NAVEX GLOBAL®
The Ethics and Compliance Experts

2017 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, NAVEX Global

CONTENTS

INTRODUCTION 2

SURVEY RESPONDENT PROFILE 4

EXECUTIVE SUMMARY 7

KEY FINDINGS

- 1: Foundational Data 10
- 2: Third-Party Risk Management Issues 12
- 3: Third-Party Risk Management Practices 20
- 4: Best Practices in Third-Party Risk Management Program Performance 46

CONCLUSION & KEY TAKEAWAYS 57

ABOUT NAVEX GLOBAL'S THIRD-PARTY RISK MANAGEMENT SOLUTION 58

ADDITIONAL THIRD-PARTY RISK MANAGEMENT PROGRAM RESOURCES 59

ABOUT THE AUTHOR 60

ABOUT NAVEX GLOBAL 61

INTRODUCTION

In 2017, NAVEX Global partnered with an independent research firm to survey 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 427 survey respondents. (See respondent profile in the next section for additional details.)

Our report provides insights and analysis of questions such as:

- What does the market indicate is the right approach to third-party risk management and due diligence based on common program elements and outcomes?
- What does the inconsistency of top concerns year over year indicate?
- How are organizations using outside providers to help with third-party due diligence?

How to Use This Report

This report will help you benchmark your third-party risk management program and its performance against trends in the market and best practices. If your program is not performing at the level you desire, this report may reveal program performance improvement insights. This report can help you:

- Determine whether your third-party due diligence practices are protecting your organization or exposing it to risk
- Benchmark your third-party risk management program against peers, industry norms and best practices
- 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 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?

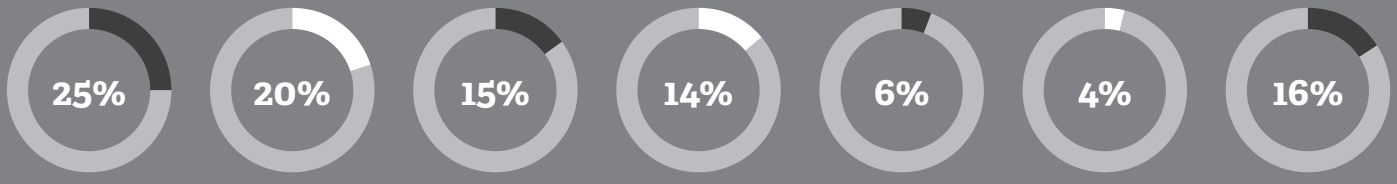
For the purposes of this report, third-party risk management is an umbrella term that refers to all risk management activities related to your third parties, including screening, data collection, documentation and ongoing monitoring.

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 recent changes to the third party's risk profile.

SURVEY RESPONDENT PROFILE

N=427

Job Function



Job Level

- 8% C-Level
- 42% Senior Management / Director
- 28% Other Management
- 16% Non-Management
- 6% Other

Company Annual Revenue

- 14% < $50M
- 33% $50M - $999M
- 38% $1B+
- 6% Not for Profit / Government
- 9% Don't Know

Company Size

Large: 5,000+ Employees — 38%

Medium: 501-5,000 Employees — 34%

Small: < 500 Employees — 28%

Regions Where Respondents Engage with Third Parties

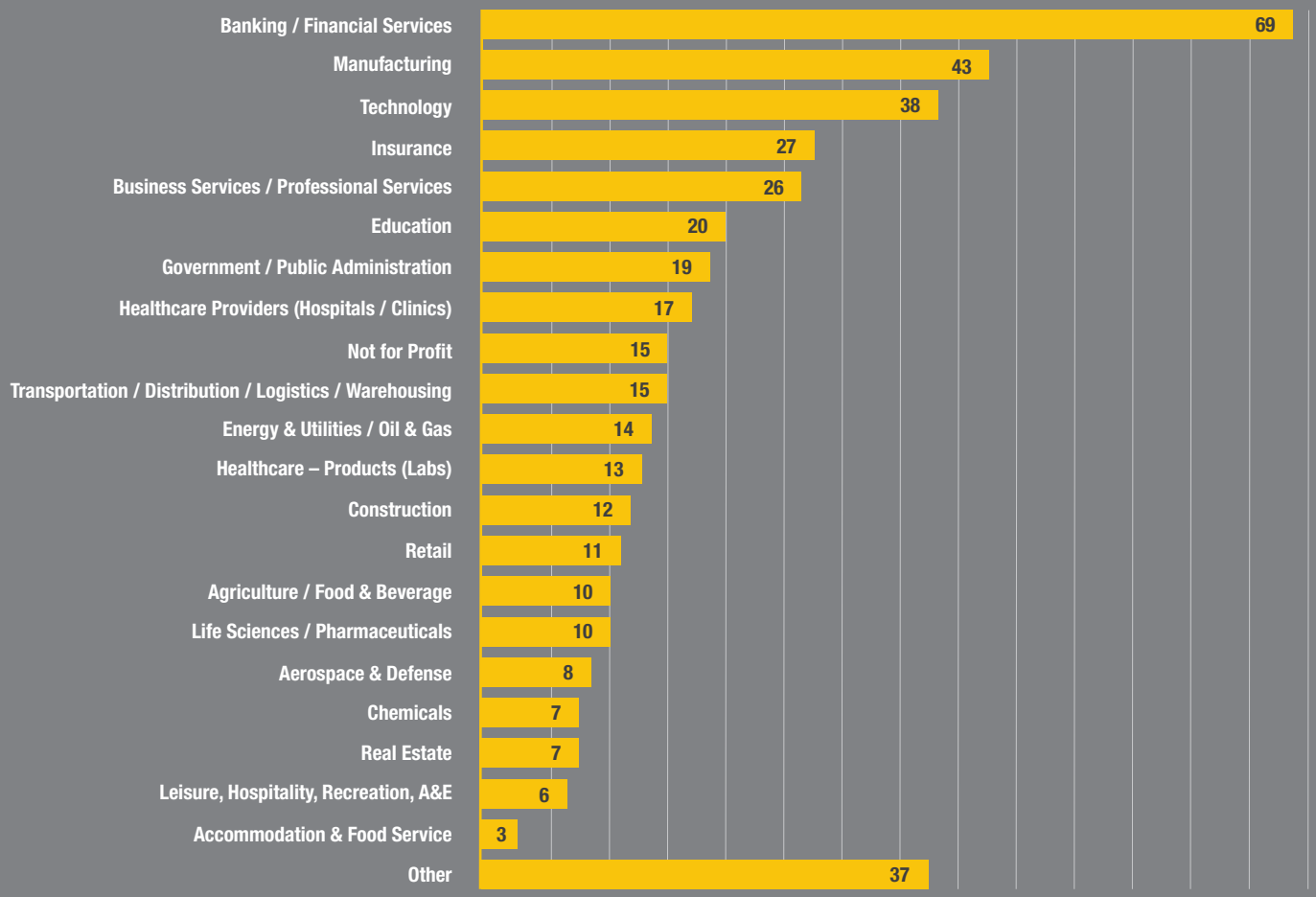
United States	78%	Middle East	33%
Europe	54%	Australia / New Zealand / Pacific Islands	32%
Asia	50%	Africa	28%
Latin America	42%	Caribbean	21%
Canada	41%		

Location of Headquarters

North America	69%
Europe	17%
Asia Pacific	6%
South America	4%
Middle East / Africa	4%

Note: Totals may be over 100% due to multiple selection options

Industries (Number of Respondents)



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. Over the last six years, we have identified clear trends in the market toward program consolidation, automation and sophistication. At the same time, we continue to see organizations facing difficulty when assessing and reporting program performance to demonstrate that high performing ethics and compliance programs both protect the organization from risk and positively influence the enduring character and culture of the organization.

This report is the third NAVEX Global benchmark report on third-party risk management. In the last two years, we have seen both encouraging and discouraging shifts in the market. More organizations take a structured approach to managing their risk; however, respondents tell us that their programs are still not fully delivering. Once again, we've asked respondents to self-assess the maturity of their third-party risk management programs and we've asked for details in terms of what specific elements deliver program value.

Third-party risk management is a top concern among compliance leaders. Inherent risks increase with the number and diversity of third parties with which organizations engage. This risk is exacerbated by the increasing complexity of applicable regulations, emerging nation-specific regulations, and lack of full transparency into third-party organizations' compliance efforts. Further, government guidance on managing third-party risks is often hedged in ambiguous terms, such as "reasonable" and "recommended." In this environment, it's not surprising that organizations engaged with third parties find it challenging to identify, mitigate and prevent third-party risk.

A series of often-cited regulations and guidelines govern the third-party risk space. Many of the perspectives in this report are informed by these regulations and guidelines. To get a better picture of the expectations on third-party risk management programs, consider the following:

- The first rendition of the Foreign Corrupt Practices Act (FCPA) was passed by the U.S. Congress in 1977. It has been amended twice, in 1988 and 1998. The FCPA continues to be the benchmark legislation that defines bribery and corruption activities, relevant risks and government enforcement actions.
- In 2012, the U.S. Department of Justice and the Securities and Exchange Commission jointly published its *Resource Guide to the U.S. Foreign Corrupt Practices Act (FCPA Guide)*. This guide offers definitions and recommendations for the FCPA anti-bribery provisions, accounting provisions, other relevant U.S. laws, principles of enforcement, penalties and resolutions. An indispensable reference for anyone working with third parties, the FCPA Guide informs many of the best practices and insights explored in this report.
- In 2010, the Bribery Act was enacted in the United Kingdom (the UKBA), which is similar to, yet in some ways stricter than, the U.S. FCPA. Combined with the FCPA, these two

regulations define much of the risks, best practices and enforcement policies related to third-party risk for organizations around the world.

