2018 Ethics & Compliance Third-Party Risk Management Benchmark Report

Data and Insights to Get More Value from Your Program
PREPARED BY:

Michael Volkov,
CEO and Founder of The Volkov Law Group, LLC

WITH:

Loren Johnson,
Senior Manager Product Marketing, NAVEX Global

Tanya Stricker,
Senior Manager Demand Generation, NAVEX Global
## CONTENTS

**INTRODUCTION**
- How to Use This Report 2
- How This Report Is Different 3
- How Do We Define “Third Parties”? 3
- What Is Third-Party Risk Management & Third-Party Due Diligence? 3

**SURVEY RESPONDENT PROFILE** 4

**EXECUTIVE SUMMARY** 6

**KEY FINDINGS** 10
- 1: Foundational Data 11
- 2: Ethics & Compliance Program Performance 14
- 3: Third-Party Risk Management Programs 26

**CONCLUSION & KEY METRICS** 45

**ABOUT NAVEX GLOBAL’S THIRD-PARTY RISK MANAGEMENT SOLUTION** 49

**ADDITIONAL RESOURCES** 50

**ABOUT THE AUTHOR** 51
INTRODUCTION

In 2018, NAVEX Global partnered with an independent research firm to survey professionals from a wide range of industries about their approach to building an effective ethics and compliance (E&C) program.

The findings in this report are based on survey results from 1,200 respondents who influence or manage their organization’s ethics and compliance programs, and from approximately 500 of the 1,200 respondents who influence or manage the third-party risk management function within their organization. (See respondent profile in the next section for additional details.)

This report provides insights and analysis of ethics and compliance programs and specific third-party risk management questions including:

- What are the top priorities of ethics and compliance programs?
- What resources are dedicated to ethics and compliance programs?
- How do respondents measure the effectiveness of their ethics and compliance program?
- What factors influence ethics and compliance program performance?
- How are organizations managing third-party risks?
- What strategies and procedures do organizations use to manage third-party risks?
- How do organizations employ risk-based procedures to manage third-party risk?

How to Use This Report

This analysis reflects the perspective of ethics and compliance professionals on the importance of third-party risk management as part of an overall ethics and compliance program. The data presented provides important insights, benchmarks and trends needed to make informed decisions on how to improve your own ethics and compliance program. By providing a picture of E&C program trends and insights, this report outlines how third-party risk management fits into overall activities. In this report, we analyze the performance of third-party risk management programs within the larger context of a complete compliance program.

This report can help you:

- Assess and benchmark your organization’s ethics and compliance program.
- Review your ethics and compliance program priorities and effectiveness in comparison to factors identified by respondents summarized in this report.
- Determine whether your third-party due diligence screening, monitoring and risk mitigation practices are protecting your organization or exposing it to risk.
- Benchmark your third-party risk management program against peers, industry practices and best practices – including assessing your program maturity and steps you can take to improve its performance.
- Leverage report data and recommendations to gain additional organization buy-in and understanding of the value of a comprehensive third-party risk management program.
We hope the insights presented here will provide the inspiration, justification and direction necessary to make key decisions about the future of your organization’s approach to third-party risk management.

How This Report Is Different
This is the fourth year NAVEX Global has published its third-party risk management market benchmark report. This year, the survey was designed to collect data concerning overall ethics and compliance programs, including general program performance as well as approaches toward hotline and incident management services, policy and procedure management, ethics and compliance training and third-party risk management. Within this holistic context, we have discovered important insights concerning third-party risk management and identified trends and performance measurements for third-party risk management strategies.

We have noted specific findings and analysis where the results were based on responses to ethics and compliance program questions, and those that were based on respondents responsible for third-party risk management programs. This new approach allows readers to understand the general context from which specific insights about third-party risk solutions are made.

How Do We Define “Third Parties”?
For the purposes of this report, the term “third parties” is defined broadly and includes:

- Consultants: auditors, lobbyists, management consultants
- Contractors: temporary employees, subcontractors
- Agents: international intermediaries, domestic agencies, local advertisers and marketers
- Vendors: data vendors, maintenance, on-demand service providers, offshore service providers
- Suppliers: branded, white-branded or third-party branded material suppliers and manufacturers as well as those suppliers’ suppliers
- Distributors: dealers and resellers, foreign distribution firms and their local resellers
- Joint ventures: partnerships, international joint ventures (factories, manufacturers, dealers), franchisees

What Is Third-Party Risk Management & Third-Party Due Diligence?
For the purposes of this report, third-party risk management is an umbrella term that refers to all risk management activities related to your third parties, including onboarding, screening, monitoring, in-depth risk analysis, and associated relevant processes meant to identify, stratify and mitigate third-party related risks.

Third-party due diligence refers to the studied assessment of third parties before, during and after an engagement. It can include conducting internal business justifications, external preliminary risk assessments, establishing business rules and authorizations, processing documentation and policies (codes of conduct and ethics training), as well as analysis of databases and reputational reporting. It also includes active monitoring of your third-party engagements for new “red flags” and changes to the third-party’s risk profile.
SURVEY RESPONDENT PROFILE

N = 503

Job Function

- Ethics & Compliance: 37%
- Human Resources, Employee Relations: 13%
- Legal: 9%
- Internal Audit: 8%
- Risk Management: 7%
- Other: 26%

Job Level

- C-Level: 16%
- Senior Management / Director: 41%
- Other Management: 31%
- Non-Management: 12%

Company Annual Revenue USD

- $0 < $50M: 26%
- $50M - $999M: 32%
- $1B+: 31%
- Not for profit / Government: 11%

Company Size

- Large: 5,000 + Employees: 21%
- Medium: 501 - 5,000 Employees: 40%
- Small: < 500 Employees: 39%

Role in Third-Party Risk Management Programs

- Decision Maker: 41%
- Influencer / Advisor: 59%
### Location of Headquarters

- **North America**: 70%
- **Europe**: 14%
- **Asia Pacific**: 5%
- **Africa**: 5%
- **Caribbean**: 1%
- **Middle East**: 1%
- **Central America**: 1%
- **South America**: 3%

### Industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare &amp; Social Assistance</td>
<td>17%</td>
</tr>
<tr>
<td>Finance &amp; Insurance</td>
<td>13%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>12%</td>
</tr>
<tr>
<td>Educational Services</td>
<td>7%</td>
</tr>
<tr>
<td>Professional, Scientific &amp; Technical Services</td>
<td>7%</td>
</tr>
<tr>
<td>Transportation / Distribution / Logistics, etc</td>
<td>6%</td>
</tr>
<tr>
<td>Mining, Quarrying, Oil &amp; Gas Extraction</td>
<td>3%</td>
</tr>
<tr>
<td>Retail Trade</td>
<td>3%</td>
</tr>
<tr>
<td>Agriculture, Forestry, Fishing &amp; Hunting</td>
<td>2%</td>
</tr>
<tr>
<td>Construction</td>
<td>2%</td>
</tr>
<tr>
<td>Leisure, Hospitality, Recreation &amp; AE</td>
<td>2%</td>
</tr>
<tr>
<td>Public Administration</td>
<td>2%</td>
</tr>
<tr>
<td>Utilities</td>
<td>2%</td>
</tr>
<tr>
<td>Wholesale Trade</td>
<td>2%</td>
</tr>
<tr>
<td>Other Services</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td><strong>18%</strong></td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

NAVEX Global produces a series of market benchmark reports throughout the year on multiple ethics and compliance topics – whistleblower hotlines and incident management, policy management, compliance training and third-party risk management. Each report captures a peer-generated, state-of-the-market view that is unavailable elsewhere. Combined, these reports deliver a comprehensive picture of the global ethics and compliance marketplace, trends and best practices.

For this year’s third-party risk management report, we collected information on respondents’ ethics and compliance programs as well as data specific to third-party risk management programs. This holistic perspective focuses on the overall ethics and compliance market and includes insights on a range of specific issues relating to third-party risk management.

Our approach targets issues surrounding how third-party risk management fits into overall ethics and compliance programs. No one doubts the importance of addressing third-party risks as part of an E&C program. While third-party risks are certainly one of the major risks, organizations face a variety of risks and are forced to prioritize risk mitigation strategies within a broader context. In this process, organizations have to identify efficient and effective ways to mitigate third-party risks. Our report specifically addresses this important issue with relevant data points, trends and observations, and identifies several important factors to consider in managing third-party risk. These factors include maturity of the third-party risk management program, adequate resources and budget, and reliance on software and automated solutions.

As confirmed in this report, our comprehensive survey found that the objectives of an ethics and compliance program and a third-party risk management program are closely aligned – both share the objective of advancing the organization’s culture of integrity, ethics and respect (page 14). This finding reflects the growing emphasis ethics and compliance programs have placed on corporate culture and ethics over the last few years. Our survey and report bolsters recent trends showing that corporations have recognized the inextricable link between ethical culture, reduced employee and third-party misconduct, and financial performance and sustainable growth.

In this context, an effective third-party risk management program is a critical component to ensure that an organization’s reputation is protected from third-party misconduct and aligns third parties to the values, ethics and risk management approach of the organization. Yet, while ethics and compliance program leadership may have broad visibility into the behaviors and efforts within their own organizations to build and nurture strong, positive cultures, few organizations have the same level of visibility into their third parties. For many, the need to align their third parties to organizational values reinforces the importance of an organization investing in and maintaining a best practices, high-quality third-party risk management program.

