure process consistency. Your program should include standardized documentation and practices, managed through a centralized system with a well-defined chain of command for any program changes, exceptions, or enhancements. This ensures when changes are made, everyone in the organization is equally informed.

Onboard and screen third parties

Develop clear expectations of each third party based on the work to be done. Clearly define individual

executives and contacts by name and by role, service-level agreements, performance expectations, specific criteria for termination and who can take actions to pursue termination, and under what conditions other actions should be taken.

Your third-party onboarding process should be familiar and standardized to avoid missing key requirements – and so your third parties can easily complete the process. Be sure to include third-party education on your key policies and requirements.

Though it may be simplest to identify contacts by name, be sure to identify key roles as well to prepare for inevitable personnel changes.

Every organization will have a few unique reporting needs or assurances, but the core steps of onboarding a third party, including initial due diligence inquiries, are likely to be similar. Process and document standardization will help you address and include steps that may not be obvious when initially defining the onboarding process.

Though you will define the timeline and your organization's particular requirements to formally onboard a new third party, at some point you will need to conduct a deeper screening of the third party after collecting the necessary information to build a third-party profile. Screening should include financial and reputational checks, multiple internal review channels, and experts engaging with and conducting independent research on the third party and its officials.

During onboarding and the consideration phase, it's important to screen your third parties for regulatory and reputational risks they can bring to your organization – these risks can be indicators that may be pathways to deeper research and reporting requirements.

Adverse media Look for reports on stories in published media that mention the third-party organization or its key stakeholders. Be sure to incl ude search terms that look for violations of modern slavery or other human rights violations, in addition to other financial and reputational flags.

Sanctions and watch lists Check governmental reports for organizations on which official sanctions are placed and the reasons for doing so.

Politically exposed persons Seek resources that reveal the political connections of executives and individuals associated with the third party and their implications.

In addition to screening third parties for regulatory and reputational risks, it's important to understand how integrated each third party will be with your organization's operations. The first step is knowing which third parties have access to internal company or customer data, systems, processes, or other privileged information, and to what extent. After understanding this group, a standardized risk assessment to learn how third parties handle data, what security measures are in place, and plans for any breach or disruption, should be completed during the consideration phase.

The outcome of a screening during the onboarding process should be an approval, disapproval, or deferment of the engagement.

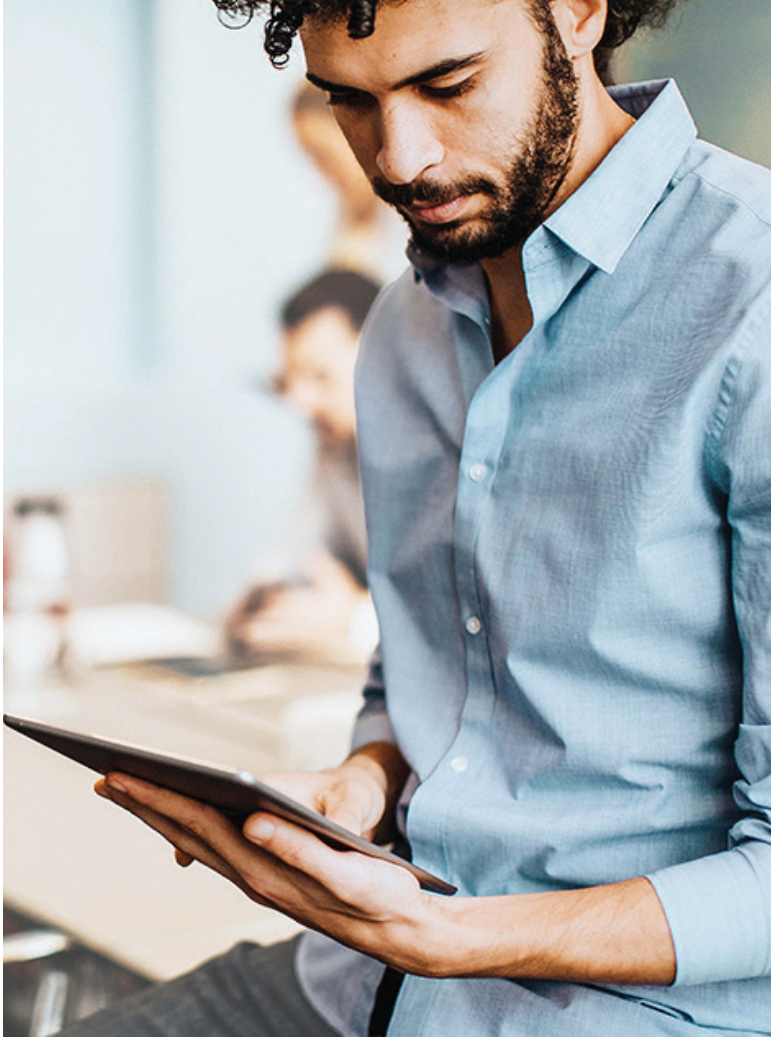
Gain a deeper understanding of risks and beneficial owners