- In February 2017, the U.S. Department of Justice published the *Evaluation of Corporate Compliance Programs*, including a set of evaluation criteria for managing ethics and compliance programs in a checklist format, for easier understanding and alignment.
- In addition to the FCPA and the UKBA, many new laws have been enacted around the world, such as Sapin II. This recent French law goes further than past French anti-bribery and corruption regulations. Germany has also been expanding the reach of its Administrative Offenses Act, while Brazil has been strengthening its Clean Company Act, which defines and prohibits bribery and corruption.
- ISO 37001 is the most recent example of an attempt to add some consistency around the standards and best practices for anti-bribery and corruption management systems. Published October 15, 2016, it seeks to provide certifiable standards and clarity by using "shall," "should," "may" and "can" standards to identify expectations.

A common theme is the pursuit of a risk based, properly resourced, balanced, effective and repeatable third-party risk management program. This includes well-defined procedures that apply across all third parties and creates an audit trail that demonstrates a logical evaluation of potential risk with reasonable mitigation replace. The same standards should apply across all third parties, all the time, to ensure program consistency and accuracy. These procedures include an approach that allows for tailoring for each organization's third-party risk profile along with an initial assessment of each third party and a risk-based due diligence screening, investigative and mitigation process. Third-party risk factors may include the industry, country or region of operations, the type of third party (reseller, supplier, agent, etc.), the financial commitment you have with the third party, past relationships and the depth of operational integration you have with the third party. The FCPA Guide recommends additional diligence based on multiple factors: "the degree of appropriate due diligence may vary based on industry, country, size and nature of the [third-party] transaction, and [the] historical relationship with the third party."

While no guideline or standard requires or expects a "one size fits all" approach, there is an expectation that organizations make common sense and risk-based decisions, grounded in business needs. Enforcement agencies often seek assurances from organizations that they are pursuing a risk-based approach to third-party risk management. Structured processes can both enable organizations to validate the logic behind third-party engagement decisions and protect them from scrutiny and enforcement actions. The U.S. Department of Justice reviews third-party bribery and corruption cases individually and evaluates the risk management program and efforts pursued by the organization – including meticulous recordkeeping – when deciding on enforcement actions or declinations.

A risk-based program allows organizations to allocate resources appropriately for their organization's risk profile. This may mean a lower level of due diligence for domestic third parties with well-known track records of compliance and increased scrutiny for higher risk third parties. It does not mean that organizations cannot work with third parties whose risk ratings indicate further need for review and due diligence, but it does mean that they should appropriately adjust their scrutiny, recordkeeping, training and monitoring of the third party, based on the level of potential risk. Organizations may also consider representations and warranties from the third party, specialized contract provisions and detailed agreed-upon processes for possible disengagement.

We see the question often – can we work with an organization that generates a red flag? The answer depends on the nature of the red flag. A third party may generate a red flag during initial review or continuous monitoring due to multiple risk factors. Deeper analysis may negate the risk rating, or you may find that the risks do not apply to your engagement with that third party. Importantly, you have to make an educated decision based on reasonable assurances and actions you've taken to reduce that risk and protect your organization. The important thing to keep in mind when addressing red flags, particularly if you intend to still engage with the third party, is to make sure the decision is logical, consistent and well documented. A red flag that is overlooked solely because of insistence from a high level executive or a foreign official who may have "recommended" the third party will get (and probably deserve) much more scrutiny.

Many of the processes discussed in this report demonstrate best practices in terms of program structure, recordkeeping and risk mitigation. The results demonstrate that an approach to third-party risk management that includes these key functions reduces third-party risk and improves program performance. Well-run programs with well-defined policies and automated processes see fewer competency gaps. This, in turn, reduces loose ends and aggressive "fishing expeditions" or enforcement actions. Yet, many organizations continue to struggle with these improvements and recommendations and continue to work to deliver effective third-party risk management.

1: Foundational Data

Program Ownership

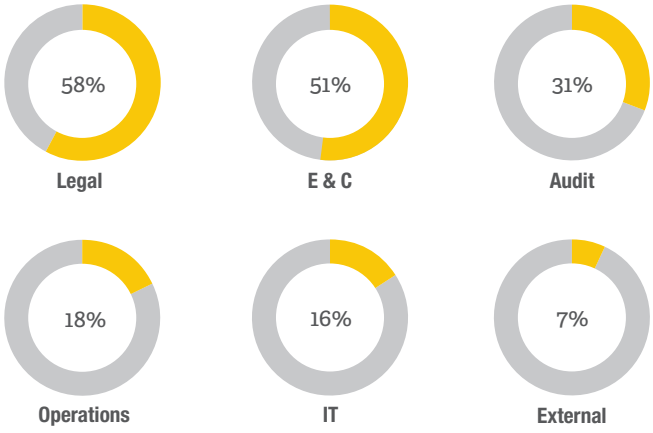
Legal (58%) and Ethics & Compliance (51%) are the departments most often charged with managing and ensuring compliance with new or revised regulatory standards for third-party risk management.

Teams that own third-party risk management programs should be aligned with and in communication across all teams that vet, engage and work with third parties. A breakdown in understanding requirements, priorities, documentation and policies within any of these teams can leave the organization vulnerable.

In terms of which department owns third-party risk management, Ethics & Compliance (45%) and Legal (41%) typically hold ownership. One change since our 2016 report is that shared ownership models are becoming more common: in 2017, 54 percent of organizations indicated shared ownership compared to 45 percent in 2016.

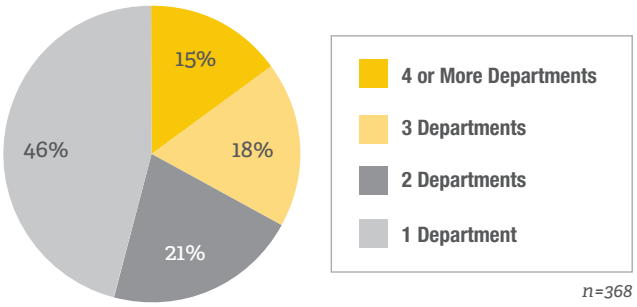
At a minimum, legal and compliance teams must have visibility into and an ability to guide third-party relationships to reduce compliance and enforcement risks.

Which of the following departments in your organization are responsible for managing and ensuring compliance with new or revised legal and regulatory standards for third-party risk management?



n=427

Number of Departments Owning Third-Party Risk Management



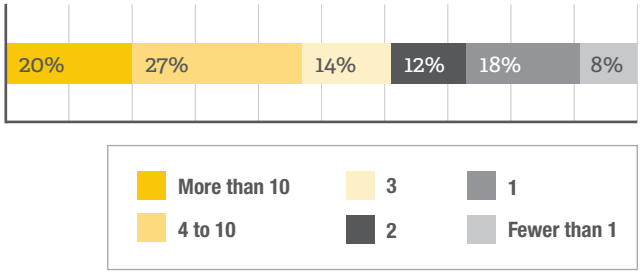
n=368

Full-Time Employees (FTEs)

The number of FTEs assigned to manage third-party risk management remains fairly consistent with the 2016 results. Almost half of organizations (47%) have four or more full-time employees (FTEs) assigned to manage their third-party risk management programs and only 8 percent have less than one.

While the number of FTEs dedicated to third-party risk management may indicate resource commitments to manage risks, it does not necessarily indicate a mature or sophisticated

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



Note: Totals may not add up to 100% due to rounding.

program. We see organizations with many third parties allocating fewer FTEs with better risk management results. Ultimately, when it comes to program performance, we see program sophistication, processes and often automation trumping resource (budget and FTE) allocation.

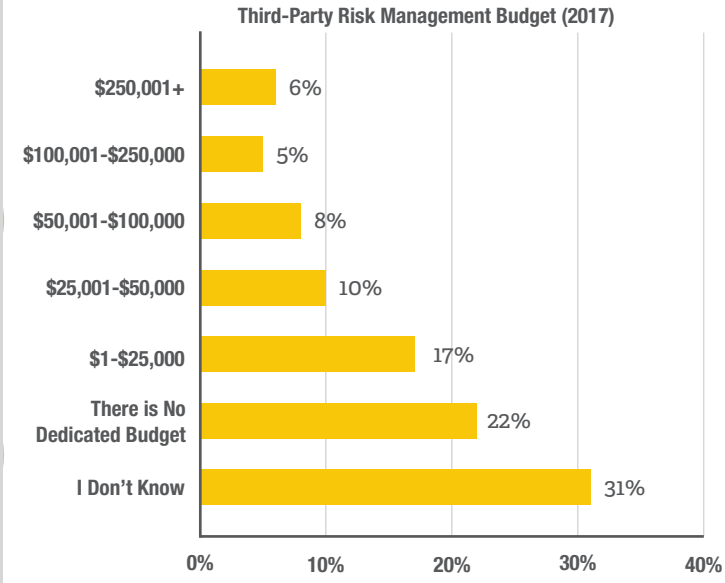
Program Expenditures

Almost one-quarter (21%) of organizations have no dedicated budget for third-party risk management, while 27 percent have a budget of $50,000 or less. Almost one in five organizations (19%) report budgets in excess of $50,000.