Consistent with this key finding of our report, respondents also cited two other significant objectives of their third-party risk management program – implementing preventative measures to avoid future issues or misconduct, followed by navigating and complying with laws and regulations. Both of these objectives reflect
significant priorities to ensure compliance with global laws, regulations and expectations, and preventing misconduct and any follow-on investigation. Anti-bribery, fraud and corruption laws are changing across the globe and respondents recognized that they face significant challenges in staying up to date and keeping their organizations in compliance.

Taking the Right Approach

Over the last six years, NAVEX Global has identified clear trends in the ethics and compliance market toward program consolidation, automation and sophistication. This evolution is unmistakable. The ethics and compliance marketplace continues to change. The advent of new technologies is also changing regulatory expectations and therefore program best practices. Despite these significant gains, our surveys consistently demonstrate that programs are challenged when seeking effective practices to assess, measure and report on program performance. To E&C professionals, these issues are critical to demonstrate that high performing programs both protect the organization from risk and advance the enduring character and culture of the organization.

Over the last three years, we have seen significant shifts in the market. While more organizations take a structured approach to managing third-party risk, many respondents indicate their program is still not fully delivering expected value.

Our survey included several questions focusing on how organizations design and implement their third-party risk management programs. While most organizations understand the potential risks associated with third parties, many have not committed to a fully compliant or best practice program. Too many either ignore or make assumptions about potential risk without qualifying judgements with data. This is exacerbated by a lack of visibility necessary to prioritize risk and take strategic steps to protect the organization. Too often, insufficient resources are dedicated to third-party risk management – including budget, personnel and technologies.

In this year’s report, we defined program maturity based on responses to key questions that exemplify best practices for third-party risk management. These best practices are based on global regulatory requirements (primarily the U.S. Foreign Corrupt Practices Act, Resource Guide to the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, program elements defined in the U.S. Department of Justice's Evaluation of Corporate Compliance Programs document published in February 2017, and discernable patterns in global enforcement actions and outcomes).

While some government guidance on managing third-party risks is vague, such as pursuing “reasonable” and “recommended” actions, there is some consistency in program structure and expected activities to protect engaging organizations from third-party risk. Please refer to NAVEX Global’s Definitive Guide to Third-Party Risk Management for details on best practice approaches.
A common theme in well-run compliance programs is the importance of risk-based, properly resourced, balanced, effective and repeatable third-party risk management policies and procedures. This includes defined procedures that apply across all third parties to screen, assess and create a documented audit trail to demonstrate a logical evaluation of potential risk with reasonable mitigation practices. The same standards apply across all third parties, every time, in every location, role and level of engagement to ensure program consistency and accuracy. Such a strategy permits organizations to vary the level of inquiry beyond a basic screening and assessment depending on the specific risk factors underlying the organization’s third-party risk profile.

Global enforcement agencies expect organizations to make common-sense and risk-based decisions when assessing, prioritizing and mitigating third-party risk, based on business requirements and steps taken to protect the engaging organization from such risks. These agencies seek assurances that organizations take third-party risk seriously, adequately extend their own ethics and compliance program to their third parties and implement a reasonable approach to reduce associated risks.

A risk-based third-party compliance program provides numerous positive benefits: enhancing the organization’s ethical culture and extending such culture to its third parties, preventing possible third-party misconduct, and avoiding government investigations, enforcement actions and damaging collateral consequences from such misconduct. When investigating a company for potential misconduct, the U.S. Department of Justice and the Securities and Exchange Commission typically evaluate the company’s ethics and compliance program and its commitment to prevent employee and third-party misconduct. In numerous situations, this determination can have direct and significant consequences for the overall resolution of the investigation. The government’s decision to decline prosecution or initiate a formal enforcement matter can turn on the extent to which a company was committed, both in words and in action, to an effective ethics and compliance program, and a third-party risk mitigation strategy to prevent misconduct.

Helping the Market Succeed

In surveying the ethics and compliance market, we consistently find that many practitioners remain uncertain as to program best practices and how to prioritize among competing demands. We recognize that our report helps practitioners gain insights into the ethics and compliance marketplace and benchmark their programs against other organizations’ programs. NAVEX Global is committed to helping our customers understand the current market, organizations meet internal and external expectations and to protecting companies from third-party risks. To that end, we are confident that education is essential to inform decisions and implementation of effective risk mitigation strategies.
Many of the processes discussed in this report demonstrate best practices in terms of program structure, recordkeeping, automation and risk mitigation. The results demonstrate that including these key functions in third-party risk management reduces risk and improves program performance. Well-run programs with defined policies and automated processes are more effective and efficient in managing third-party risks.

Adopting best practices around managing third-party risk is analogous to buying an effective insurance policy. An effective third-party risk management program provides a solid foundation for every compliance program and protects an organization from significant risks and threats to the organization.
As noted in the executive summary, this report includes data and analysis relating to ethics and compliance programs and third-party risk management practices based on the responses of 1,200 industry professionals. This section provides foundational information about how organizations approach ethics and compliance strategies today and trends within the market.

This information provides the backdrop against which third-party risk management programs are designed, implemented, measured for effectiveness and improved. Of the 1,200 respondents, approximately 500 individuals completed a specific section of the survey focused on third-party risk management. The third-party risk management questions were designed to develop insights relating to third-party risk management market and program trends.

How Many FTE (Full-Time Employees) or Equivalent are Assigned to Your E&C Program?

<table>
<thead>
<tr>
<th>Number of FTEs</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 1</td>
<td>9%</td>
</tr>
<tr>
<td>1 to 4</td>
<td>50%</td>
</tr>
<tr>
<td>5 to 10</td>
<td>17%</td>
</tr>
<tr>
<td>11 or More FTEs</td>
<td>24%</td>
</tr>
</tbody>
</table>

Organizations are required to dedicate adequate resources to their ethics and compliance program. The number of full-time (or equivalent) employees assigned to E&C teams and a dedicated budget are essential indicators of an organization’s commitment to program success. The results outlined below were generated from respondents to the survey questions relating to ethics and compliance program management.

Interestingly, the results discussed below confirm a continuing trend noted in prior benchmark reports – organizations that maintain a dedicated compliance program budget and assign additional full-time employees also have a dedicated budget for third-party risk management and are increasing the assignment of full-time employees to third-party risk management.
part risk management. This trend may reflect that third-party risk management duties are being executed within the organization’s ethics and compliance program. We will continue to monitor this trend and the consolidation of third-party risk management responsibilities from other functions (e.g., procurement, supply chain management) into ethics and compliance programs.

As we have seen in our prior benchmark reports, the performance and program maturity of an ethics and compliance program is significantly influenced by the number of full-time employees dedicated to a program and the budget.

**Program Expenditures**

An organization that maintains a dedicated budget for its E&C program is committed to compliance. Twenty-three percent of respondents reported they have no dedicated budget for its ethics and compliance program. We observed a similar result in last year’s third-party risk management report.

Without a dedicated budget, organizations find it more difficult to plan year-by-year activities and performance improvements. The absence of a budget framework complicates an organization's ability to identify relevant risks and implement effective mitigation strategies to maintain regulatory compliance. The inability to retain and grow experienced ethics and compliance professionals due to a lack of budget forces organizations to reinvent or repeat program planning and implementation every few years. As a consequence, E&C programs fail to mature or evolve. This disconnect is even more disturbing given changes in the organization’s risk profile. Defining a budget allows organizations to consistently know where they stand and build long-term strategies independent of employee retention.

The good news is that budgets for third-party risk management are slated for the largest expected increase in funding among ethics and compliance program components. Just over one-quarter (27%) of the respondents indicated that their third-party risk management program expects to see at least a 10 percent budget increase in the next year.
What is Your Dedicated Annual Budget for E&C, not Including Employee Salaries (in U.S. Dollars)?

![Bar chart showing budget distribution]

- $1-50,000: 41%
- $50,001-100,000: 11%
- $100,001-250,000: 10%
- $250,001-500,000: 6%
- $500,001+: 9%
- We Have No Dedicated Budget: 23%

How Will Your E&C Program Budget Change in the Next Year?

![Bar chart showing budget change percentages]

- Hotline and Incident Management: 83% Decrease, 8% Decrease More, 6%
- Policy and Procedure Management: 79% Decrease, 12% Decrease More, 6%
- E&C Training: 71% Decrease, 16% Increase, 9%
- Third-Party Risk Management: 68% Decrease, 18% Increase, 9%

Base: Respondents involved in decisions for specific E&C programs, n=556-748.
Top Training Objectives

Findings: Creating a culture of ethics, integrity and respect is the top ethics and compliance program objective (68%) and is seen as more important than implementing preventative measures and practices to avoid future issues (62%) and navigating and complying with laws and regulations across jurisdictions (47%).

- Organizations with annual revenues of $1 billion or more are more likely to focus on navigating and complying with laws and regulations across jurisdictions than organizations with less than $50 million in revenue (56% vs. 42%).
- Responses from third-party risk management professionals about program objectives correspond with overall ethics and compliance professionals – 69 percent indicated commitment to a culture of ethics, integrity and respect; 65 percent selected implementing preventative measures and practices to avoid future issues; and 49 percent selected complying with laws and regulations across jurisdictions as top program objectives.

Which E&C Program Objectives Are Most Important to Your Organization Over the Next 12 Months?

