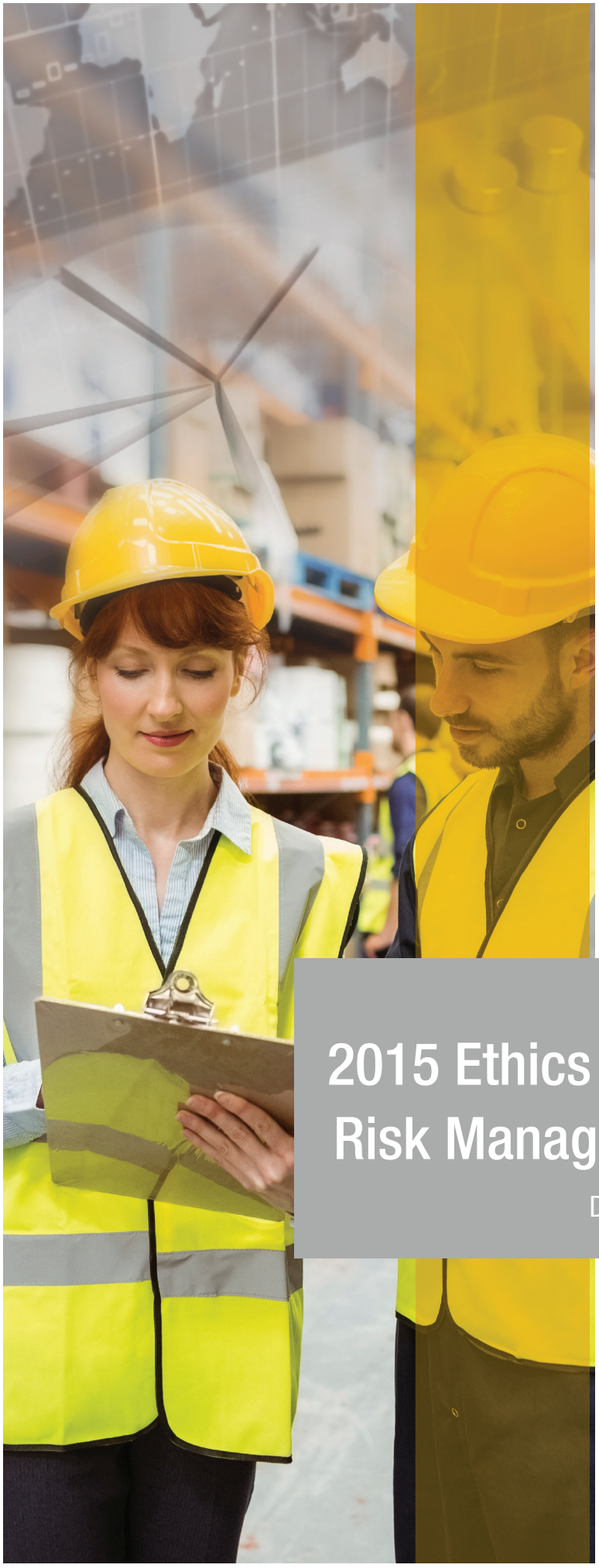


NAVEX GLOBAL®
The Ethics and Compliance Experts

2015 Ethics & Compliance Third Party Risk Management Benchmark Report

Data and Insights to Put to Work in Your Program Today

PREPARED BY:

Randy Stephens, J.D.

Vice President, Advisory Services, NAVEX Global

TABLE OF CONTENTS

I. INTRODUCTION

In 2015, NAVEX Global partnered with an independent research firm to survey senior professionals from a wide range of industries about their approach to third party risk management and due diligence.

The findings in this report are based on data from 321 survey respondents. (See respondent profile in the next section for additional details.)

Our report provides insights and analysis of questions such as:

- Who owns third party risk management and due diligence activities?
- How are organizations using outside providers to help with third party due diligence?
- Does continuous, automated due diligence affect ROI and reduce exposure to risk?

How To Use This Report

If your third party risk management program is not performing at the level to which you need it, your risks increase and the opportunity for long term program success decreases significantly. This report will help you:

- Determine whether your third party due diligence practices are protecting your organization—or putting it at risk;
- Benchmark your third party risk management program against peers, industry norms and best practices; and
- Leverage report data and recommendations to improve your program effectiveness.

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 Do You Define "Third Parties"?

For the purposes of this report, the term "third parties" 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 & 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 and Third Party Due Diligence?

For the purposes of this report, third party risk management is an umbrella term that refers to all activities related to your third parties, including screening, data collection, documentation, and ongoing monitoring.

Third party due diligence refers to the studied assessment of third parties both before and during an engagement. It can include conducting a business culture and ethics review of the third party provider via questionnaires and interviews, as well as analysis of databases and reputational reporting. It also includes active monitoring of your third party engagements for new "red flags" and any publicly available recent changes to the third party's risk profile.

SURVEY RESPONDENT PROFILE

n=321

Job Function

- Ethics & Compliance — 39%
- Human Resources/Employee Relations — 1%
- Risk Management — 11%
- Legal — 10%
- Audit — 17%
- Information Security — 2%
- Other — 20%

Job Level

- C-Level — 5%
- Senior Management/Director — 43%
- Management — 34%
- Non-Management — 11%
- Other — 7%

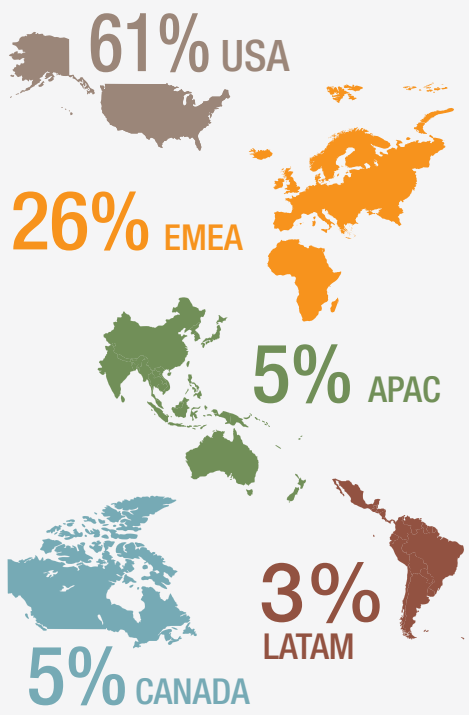
Organization Size

- Small: < 500 Employees — 21.5%
- Medium: 501-5,000 Employees — 33%
- Large: 5,000+ Employees — 45.5%

Company Annual Revenue

- $0 < $50M — 13%
- $50M -$999M — 32%
- $1B+ — 46%
- Don't Know — 9%

Geography of Headquarters



Top 10 Industries

1. Banking & Financial Services
2. Manufacturing
3. Technology
4. Energy & Utilities
5. Insurance
6. Pharmaceuticals
7. Healthcare Providers
8. Business Services
9. Education
10. Not for Profit

22 INDUSTRIES REPRESENTED

NAVEX GLOBAL®
The Ethics and Compliance Experts

III. EXECUTIVE SUMMARY

Organizations are still coming to terms with the breadth and depth of their third party risk. An effective third party risk management program is in the interest of all organizations—regardless of their size, industry, and degree of involvement with third party providers. Regulatory agencies, the press, and the market are quick to link organizations to the behaviors of their vendors, partners, and resellers – and to hold them accountable.

As this report shows, despite growing scrutiny of third parties from regulatory agencies and the press, many organizations are not yet executing third party risk management programs that adequately communicate expectations to their third parties, provide defensibility in the case of compliance failures, and reduce the impact of bad behavior by third parties. Though there are signs that organizations—often at the behest of their Boards—are ramping up investments in third party due diligence and risk management programs, there are many organizations that appear to be struggling to align their program investment and management to deliver the confidence they need in their third party risk management programs.

Survey data revealed the top objectives, pain points and third party risk management program strategies for ethics and compliance professionals. The following key themes emerged:

- **Budgeting ownership for third-party risk management often does not align with program responsibility.** While most respondents recognize the severity of third party risk, our data shows that many organizations use a decentralized and manual approach to program budgets, ownership and processes, with varying degrees of success. In many organizations surveyed here, third party due diligence program leaders do not control their own budgets.
- **"Bribery and corruption" is, by far, organizations' top ethics and compliance concern regarding third party misconduct (39%).** High levels of concern about bribery and corruption, fraud and conflicts of interest are not surprising given the amount of regulatory action being pursued related to third party compliance failures committed in the service of the organizations that contracted with them. Bribery and corruption in particular are on many organizations' radars due to increasing enforcement and high profile prosecutions of the Foreign Corrupt Practices Act (FCPA) by the US Department of Justice, the UK Bribery Act, and the volume of whistleblower tips being communicated to the SEC's Office of the Whistleblower.
- **Most organizations (68%) evaluate third parties before engaging with them, and organizations are more likely to monitor third parties themselves than to outsource third party monitoring.** Thirty-seven percent of organizations work with an outsourced third party due diligence provider to some degree, but just 14% use such a vendor to conduct continuous third party due diligence screening; 31% report that they continuously monitor third parties using internal resources only. Inconsistencies in program performance shown within this report indicate that in many cases, the initial evaluation is not robust enough. And without a consistent and continuous process where existing third parties are reevaluated prior to contract renewal or adjustment, inadequate screening which is not risk based and documented may come back to haunt the organization.
- **Organizations that outsource third party due diligence are significantly more pleased with the effectiveness of their third party risk management program.** Within this analysis, organizations that use an outsourced provider to help manage their third party due diligence programs report significantly higher program satisfaction ratings than those who do not. These higher satisfaction ratings apply across multiple best practice program criteria, including:
  - Compliance with legal and regulatory demands: 78% compared to 65%
  - Ensuring a Culture of Compliance: 65% compared to 44%
  - Documentation Management: 49% compared to 41%
  - Program Defensibility: 52% compared to 41%
  - Overall Program: 53% compared to 32%