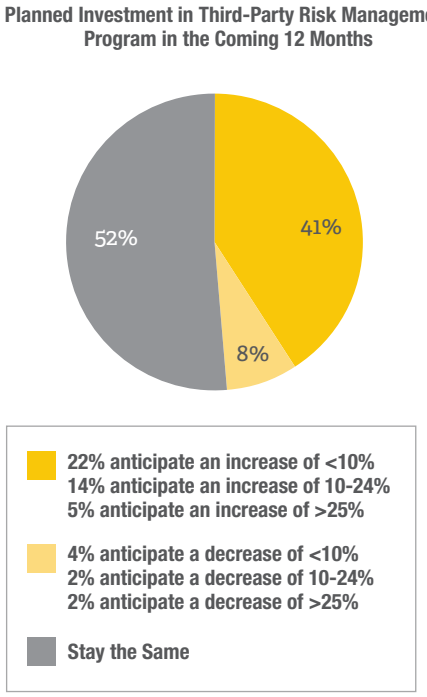
Having no dedicated budget does not allow program stakeholders to build on successes, to strategize for improved risk mitigation and align to changes in global regulations.

A greater number of organizations are predicting an increase in their budget over the next year, with 41 percent predicting they will increase budget (compared to 33% in 2016). Only a minority of organizations (8%) indicate their budgets will decrease, and the remainder of organizations (51%) anticipate they will remain unchanged.

Responsible program managers should make sure that budget is always available to complete the third-party risk management processes required throughout the year. Annual budget planning should not overlook the need to adapt as the program requires additional funding to complete screening, monitoring or mitigation actions when an engagement requires more scrutiny, risk review or replacement.



Note: Totals may not add up to 100% due to rounding. n=367



Don't know responses excluded from analysis
Note: Totals may not add up to 100% due to rounding. n=238

2: Third-Party Risk Management Issues

Top Objectives

Findings: The top objective for third-party risk management program stakeholders is to protect our organization from legal and financial risk (69%). This is followed by comply with laws and regulations (63%) and protect our organization from reputational risk (45%).

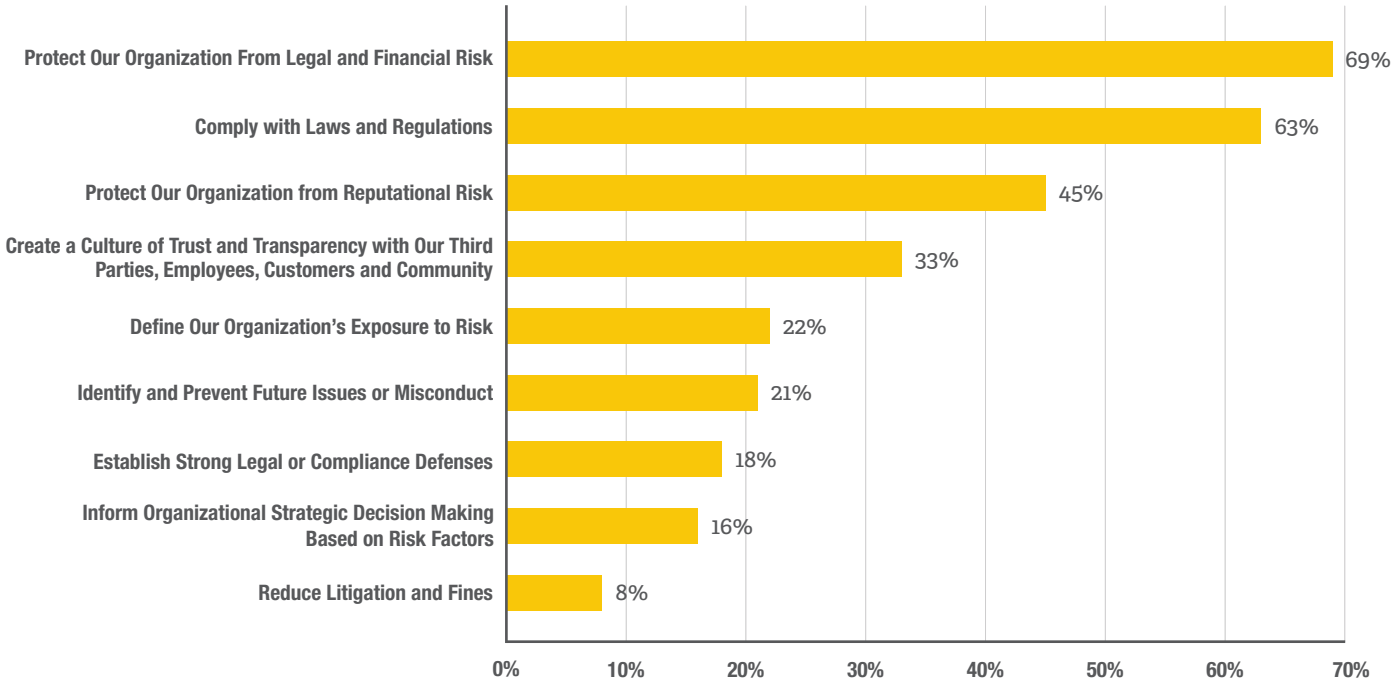
- Organizations with high annual revenues ($1 billion +) are more likely to prioritize protecting their organization from reputational risk (52%) than organizations with annual revenues of less than $50 million (36%).
- Organizations with a greater number of staff assigned to manage third-party risk management are more inclined to prioritize cultivating a culture of trust and respect with their third parties (48% of organizations with 10 or more full-time employees assigned to third-party risk management, compared to 28% of organizations with fewer than 10 such assigned staff).
- Not surprisingly, reducing litigation and fines and establishing strong legal or compliance defenses is a higher priority among organizations that have seen enforcement action in the past (reducing fines/litigation prioritized by 13% of organizations that faced legal action in the past 3 years vs. 6% of ones that did not).

Analysis: The top two responses – protect our organization from legal and financial risk, and comply with laws and regulations – have been consistent over the last three years.

These responses indicate that while third-party risk management programs may mature over time, the focus on protecting the organization from legal and financial risk and complying with regulations are both closely related and remain the persistent concern. Given the shifting legislative landscape within the U.S., the U.K., and around the world, it's logical that these concerns are again top-of-mind for third-party risk management stakeholders. Coincidentally, these concerns are two of the most critical goals of compliance programs overall.

The number three response, protect our organization from reputational risk, is not as high as we expected. While fees and fines related to third-party risk and enforcement action may be significant, the long-term brand, market and financial impact of loss of reputation can be much worse. While a third-party engagement can be ended and a government fine paid, reputational costs are often far more severe than any fine.

What Are Your Organization's Top Three Objectives for Your Third-Party Risk Management Program?



Note: Multiple choice question, percentages total more than 100%. Respondents select up to 3. n=427

Top Issues

Findings: Unlike the top objectives, the top concerns and challenges for third-party risk management have changed over the past three years. This year, cyber security and data protection (49%), bribery and corruption (42%) and conflicts of interest (34%) are still the top concerns. However, compared to last year's results, conflicts of interest has shifted from the top concern to the third. Cyber security jumped to the top concern this year.

Our data shows that the size of an organization and its location often seems to drive the top challenges.

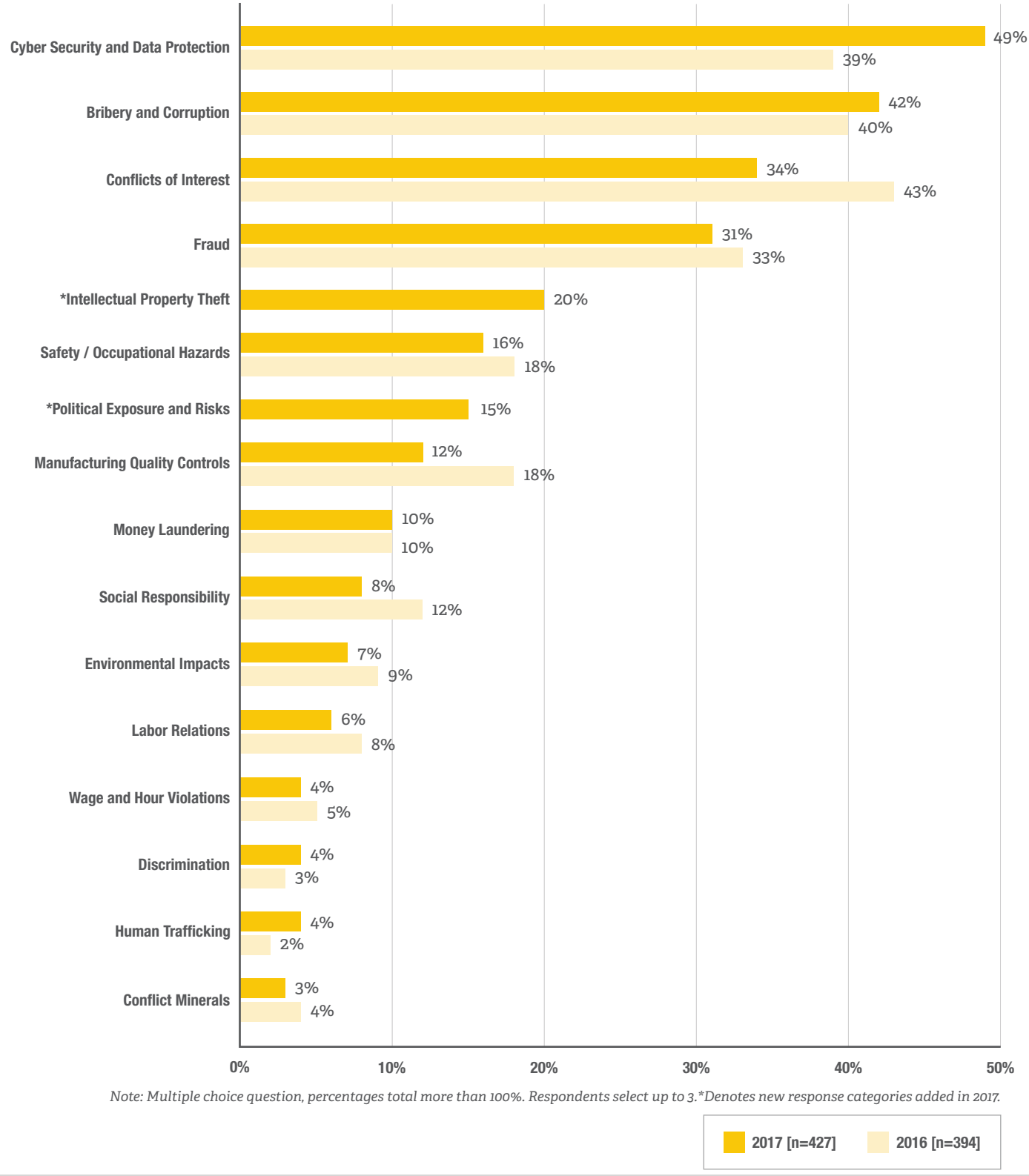
- Cyber security is of the greatest concern in organizations headquartered in North America (56%), but less so with those headquartered in EMEA (39%), Asia Pacific (28%) and Latin America (18%).
- Bribery and corruption is more of a concern in EMEA (65%) and Asia-Pacific (64%) than it is in North America (32%).
- Bribery and corruption is a more significant challenge among large organizations with 5,000+ employees (58% vs. 32% of smaller organizations) and among those with higher annual revenues (53% of organizations with $1 billion or more in annual revenue).
- Bribery and corruption is also a greater concern among organizations where 20 percent or more of annual revenue is related to or generated by their third parties.