Multiple response question, totals may not add up to 100%. n=1,264.
Analysis: The results reflect an important trend in ethics and compliance programs and third-party risk management – organizations are recognizing the importance of promoting an ethical culture. This year’s results reflect an important transformation in E&C program objectives. In past years, the top objective was to avoid legal and regulatory enforcement matters. This perspective has evolved. This year, both ethics and compliance and third-party risk management professionals indicated that their top objective is their organization’s ethical culture. It is clear that ethics and compliance professionals understand the importance of an ethical culture to a company’s overall financial performance and sustainability. Third-party risk management plays a critical role in promoting and protecting a company's ethical culture from third-party misconduct.

As noted in the executive summary, we continue to see the rise in the importance of third-party risk managers in ethics and compliance programs. As these professionals take on greater responsibilities, they usually have a dedicated budget for their function and exercise increased decision-making authority.

The increase in, and consolidation of, third-party risk management responsibilities into ethics and compliance programs is a natural development as regulations and enforcement agencies expect organizations to expand their programs to manage and mitigate third-party risks. As part of this overall responsibility, ethics and compliance programs share their company’s code of conduct, implement ethics training and other program elements with their third parties, and often require attestation to policies and behavioral expectations before agreements can be completed.
Top Program Concerns

Findings: Ethics and compliance departments face a broad array of risk in today's global economy and regulatory framework. According to our survey respondents, E&C professionals are most concerned about implementing an effective business code of conduct (46%) and responding to cyber security events (44%). Procedure management/quality control (28%), conflicts of interest (25%) and anti-bribery (21%) round out the top five concerns identified by respondents.

- Organizations with more than 5,000 employees identified anti-bribery and fraud as top concerns almost three times as often as small organizations with fewer than 500 employees (35% vs. 12%) and nearly two times as often as midsize organizations with 500-5,000 employees (19%).

Which of the Following E&C Topics Are Top Concerns in Your Organization?

- Ethics and Code of Conduct: 46%
- Cyber Security and Data Privacy: 44%
- Procedure Management / Quality Control: 28%
- Conflicts of Interest: 25%
- Anti-Bribery and Corruption / Fraud: 21%
- Speaking Up and Retaliation: 19%
- Workplace Harassment: 19%
- Diversity and Discrimination: 16%
- Social / Environmental Responsibility: 14%
- Intellectual Property and Asset Protection: 12%
- Wage and Hour Violations: 8%
- Political Exposure and Risks: 7%
- Financial Integrity and Insider Trading: 7%
- Anti-Money Laundering: 7%
- Workplace Violence: 6%

Multiple response question, totals may not add up to 100%, n=1,264.
Organizations with fewer than 500 employees identified procedure management/quality control as a top-three concern more than larger organizations (37% vs. 29% 500-5,000, 15% >5,000).

Organizations with $1 billion in revenue were more likely to indicate cyber security and data privacy as a top concern than lower revenue or government/non-profit organizations (53% vs. 36% and 45% respectively).

**Analysis:** Reflecting the recent focus on ethical culture and integrity, respondents identified ethics and code of conduct as their top concern (46%). Consistent with past results, cybersecurity and data privacy (44%), conflicts of interest (25%) and anti-bribery (21%) fell within the top five concerns.

Corporate compliance program best practices and government expectations for third-party risk management programs have stressed the importance of providing positive incentives for third parties to adhere to ethical behavior and compliance. To this end, an organization can craft and disseminate an engaging code of conduct – an all-encompassing policy on expected behaviors, compliance and reporting – and require third parties to attest to its understanding of its obligations under the code of conduct. An organization has to infuse its procedures for onboarding, monitoring and auditing its third parties with robust reinforcements of its ethical culture and its commitment to integrity.

Cyber security is a constant high-risk concern to ethics and compliance professionals. While cyber security risks pose significant potential harm from outside actors who are dedicated to launching sophisticated cyber-attacks, organizations are fighting back with encryption to protect against such attacks. However, companies continue to face significant risks through internal actors who may deliberately seek to steal or breach company data, or inadvertent actors who fall prey to phishing and other cyber-schemes designed to launch malware attacks. As a result, ethics and compliance professionals have focused on training, security and awareness strategies to prevent employees from falling for phishing schemes and to protect the organization from employee sabotage. Third parties also create significant cyber security risks through access to corporate data that should not be ignored.
Ethics & Compliance Program Elements

**Findings:** A code of conduct (87%) and effective policies and procedures that reduce misconduct (83%) are the most common E&C program elements. Audit programs (56%), a dedicated chief compliance officer (54%) and a risk-based due diligence program for third parties (45%) are less commonly included.

**Analysis:** These findings correspond and relate to addressing the top program objectives and concerns. It’s encouraging to see that 87 percent of respondents have a code of conduct, especially as the *U.S. Federal Sentencing Guidelines for Organizations* require organizations to establish and distribute a code of ethics.

When properly done, a code of conduct can be one of the most effective channels through which an organization commits to and drives positive

Does Your E&C Program Include the Following Elements?

<table>
<thead>
<tr>
<th>Element</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code of Conduct</td>
<td>87%</td>
</tr>
<tr>
<td>Effective Policies and Procedures That Prohibit and Reduce Misconduct</td>
<td>83%</td>
</tr>
<tr>
<td>Training Based on Your Organization’s Risks and Individual Roles</td>
<td>73%</td>
</tr>
<tr>
<td>Non-Retaliation Policies Across the Organization</td>
<td>70%</td>
</tr>
<tr>
<td>An Anonymous (e.g., Hotline) Reporting Channel with Consistent Investigations</td>
<td>67%</td>
</tr>
<tr>
<td>Buy-In, Oversight and Commitment from Senior Leadership</td>
<td>66%</td>
</tr>
<tr>
<td>Periodic Assessment of Your Organization’s Risk Profile and Program Effectiveness</td>
<td>61%</td>
</tr>
<tr>
<td>An Audit Program That Measures Compliance Program Effectiveness and Makes Improvements</td>
<td>56%</td>
</tr>
<tr>
<td>A Dedicated Chief Compliance Officer</td>
<td>54%</td>
</tr>
<tr>
<td>A Risk-Based Due Diligence Program for Third Parties</td>
<td>45%</td>
</tr>
</tbody>
</table>

Multiple response question, totals may not add up to 100%. n=1,264.
behavioral standards and cultural change. Because a code reflects what matters to the organization and how it celebrates its people, processes and goals, it should define and connect all stakeholders to its mission and values, including its third parties. NAVEX Global sees an optimized code of conduct as the cornerstone of an effective ethics and compliance program.

Both enforcement agencies and organizational stakeholders expect ethics and compliance programs to abide by the law and develop and maintain a positive working environment. A code is a central element of a successful program. The second most commonly included program element, effective policies and procedures that prohibit and reduce misconduct, is similarly central to a compliance program and instrumental to an effective third-party risk management program.

A risk-based due diligence program for third parties is the lowest-ranked program element in this group of responses. As noted above, the responses in this chart include every survey taker, not restricted to those who know and manage their third-party risk. The response, at 45 percent (representing 569 respondents), aligns to our expectation for where the market is today and how third-party risk management is evolving in the ethics and compliance space. That said, many organizations may take too lightly the damage that third-parties can inflict on their reputation and finances by minimizing their focus or ignoring this essential compliance program element completely.
Ethics & Compliance Program Priorities

Findings: Ethics and compliance departments identified their priorities for the next 12 months. The top three were: increasing awareness of the company’s policies and regulations (50%); improving or increasing ethics and compliance training activities (40%); and training and supporting frontline managers and supervisors on their responsibilities (39%). These priorities are consistent with an increasing focus on ethics, integrity and respect as a mission-critical objective. Notwithstanding this focus on ethical culture, only 19 percent of respondents identified conducting an ethics and culture assessment as a priority over the next 12 months.

→ Organizations with more than 5,000 employees and those with $1 billion in revenue are more likely to prioritize improving the effectiveness of whistleblowing channels/investigation techniques and improving third-party due diligence oversight than smaller companies with less than $1 billion in revenue.

Which of the Following E&C Activities Will Your Organization Be Prioritizing Over the Next 12 Months?

Multiple response question, totals may not add up to 100%. n=1,264.
Analysis: Even though ethics and compliance professionals have a significant number of pressing priorities over the next 12 months, it is surprising that only 23 percent of respondents indicated that improving third-party due diligence and oversight was one of their top three priorities. While this response was disturbing, it may reflect the number of competing priorities to third-party risk management. Interestingly, none of the responses topped 50 percent, indicating ethics and compliance professionals face a large number of important priorities.

That said, the program element prioritized above third-party due diligence are important tasks that contribute to a more effective third-party risk management program. Increasing awareness of policies and regulations, improving training activities, supporting frontline managers on responsibilities, auditing and conducting risk assessments will improve the overall operation of the third-party risk management program.
Compliance Program Effectiveness Measures

Findings: With the increasing focus on measuring and testing the effectiveness of ethics and compliance programs, organizations are employing a variety of methods to assess effectiveness. The most common approaches cited by respondents include: number of code of conduct breaches (43%); analysis of internal audit findings (41%), conducting exit interviews (40%); and employee surveys (40%).

- Organizations with less than $50 million in revenue (42%) and those with revenue between $50 million and $1 billion (43%) generally measure program effectiveness by exit interviews and employee turnover rates.