Though standard screening should capture most of your reporting requirements, there will be occasions when deeper dives are warranted. Depending on how your program defines your third-party assurances, you may find that a certain percentage of your third parties require additional due diligence after standard screenings, before doing business with them.

Organizations should have the freedom to develop multiple filtering frameworks that configure the results of their screening efforts to meet specific risk tolerances, which can differ due to the size and nature of a contract, geography, and industry groupings. In essence, you should be able to screen high-risk clients from one jurisdiction against all available data; high-risk clients from another jurisdiction against another subset; and further, low risk- clients against a smaller data set. This filtering significantly improves the quality of the data alerts returned, substantially enhancing both relevance and materiality for each level of risk.

When engaging in higher-risk relationships, it is important to identify beneficial ownership concerns – which can involve multiple layers of complexity – uncover litigation records and conduct interviews of former associates, regulators, and partners of the third party. Further, you should identify any possible risk factors and if any beneficial owners are listed on any sanctions watch lists.

An automated system can help you properly stratify your risk and guide the processes that will ensure proper due diligence reveals any potential risks across the engagement.



Monitor third parties continuously

Third-party relationships are fluid and it's important to maintain the most current information as third-party processes and status change. Engaging in ongoing monitoring may involve a periodic rescreening of existing third parties or rescreening driven by an alert about a change in the third party's status. Having third parties complete assessments on a regular cadence also provides you with the necessary information to know if your third parties are continuing to meet your expectations. Continuous monitoring allows you to identify and assess your third-party risk quickly and accurately, enabling you to act to eliminate or reduce risk before it impacts your organization.

Assess third-party ESG performance

Working with third parties comes with unavoidable risks, but even as you manage these risks, it's important to ensure the companies you work with hold the same values you expect internally. As organizations work to become more ethical, diverse and responsible, they need to see those same strengths in the vendors they engage with.

In addition to expecting these values from your partners, emerging global regulations, such as the German Supply Chain Act, require organizations to pursue this kind of approach to third-party risk. Specifically focusing on human rights risks in the supply chain, organizations must also include a focus on third-party ESG efforts – adding a new layer to third-party risk management.

View all risk with a comprehensive risk score

Third parties are integral to business operations, but it's important to consider that as partners become more integrated with your business, the risks that come with them are more far reaching.

Understanding the impact your third parties have throughout your business is an important step to managing risk. Collecting risk information – including operational, information security, financial, and compliance-related risks – is the first step. By considering third-party risk as one piece to the overall risk your organization faces you can understand the effectiveness of your program, but more importantly, identify areas to increase focus.

Know how third parties protect their it risks

IT risks have the potential to damage business value, and often come from poor management of processes and events. IT risk programs, including those that comprehend vendor IT risk, focus on identifying and mitigating events that will compromise IT functions.