THE STATE OF THIRD PARTY RISK MANAGEMENT

IV. KEY FINDINGS

The State of Third Party Risk Management

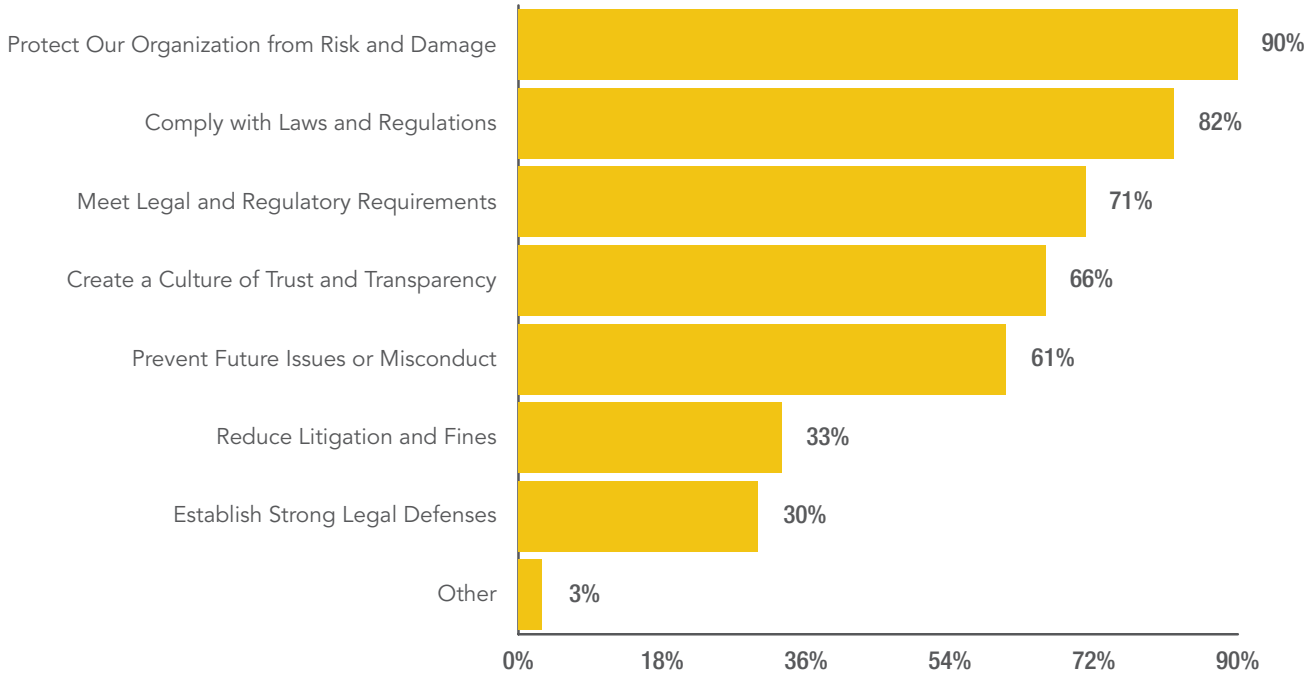
1) Top Objectives

FINDINGS: Ninety percent of survey respondents cite "protect our organization from risk and damage" as a top objective for their third party risk management program. This is followed by "comply with laws and regulations" (82%) and "meet legal and regulatory requirements" (71%).

ANALYSIS:

- The top priorities generally show that organizations are most concerned with ensuring that their third parties deliver benefits that serve the good of the organization while complying with laws.
- If third party management programs were purely check-the-box exercises, we would expect to see "reduce litigation and fines" (33%) and "establish strong legal defenses" (30%) as more popular top third party risk management objectives.

What are Your Top Third Party Risk Management Program Objectives?



Note: Because respondents could choose more than one option, percentages total more than 100%.

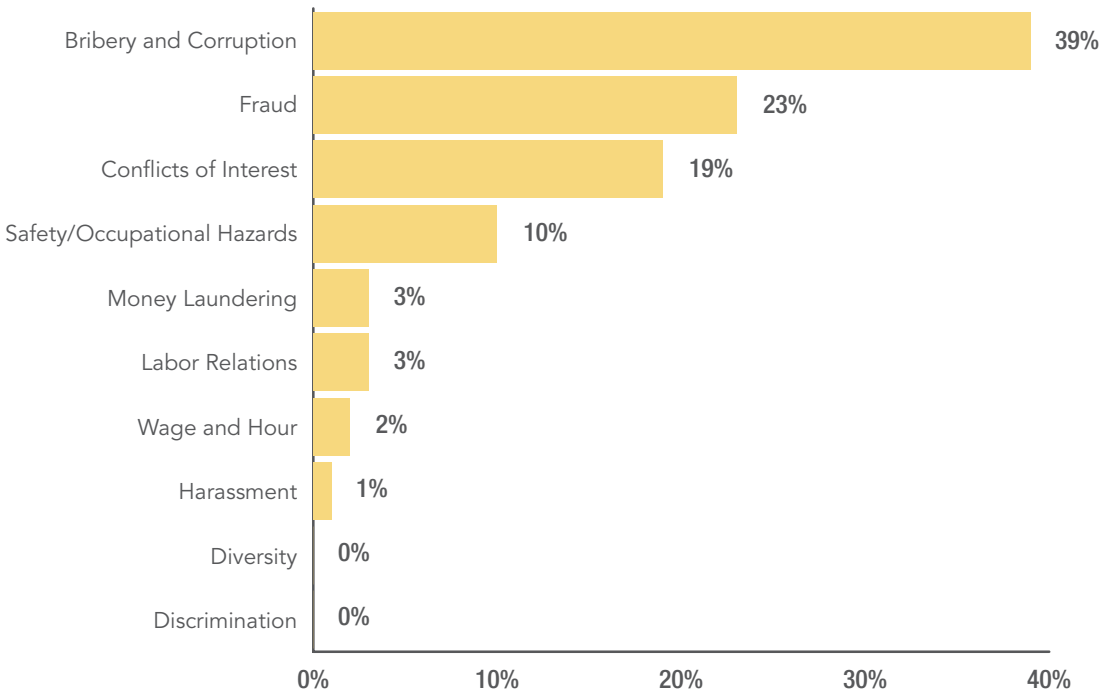
2) Top Challenges

FINDINGS: Organizations exhibit variation in what they consider their top concerns and challenges for third party risk management. Bribery and corruption is the top ethics and compliance (E&C) issue of concern (39%), while certification on policies (51%) and training on policies and requirements (48%) are the top external program challenges. Difficulty monitoring third party relationships and a lack of program resources tie at 51% for the top spot in internal program issues respondents feel could undermine success.

ANALYSIS:

- It is no surprise that bribery, fraud and conflicts of interest top the list of third party concerns. Many such cases carry large fines and penalties along with civil and criminal sanctions, including debarment—some against individuals and insiders in the organization.
- Notably, many of the concerns respondents believe could undermine program effectiveness are issues that automated due diligence software tools are created to address.

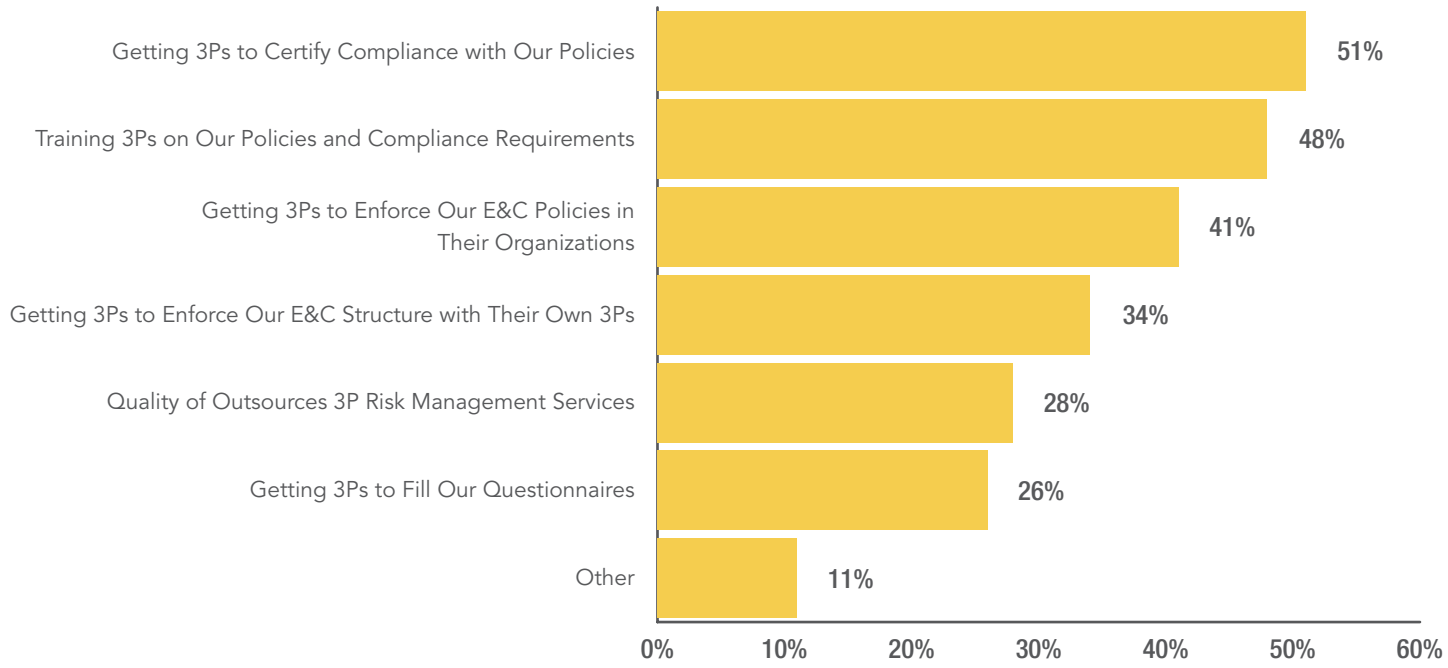
Which E&C Issues are You Most Conerned About in Relation to Third Party Misconduct?