Analysis: Given the absence of any “one-size-fits-all” approach to the design and implementation of ethics and compliance programs, it is not surprising that developing appropriate tools and metrics to evaluate program effectiveness has been difficult and subject to a variety of techniques. Once an established set of metrics is developed, companies face challenges in deciding how to use relevant metrics to assess and improve program performance. Interestingly, many companies use a mix of qualitative and quantitative measurements to evaluate ethics and compliance programs.

As demonstrated in the table below, ethics and compliance professionals have a variety of metrics and types of measures to assess their program effectiveness. Almost half of third-party risk management leaders rely on periodic risk assessments and program audits to assess their program performance.
What Metrics Do You Use to Measure Compliance Program Effectiveness?

- Breaches of the Code-of-Conduct / Internal Policies: 43%
- Analysis of Internal Audit Findings: 41%
- Conducting Exit Interviews and Measuring Employee Turnover: 40%
- Employee Surveys: 40%
- Tracking Whistleblowing Reports, Retaliation and Substantiation Rates: 34%
- Comparisons Using Third-Party Measurements or Benchmarks: 29%
- Attestation Rates on Training and Policy Programs: 21%
- Comprehension Questionnaires on Training or Policies: 21%
- Monitoring Reviews on “Glassdoor” / Social Media Articles / News Reports: 18%
- Independent Evaluations by Outside Counsel and / or Consultants: 16%
- Case Closure Times: 14%
- Reduction of Regulatory Fines or Penalties: 11%
- Employee Surveys: 9%
- We Don’t Formally Assess the Effectiveness of Our E&C Programs: 9%
- Comprehension Questionnaires on Training or Policies: 8%
- Reducing Breaches of the Code of Conduct / Internal Policies: 7%
- Reducing Costs: 7%
- Employee Surveys: 7%
- Reducing Breaches of the Code of Conduct / Internal Policies: 7%
- Reducing Costs: 7%
- Employee Surveys: 7%

Multiple response question, totals may not add up to 100%, n=1,264.
Rating Ethics & Compliance Program Performance

Findings: Most respondents were satisfied with the performance of their organization’s ethics and compliance program. Less than a fifth of respondents rated their ethics and compliance program performance as Poor or Fair. However, a significant number of respondents rated measuring effectiveness (25%) and managing third-party risks (21%) as Poor or Fair.

Analysis: The survey results provide important insights into how ethics and compliance professionals view the performance of their compliance program. In general, E&C professionals view their program performance as Good. For each category of performance, the Good response was the highest selected response. This reflects a positive attitude and approach to managing an ethics and compliance program. The large number of positive responses may reflect recent accomplishments, senior management support and some aspirational influence.

With respect to third-party supervisors of third-party risk management programs, most respondents assessed their programs as either Average or Good, and generally avoided an Excellent or Poor rating. In the absence of any significant negative events relating to ethics and compliance functions, respondents are likely to perceive that their program is operating well enough.

Please Rate the Performance of Your Organization’s E&C Program in the Following Areas:

<table>
<thead>
<tr>
<th>Category</th>
<th>Poor</th>
<th>Fair</th>
<th>Average</th>
<th>Good</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing Policies and Tracking Attestations</td>
<td>5%</td>
<td>9%</td>
<td>27%</td>
<td>43%</td>
<td>16%</td>
</tr>
<tr>
<td>Keeping Up to Date with New Regulations</td>
<td>3%</td>
<td>6%</td>
<td>21%</td>
<td>45%</td>
<td>25%</td>
</tr>
<tr>
<td>Managing Third-Party Risks</td>
<td>8%</td>
<td>13%</td>
<td>35%</td>
<td>36%</td>
<td>8%</td>
</tr>
<tr>
<td>Addressing Environment, Health and Safety Issues</td>
<td>4%</td>
<td>6%</td>
<td>24%</td>
<td>41%</td>
<td>25%</td>
</tr>
<tr>
<td>Legal Defensibility and Governance</td>
<td>2%</td>
<td>6%</td>
<td>23%</td>
<td>47%</td>
<td>22%</td>
</tr>
<tr>
<td>Whistleblowing Channels (e.g., Telephone, Web Intake, Open Door)</td>
<td>8%</td>
<td>8%</td>
<td>21%</td>
<td>35%</td>
<td>28%</td>
</tr>
<tr>
<td>Managing Incident Reports and Investigations</td>
<td>4%</td>
<td>6%</td>
<td>20%</td>
<td>44%</td>
<td>26%</td>
</tr>
<tr>
<td>Measuring Compliance Program Effectiveness</td>
<td>11%</td>
<td>14%</td>
<td>28%</td>
<td>36%</td>
<td>11%</td>
</tr>
<tr>
<td>Compliance Training and Awareness Efforts</td>
<td>5%</td>
<td>11%</td>
<td>25%</td>
<td>40%</td>
<td>19%</td>
</tr>
<tr>
<td>Improving Workplace Behavior and Organizational Culture</td>
<td>7%</td>
<td>10%</td>
<td>29%</td>
<td>42%</td>
<td>12%</td>
</tr>
<tr>
<td>Board Reporting and Engagement</td>
<td>8%</td>
<td>10%</td>
<td>26%</td>
<td>36%</td>
<td>20%</td>
</tr>
<tr>
<td>Data Privacy and Security</td>
<td>4%</td>
<td>7%</td>
<td>24%</td>
<td>44%</td>
<td>21%</td>
</tr>
</tbody>
</table>

n=1,264.
Ethics & Compliance Program Functions & Preventing Misconduct

Findings: According to respondents, the top three functions that helped prevent misconduct and/or ethical violations include ethics and compliance training (54%); policy and procedure management systems (47%) and whistleblower hotline systems (36%).

Analysis: The connection between training, policy management, whistleblowing hotline systems, and preventing misconduct is unsurprising. The findings reinforce what ethics and compliance professionals know intuitively and by observation – training and awareness increases employee awareness and respect for company rules and laws; policy and procedure management informs employees of rules and relevant controls to mitigate risk; and whistleblower hotline systems result in intervention to prevent or stop employee misconduct. Each of these cited elements are well-established functions of an ethics and compliance program, and required by law, regulation or long-standing practices.

Forty-five percent of respondents indicated their E&C program included a risk-based due diligence program for third parties, and 17 percent of those respondents selected that their third-party risk management program helped prevent misconduct or ethical violations over the last three years. This result does not capture the extent to which a third-party risk management program helped a company to avoid regulatory actions or fines, but rather is limited to preventing misconduct or ethical violations. The core benefit of a third-party risk management program is to reduce a variety of associated risks and is not limited to avoiding regulatory fines or penalties.

The next section of this report provides important insights concerning third-party risk management program best practices, development and benefits.

Did Any of These Programs Help Prevent Misconduct or Ethical Violations in Your Organization in the Past Three Years?

Multiple response question, totals may not add up to 100%, n=1,264.
3: Third-Party Risk Management Programs

Program Maturity

Findings: More than half of responding organizations (58%) have a Mature (41%) or Advanced (17%) third-party risk management program. Almost a third (31%) have programs that are Basic and 11 percent categorized their program as Reactive.

Analysis: This year’s survey is the third year in which we asked respondents to self-assess the maturity of their third-party risk management program. In our prior reports, we noted that respondent’s self-assessments did not align with actual program design and performance. To avoid this gap, we included individual questions and responses to accurately reflect program elements and overall maturity.

A key finding is that mature, well-run third-party risk management programs outperform less mature programs and those still developing their programs. A mature program is based on the organization’s approach to third parties, current third-party risk management practices, technologies used to manage third-party risk and methodology to assess the third-party risk management program’s effectiveness.

Maturity Level for Third-Party Risk

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>17%</td>
</tr>
<tr>
<td>Maturing</td>
<td>41%</td>
</tr>
<tr>
<td>Basic</td>
<td>31%</td>
</tr>
<tr>
<td>Reactive</td>
<td>11%</td>
</tr>
</tbody>
</table>

n=479.
Third Parties & Risk

Findings: Over half of responding organizations (58%) engage more than 100 third parties, and more than one quarter (29%) engage more than 1,000 third parties.

While 42 percent of respondents manage relationships with fewer than 100 third parties, the number of third parties varies within this category depending on the size of the organization. For example, small organizations with fewer than 500 employees engage less than 100 third parties (74%), compared to mid-sized organizations with between 500 and 5,000 employees (33%) and large organizations with more than 5,000 employees (11%). Larger organizations, not surprisingly, engage a large number of third parties, with almost half (45%) engaging more than 5,000 third parties, compared to only 9 percent of mid-sized organizations and 2 percent of small organizations.

Most organizations engage risky third parties, although most classify only a small number of third parties as high risk (just over half indicated 10% or fewer would be considered high risk). However, a sizeable number of organizations (24%) indicate that between 10 and 25 percent of their third parties are high risk.

- Organizations with Advanced third-party risk management programs engage more third parties than organizations that have less mature programs.
- More Reactive organizations (i.e., least developed third-party risk management programs) indicated that they do not engage any high-risk third parties (30%), compared to more mature programs.