These may include network communications difficulties, hardware and software failure, natural disasters, human error, and malicious attacks. When outsourcing operations to a third party, establishing detailed insight into each third party's policies, processes, and practices, and ensuring the safeguards in place are comprehensive is a necessary step to protecting your organization. Successfully managing any operational or system-related risk requires a systematic approach that takes the following steps:

- Risk assessments and analysis
- Risk evaluation
- Prioritization
- Control testing

Third parties are considered an arm of your business and should be subject to the same processes your internal employees take to safeguard your data.

Uncover supply chain integrity and plan for interruptions

Understanding how your supply chains operate is crucial to the success of your business. In our digital age, interruptions occur with greater frequency and severity than ever before. Events that prevent businesses from fulfilling their mission are not just the obvious ones of natural disasters, IT outages, or security breaches. Also included are supply chain failures, regulatory fines, social governance issues, and more.

When engaging with third parties, organizations must develop business continuity and mitigation plans ahead of potential supply chain failures. Having mitigation plans in place enables your teams to act quickly in such scenarios, shifting necessary resources and responding to unexpected situations to continue delivering on business needs.

Measure

The overall purpose of measuring your third-party risk management program's effectiveness is to ensure the program is meeting its goals and your organization is well protected from risk.

Measuring effectiveness is often unique to each organization based on its industry, geographic location and the type of third parties engaged. There are several ways to measure the effectiveness of your program, including:

- The scalability of your unified and centralized solution
- The speed and accuracy through which you can onboard new third parties
- The consistency and actionability of your program reporting
- The timeframe and costs associated with remediation of screening and monitoring alerts

Alternatively, you can compare your program performance with an earlier state through:

- The improved quality of your third-party engagements in terms of the number of risks you're identifying
- Your ability to more accurately identify third-party characteristics that represent increased risk to your organization
- Your ability to better manage or mitigate associated risks, including swapping out poorly performing third parties for more responsive partners
- The relative business costs of onboarding, screening, monitoring, and lifecycle management, as well as the impact of your solution to shorten downtime and reduce related costs

Ultimately, when you review your program performance, consider the initial risk assessment you completed. This risk assessment should inform your return on investment. When you calculated your risk based on the regulatory environment, the number of third parties you engage with, their criticality to your operations, and the financial risks your third parties represented, you created a risk score.

That risk score can be contrasted against the goals of a third-party risk management program and your progress on them. Those goals are:

- Avoid fines, regulatory enforcement action and legal costs
- Promote your organization's culture
- Promote a more accurate picture of risk
- Promote continuity
- Promote the organization's reputation

Where your program helped the organization avoid fines, improve defensibility, and drive program precision through documented processes, controls, protocols, and outcomes, you can link it to a reduced risk score.

If you use a third-party risk management provider, you can use strong reporting tools to detect problems, analyze trends, and automate the program without relying on in-house staffing and reporting. The best, most effective reporting programs are ones that take advantage of data and use it to gauge the success of interventions, track trends, and evaluate the overall health of third-party relationships.

Conclusion

An effective, well-resourced, consistent third-party risk management program is in your best interest. Not only can you confidently engage with a growing network of vendors, suppliers, resellers, and distributors, you can also have a positive impact on the GRC program as a whole.

Effective third-party risk management is a crucial component of business programs. As detailed in this guide, a robust program requires commitment, focus and structure. Better managing your third-party risk does not necessarily require a large budget or staff. Instead, focus on building an effective program that scales to the level and types of risks your organization faces in its third-party landscape.

NAVEX®

NAVEX is the recognized leader in risk and compliance management software and services, empowering thousands of customers around the world to manage and mitigate risks with confidence. NAVEX's mission is to help customers promote ethical, inclusive workplace cultures, protect their brands and preserve the environment through sustainable business practices.

For more information, visit NAVEX.com and our blog. Follow us on Twitter and LinkedIn.

AMERICAS

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

1 Queen Caroline Street
London, W6 9HQ
United Kingdom
info@navex.com
www.navex.com
+44 (0) 20 8939 1650

COPYRIGHT © 2023 NAVEX GLOBAL. ALL RIGHTS RESERVED.