Analysis: The fluidity of top concerns and challenges indicates a kind of hyper-awareness or risk modeling of external risks among third-party risk management stakeholders. Two years ago, bribery and corruption was the top challenge, last year, conflicts of interest topped the list. This year, cyber security surpasses both of these. Cyber security and the risk of losing critical customer, financial and other private company data is a legitimate top concern, perhaps exacerbated by recent headlines that showed secure organizational cyber defenses hacked and defeated through security holes at trusted third parties.

A strong cyber defense includes integrating many of the standard third-party risk management best practices regarding onboarding, screening, training and monitoring, adapted to assure a third party's cyber security approach is robust enough to prevent cyber loss.

Be aware of and assess all risks associated with third-party management. Often they are interrelated and a solution for one often addresses many risks. It is important to focus on the basics and not necessarily "chase" the latest headlines. Of course, major issues need to be addressed to the satisfaction of stakeholders but a focus on finding, vetting and monitoring third parties provides a strong foundation for risk reduction of all of these concerns.

Which of the Following Ethics & Compliance Issues is Your Organization Most Concerned About in Relation to Third-Party Misconduct?



*Note: Multiple choice question, percentages total more than 100%. Respondents select up to 3.*Denotes new response categories added in 2017.*

Top Challenges

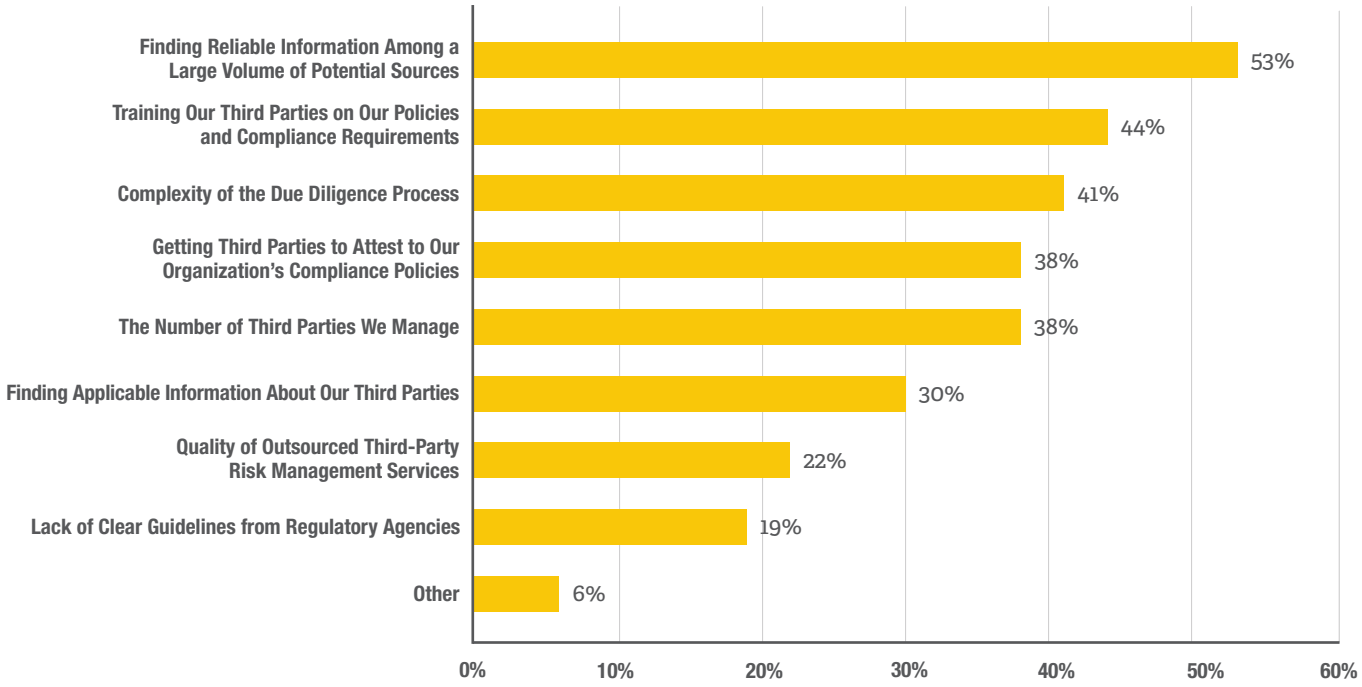
Findings: Top external resource challenges for third-party risk management programs are myriad, with a broad range of top concerns. Finding reliable information among a large volume of potential sources (53%) is core to the success of a third-party risk management program. Finding the proverbial signal in the noise requires discipline, trusted resources, testing false positives and other reporting to validate accuracy.

- The point at which managing third parties appears to become challenging is when the number of third parties reaches 100 (13% of organizations with fewer than 100 third parties indicate management challenges, whereas 45% of those with between 100 and 999 third parties and 58% of organizations with 1,000 or more third parties report management challenges).
- Among organizations with revenue that is highly depenent on third-party engagements, finding reliable information is a consistent challenge (48% of organizations in which half or more of their revenue is related to or generated by third parties vs. 29% or organizations less dependent on third parties).

Analysis: These results get to the heart of the challenges third-party risk management stakeholders face. They're tasked to conduct meaningful due diligence to clearly identify the risk associated with each third party and to make business-critical decisions based on that information. However, they are often unsure of the information's reliability and trustworthiness. These issues scale with the number and locations of third parties engaged. Even organizations that employ a proportionally increased number of FTEs to manage their larger population of third parties find it difficult to consistently train, align, monitor and manage third parties.

A centralized and automated solution that can deliver a relative scoring model and provide real-time updates is essential when an organization is struggling to evaluate third-party risk across hundreds or thousands of third parties. A centrally accessible solution with consistent policies, processes and recordkeeping can help reduce the seemingly insurmountable challenges indicated below – while helping ensure compliance with regulatory expectations.

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



Note: Multiple choice question, percentages total more than 100%. Respondents select up to 3. n=427

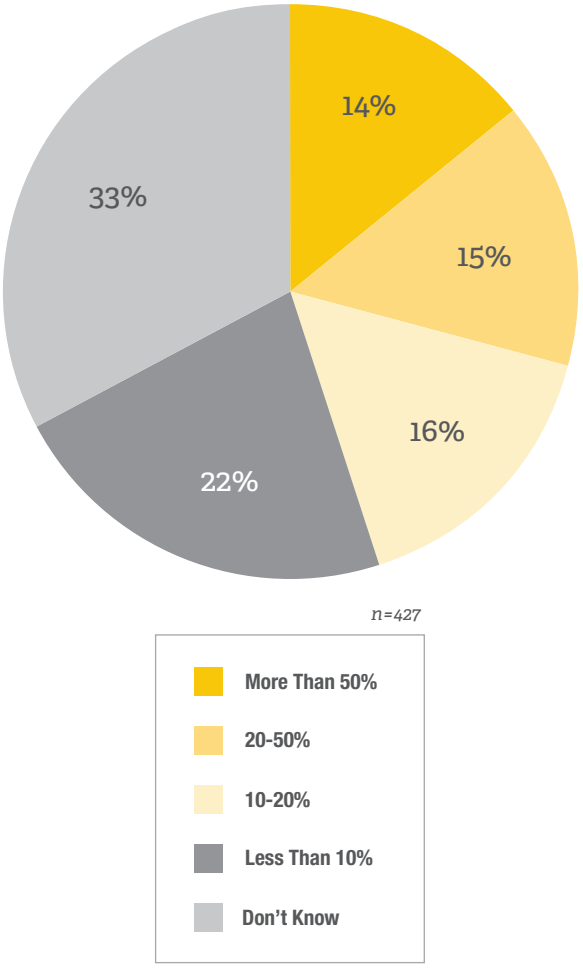
Number of Third Parties Managed & Relative Revenue Generation

Findings: Overall, the number of third-party engagement remains fairly consistent with 2016, with 29 percent of organizations engaging with fewer than 100 third parties, 30 percent engaging with between 100 to 999 third parties, and 27 percent with 1,000 or more.