Analysis: The number of third-party relationships is a relevant factor in defining an organization’s overall third-party risk. It is an important factor but not indicative of overall risk. Other risk factors have to be measured to determine a company’s overall risk profile. These risk factors, aside from the total number of third parties, include:

- Regulatory environment, industry risks and appetite for risk. A key element of an effective third-party risk management program is an accurate assessment of its own risk profile. This assessment should recognize the organization’s need to engage third parties, the risks that they pose and the alternatives to engaging third parties for specific purposes. When onboarding third parties, the organization has to require business justifications and identify the level of risk created by each proposed engagement.

- Geolocation of the third parties. The geographic location of third parties is one of several factors to consider but should not be blindly applied without considering specific business operations. A specific examination of a third-party should involve more than general assumptions as to local business practices, customs and culture and anecdotal evidence of misconduct.

- Governmental interaction. A key determinant of risk is the nature and extent of third-party interaction with foreign government officials. These interactions can involve business with a state-owned enterprise or a government agency. Many third parties also interact with foreign government officials for regulatory and permitting purposes. The level of regulation varies from country-to-country and third-party interactions vary depending on the specific regulatory framework. The
extent to which businesses are dependent on foreign government for commercial business (e.g., tenders and contracts) and regulatory approvals and licenses increases the level of risks when engaging a third-party.

- **Type of third-party.** Some types of third-party relationships create more risks than others. While the specific level of risk will vary depending on the mix of various factors discussed herein, some third parties create higher risks because of the nature of their operations. In most cases, commercial agents, distributors and resellers tend to represent higher risk than consultants and contractors.

- **Financial commitment of the engagement.** Third parties that assist in generating significant revenues and large contracts create higher risks because they have more opportunities to use money for illegal purposes. As a result, the higher the revenue earned by a third-party on behalf of the engaging organization, the greater the risk that the third-party may siphon off money to fund illegal activity. When an organization retains a third-party to conduct all of its business in a specific area, and the third-party may be responsible for a large amount of the organization’s revenue, the organization’s level of scrutiny over the third-party should increase.

- **Historical engagement with that third-party.** An organization’s historical relationship with a specific third-party should be reviewed as a separate risk factor. If there were red flags identified in prior reviews, the organization should review the history of the company’s relationship with the third-party, the performance of the third-party and the occurrence of any unusual events during the relationship.

A key component of an effective third-party risk management program is the specific risk assessment of each third-party, the measurement of such risk, and an ability to rank third parties based on their risk levels.
on a risk calculation. Such a structure ensures that the organization is able to stratify risk among the organization’s entire third-party risk environment.

This is reinforced by the Department of Justice’s (and Securities and Exchange Commission’s) Resource Guide to the U.S. Foreign Corrupt Practices Act that states the nature and extent of third-party risk should determine how the engaging organization identifies, manages and mitigates that risk. A successful risk-based program, built on a comprehensive understanding of where third-party risk lies, allows organizations to reasonably allocate resources to higher risk situations.

As we noted in last year’s report, we often receive questions about whether organizations should engage high-risk third parties. In some cases, the engaging organization may find that there are no reasonable alternatives. And retaining a high-risk third party can be justified provided that the organization applies a robust due diligence review based on an accurate risk-ranking, monitors the third party’s conduct and reputation and audits the third party.

When conducting due diligence, an organization may identify one or more red flags during the initial business justification, a preliminary risk assessment, or during screening or monitoring. A risk-based automated program can help identify and reveal red flags. Depending on the nature and significance of red flags, the organization can review its risk policies, procure additional relevant information and decide whether the red flag is a deal killer or not. Deeper analysis may negate the red flag, or it might show that the risks are not related to the existing engagement. Importantly, engaging organizations must make an educated decision based on reasonable assurances and actions taken to reduce the risk and protect the organization.

When addressing red flags it is important to make sure the decision to engage is logical, consistent with handling of other third parties and well documented. A red flag that is overlooked because of insistence from a high-level executive or circumvented because a foreign official may have recommended the third party will create significant risks of misconduct and government enforcement.

### What Percent of Your Third Parties Do You Consider to Be High Risk?

<table>
<thead>
<tr>
<th>Third-Party Risk Management Programs Continued</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What Percent of Your Third Parties Do You Consider to Be High Risk?</th>
<th>Reactive ( n=53 )</th>
<th>Basic ( n=149 )</th>
<th>Maturing ( n=197 )</th>
<th>Advanced ( n=80 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 50%</td>
<td>4%</td>
<td>4%</td>
<td>6%</td>
<td>2%</td>
</tr>
<tr>
<td>26% to 50%</td>
<td>6%</td>
<td>4%</td>
<td>5%</td>
<td>8%</td>
</tr>
<tr>
<td>10% to 25%</td>
<td>24%</td>
<td>15%</td>
<td>26%</td>
<td>29%</td>
</tr>
<tr>
<td>10% or Fewer</td>
<td>55%</td>
<td>47%</td>
<td>56%</td>
<td>58%</td>
</tr>
<tr>
<td>None</td>
<td>11%</td>
<td>30%</td>
<td>11%</td>
<td>9%</td>
</tr>
</tbody>
</table>

Base: All respondents, \( n=506 \).
Numbers may not add up to 100% due to rounding.
Third-Party Risk Management Program Challenges

Findings: The top three challenges facing organizations managing third-party risks are consistently monitoring third parties (53%); a lack of internal resources (45%); and training third parties and securing attestation to comply with applicable policies and procedures (36%).

Approximately one-quarter of responding organizations indicated that some of the top challenges are the complexity of due diligence requirements, lack of clear program ownership and the number of third parties they manage. Only a small minority (14%) of respondents indicated that the lack of clear guidelines from regulatory agencies is problematic.

More than half of Reactive or Basic organizations cited a lack of resources as a top challenge, significantly higher than organizations with more mature programs.

Organizations with more advanced programs indicated that the number of third parties they manage, complexity of the due diligence requirements and finding reliable information are top challenges.

Interestingly, government/non-profit organizations indicated a lack of clear guidelines from regulatory agencies as a top challenge (26%).

Almost half (46%) of responding organizations with $1 billion or more in annual revenue indicate that the number of third parties they manage is a top challenge.

What Are the Top Three Challenges for Your Third-Party Risk Management Program?

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Reactive n=53</th>
<th>Basic n=149</th>
<th>Maturing n=197</th>
<th>Advanced n=80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistently Monitoring Third Parties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of Internal Resources (People / Budget)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Our Third Parties and Getting Attestation on Our Policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity of the Due Diligence Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of Clear Program Ownership</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Number of Third Parties We Manage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finding Reliable Information Among a Large Volume of Potential Sources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of Outsourced Third-Party Risk Management Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of Clear Guidelines from Regulatory Agencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Base: All respondents, n=503.
Third-Party Risk Management Programs Continued

- A sizeable number (39%) of organizations managing 100 or more third parties indicate the volume of third parties they manage is a top challenge.

**Analysis:** The top challenge cited by responding organizations (53%) is **consistently monitoring third parties**. On page 34 of this report, we note that 61 percent of respondents report monitoring their third parties. Though nearly two-thirds of respondents monitor their third parties, half of the respondents find it challenging to do so, but more than a third of respondents believe that monitoring third parties is an important priority.

The FCPA Guidance cites continuous monitoring as a key element of an effective third-party risk management program. However, it does not specify how such monitoring should be conducted. Given the absence of specific directions, organizations struggle with execution of monitoring programs.

In terms of program maturity, the survey found that **Reactive** and **Basic** programs struggle with a lack of internal resources, training third parties on policies and expectations and monitoring their third parties. **Reactive** and **Basic** programs are chronically lacking in resources and budget authority to devote to implementing an effective third-party risk management program. Alternatively, mature programs are challenged by different issues – the number of third parties they manage, training, monitoring and the complexity of due diligence program requirements.

When implementing a robust third-party risk management program, most organizations underestimate the number of third parties they engage, especially when they consider agents, resellers and contractors, and the level of risk each of these types of third parties create. Nearly 20 percent of our respondents engage 5,000 or more third parties. That is a large number to scrutinize, assess and manage.

A small number of respondents indicated that a lack of clear guidelines from regulatory agencies is a top challenge. Enforcement agencies in the U.S. and UK in particular have been issuing more guidance, explaining how they evaluate ethics and compliance programs and third-party risk management programs.
Approach to Managing Third-Party Risk

**Findings:** There is no well-established procedure or strategy to implement an effective third-party risk management program. However, respondents indicated they apply due diligence based on the classification and the risk level assigned to the third-party (37%), or by treating all third parties the same regardless of risk level (27%).

- **Advanced** programs apply a risk-based approach to third-party due diligence (69%), while organizations with **Maturing** programs are mixed between using risk-based approaches (45%) or applying the same procedure to all third parties regardless of risk level (31%).
- A sizable number of government/non-profit organizations apply the same procedure regardless of risk level (40%).

The most common practices for managing third-party risk across all levels of program maturity are screening (70%) and monitoring (61%).

- **Advanced** programs are more likely to employ all approaches to managing risk compared to less mature programs, although only just over a third (39%) deliver third-party training incentives, certifications or program compliance.
- Almost half of **Mature** programs perform enhanced due diligence (47%).
- Only a minority of **Basic** and **Reactive** programs employ any specific third-party risk management practices beyond screening and monitoring.

