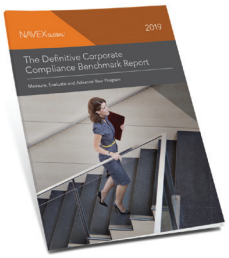
NAVEX GLOBAL®

2020 Third Party Risk Management

Top Market Trends & Analysis

Data & Insights for Maturing Programs



2019 Definitive Corporate Compliance Benchmark Report

Key Findings and Analyses

There is perhaps no topic as top of mind for risk and compliance management professionals as third party risk management. While organizations may have considerable visibility into their own ethics, compliance and risk management practices, they often have little insight into, or understanding of, the risks posed by associated businesses. These threats are heightened by today's regulatory environment, in which world governments and enforcement agencies are increasingly holding organizations responsible for the values, ethics and business behaviors of their third parties – heightening the need for firms to continually monitor and protect against third party risks.

The potential harm posed by third parties isn't limited to regulatory action. The reputational damage firms can experience for associating with an unscrupulous or negligent third party can be far more substantive and lasting than regulatory fines. Businesses can also be held accountable for the past actions and prior associations of the companies they acquire. In some cases, the relationship with the offending party may not even be known to the acquiring organization, yet the damage can be far-reaching, long-term and difficult to recover from.

To keep pace, organizations are expected to employ mechanisms designed to identify whom their third parties are, understand how they do business and determine how committed they are to ethical business and people practices. Centralized, automated and efficient software solutions are key to enabling organizations of any size, shape, industry and location to better manage these third party risk management expectations. With the right solution, organizations will be equipped to operationalize a risk-based approach to due diligence and monitoring throughout their entire vendor and supply chain.

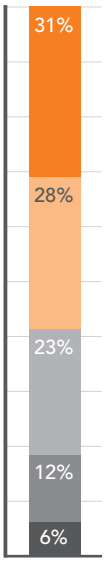


Figure 01

Which best describes your organization's approach to third party risk management?

- None
- High-risk parties only
- All parties
- All parties, risk-based
- All parties, risk-based, continuous

Organizations Should Adopt a Risk-Based Approach to Third Party Risk Management

"Risk-based" is the operative word for modern third party risk management (TPRM). As multiple U.S. agencies have made clear through the issuance of new guidance and frameworks, all organizations are now expected to employ a risk-based approach to the development and implementation of their compliance programs.[1] Such a risk-based approach begins by applying objective criteria to all third parties, creating logical evaluations of potential risks that can be used to formulate tailored risk-mitigation strategies. Organizations identified as high-risk can then be designated for further screening, depending on the specific red flags and risk factors posed. Finally, a risk-based approach to TPRM requires a continuous monitoring of all third parties, with assessments routinely updated to reflect any "apparent violations or systemic deficiencies identified."[2]

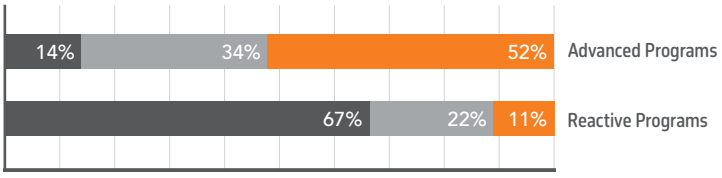
Adopting a risk-based TPRM program provides numerous benefits, including preventing third party misconduct, avoiding government investigations and enforcement actions, enhancing your organization's ethical culture and extending that

ethical culture to your organization's third parties. In 2019, *NAVEX Global's Definitive Corporate Compliance Benchmark Report* collected survey data from risk and compliance professionals across all industries to more closely examine the association between a compliance program's TPRM practices and its broader experiential outcomes. The following report details those conclusions.

Mature Programs Incorporate TPRM Best Practices

Despite greater global regulatory guidance and consistency on the criteria used to evaluate the effectiveness of an organization's TPRM, many compliance programs still lack the tools and practices necessary to meet those expectations. For example, only 59% of all organizations (Figure 01) report applying a risk-based approach to all third parties according to their unique risk factors. Further, less than a third (31%) report doing so on a continuing basis (Figure 02).

However, responses concerning TPRM best practices vary considerably by compliance program maturity.[3] More than half (52%) of *advanced* programs, for example, conduct risk-based assessments of third parties on a continuing basis. Two-thirds (67%) of *reactive* programs, in contrast, fail to conduct any kind of risk-based assessment (Figure 03).