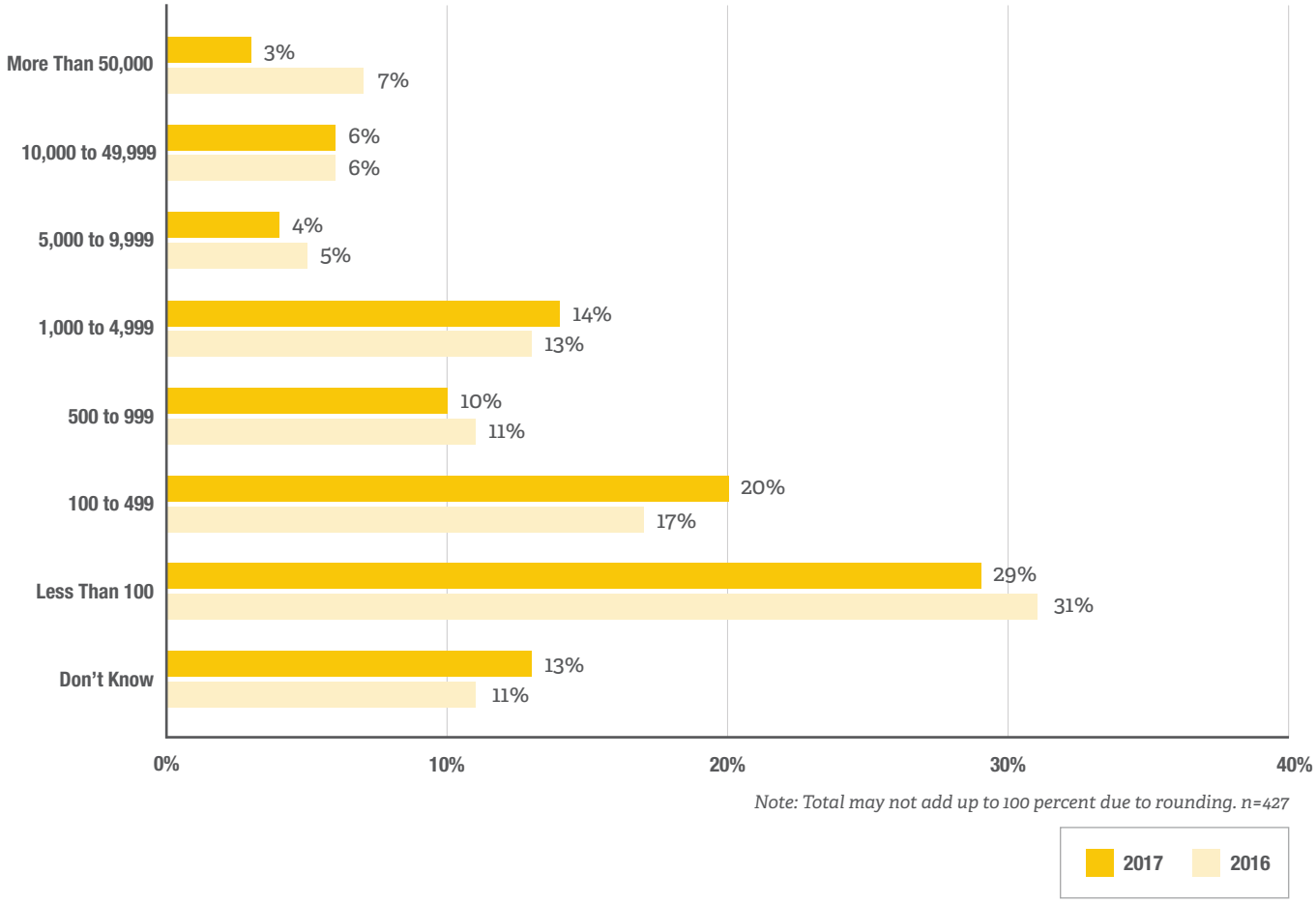
- A sizeable number of organizations that have assigned 10 or more FTEs to manage third parties are managing more than 1,000 third parties (44%), while organizations with 0-3 FTEs assigned are most likely to be managing fewer than 100 third parties (34%).

Analysis: The number of third-party engagements managed is a stronger risk indicator than many other organizational factors. However, the absolute number of third parties is likely less of a factor in causation or risk than the effectiveness of the vetting and management of third parties against risk factors. The fact that organizations with fewer than 100 third parties were more likely to have faced legal action may indicate more *Reactive* or *Basic* programs.

How Much of Your Organization's Revenue is Related to or Generated by Your Third-Party Engagements?



How Many Third Parties Does Your Organization Engage With?



Note: Total may not add up to 100 percent due to rounding. n=427

3: Third-Party Risk Management Practices

Third-Party Due Diligence Policy

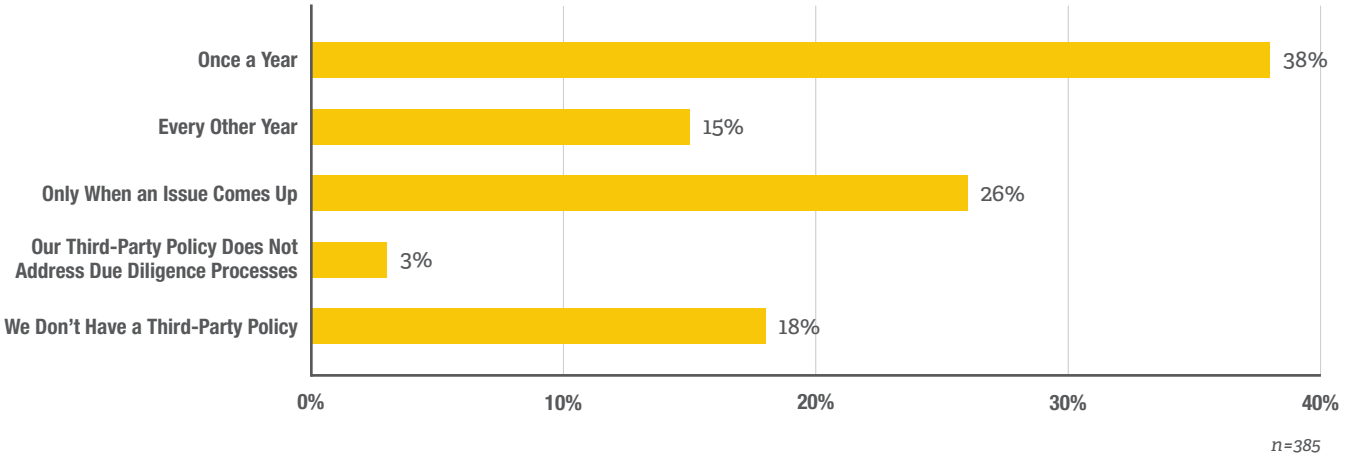
Findings: More than half of organizations assess their third-party due diligence policy every year or every two years.

- Almost half (49%) of organizations with *Maturing/Advanced* programs assess their policy on an annual basis, while a sizable number of *Reactive* and *Basic* programs indicate that they do not have a policy (44% and 28%, respectively). See page 22 for program maturity model.
- Organizations using automated systems are more likely to assess annually (48% vs. 32% of those not using automated systems). Organizations not using automated systems are also more inclined to indicate they do not have a policy (21%).

Analysis: It is critical that your program stakeholders monitor global regulations and market trends and adapt the program universally when needed. A structured and centrally managed program is more likely to weather these inevitable market changes well.

Policy utilization and effectiveness improves when an organization uses automation. The policy becomes the basis for the automation of risk identification, red flag mitigation and consistency of approach. It is important that the policy is regularly reviewed and updated to address the risk tolerance of the organization based on current risk factors and mix of third parties as well as past experience.

When Do You Reassess or Update Your Third-Party Policy, Including Your Third-Party Due Diligence Policy?