**Analysis:** The increased focus on managing third-party risk is confirmed in the fact that 37 percent of respondents indicated they rely on a risk-based program that applies different degrees of due diligence based on certain classification criteria and risk level. Even more positive is the
fact that 69 percent of Advanced programs and 45 percent of Maturing programs are building a robust risk-based program. Aside from these positive developments, the survey results revealed that there are still a number of organizations with Reactive programs that do not classify nor assign risk levels to third parties. The three-quarters of Reactive programs that don’t do anything currently to address third-party risks reflects a lingering group of organizations that have failed to make any commitment to addressing third-party risks.

A majority of all survey respondents screen and monitor their third parties. Such steps are a basic requirement for any organization that engages third parties. Still, it is surprising that 30 percent of all respondents do not perform screening, and nearly 40 percent of respondents do not monitor their third parties.

As explained in the FCPA Guidance, a third-party risk management program is incomplete and unable to effectively accomplish its purpose if the engaging organization does not screen all of its third parties consistently and comprehensively. There is no way to accurately risk-score third parties and to identify and stratify their respective risks unless all data points are reviewed. Risk data allows organizations to gain visibility across third parties and unambiguously identify where their third-party risk lies. With such information, organizations are able to mitigate their risks, including conducting enhanced due diligence of third parties when necessary. Without doing so, organizations are needlessly exposing themselves to avoidable risk.

While some may suggest that a comprehensive screening and risk identification process is impracticable for Reactive and Basic programs,

---

### What Are Your Current Third-Party Risk Management Practices?

<table>
<thead>
<tr>
<th>Practice</th>
<th>Reactive n=53</th>
<th>Basic n=149</th>
<th>Maturing n=197</th>
<th>Advanced n=80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Our Third Parties</td>
<td>70%</td>
<td>55%</td>
<td>71%</td>
<td>67%</td>
</tr>
<tr>
<td>Monitor Our Third Parties</td>
<td>61%</td>
<td>38%</td>
<td>53%</td>
<td>63%</td>
</tr>
<tr>
<td>Perform Enhanced Due Diligence on Our Third Parties</td>
<td>41%</td>
<td>4%</td>
<td>23%</td>
<td>47%</td>
</tr>
<tr>
<td>Send Questionnaires and Collect Documents and Information from Third Parties in a Centralized Location</td>
<td>36%</td>
<td>11%</td>
<td>23%</td>
<td>36%</td>
</tr>
<tr>
<td>Advise Our Organization on Our Third-Party Due Diligence Program Structure and Effectiveness</td>
<td>29%</td>
<td>4%</td>
<td>10%</td>
<td>33%</td>
</tr>
<tr>
<td>Continuous, Automated Enhanced Due Diligence Actions Based on Our Organization’s Definitions of High, Medium and Low Risk</td>
<td>20%</td>
<td>0%</td>
<td>3%</td>
<td>17%</td>
</tr>
<tr>
<td>Automate and Track All Aspects of Third-Party Risk Management Through the Lifecycle of Each Third-Party Engagement</td>
<td>12%</td>
<td>0%</td>
<td>3%</td>
<td>9%</td>
</tr>
<tr>
<td>Deliver Third-Party Training Incentives, Certifications or Program Compliance</td>
<td>12%</td>
<td>2%</td>
<td>3%</td>
<td>9%</td>
</tr>
</tbody>
</table>

Base: All respondents, n=491.
such an attitude is short-sighted and ignores the fact that a single third-party can create significant enforcement risks and threaten a company’s reputation. A malignant third-party can create risks for all the organizations with which it interacts. Depending on the size of the engaging organization, the consequences can vary and even threaten the very existence of smaller organizations. There is no excuse for organizations to avoid basic due diligence procedures to manage third-party risks, particularly when – as seen earlier – almost everybody now understands the requirements of regulatory agencies.

Third-party risk management programs are designed to protect engaging organizations from multiple forms of risk, including an ethical, financial or operational failure by the third-party, agency enforcement activity and reputational damage. Pursuing a consistent risk-based, third-party risk management program that applies to all third parties that includes identifying, stratifying and mitigating risks is a competitive and basic requirement for all organizations, big or small, Reactive or Advanced.
Technologies

**Findings:** Organizations use different technologies to support third-party risk management programs. More than a third of survey respondents use an internally built or manual system; more than one-quarter use an office productivity solution; and one-fifth use a CRM or ERM solution. Only a minority use specific third-party risk software (13%) or an automated solution (5%).

- The use of technologies varies markedly by third-party risk management program maturity. Half (49%) of Advanced organizations indicate they use a purpose-built third-party solution, while organizations with less mature programs rely on solutions not designed specifically to manage third-party risks.

- Among those organizations using a third-party management software solution, most indicated that the solution results have been Good or Excellent.

**Analysis:** Third-party risk is specific to each organization. In other words, your third-party risk is your risk. It does not matter if you are a small or a large organization or if your organization employs a large or small number of third parties. It is critical for each organization to protect itself from third-party risks. There are a number of solutions available to help, with varying degrees of effectiveness. It is well established that best practices require companies to implement third-party risk management programs coupled with technologies to leverage resources and capabilities to enable the consistent management of all third-party relationships.

While internally built or highly manual systems may provide some benefits, such solutions become far less effective when an organization has to manage more than a few third-party relationships. Office productivity tools, CRM and ERP solutions often offer some centralization of records and visualization, but are not built to assess and score risk or for broader ethics and compliance purposes, which are key to satisfying enforcement agencies’ expectations. Similarly, the reconfiguration of an automated solution designed for other purposes to address third-party risk may provide some level of record keeping and assessment, but can compromise program effectiveness due to gaps and inconsistent risk management capabilities.

Still, these programs provide some level of risk management capabilities and may suffice while program leadership seeks to gain support and resources for a more effective, purpose-built solution. Advanced programs have moved to purpose-built, automated solutions more than other programs and, as seen below, they have experienced improved performance.

Automation is important not only for centralizing the management of third-party risk management processes. An automated solution provides resource savings in terms of integration with complementary solutions like vendor management, ERP and CRM solutions, as well as with workflows, business rules and policies, escalations and authorizations and other process-oriented management. Further, it enables auditability, consistency and program visibility inaccessible without automation. Automation enables purpose-built third-party risk management and due diligence solutions to function as intended.
What Technology Are You Currently Applying to Manage Your Third-Party Risk?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Reactive n=53</th>
<th>Basic n=149</th>
<th>Maturing n=197</th>
<th>Advanced n=80</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Internally Built or Highly Manual System (Paper-Based or Stitched-Together Software)</td>
<td>35%</td>
<td>64%</td>
<td>62%</td>
<td>17%</td>
</tr>
<tr>
<td>An Office Productivity Solution (Spreadsheets, Word Processing or Email Program)</td>
<td>27%</td>
<td>30%</td>
<td>22%</td>
<td>38%</td>
</tr>
<tr>
<td>A Customer Relationship Management (CRM) or Enterprise Resource Management (ERM) Solution</td>
<td>20%</td>
<td>6%</td>
<td>11%</td>
<td>26%</td>
</tr>
<tr>
<td>A Purpose-Built Third-Party Risk Management Software Solution</td>
<td>13%</td>
<td>0%</td>
<td>2%</td>
<td>11%</td>
</tr>
<tr>
<td>A Reconfigured Automated Solution to Manage Third-Party Risk</td>
<td>5%</td>
<td>0%</td>
<td>2%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Base: All respondents, n=485. Numbers may not add up to 100% due to rounding.

Please Rate Your Third-Party Technology Solution on the Following:

<table>
<thead>
<tr>
<th>Category</th>
<th>Poor</th>
<th>Fair</th>
<th>Average</th>
<th>Good</th>
<th>Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaining Defensibility of Our Program with Enforcement Agencies</td>
<td>5%</td>
<td>6%</td>
<td>22%</td>
<td>56%</td>
<td>11%</td>
</tr>
<tr>
<td>Documenting Processes and Protocols</td>
<td>6%</td>
<td>5%</td>
<td>25%</td>
<td>50%</td>
<td>14%</td>
</tr>
<tr>
<td>Ability to Promptly Resolve Newly Identified Risks</td>
<td>6%</td>
<td>31%</td>
<td>52%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Complying with Laws and Regulations</td>
<td>5%</td>
<td>32%</td>
<td>41%</td>
<td>19%</td>
<td>9%</td>
</tr>
<tr>
<td>Determining the ROI of Our Program</td>
<td>8%</td>
<td>17%</td>
<td>32%</td>
<td>34%</td>
<td>9%</td>
</tr>
</tbody>
</table>

Base: Respondents whose organization uses a third-party risk management software, n=64.
Third-Party Risk Management Program Assessment

Findings: Among those organizations that have an automated third-party risk management solution (i.e., software), most (75%) monitor program effectiveness, with the most common assessment methods being periodic risk assessments and program audits or legal review.

Very few respondents rated their third-party risk management programs as Excellent (3%). The bulk of respondents (67%) view their programs as Average or Good. A sizeable number of organizations (38%) consider their program to be Average, while one in five rated their program as Fair. A small minority of organizations (9%) consider their program Poor.

How Do You Access the Effectiveness of Your Third-Party Due Diligence Program? Select Up to 3 Primary Methods.