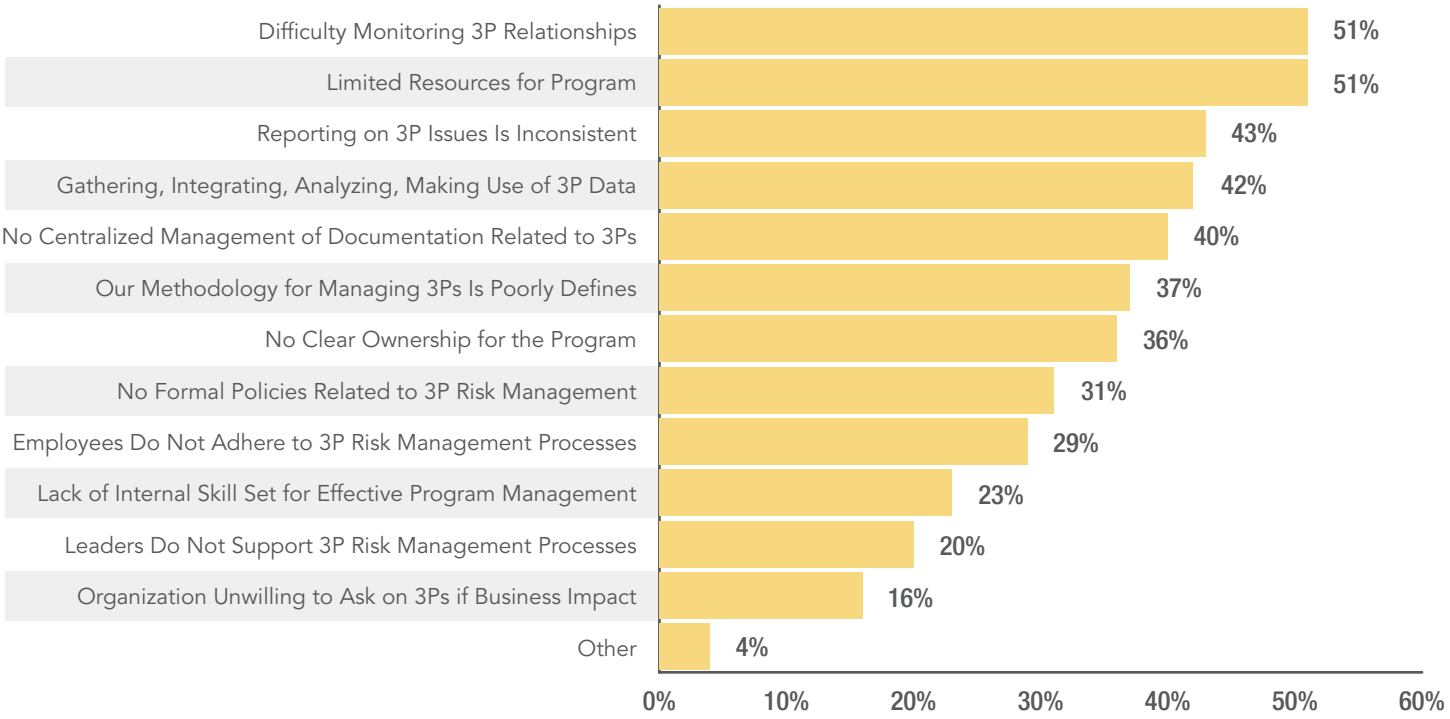
Note: Because respondents could choose more than one option, percentages total more than 100%.

2) Top Challenges (Continued)

What are the Top External Challenges for Your Third Party Risk Management Program?



Which of the Following Internal Issues Do You Feel Could Undermine Your Program Effectiveness?



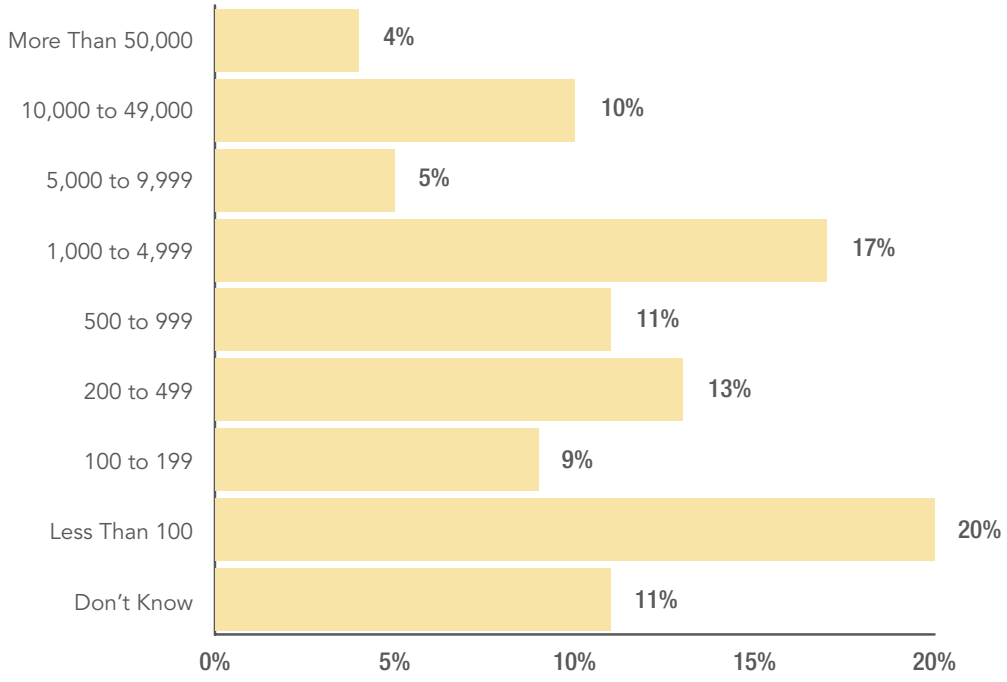
3) Number of Third Parties Managed

FINDINGS: While 50% of respondents manage between 100 and 4,999 third parties, and an additional 20% manage fewer than 100, eleven percent of respondents don't know how many third parties their organization manages.

ANALYSIS:

- Most concerning is that 11% of respondents do not know how many third parties they manage. This may mean that third parties haven't all been identified or that they are not tracked in a meaningful way. It could also mean that within those 11% of respondents, there are ongoing third party engagements without any risk or compliance oversight. If an organization cannot identify all of their third parties, they cannot possibly assess risk accurately.
- The third parties with which an organization engages should dictate the type of risk management program they deploy. Those that work with a greater number of high risk third parties require more resources to effectively manage those risks. This is particularly true if they do not use an automated due diligence and risk management solution, which can reduce the number of FTEs needed to be effective.

How Many Third Parties Does Your Organization Work With Today?



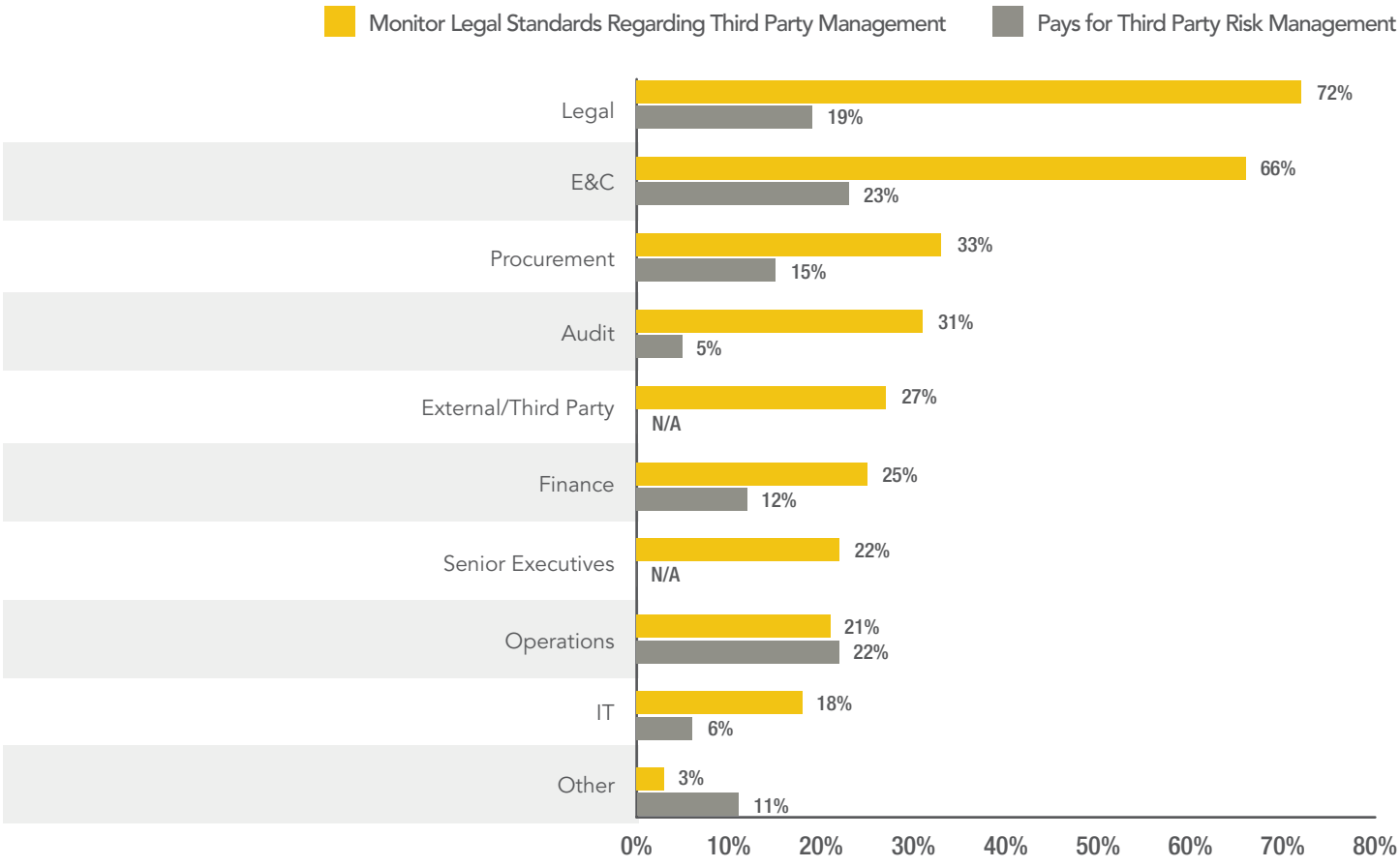
4) Program Ownership

FINDINGS: Ethics & Compliance (23%) and Operations (22%) are the departments that most commonly pay for third party risk management (including due diligence). Legal (72%) and Ethics & Compliance (66%) are the most likely to be responsible for monitoring legal standards relating to third party risk management.

ANALYSIS:

- While Legal and Ethics & Compliance departments often control both the budgets and the monitoring and effectiveness standards (KPIs), Operations may pay for third party risk management without owning KPIs. In a substantial minority of organizations, a combination of functions pays for third party risk management.
- While budget control and monitoring under different ownership might seem to be a disconnect, it is not unusual. The critical element is to be sure that those who do not have budget control are still accountable for program KPIs. Those with KPI accountability need to have appropriate input and influence with the budget owner to ensure access to the resources needed to conduct an effective program.

Which Departments Have Key Reponsibilities for Your Third Party Risk Management Program?



Note: Because respondents could choose more than one option, percentages total more than 100%.