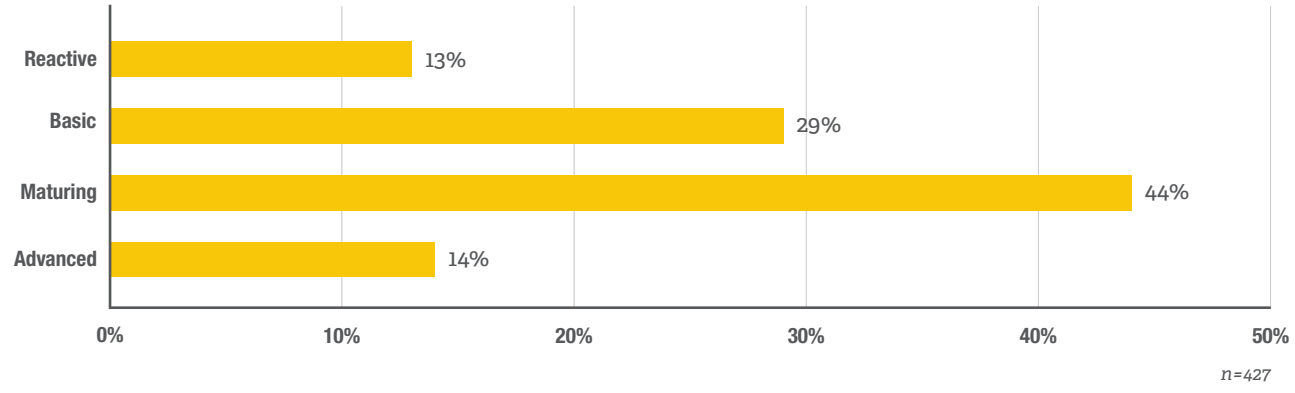
n=385

Program Maturity

Findings: Respondents were asked to categorize the maturity of their third-party risk management program:

- *Reactive* (13%): We address issues as they arise, but do not have a formal program in place.
- *Basic* (29%): We are seeking to develop procedures to manage our third-party engagements, but our due diligence efforts lack consistency and uniformity between business units or geographies. We send questionnaires and screen a limited number of third parties. Management of third-party engagements lacks centralization and we have an incomplete understanding of our organizational exposure to risk associated with third parties.
- *Maturing* (44%): We have an understanding of our organizational exposure to risks associated with our third parties, have some level of uniform policy and are moving toward a centralized third-party risk management system. We are identifying internal stakeholders who will be accountable for defining risk and owning third-party engagements. We perform audits and require training and policy attestation from a limited set of third parties. We have confidence that we're taking a risk-based approach to third-party due diligence but expect we still have gaps to cover.

Please Choose the Option Below That Best Describes Your Current Third-Party Risk Management Program at Your Organization



- *Advanced* (14%): We have consistently identified and stratified potential exposure to risk across the organization and have a clearly defined global policy. We regularly perform audits, train third parties on our policies and gain attestation at clearly defined intervals. Key internal stakeholders are informed and involved in the entire third-party risk management lifecycle. We measure program success and KPIs and adapt our program based upon results. We have confidence that our program is defensible and would withstand enforcement action.

Analysis: Overall, more than half of organizations (58%) self-classify as either *Maturing* (44%) or *Advanced* (14%). More than one quarter would describe their program as *Basic*, while 13 percent would categorize their program as *Reactive*. Not surprisingly, *Reactive* programs are most often found in smaller organizations employing fewer than 500 people and in government / not for profit organizations.

This year, we adjusted the program maturity definitions to include tighter alignment to the FCPA Guide and market best practices, including performing audits, requiring training and centralizing risk management operations. Yet, even with these additional details, the distribution is similar to what we saw in 2016.

This maturity scale is used throughout the remainder of this report to identify performance outcomes related to program maturity to help you define missing elements of your program, prioritize changes and benchmark outcomes. Not surprisingly, the more mature a program – as defined by the criteria above – the better the performance in general.

Notably, much of the maturity scale criteria is based on process, structure and alignment, not budget, FTEs and numbers of third parties. While we typically see more budget and FTEs where organizations work with more third parties, maturity and performance can be seen across programs of all sizes and complexity.

Defining Risk

Findings: Almost two-thirds of organizations (62%) are using specific criteria to classify third-party risks as high, medium and low, while 22 percent indicate they do not, and 15 percent of respondents did not know.

Among organizations that classify third parties by risk level, the main criteria are the Type of third party (82%), Amount of the contract (62%), and Geography of the third party (61%). A risk-based approach includes applying different degrees of due diligence based on these classification criteria.

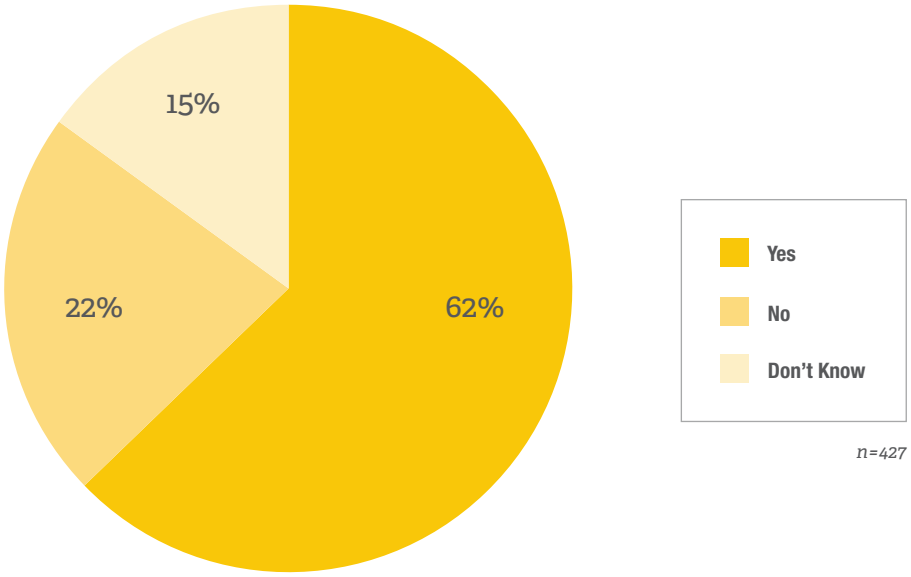
- Organizations managing 1,000 or more third parties are shown to be more inclined to use specific criteria to classify third party risks as high, medium and low (81%).
- Organizations with *Maturing* and *Advanced* programs are more likely to use specific criteria to classify risk (87%) than *Reactive* and *Basic* programs (52%).
- Organizations using automated systems (91%) and third-party due diligence providers (90%) are more inclined to use specific criteria to classify risk than those not using automated systems (66%) or third-party due diligence providers (67%).

Analysis: Overall, most respondents consider 10 percent of their third parties to fall in the high risk category (39%). But thirty-one percent estimate that between 10 and 25 percent of their third parties could be considered high risk, and 11 percent consider *more than* 25 percent of their third parties as potentially high risk. Notably, just 3 percent of organizations feel they engage with no high-risk third parties – a significant shift from 25 percent in 2016. We believe this is due to a reassessment of potential risk factors rather than a shift to lower risk third parties. This is a critical step in third-party program management and efficient use of resources. Remember that FCPA Guide and most third-party anti-bribery and corruption guidance make it clear that due diligence can be risk based and does not need to be one size fits all. Don't waste resources conducting the same level of due diligence on low-risk third parties. Save and redirect those resources to the higher risk candidates.

It is not surprising to see organizations with higher numbers of third-party engagements adopting consistent, highly-specific vetting procedures. Similarly, we see those with more complex engagements gravitating toward automated and third-party provided risk management solutions. Given the program management expectations outlined in the FCPA Guide, it makes sense to centralize, consistently evaluate risks, and manage the hundreds or thousands of individual third-party engagements through an automated and purpose-built software solution. At this level, an ad hoc approach to reviewing and dealing with third parties could dramatically increase the risk of engaging third parties with higher risk of misconduct.

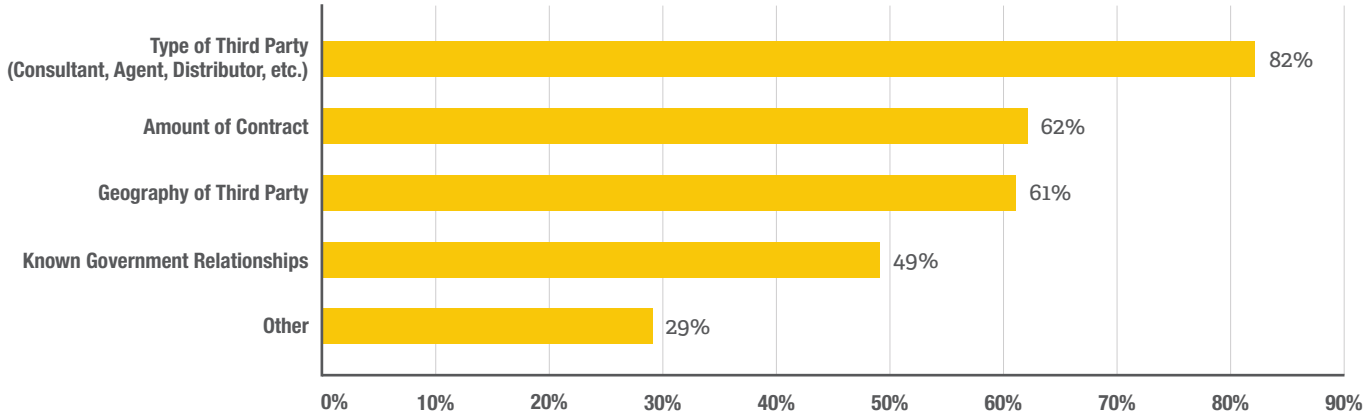
Accordingly, organizations that use third-party risk management systems are more confident that they are adequately limiting their risk, with almost half (at 48%) indicating they feel they have their bases covered, compared to 35 percent that do not use similar systems. Those not using third-party risk management systems on the other hand, indicate they do not feel their bases are adequately covered (33% vs. 23% of organizations using automated risk management systems).

Do You Use Specific Criteria to Classify Third-Party Risks as High, Medium & Low?