- Periodic Risk Assessment: 46%
- Program Audits or Legal Review: 30%
- Ability to Proactively Identify and Mitigate Third-Party Risks: 27%
- Onboarding and Screening Efficiencies: 25%
- Benchmarking Program Performance Against Peers: 13%
- Third-Party Training Completion and Attestation Rates: 12%
- Reduction in Enforcement Action: 8%
- We Do Not Assess Program Effectiveness: 25%
- Other: 2%

Base: Respondents whose organization uses a third-party risk management software, n=65.
**Analysis:** The most common assessment methodologies used by third-party risk management programs employing software solutions are periodic risk assessment and program audits or legal review. A software-based third-party risk management program centralizes management and increases program efficiencies. Such a program reduces the risk of an enforcement action which can result in serious harm to an organization. Assessment of a software-based third-party risk program’s performance, however, should not be limited to just avoidance of an enforcement action, but should encompass overall risk mitigation factors such as operational efficiencies in processing of third-party risk candidates, and continuous monitoring and audits of third parties. Organizations are designing robust assessment programs to capture and monitor the benefits of more sophisticated third-party risk management programs.

It’s important to note that third-party risk management programs should do more than reduce regulatory action. Though regulatory action generates headlines, third-party failures can be much more damaging to an organization’s reputation, operational integrity and revenue. Assessing program performance should therefore include not only an absence of regulatory action, but also qualitative measures revealed through risk assessments and audits, such as program breadth and capacity, process efficiency and consistency and an ability to allow program leaders to confidently sleep at night.

**How Would You Rate Your Third-Party Risk Management Program Overall?**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Reactive n=53</th>
<th>Basic n=148</th>
<th>Maturing n=197</th>
<th>Advanced n=80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>3%</td>
<td>2%</td>
<td>2%</td>
<td>13%</td>
</tr>
<tr>
<td>Good</td>
<td>29%</td>
<td>4%</td>
<td>19%</td>
<td>56%</td>
</tr>
<tr>
<td>Average</td>
<td>38%</td>
<td>19%</td>
<td>35%</td>
<td>26%</td>
</tr>
<tr>
<td>Fair</td>
<td>21%</td>
<td>42%</td>
<td>37%</td>
<td>4%</td>
</tr>
<tr>
<td>Poor</td>
<td>9%</td>
<td>34%</td>
<td>12%</td>
<td>4%</td>
</tr>
</tbody>
</table>

*Base: All respondents, n=478. Numbers may not add up to 100% due to rounding.*
Findings: Just over half of organizations (56%) agreed that their third-party due diligence program significantly reduces a variety of risks. One-third of organizations (33%), however, are neutral on whether their program reduces risks, reflecting a need to focus on understanding their program effectiveness.

Although the vast majority of Advanced organizations indicated that their risks are reduced as a result of their program (84%), only 41 percent of those with Basic programs and 13 percent with Reactive programs observed risk reduction.

Analysis: There is a significant disparity among third-party risk management programs on the overall reduction of risk depending on the maturity of the program. Advanced organizations observed substantial risk reduction. Organizations that commit to implementing best practices and effective strategies achieve significant benefits in risk reduction, while less mature programs still face major third-party risks.

Rate Your Agreement With the Following Statement: Our Third-Party Due Diligence Program Significantly Reduces Our Legal, Financial and Reputational Risks.

<table>
<thead>
<tr>
<th></th>
<th>Reactive n=53</th>
<th>Basic n=148</th>
<th>Maturing n=197</th>
<th>Advanced n=80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>13%</td>
<td>4%</td>
<td>15%</td>
<td>30%</td>
</tr>
<tr>
<td>Agree</td>
<td>43%</td>
<td>9%</td>
<td>53%</td>
<td>54%</td>
</tr>
<tr>
<td>Neither Agree</td>
<td>33%</td>
<td>57%</td>
<td>41%</td>
<td>28%</td>
</tr>
<tr>
<td>or Disagree</td>
<td></td>
<td></td>
<td>28%</td>
<td>15%</td>
</tr>
<tr>
<td>Disagree</td>
<td>9%</td>
<td>21%</td>
<td>16%</td>
<td>4%</td>
</tr>
<tr>
<td>Strongly Disagree</td>
<td></td>
<td>9%</td>
<td>3%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Base: All respondents, n=478. Numbers may not add up to 100% due to rounding.
Impact of Third-Party Risk Management Programs

Findings: A majority of organizations with third-party risk management solutions indicated they have not incurred any damages in the past three years. Only 10 percent of those with authority over their third-party risk management programs reported third-party-related damage. While we have surveyed organizations on this issue in the past, we substituted the key term of “damage” for “failure” in our survey because we found that the term “failure” was too vague to measure the level of impact on the engaging organization. The term “damage” is more accurate because it suggests a tangible harm that likely required remediation.

- Across maturity levels, most organizations experienced similar ethics related damages.
- Larger organizations (38%) and mid-sized organizations (36%) are more likely to experience employee litigation against the organization compared to smaller organizations with fewer than 500 employees (18%).
- Seven in 10 (71%) organizations with fewer than 500 employees report no damages related to ethics issues.

What Damage Has Your Organization Incurred in the Past Three Years Resulting from an Ethics Issue?

<table>
<thead>
<tr>
<th>Damage Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Action Taken Against the Organization by Governing Body</td>
<td>14%</td>
</tr>
<tr>
<td>Employee Litigation Against the Organization</td>
<td>30%</td>
</tr>
<tr>
<td>Reputational Damage Due to Ethics Violation</td>
<td>15%</td>
</tr>
<tr>
<td>Violation of Wage and Hour Laws (i.e., Penalties or Class Action Suits)</td>
<td>7%</td>
</tr>
<tr>
<td>Third-Party Ethics Failure</td>
<td>10%</td>
</tr>
<tr>
<td>None of the Above</td>
<td>56%</td>
</tr>
</tbody>
</table>

*Note: Includes results only for respondents who indicated they are a decision maker/influencer when it comes to Third-Party Risk Management, n=888.*
Analysis: While one third-party failure can cause significant damage to an organization, the survey measured how organizations viewed their risk in comparison to how organizations reported third-party-related failures. The comparison confirmed that organizations that view their third-party risks as substantial reported higher risk and organizational damage.

We further analyzed third-party-related damage tied to other important measures in this report. For example, we found that of those who identified their third-party risk at 75 percent or higher, only 25 percent relied on a purpose-built solution to manage their third-party risks. This disconnect is disturbing and reflects an organization’s failure to address a real and substantial threat to the organization and the need to target third-party risk for mitigation.

In the table below, we further divide the analysis on expected risk, and reported organizational damage due to third-party risk by key industries. As we can see, transportation and manufacturing represent elevated relative risk, yet the predominance of respondents expect ten percent or fewer of their third parties should be considered high risk. Given the outcomes for these industries, it is likely that for many organizations, there is a tendency to underestimate third-party risk.

Percentage of High Risk Third Parties

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>No Risk</th>
<th>10% or Less</th>
<th>10 to 25%</th>
<th>26 to 50%</th>
<th>50% or More</th>
<th>Percent of Respondents Indicating Third-Party Related Organizational Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>3%</td>
<td>71%</td>
<td>21%</td>
<td>5%</td>
<td>0%</td>
<td>10%</td>
</tr>
<tr>
<td>Transportation</td>
<td>13%</td>
<td>47%</td>
<td>23%</td>
<td>10%</td>
<td>7%</td>
<td>13%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>13%</td>
<td>51%</td>
<td>28%</td>
<td>4%</td>
<td>5%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Numbers may not add up to 100% due to rounding.
Given these elevated risks related to third parties, we further analyzed what steps are commonly taken within these industries to better manage and reduce their third-party risk. Needless to say, it is concerning that within those industries in which we see elevated third-party risks, many organizations are applying paper-based or stitched-together software solutions to manage that risk. Manufacturing is ahead of the game by deploying purpose-built third-party risk management solutions 18 percent of the time. Yet, that is still discouragingly low considering the level of third-party risks we see in the manufacturing vertical.

When we questioned respondents on whether their third-party due diligence program reduces their third-party risks (page 40), 53 percent of respondents who experienced third-party related damage in the last three years either agreed or strongly agreed that their program significantly reduces their organization’s third-party risks. This finding suggests that organizations that have experienced third-party related damage understand and respond to such risks by tailoring their program to reduce such risks.

Further, this result underscores the importance of a comprehensive third-party risk management system to help identify and mitigate risk prior to significant enforcement, operational or reputational impact.
CONCLUSION

In this, our fourth consecutive report on third-party risk management, we see positive trends in terms of organizations working to pursue effective third-party risk management programs.

- **Start at the right place.** If your organization has not formalized its third-party risk management program, understanding best practice design and operations is important. Out-of-the-box, one-size-fits-all solutions don’t work; each organization has different inherent risks. Your 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, IT and others, so everyone can understand objectives and identify and score the organization’s unique risk profile. That profile should steer all other processes, including scoring and prioritizing risk review, screening, monitoring and conducting deep dives to ensure the risk is understood and reduced.

Once the organizational risk is identified, it is the first sounding board against which any and all third-party engagements are reviewed and justified. Only after risk criteria is set should third parties be approved, screened, monitored and engaged. The life cycle management of third-party risk requires consistent and constant review, adaptation to new requirements and realities and an ability to suspend or end engagements where risk is unmanageable.

Keep in mind that many organizations do business with third parties that operate in high-risk regions or that throw red flags resulting from inconsistencies with the organization’s risk profile, and screening or monitoring results. There is no legal requirement not to do business with a third party that generates an alert or red flag. But the engaging organization must be able to justify the engagement and showcase protections and actions against that risk should the engagement be audited or the third-party fail.