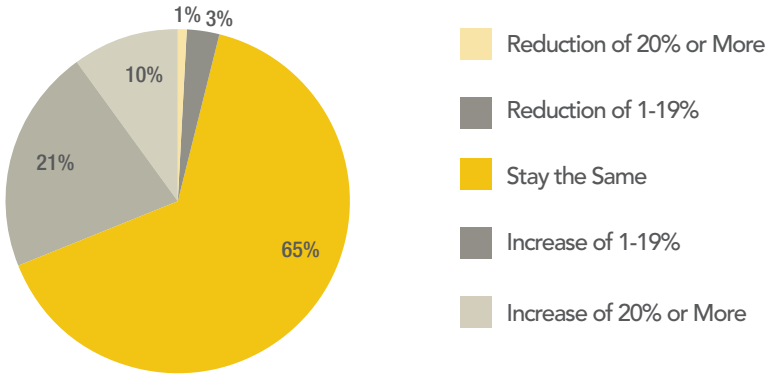
5) Program Budgets

FINDINGS: Almost half of the respondents have no dedicated budget for third party risk management, while roughly one in four respondents don't know their organization's budget. Approximately one-third of respondents anticipate an increase in their budgets.

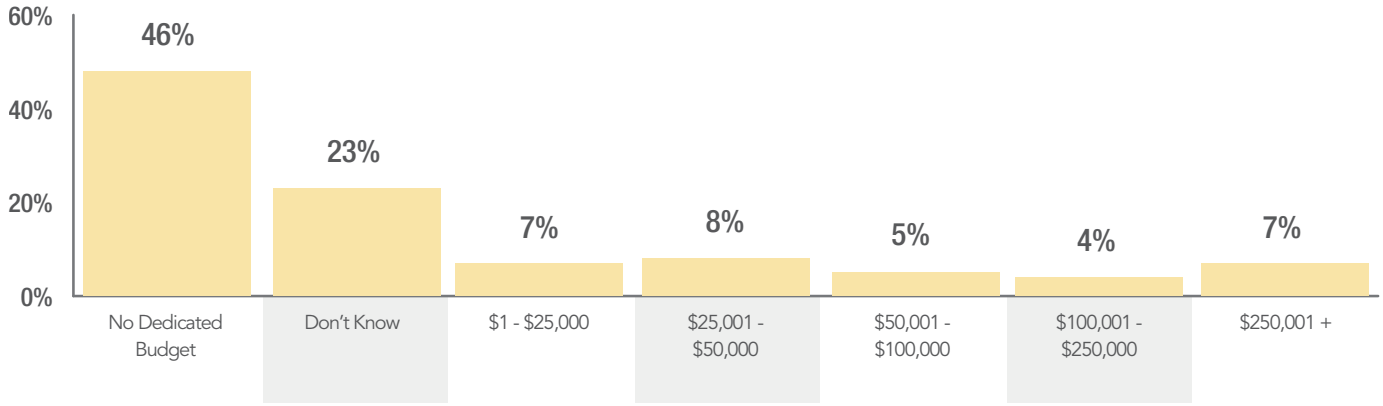
ANALYSIS:

- Actual budget amounts are not the important measure here. The Federal Sentencing Guidelines for Organizations (FSGO) state that an effective compliance program should have "adequate resources," but the Guidelines do not define "adequate." Organizations must establish a reasonable budget based on their third party ecosystem, risk profile and a risk-based assessment.
- The high percentage (46%) of respondents that report no dedicated budget is not unusual as many third party risk management budgets are lumped into larger operations budgets. The danger here is that spending cannot be adequately tied to the effectiveness of third party risk management efforts.

Planned Investment in Third Party Risk Management Program in the Coming 12 Months



Third Party Risk Management Budget



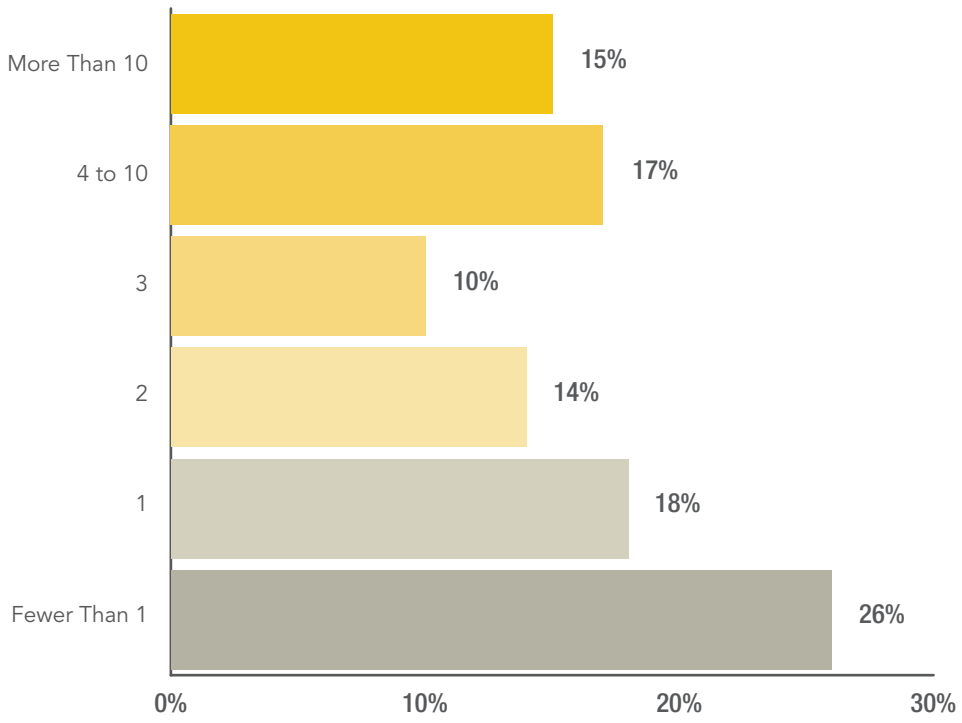
6) Full Time Employees (FTEs)

FINDINGS: Twenty-six percent of organizations have less than one full-time employee (FTE) assigned to manage their third party risk management programs. Among the remaining 74% of organizations that assign one or more employees to the task, the number of assigned employees varies considerably.

ANALYSIS:

- Organizations with personnel dedicated to managing third party engagements have been shown to perform better in audits and regulatory actions. Even more so than higher budgets, FTE allocation has a positive impact on performance.
- One of the most important aspects of a functional third party risk management program is the dedication and allocation of staff to actively and effectively manage the program. Automated risk management systems may reduce the need for FTEs.

How Many Full-Time Employees (FTEs) are Assigned to Manage Third Party Risk Management at Your Organization?



APPROACH TO THIRD PARTY DUE DILIGENCE

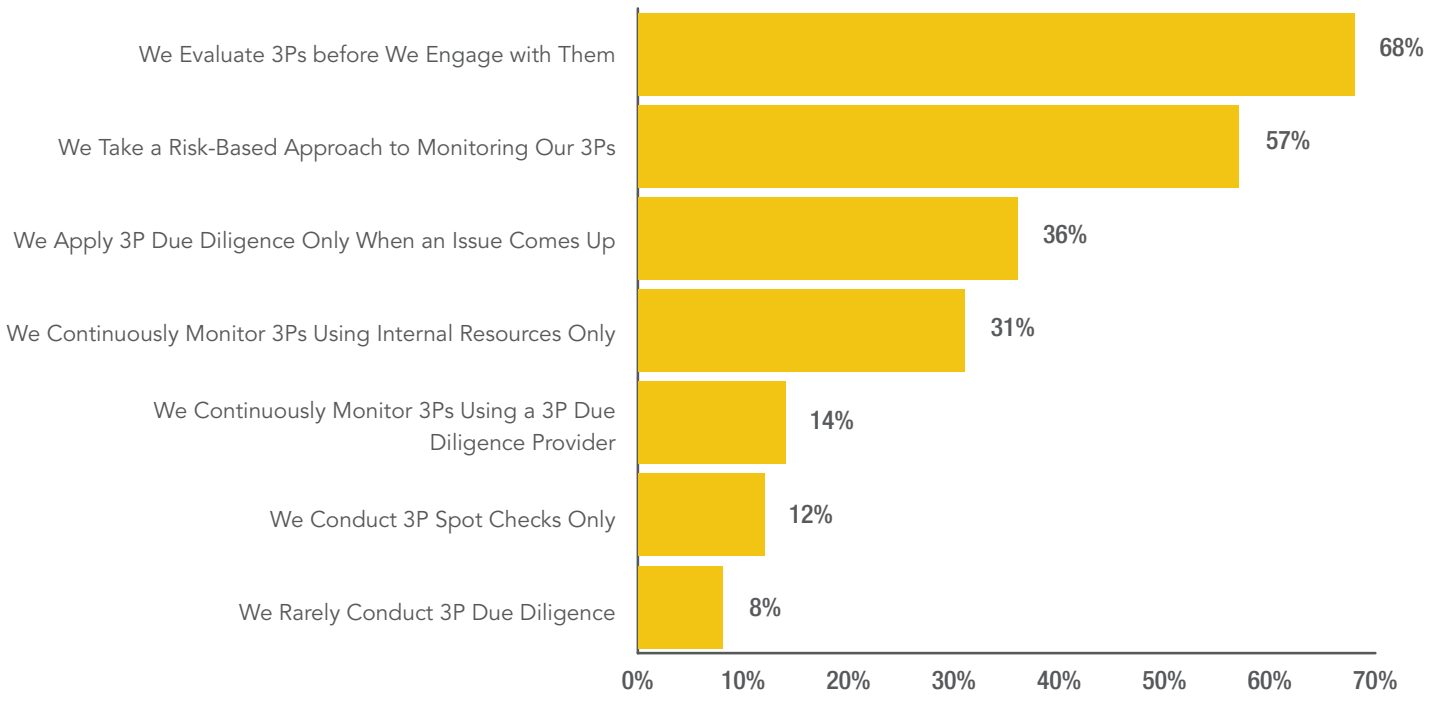
1) Approach to Conducting Third Party Due Diligence

FINDINGS: The majority of organizations (68%) evaluate third parties before engaging with them. This is in contrast to 36% of organizations that conduct due diligence only after an issue arises. And 8% rarely conduct due diligence at all. In addition, only 57% use a risk based approach to monitoring third parties.

ANALYSIS:

- Third party risk attaches at the time of engagement. So, while conducting due diligence after a disclosure may be better than nothing, anything that occurred prior to it will be indefensible. Organizations that do not conduct due diligence before engaging with third parties are exposing themselves to significant risk.
- A third of respondents indicated that they monitor with internal resources. This may also increase risk as continuous monitoring can be difficult, especially if third parties are in remote areas and monitoring requires reviewing local publications in languages that cannot be easily translated.