Our data demonstrates a correlation between program maturity and multiple TPRM best-practice trends, particularly with regard to advanced compliance programs. Of *advanced* programs (Figure 04):

- 80% **thoroughly screen** their third parties for defined risk factors, including relationships to government actors, adverse media stories, etc.
- 77% compile their TPRM data into a **centralized, automated portal**
- 73% perform **enhanced due diligence** on third parties determined to pose comparatively greater risks
- 70% screen potential third parties **prior to engagement**
- 59% **continuously monitor** high-risk third parties for changes in risk

In fact, advanced compliance programs had significantly higher adoption rates for almost all TPRM best practices listed in the survey relative to programs overall, directly linking program maturity with best-practice implementation. *Reactive* programs, in contrast, were significantly less likely than their peers to compile their data into a centralized portal, making their lack of centralization a defining trait.

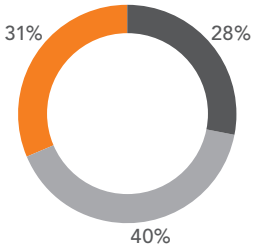


Figure 02

Do You Apply Risk Management According to Individual Third Party Risk?

- 28% No, We Don't
- 40% Yes, As Assessed During the Onboarding Process
- 31% Yes, As Assessed on a Continuing Basis

Figure 03

Advanced Programs: Do You Apply Risk Management According to Individual Third Party Risk?

- 14% No, We Don't
- 34% Yes, As Assessed During the Onboarding Process
- 52% Yes, As Assessed on a Continuing Basis

Reactive Programs: Do You Apply Risk Management According to Individual Third Party Risk?

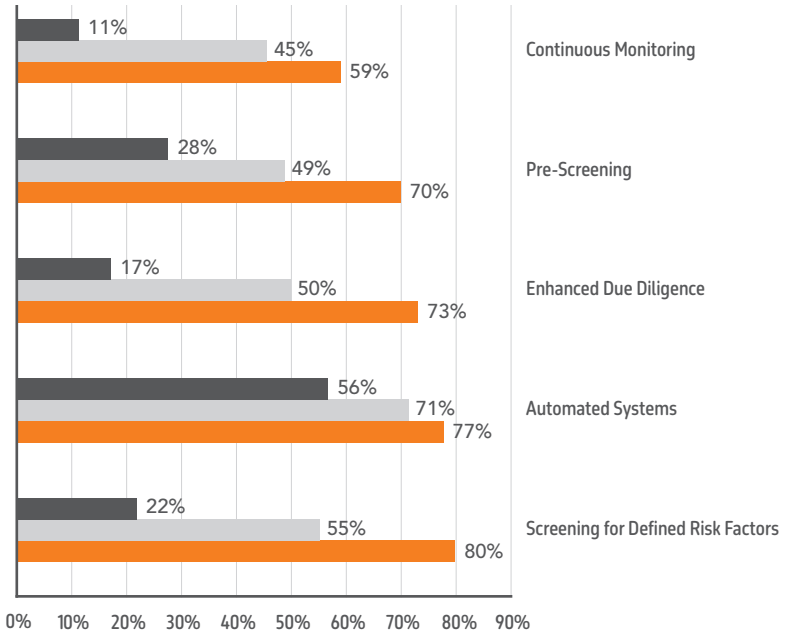
- 67% No, We Don't
- 22% Yes, As Assessed During the Onboarding Process
- 11% Yes, As Assessed on a Continuing Basis

Perhaps most surprising is the finding that more than half (55%) do not practice continuous monitoring, while 45% of all respondents do not perform any screening for defined risk factors. These are perhaps the most basic steps that any organization

Figure 04

What Are Your Current Third Party Risk Management Practices?

- Reactive Programs
- Programs Overall
- Advanced Programs



wanting to engage with third parties should take. Without even basic screening and monitoring techniques, there is no way to confidently identify whom the organization is doing business with and what potential risks are involved. These "unknown unknowns" can pose a unique threat to your organization; TPRM programs are incomplete without comprehensive and consistent screening of all third party entities.