Finally, use a solution that’s designed and built to make your job easier. Although NAVEX Global offers a solution designed to do so (see the next page), beyond marketing our own solution, it is beneficial to the entire market for educated buyers to understand capabilities and demand innovations that help their organizations better manage and reduce their third-party risks. As we see in this report, even when organizations understand their third-party risks, too many are not yet applying automated and purpose-built software to manage and reduce that risk. Yet, the evidence of effectiveness from doing so is conclusive.

As enforcement agencies investigate organizations for compliance with the laws and regulations, it is imperative companies are able to demonstrate reasonable efforts to identify, prioritize and mitigate third-party risk. Given the significant benefits to mature third-party risk management programs in reducing risk due to consistent mitigation practices from a state-of-the-art third-party risk management solution, organizations have to embrace the inevitable expectation that investing in robust risk management solutions will become the norm for a large percentage of ethics and compliance programs.
Don’t do half the job. We often refer to a third-party risk management program as an insurance program. If an organization owned a fleet of automobiles but didn’t know the inherent risk to the organization of operating those cars, the organization would be at great risk.

If those cars were distributed through third parties – agents and resellers, for example – to distant regions of the world where the engaging organization could not keep a watchful eye on them, and if they were expensive to replace and might be inappropriately used to service government officials, such a risk would be potentially devastating to the organization.

If that organization insured only some of those cars, or only those in a certain region, the organization is putting itself in unnecessary peril. Like a third-party failure, if even one of those cars was used in a robbery or other unethical action and the organization did not maintain appropriate insurance, such an event could threaten the organization’s reputation, financial stability and even survival.

Third-party failure threatens reputation and sustainability. Third-party misconduct and illegal behavior can have devastating consequences to an organization. In 2016 and 2017, the U.S. Department of Justice initiated more than 100 FCPA investigations. In day-to-day operations, organizations regularly face potential harm from third-party misconduct and illegal behavior, even though the chances that such conduct could lead to an enforcement action are relatively low. Significantly, the risk of an enforcement action is not the key driver of risk mitigation strategies – an organization’s culture and reputation are its most valuable intangible assets, and every incident of misconduct threatens them.

Third-party risk management is much more than just avoiding enforcement actions. As noted in this report, effective third-party risk management programs promote an ethical culture, integrity and respect, while minimizing risk of an enforcement action. A consistent and robust third-party risk management program is a critical component of every ethics and compliance program. We recommend that organizations build a third-party risk management program to improve visibility and risk identification, to increase consistency and reduce third-party related risks, and to gain significant operational efficiencies.

Technological solutions using software or automated systems are rapidly advancing third-party risk management programs. Software and automated platforms offer unique opportunities to leverage resources and build efficient due diligence, monitoring and auditing functions. Organizations are aware of these benefits and increasingly seek resources to implement these cost-effective solutions.
Key Metrics

Ethics & Compliance Program Performance

- Creating a culture of ethics, integrity and respect is the top ethics and compliance program objective (68%) and is seen as more important than implementing preventative measures and practices to avoid future issues (62%) and navigating and complying with laws and regulations across jurisdictions (47%).

- Ethics and compliance professionals are most concerned about implementing an effective business code of conduct (46%) and responding to cyber security events (44%). Procedure management/quality control (28%), conflicts of interest (25%) and anti-bribery (21%) round out the top five concerns identified by respondents.

- Ethics and compliance departments identified their priorities for the next 12 months. The top three were: increasing awareness of the company’s policies and regulations (50%); improving or increasing ethics and compliance training activities (40%); and training and supporting frontline managers and supervisors on their responsibilities (39%).

- With the increasing focus on measuring and testing the effectiveness of ethics and compliance programs, organizations are employing a variety of methods to assess compliance program effectiveness. Some of the metrics cited by respondents include: number of code of conduct breaches (43%); analysis of internal audit findings (41%), conducting exit interviews (40%) and employee surveys (40%).

Third-Party Risk Management Programs

- More than half of responding organizations (58%) have a Mature (41%) or Advanced (17%) third-party risk management program. Almost a third (31%) have programs that are Basic and 11 percent categorized their program as Reactive.

- Most organizations engage risky third parties, although most organizations classify only a small number of third parties as high risk (just over half indicated 10% or fewer would be considered high risk). However, a sizeable number of organizations (24%) indicate that between 10 and 25 percent of their third parties are high risk.

- The top three challenges facing organizations managing third-party risks are consistently monitoring third parties (53%), a lack of internal resources (45%), training third parties and securing attestation to comply with applicable policies and procedures (36%).

- Approximately one-quarter of responding organizations indicated that some of the top challenges to its program are the complexity of due diligence requirements, lack of clear program ownership, and the number of third parties they manage.

- More than half of Reactive or Basic organizations cited a lack of resources as a top challenge, significantly higher than organizations with more mature programs.
• Organizations with more advanced programs indicated that the number of third parties they manage, complexity of the due diligence requirements, and finding reliable information are top challenges.

• Almost half (46%) of responding organizations with $1 billion or more in annual revenue indicate that the number of third parties they manage is a top challenge.

△ A large percentage of respondents (37%) indicated they apply due diligence based on the classification and the risk level assigned to the third party. The most common practices for managing third-party risk across all levels of program maturity are screening (70%) and monitoring (61%).

△ Organizations use different technologies to support third-party risk management programs. More than a third of survey respondents use an internally built or manual system; more than one-quarter use an office productivity solutions; and one-fifth use a CRM or ERM solution. Only a minority use specific third-party risk software (13%) or an automated solution (5%).

• The use of technologies varies markedly by third-party risk management program maturity. Half (49%) of Advanced organizations indicated they use a purpose-built third-party solution, while organizations with less mature programs rely on solutions not designed specifically to manage third-party risks.

• Very few respondents rated their third-party risk management programs as Excellent (3%). The bulk of respondents (67%) view their programs as Average or Good. A sizeable number of organizations (38%) consider their program to be Average, while one in five rated their program as Fair. A small minority of organizations (9%) consider their program Poor.

• Overall program ratings correlate with program maturity level. Three-quarters of Reactive programs indicated that their programs were either Poor (34%) or Fair (42%); Nearly three-quarters of Basic programs (72%) indicated that their programs were either Fair (37%) or Average (35%); Most Mature programs (85%) indicated that their programs were either Average (50%) or Good (35%); and most Advanced programs (82%) indicated that their programs were either Good (56%) or Average (26%).

• Organizations identified four specific assessment methodologies: periodic risk assessment (46%); program audits or legal review (30%); proactive identification and mitigation of third-party risks (27%); and onboarding and screening efficiencies (25%).
ABOUT NAVEX GLOBAL’S THIRD-PARTY RISK MANAGEMENT SOLUTION

RiskRate®, by NAVEX Global, helps organizations structure, automate and simplify the management of their third-party risks. RiskRate enables clients to define and capture critical information about their vendors, resellers, agents, suppliers, distributors, contractors and other third parties and to score the risks they represent. Foundationally based on the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act guidance, RiskRate delivers end-to-end third-party risk management. This includes the ability to centralize and apply consistent risk scoring and evaluation processes across all third parties, stratify and mitigate third-party risks and conduct reputational screening, monitoring and third-party enhanced due diligence as necessary.

To learn more about RiskRate Enterprise Due Diligence or to schedule a demo, visit www.navexglobal.com/products/third-party-risk-management or call us at +1 866 297 0224.
ADDITIONAL RESOURCES

NAVEX Global offers many valuable resources to help you increase your training program effectiveness. Visit our resource library at http://www.navexglobal.com/resource-center to find these tools and more.

White Papers:
- Fighting Bribery & Corruption on the Global Stage
- Anti-Bribery and Corruption Risk Assessment Checklist
- How to Go from Manual to Automated Third-Party Due Diligence Monitoring: Ten Steps to Success
- A Prescriptive Guide to Third-Party Risk Management

Use Cases:
- Pursue a Risk-Based Approach
- Effectively Communicate Third-Party Risk
- Automate Your Third-Party Risk Management
- Gain Visibility Across Your Third-Party Risk

Additional Tools:
- Third-Party Risk Management ROI Calculator
- Compliance Next Education and Thought Leadership Resources for the Ethics and Compliance Professional
ABOUT THE AUTHOR

Michael Volkov
CEO and Founder of The Volkov Law Group, LLC

Michael Volkov, CEO and founder of The Volkov Law Group, LLC, has over 35 years of experience in practicing law. A former federal prosecutor and veteran white collar defense attorney, he has expertise in areas of ethics and compliance, internal investigations and enforcement matters.

The Volkov Law Group is a recognized leader in the ethics and compliance field. As a former federal prosecutor and Justice Department official, Michael Volkov has extensive experience with best practices, government expectations, and industry standards for ethics and compliance programs.

Michael Volkov maintains a highly popular FCPA blog – Corruption, Crime & Compliance. He is a regular speaker at events around the globe, and is frequently cited in the media for his knowledge on criminal issues, enforcement matters, ethics and compliance and corporate governance.
NAVEX Global’s comprehensive suite of ethics and compliance software, content and services helps organizations protect their people, reputation and bottom line. Trusted by 95 of the Fortune 100 and more than 13,000 customers, our solutions are informed by the largest ethics and compliance community in the world. For more information, visit www.navexglobal.com.