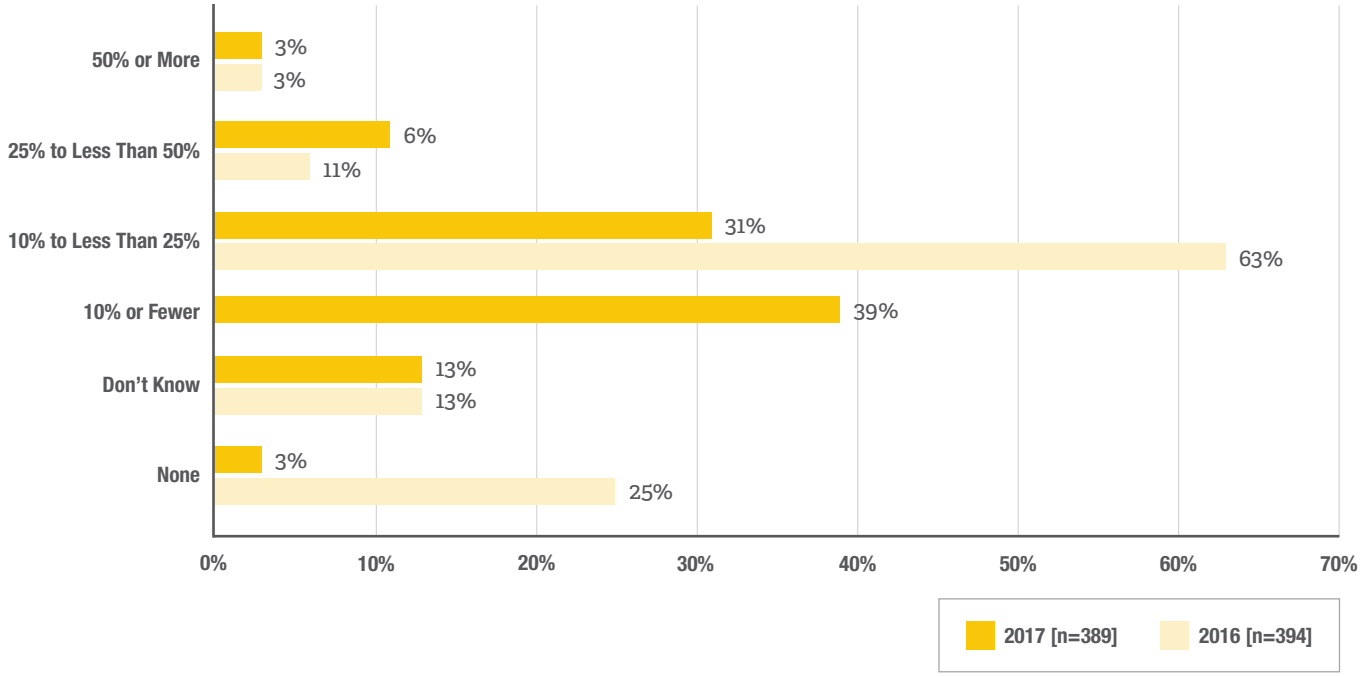
n=427

What Criteria Does Your Organization Use To Classify Third Parties as High, Medium & Low Risk?

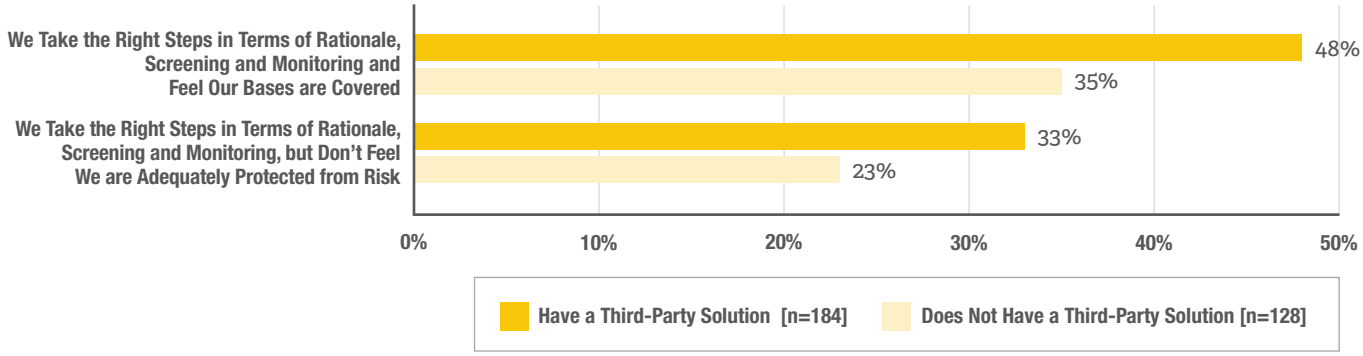


n=266

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



How Much Confidence Do You Have That You're Adequately Limiting Your Organizational Third-Party Risk with Your Existing Program?



Approach to Conducting Third-Party Due Diligence

Findings: Our data shows that most organizations conduct third-party due diligence by pursuing a risk management program that corresponds to the nature and level of risk their third parties represent (57%). We also see most organizations using formal processes, like capturing business rationale and conducting screening to vet third parties and filter-out high risk engagements (55%). Only about 1 in 20 organizations indicate they rarely or never conduct due diligence.

- Organizations with annual revenues in excess of $1 billion are most inclined to pursue a third-party risk management program that "corresponds to the nature and level of risk our third parties represent" (66%)," use business rationale and screening activities to vet third parties and filter-out high risk engagements" (61%), and "train and require attestation of all of third parties on the code of conduct" (32%).

Less than a third (30%) of all respondent organizations are using automated systems to manage their third-party risk management program, but that number increases to 43% for *Mature/Advanced* organizations.

- Likelihood of using an automated system increases in step with a higher number of managed third parties, with 23 percent of organizations managing fewer than 1,000 third parties using automated systems compared to 40 percent of those managing more.
- As programs mature they are more likely to be using automated systems (*Reactive* 10%, *Basic* 15%, *Maturing* 37%, *Advanced* 62%).
- Likelihood of using an automated system increases based on organization size (at only 20% of organizations with fewer than 500 employees, 28% of organizations with 500-5,000 employees, and 36% of organizations with more than 5,000 employees).
- Organizations assigning more FTEs to manage third parties are more inclined to use automated systems (0-3 FTEs 25%, 4-10 FTEs 32%, 10 or more FTEs 42%).
- Organizations with a dedicated budget are more likely to use automated systems than organizations without (32% vs. 13%).

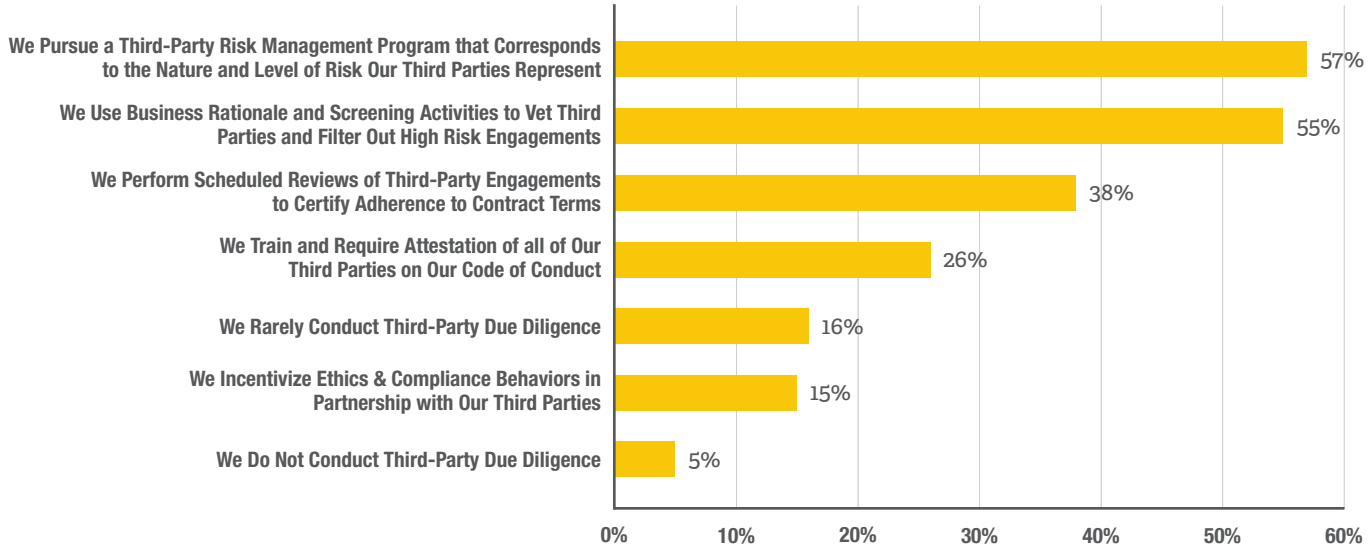
The majority of organizations that use an automated due diligence provider to help identify and manage their third-party risk use them for screening third parties (72%) and to conduct enhanced due diligence on third parties (60%).

- Most large organizations use third-party providers to perform enhanced due diligence on third parties (72%) compared to less than half or organizations with fewer than 5,000 employees (47%).

Analysis: Given that 58 percent of respondents indicate that their programs are either *Maturing* or *Advanced* and 57 percent of respondents report pursuing a third-party risk management program that corresponds to the nature and level of risk in their third parties, risk-based approaches are likely correlated to program maturity.