Compliance Program Maturity Is Linked to TPRM Program Performance & Satisfaction

This report not only demonstrates a connection between compliance program maturity and TPRM best practices; the data also found clear links between maturity and measures of TPRM performance and overall program satisfaction. Across the board, the *advanced* and *maturing* programs reported significantly higher "excellent" TPRM program outcomes across KPIs such as (Figure 05):

- Documenting processes and protocols (39%)
- Increasing report accuracy (38%)
- Reducing third-party report time (29%)
- Gaining defensibility with enforcement agencies (27%)
- Automating the management of third-party relationships (23%)

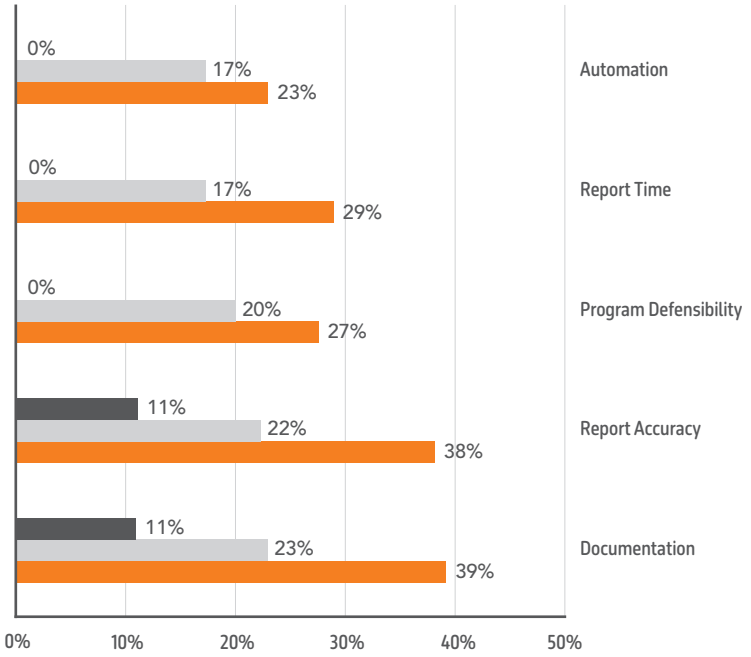


Figure 05

How Would You Rate Your TPRM Program on the Following:

(Percent of Respondents Rating Their Program Dimensions as "Excellent")

- Advanced Programs
- Programs Overall
- Reactive Programs

Conversely, *reactive* programs saw relatively low rates of "excellent" TPRM performance across every single category, with not a single *reactive* program indicating "excellent" performance in gaining defensibility, reducing third-party report time, automating the management of third party relationships, or determining program ROI.

Similar correlations between program maturity and TPRM performance can be seen in the percentage of respondents who believe their third party due diligence program reduces their legal, financial and reputational risks enterprise-wide. Put simply, the more developed and advanced an organization's compliance program, the more faith that organization tends to have in its TPRM practices and its ability to provide lasting positive impact on the business overall. Eighty percent (80%) of *advanced* programs agree that their third party due diligence program significantly reduces legal, financial and reputational risks (Figure 06). Meanwhile, only 23% of respondents from *reactive* programs affirm that their TPRM practices accomplish their risk-reduction goals.

To the extent that a compliance program's maturity level is a reliable indicator its adoption of TPRM best practices, these findings demonstrate a positive association between such practices and compliance program performance. This data also underscores the benefits of growing your organization's compliance program to greater maturity levels, and further demonstrates the potential ROI that is inextricably intertwined with overall program maturity. Organizations that commit to implementing best practices and effective TPRM strategies will achieve significant benefits in risk reduction, while less mature programs will continue to encounter major third party risks.

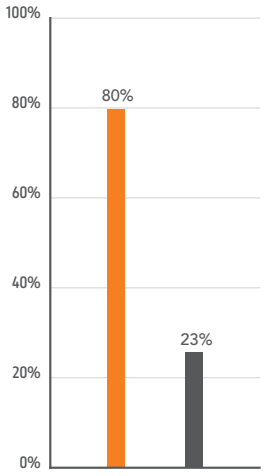


Figure 06

Rate your agreement with the following statement: Our third-party due diligence program significantly reduces our legal, financial and reputational risks

- 80% Advanced Programs
- 23% Reactive Programs

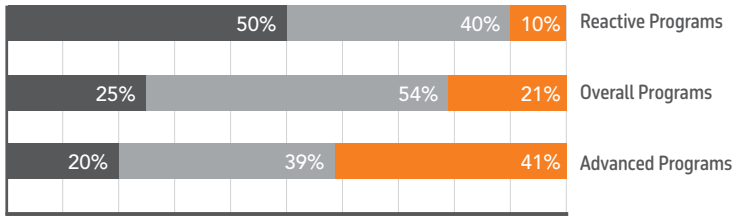
TPRM Information Technology & Automation Solutions Should Be Tailored to Risk

Of all the TPRM best practices outlined in the latest regulatory guidance, one of particular note is the emphasis information technology solutions. As the Office of Foreign Assets Control (OFAC) notes in its framework, regulators now expect organizations to employ information technology solutions specifically selected and calibrated "in a manner that is appropriate to address the organization's risk profile and compliance needs."[4] Not only are TPRM technologies required; they must now be as tailored to an organization's risk profile as the TPRM programs they support.