How Does Your Organization Conduct Third Party Due Diligence?



Note: Because respondents could choose more than one option, percentages total more than 100%.

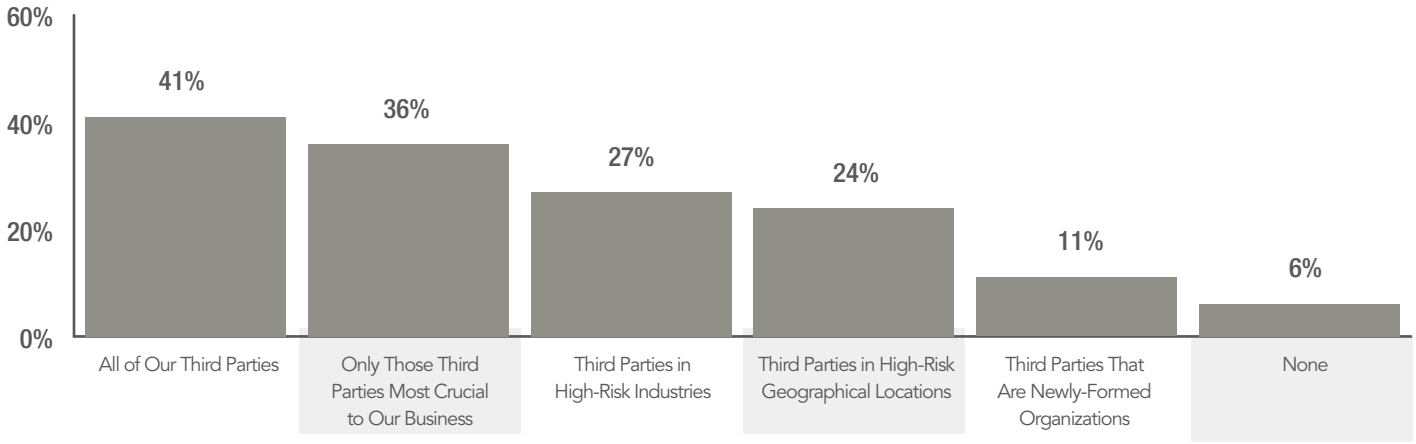
2) Screening Third Parties

FINDINGS: Forty-one percent of respondents conduct some form of due diligence on all third parties independent of risk category, while others screen by defined risk categories. Six percent do not screen by category. About three-fourths of these conduct some level of pre-engagement due diligence screens on their third parties.

ANALYSIS:

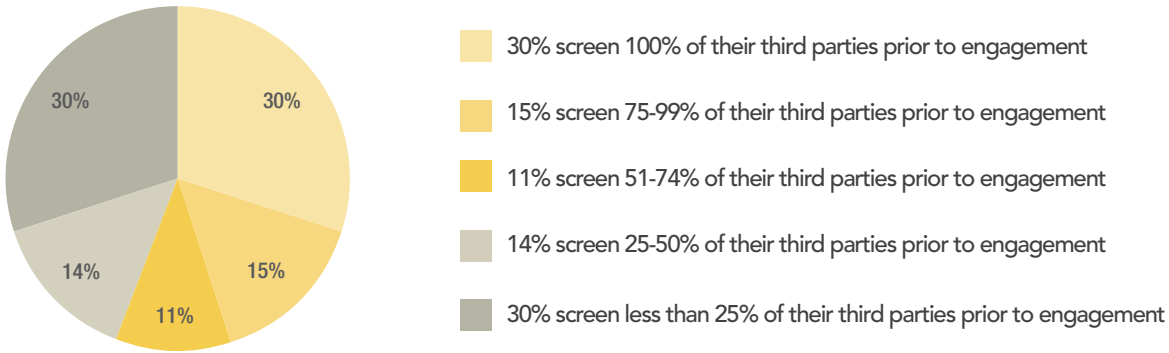
- When deciding whom to screen, a third party's industry and location are more significant contributors to risk than years of operation.
- Organizations are equally likely to subject either 100% or less than 25% of their third parties to pre-engagement due diligence screening. This type of pre-engagement due diligence indicates an "all-or-nothing" approach. Anything less than 100% means the company is assuming risk. As it may be tricky to predict which third party is most likely to expose the company to risk, it is safer to subject 100% to a risk adjusted due diligence process. All third parties do not need the same level of due diligence, but no due diligence is a roll of the dice.

On Which Third Parties Does Your Organization Complete Initial or Pre-Engagement Screening?



Note: Because respondents could choose more than one option, percentages total more than 100%.

What Percentage of Your Third Parties Do You Conduct Due Diligence on Prior to Engaging Them?



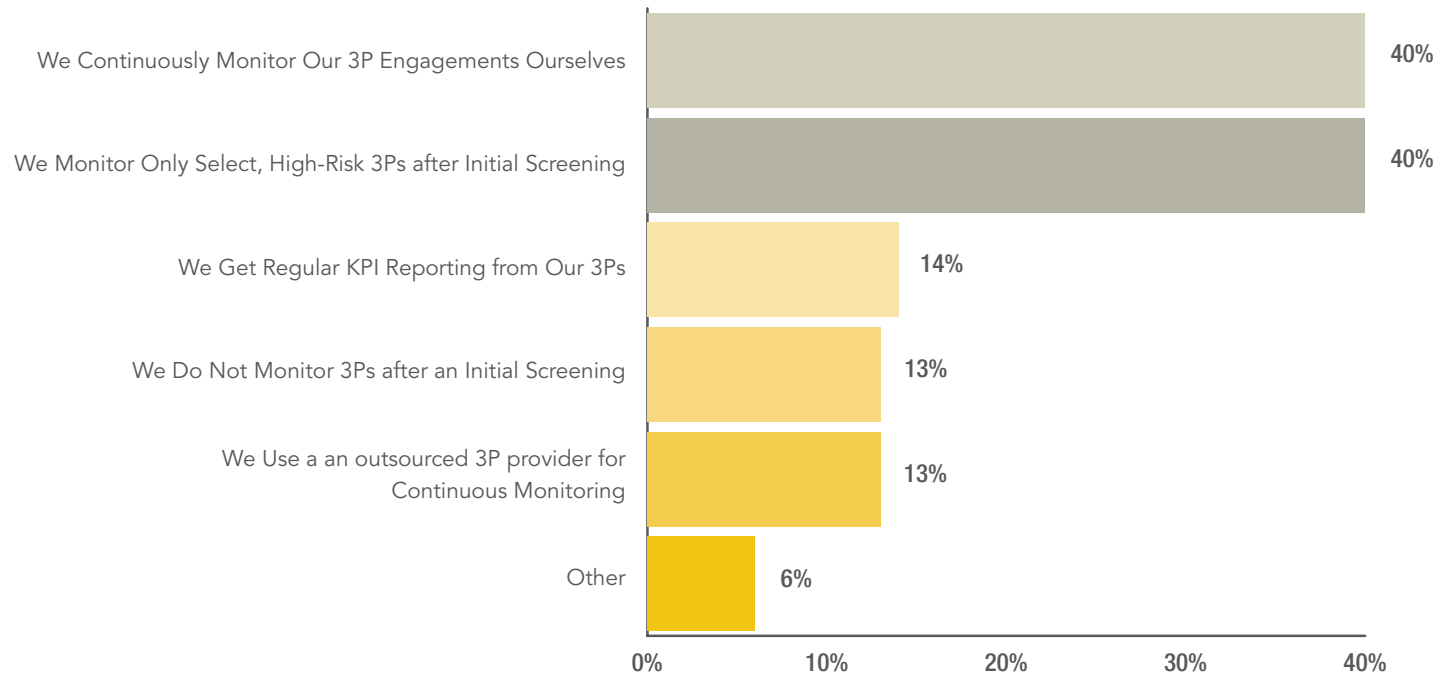
3) Monitoring Third Parties

FINDINGS: Organizations that continuously monitor their third parties are most likely to either manage the monitoring processes themselves (40%) and/or to only monitor select, high-risk third parties (40%). Thirteen percent don't do any monitoring after the third party passes the initial screening.

ANALYSIS:

- Periodic reassessments may expose red flags with a third party that had a clean bill of health on January 1. When that party is charged with bribing a government official on April 1, without continuous monitoring or periodic reassessment, this might have been missed until much later. A third party risk management policy should prescribe and document defined processes for due diligence, monitoring and follow up.

How Do You Monitor Your Third Party Providers After Their Initial Screening?



Note: Because respondents could choose more than one option, percentages total more than 100%.

PROCESSES FOR THIRD PARTY RISK MANAGEMENT

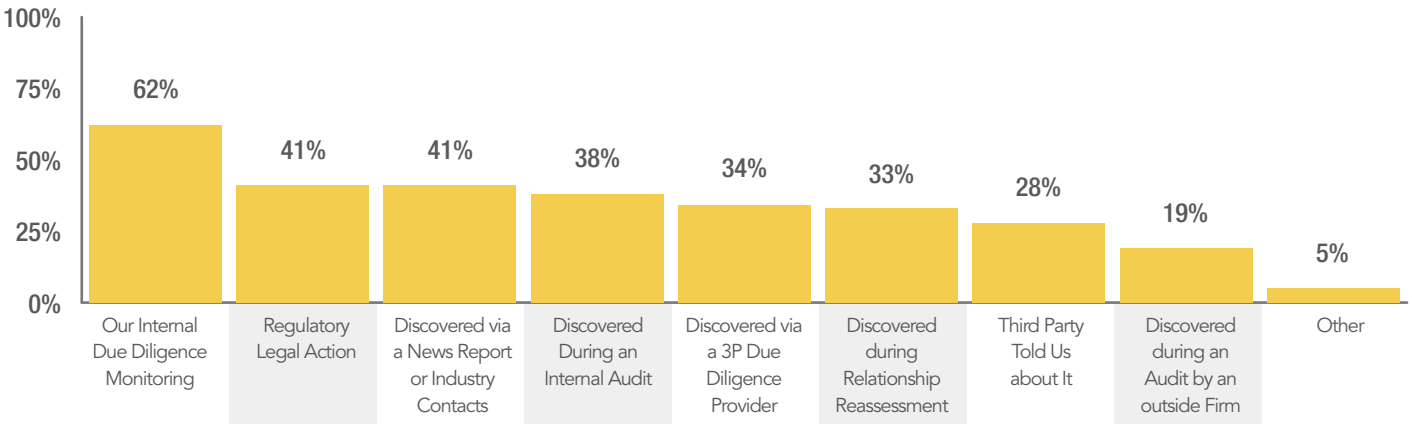
1) Approach to Discovering "Red Flags"

FINDINGS: Organizations generally discover "red flags" or other potentially negative third party information via multiple channels. Most common is through internal due diligence monitoring (62%).

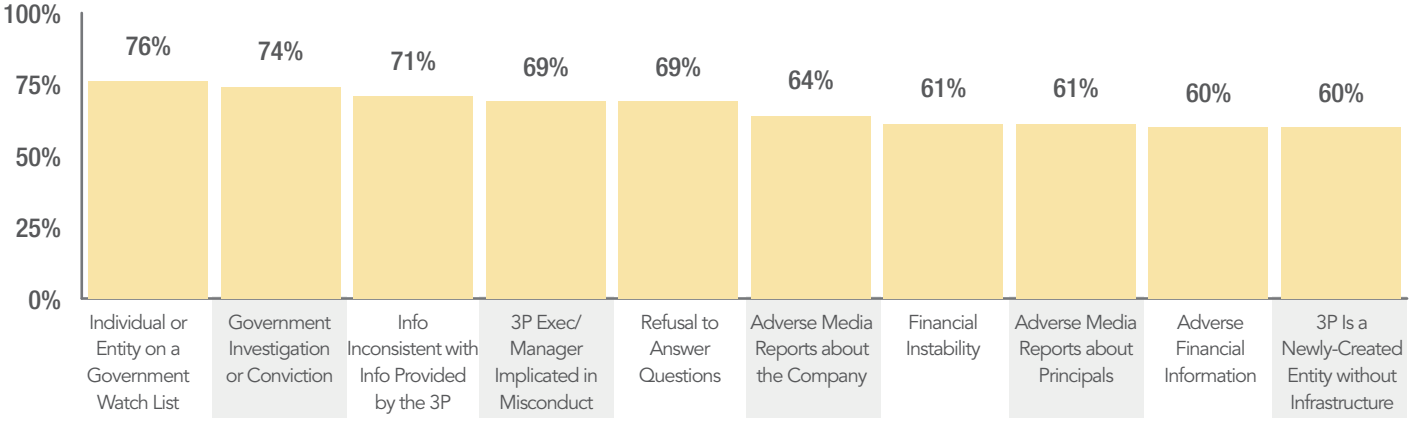
ANALYSIS:

- Forty-one percent discover such issues through regulatory or legal action, which may indicate that many organizations fail to use screening mechanisms and safeguards. That 41% discover red flags through news reports and industry colleagues may represent a dearth of dependable direct resources through which they can identify risks.
- It is troubling that the top two red flags relate to individuals or companies that are on a government watch list (76%) or are subject to government investigations (74%). If an organization conducts no due diligence prior to engaging with a third party, they are likely missing some of the most basic and damaging red flags.

How Have You Identified Red Flags or Other Negative Third Party Information?



What Would Your Organization Consider A Third Party 'Red Flag'?



Note: Because respondents could choose more than one option, percentages total more than 100%.

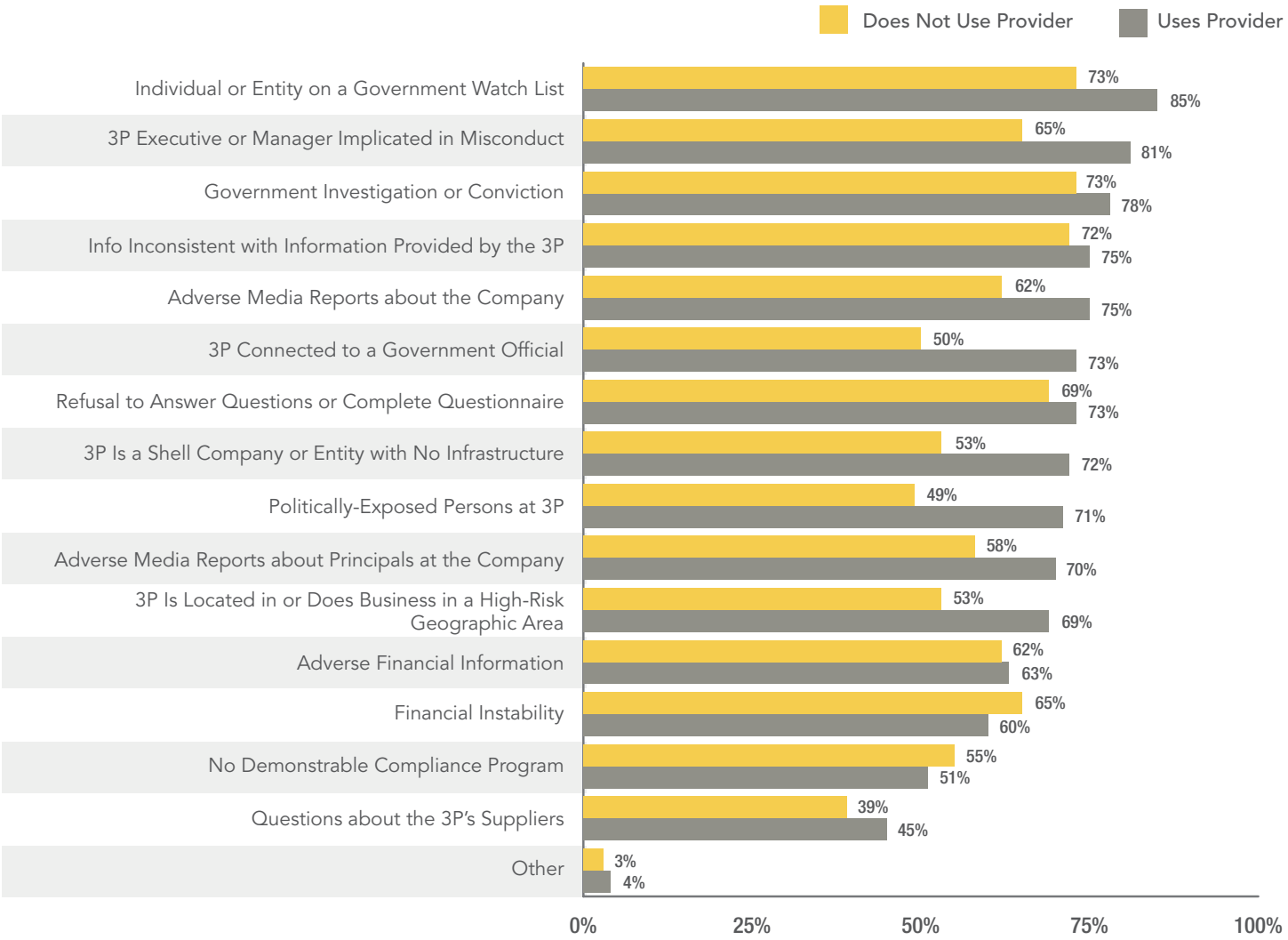
2) Use of Outsourced Providers to Discover "Red Flags"

FINDINGS: Organizations that use an outsourced third party due diligence providers discover more "red flags" or other potentially negative third party information than those who do not. For example, organizations using an outside firm uncover more managers implicated in misconduct, politically exposed persons and adverse media reports.

ANALYSIS:

- Shifting the identification of red flags to a firm that specializes in screening and monitoring third parties results in more identified issues. Many organizations that hire outside providers to identify risks have a complex program to manage and more broadly distributed risks. The below results validate their investment in outsourced provider's expertise, automation and diligence.
- Particularly where there are international third party engagements, outsourcing to an outsourced due diligence provider with local business practice and language expertise often results in more red flag discoveries.

Red Flags by Use of an Outsourced Due Diligence Provider



ADDRESSING LEGAL & REGULATORY RISK

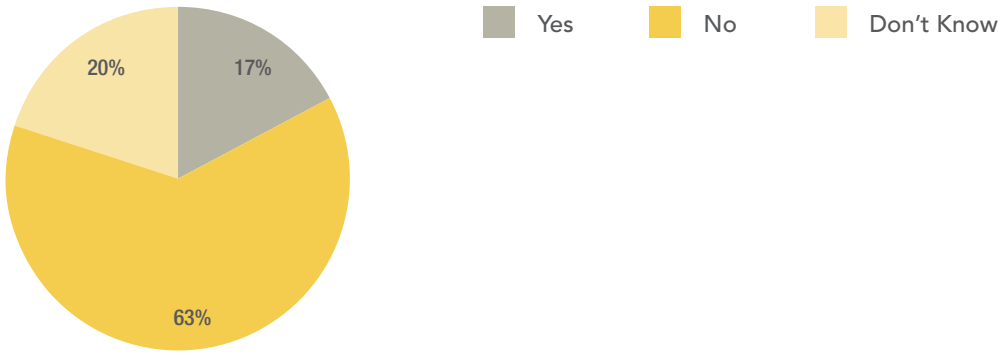
1) Legal & Regulatory Issues

FINDINGS: Seventeen percent of respondents report that in the past three years they faced a legal or external regulatory action where a third party came under review as part of the action or defense. Among those that faced such action(s), the majority (57%) faced two or fewer.

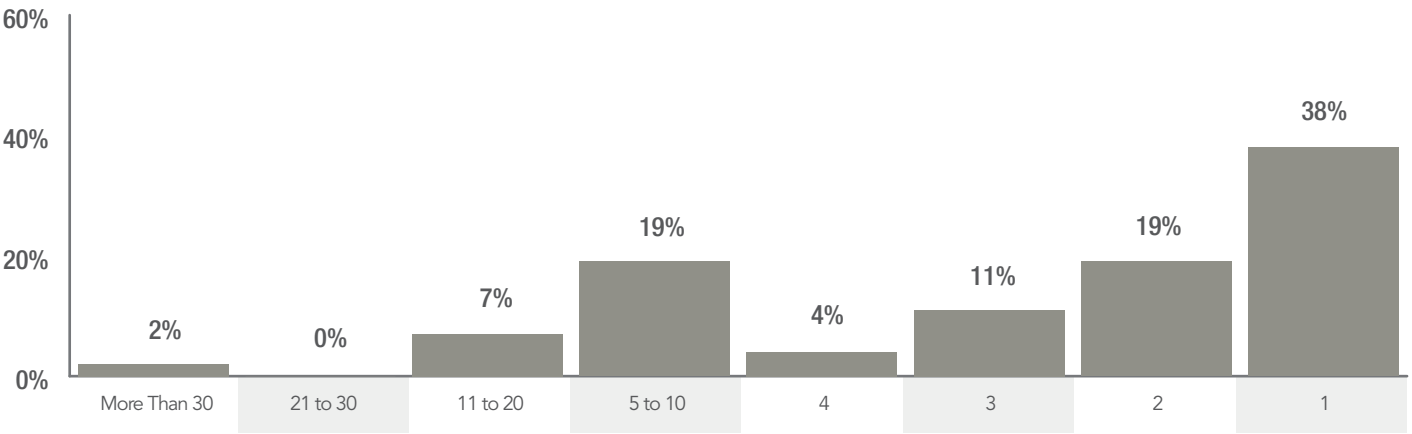
ANALYSIS:

- These findings could be interpreted as a sign that the risk of a compliance failure is low enough that you can "take a chance." This is ill-advised as in terms of risk and regulatory action, past is not prologue.
- As the OECD Foreign Bribery survey and the thousands of whistleblower tips received each year by the U.S. SEC's Office of the Whistleblower suggest, the odds of an issue are higher than the reported FCPA indictments and convictions might indicate. The OECD survey shows that the timeline for bringing a successful prosecution may be as long as seven years. Issues occurring today may not bear the fruit of sanctions or penalties for years to come.