Figure 07

What Type of System Do You Use to Manage TPRM?

- Paper-based
- Other
- Purpose-built



Certainly, different organizations make use of varied technological solutions to advance and promote their TPRM efforts. The data on compliance programs' use of technology, however, presents a stark contrast between *advanced* and *reactive* programs' overall levels of technology adoption and optimization. A plurality of *advanced* programs (41%) indicate they utilize purpose-built TPRM software solutions to organize, centralize and manage their third party data. Fully half of *reactive* programs (50%), meanwhile, rely on highly manual systems that use rudimentary technology to collect data either entirely in paper or with outdated, stitched-together software (Figure 07). Overall, while organizations' technological approaches to TPRM remain varied, there is a clear correlation between program maturity and solution sophistication, indicating a trend toward the adoption of purpose-built software to screen and monitor third party relationships.[5]

The principle goal of any software solution is to attain and implement a system that is streamlined, centralized, efficient and capable, allowing for real-time alerts, visual depictions of risk, automated risk-mitigation responses and enterprise-wide success. Custom Relationship Management (CRM) programs, Enterprise Resource Planning (ERP) programs and office productivity tools may provide some degree of record centralization and visualization. However, these methods are not built for broader compliance purposes and thus do not allow organizations to rank and stratify risk levels. Likewise, internally built or highly manual systems may offer some basic benefits, but these solutions' effectiveness is drastically reduced when organizations move beyond a handful of third party relationships.

Similar shortcomings apply to software solutions that have been repurposed or reconfigured to address third party risks. While these ideas allow for baseline levels of recordkeeping and risk assessment, the gaps and inconsistent risk-management capabilities they present tend to compromise overall TPRM program effectiveness.

Conclusion

In surveying the Ethics & Compliance market, we consistently find that many practitioners remain uncertain as to program best practices and how to prioritize compliance program initiatives among competing demands. This report is intended to help practitioners gain useful insights into the risk and compliance marketplace and benchmark their programs against those of other organizations. For the fifth consecutive year, NAVEX Global's TPRM benchmarking survey has demonstrated that an effective TPRM program is critical to overall organizational performance, as it ensures that the organization's revenue, reputation and culture are secure against third party misconduct. This survey and report fully aligns with recent market trends demonstrating that organizations have recognized the link between ethical culture, reduced third party misconduct, financial performance and sustainable growth. We continue to observe positive trends in terms of organizations working to pursue effective TPRM programs.

If your organization has not formalized its TPRM program, it is important to understand the best practices that you should be striving toward. One-size-fits-all solutions never work, as each organization has a different inherent risk profile. Your compliance program needs to reflect actual risks rather than assumptions. The first step is to gather the right stakeholders from within the organization, including the compliance team, the legal team, audit, procurement and others, so everyone can understand both the broad objectives and the organization's unique risk profile. That profile should steer all other risk-management processes.

One-size-fits-all solutions never work, as each organization has a different inherent risk profile. Your compliance program needs to reflect actual risks rather than assumptions.

[1] For further detail, please see "Evaluation of Corporate Compliance Programs" (U.S. Department of Justice Criminal Division, April 2019), https://www.justice.gov/criminal-fraud/page/file/937501/download, as well as "A Framework for OFAC Compliance Commitments" (U.S. Department of the Treasury's Office of Foreign Assets Control, May 2019), https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.

[2] "A Framework for OFAC Compliance Commitments," page 4.

[3] The 2019 Definitive Corporate Compliance Benchmark Report assigned survey respondents' compliance programs one of four distinct maturity labels – *reactive, basic, maturing,* or *advanced* – based on their responses to key survey questions.

[4] "A Framework for OFAC Compliance Commitments," p.6

[5] "Purpose-built" in this context refers to software that is designed for and dedicated to TPRM optimization.

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.**

NAVEX GLOBAL®

AMERICAS

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

EMEA + APAC

4th Floor, Vantage London
Great West Road
Brentford, TW8 9AG
United Kingdom
info@navexglobal.com
www.navexglobal.co.uk
+44 (0) 20 8939 1650

PLEASE
RECYCLE

Copyright © 2020 NAVEX Global Inc. All Rights Reserved.