In the Last Three Years, Has Your Organization Faced Legal or External Regulatory Action Where a Third Party Came under Review as Part of the Action or Defense?



How Many Times in the Past Three Years Did Your Organization Face Such Actions?



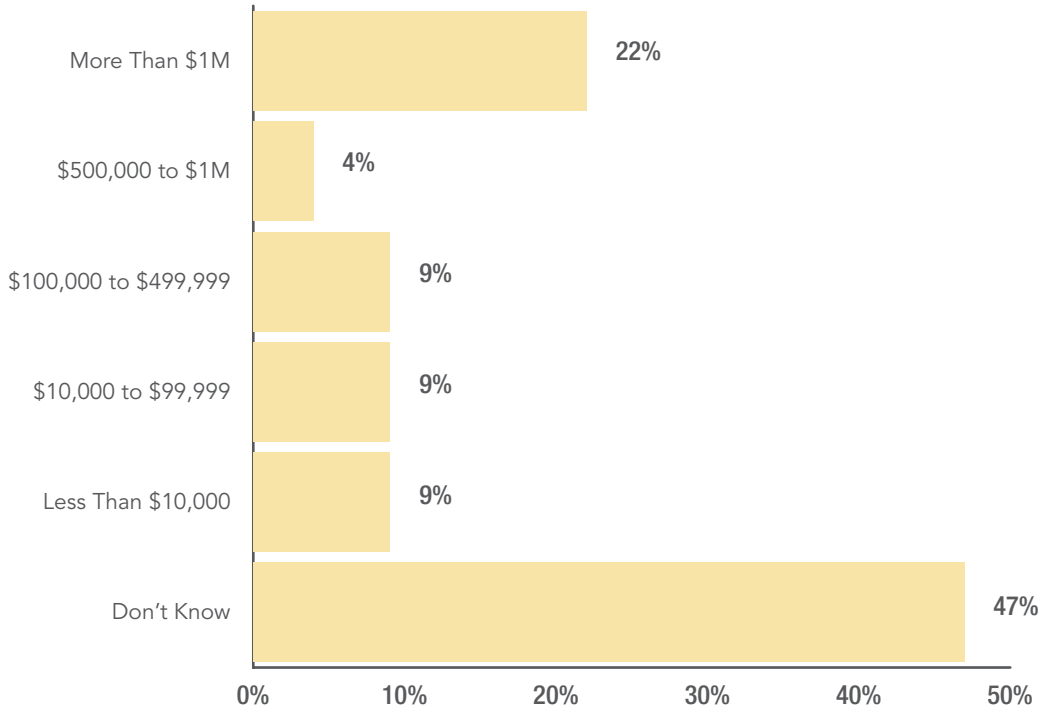
2) Cost of Legal & Regulatory Incidents

FINDINGS: Forty-seven percent of respondents don't know the average cost per legal or regulatory incident. Among those that do know, more respondents saw fines of more than $1 million than any other amount (22%).

ANALYSIS:

- That 47% of respondents don't know the average cost per incident may indicate a disconnect between performance of the program and accountability for the pain of a third party failure. Individuals managing third parties and third party risk ideally should be close enough to the each of the third parties to be able to understand the economic impact of each incident on the company.
- Those who manage third parties for which an average incident costs their organization $1 million or more should be closely monitoring and managing every third party engagement.

Average Cost per Incident



ROI & AUTOMATED THIRD PARTY DUE DILIGENCE

IV. KEY FINDINGS

ROI & Automated Third Party Due Diligence

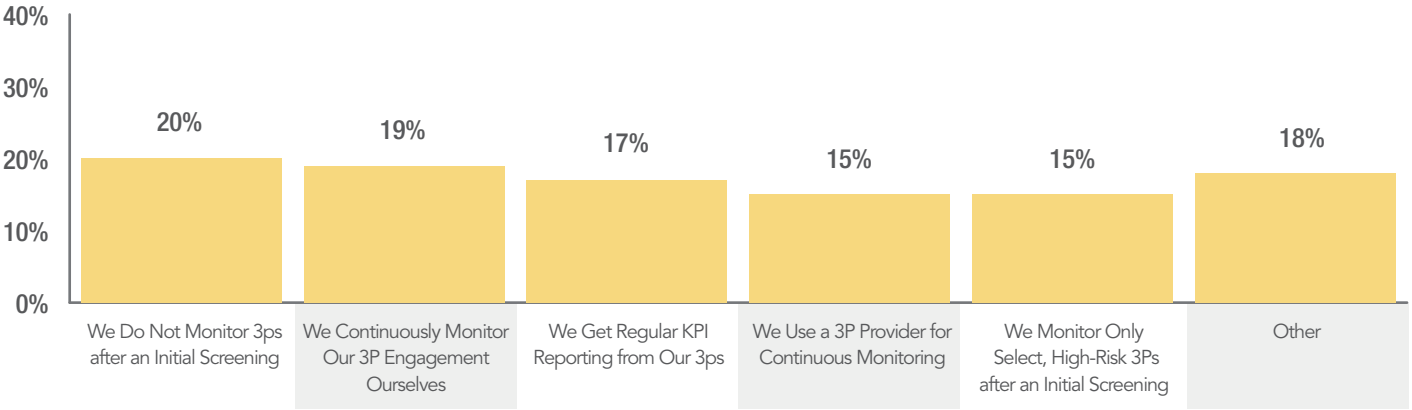
1) How do you know your program is effective?

FINDINGS: Organizations that do not monitor third parties post-engagement are the most likely to have faced legal action related to third party compliance in the past three years. Those same parties are more likely than other organizations to report costs of legal actions exceeding $500,000.

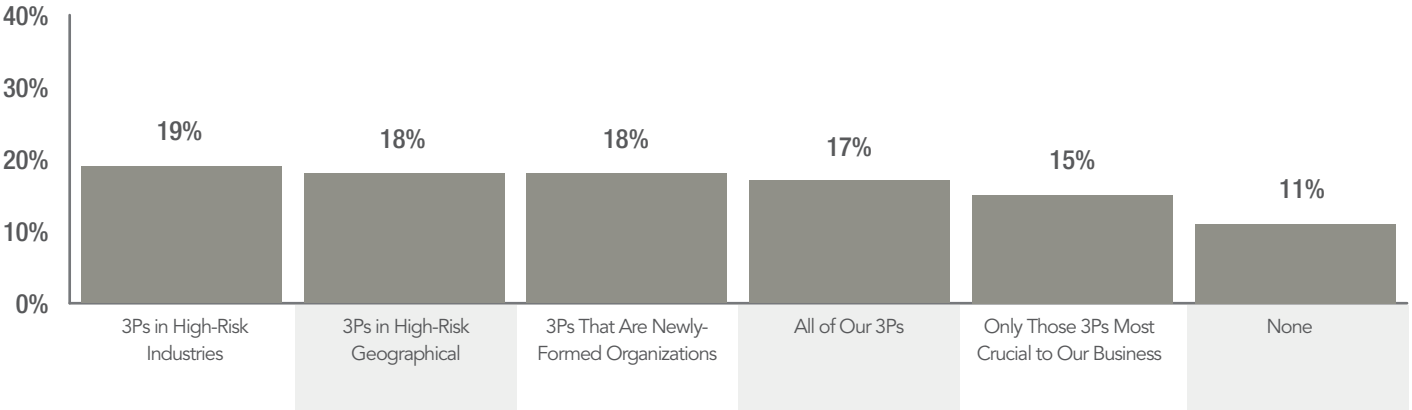
ANALYSIS:

- Dedicated third party monitoring clearly reduces legal costs. Organizations that apply adequate resources to monitoring third parties through FTEs and outsourced third party due diligence providers are less likely to have faced legal action in the past three years.
- Organizations that use an outsourced third party due diligence provider rate their third party risk management program more positively along every metric included in the survey than those that do not.

Faced Legal Action Defined by How Third Parties Are Monitored

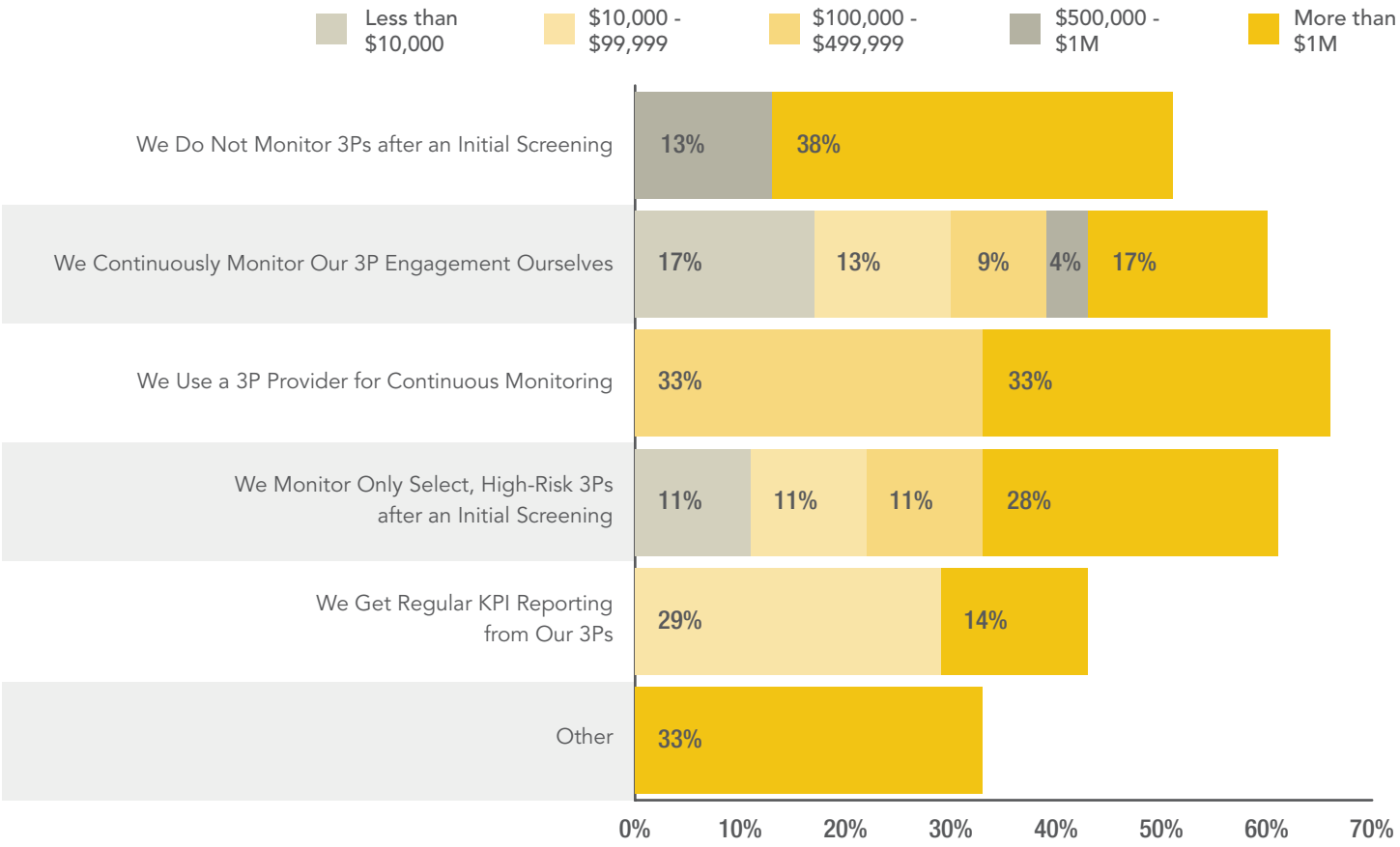


Faced Legal Action as Defined by Monitoring Practices and Risk Categories



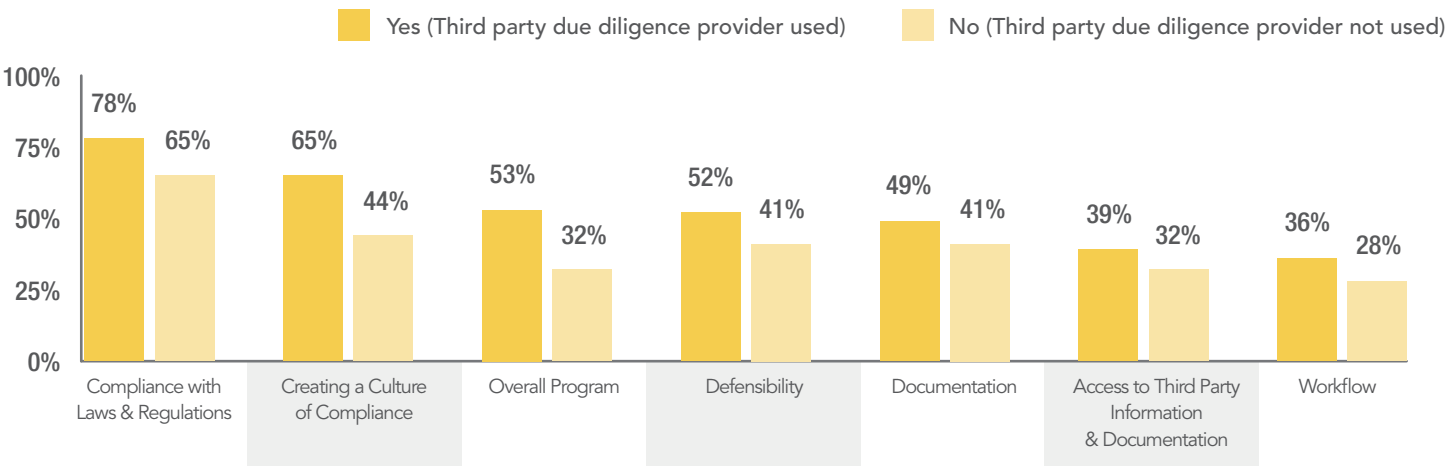
1) How do you know your program is effective? (continued)

Cost of Legal Action by Extent of Monitoring



Note: Because respondents could choose more than one option, percentages total more than 100%.

Organizations Rating Program Components "Good" or "Very Good"



V. CONCLUSION AND KEY TAKEAWAYS

Conclusion

Use of third parties is the reality of business today. Consequently, effective, risk based third party risk management is an essential component of a thriving and ethical organization. While many organizations are still building a comprehensive third party risk management program, most (68%) are conducting at least basic screening of their third parties prior to engaging with them. While fewer respondents continuously monitor all of their third party engagements, there is growing awareness of the importance of doing so and a recognition that automation produces more satisfaction than without it. As this report shows, the risks that third parties represent to organizations are too high to not actively manage.

Key Takeaways

- **Third party risk is your risk.** Today, organizations know that the behavior of agents, contractors, partners, suppliers, and intermediaries that represent them reflects upon them. Regulators, the press, and the public do not often delineate between the first and third parties when unethical behaviors are revealed. Organizations cannot afford to take risks with their people, reputations, and bottom line through neglecting to screen and monitor their third parties.
- **Though many organizations know which third party failures they should fear, they have not built sufficient programs to protect themselves from those risks.** It is worrisome that many organizations recognize that risks are out there but are not taking steps to mitigate them. There are signs that third party risk management is a maturing market with palpable demand for best practice guidance on resource allocation, risk evaluation, vendor assessment, frequency and completeness of screening and monitoring, and defining program ownership. Those organizations that perform well have found a balance of FTEs, budget, and program processes. With these elements in place, successes and confidence in the program follow.
- **While liability for the actions of third parties is embedded in the regulatory landscape, what constitutes an adequate third party risk management program is evolving.** As some organizations are publicly chastened and fined due to the behaviors of their third party providers, many are learning that the more comprehensive their program the more protected they are. Today, active third party risk management requires organizations to screen and evaluate their third parties, but to also ensure that they comply with the engaging party's Code of Conduct and other ethical and behavioral expectations. As the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) Guidance on the Foreign Corrupt Practices Act (FCPA 2012) states, *"In addition to considering a company's due diligence on third parties, DOJ and SEC also assess whether the company has informed third parties of the company's compliance program and commitment to ethical and lawful business practices and, where appropriate, whether it has sought assurances from third parties, through certifications and otherwise, of reciprocal commitments."*
- **A continuous third party due diligence monitoring program is critical to the long term success of a third party risk management program.** Initial third party screening can be effective at identifying early red flags. But those organizations that do continuous monitoring—particularly those that invest in automated third party due diligence software—report better program outcomes. They are more likely to identify risks early, less likely to experience regulatory issues and are more satisfied with their risk management programs across multiple criteria.

V. CONCLUSION AND KEY TAKEAWAYS

- **Develop well-defined, documented processes for assessing, onboarding, training and monitoring third parties.** This includes engaging with them through questionnaires, meetings, references, shared codes of conduct and contractual obligations. An effective program should include standardized documentation, record keeping methodology, timelines, well-defined expectations in terms of behavior and communications, and an ability to reassess engagements on a continuous basis.
- **Find the right level of due diligence monitoring to meet your needs.** Overdoing due diligence can be a waste of company resources, and doing too little or nothing at all may expose your company to significant business, regulatory and financial risks. Find an automated vendor that allows you to get reports at a cost point and an analysis level that makes sense for your organization.
- **As companies trend toward using more third party providers and the risk environment becomes increasingly more complex, investing in the expertise of automated third party screening and monitoring service providers has proven rewarding.** As these solution providers can typically scale and broaden screening and monitoring scope as first party demands grow, they deliver confidence where internal systems may be lacking. The best solutions enable third party review, management, and maintenance throughout the engagement life cycle.

VI. ABOUT NAVEX GLOBAL'S THIRD PARTY RISK MANAGEMENT SOLUTION

NAVEX Global's RiskRate™ Enterprise Due Diligence third party risk management solution is an affordable, automated platform that performs around-the-clock third party risk monitoring. Only an automated system that reviews all of your third parties against a standard set of screening and monitoring criteria can enable you to accurately evaluate all of your third parties, structure program efficiencies focused on risk-balancing your third party engagements, and build confidence that your approach to third party risk management delivers strategic value to your organization.

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.

VII. ADDITIONAL THIRD PARTY RISK MANAGEMENT PROGRAM RESOURCES

NAVEX Global also offers many valuable resources relating to improving third party risk management. Visit our resource center at www.navexglobal.com/resources to find these tools and more:

- **ARTICLE**: I Want To Automate My Third Party Due Diligence Processes: Where Do I Start?
- **WHITEPAPERS:** How to Automate Third Party Due Diligence Monitoring: Ten Steps to Success
- **WHITEPAPERS:** A Prescriptive Guide to Third Party Risk Management
- **ON-DEMAND WEBINAR:** Practical Strategies for Implementing Effective Due Diligence Systems
- **ON-DEMAND WEBINAR:** What You Don't Know Can Hurt You: The Top Three Anti-Bribery & Corruption Trends for 2015

III. ABOUT THE AUTHOR

Randy Stephens, Vice President, Advisory Services, NAVEX Global

Randy Stephens, J.D., is a lawyer and compliance specialist who has worked in roles with legal and compliance responsibility for over 30 years, including operations in Mexico, China and Canada. Randy has significant in-house experience leading compliance programs and working for some of the largest and most diverse public and private corporations in the United States, including Home Depot, Family Dollar and US Foods.

IX. ABOUT NAVEX GLOBAL

NAVEX Global helps protect your people, reputation and bottom line through a comprehensive suite of ethics and compliance software, content and services. The trusted global expert for 8,000 clients, our solutions are informed by the largest ethics and compliance community in the world. More information can be found at www.navexglobal.com.

NAVEX GLOBAL®

The Ethics and Compliance Experts

+1 866 297 0224 | INFO@NAVEXGLOBAL.COM | WWW.NAVEXGLOBAL.COM