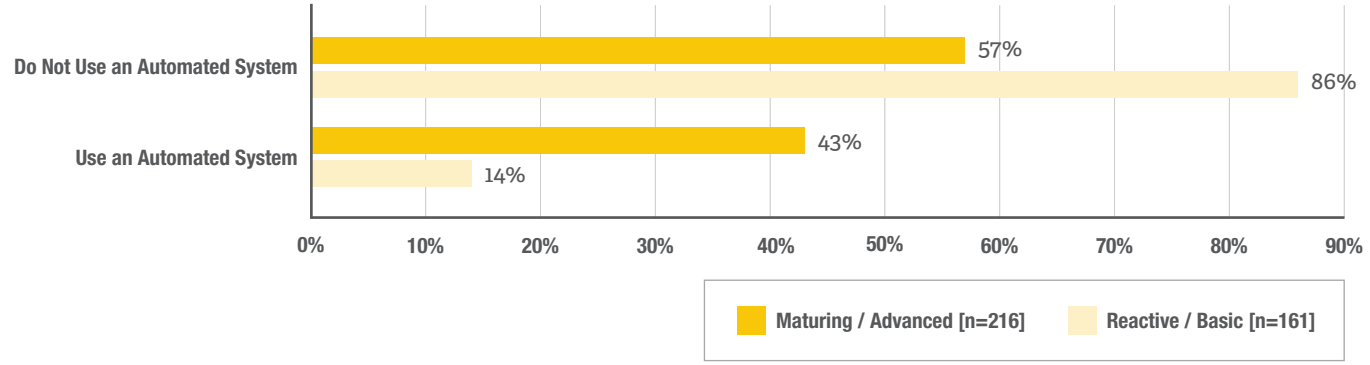
The critical risk-reduction element is conducting some form of risk-based due diligence. "The due diligence procedures implemented by the organization on its [third parties] should be consistent across similar bribery risk levels." ISO 37001, Section A103(d). In case of misconduct, it is indefensible not to have conducted some level of due diligence for even the lowest risk parties. Knowledge is critical. Luck is not a strategy. It is impossible to divine which parties will engage in misconduct. You can only make reasonable calculations based on risk factors. This is another reason that a well-thought-out policy should be the basis of the any third-party risk management program.

How Do You Conduct Third-Party Due Diligence Today?



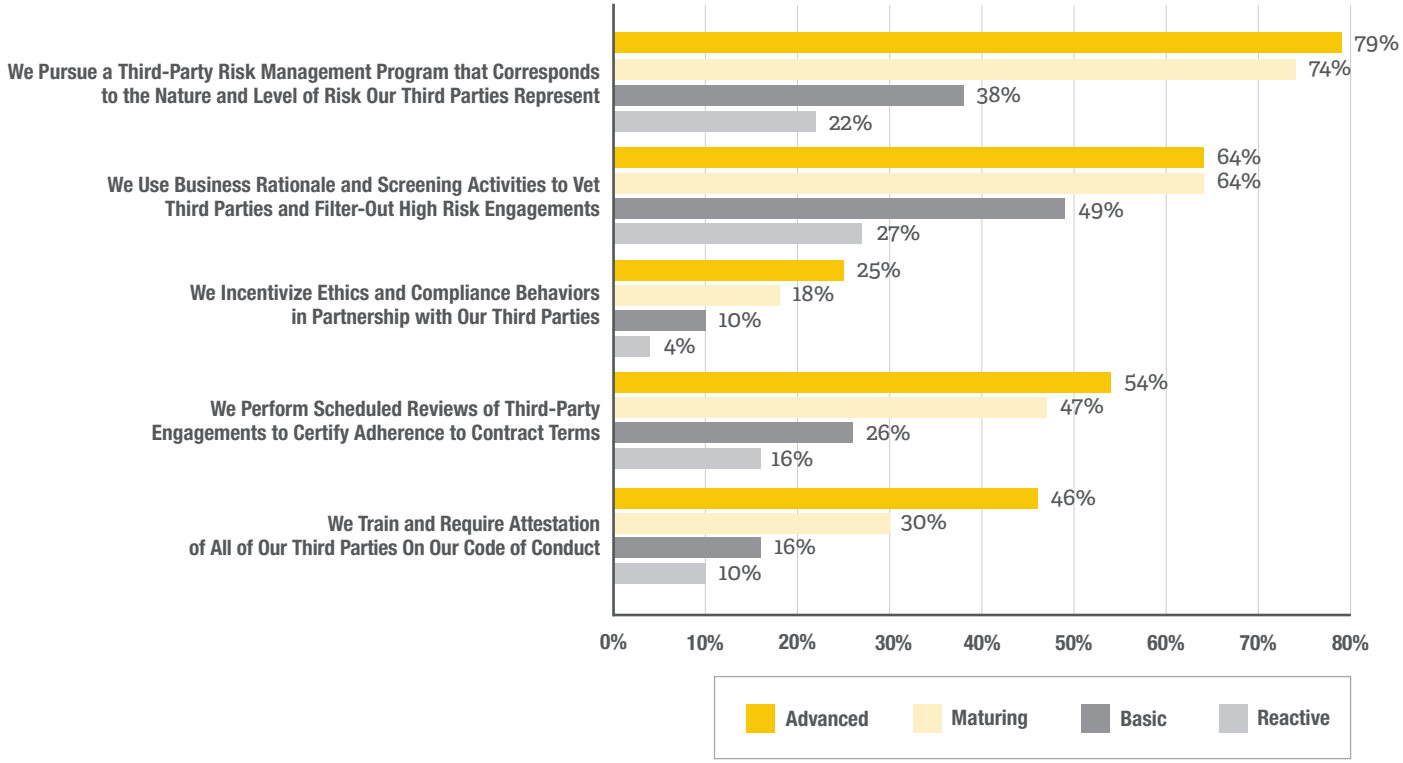
Note: Multiple response question, percentages total more than 100%. n=377

Use of Automated Technology Solutions by Maturity Level

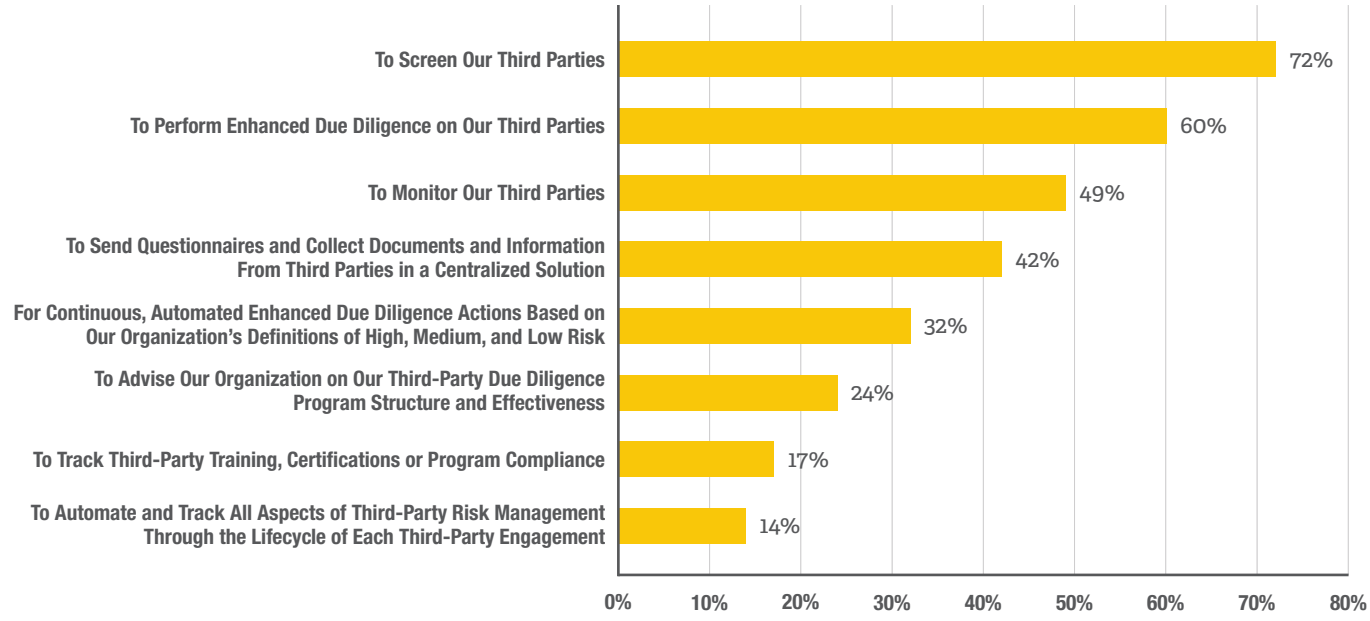


How Do You Conduct Third-Party Due Diligence Today?

(By Program Maturity)



If You Use a Third-Party Due Diligence Solution, How Do You Do So?



(Respondents Who Use a Third-Party Diligence Provider)
Note: Because respondents could choose more than one option, percentages total more than 100%. n=130

Screening Third Parties

Findings: Almost half of organizations define business rationale for the engagement, with only 12 percent indicating they never do this. When it comes to completion of an initial onboarding questionnaire and applying risk-based logic to define depth of scrutiny, just over a third (36%) of organizations conduct these activities with all third parties, while about one in five never do. And while about a quarter of organizations train all third parties on their code of conduct and require attestation, about a third never do.

Consistent with 2016 findings, 47 percent of organizations screen all third parties. Slightly fewer are only screening third parties crucial to their business, or those in high-risk industries or geographical locations. *Maturing/Advanced* programs tend to screen all their third parties, while *Reactive/Basic* programs screen only select third parties.

Analysis: The following charts address best practice vetting and onboarding processes, including defining a business justification for the engagement prior to onboarding the third party, applying risk-based logic to define required third-party scrutiny, processing a questionnaire and reputational screening of third parties prior to engagement.

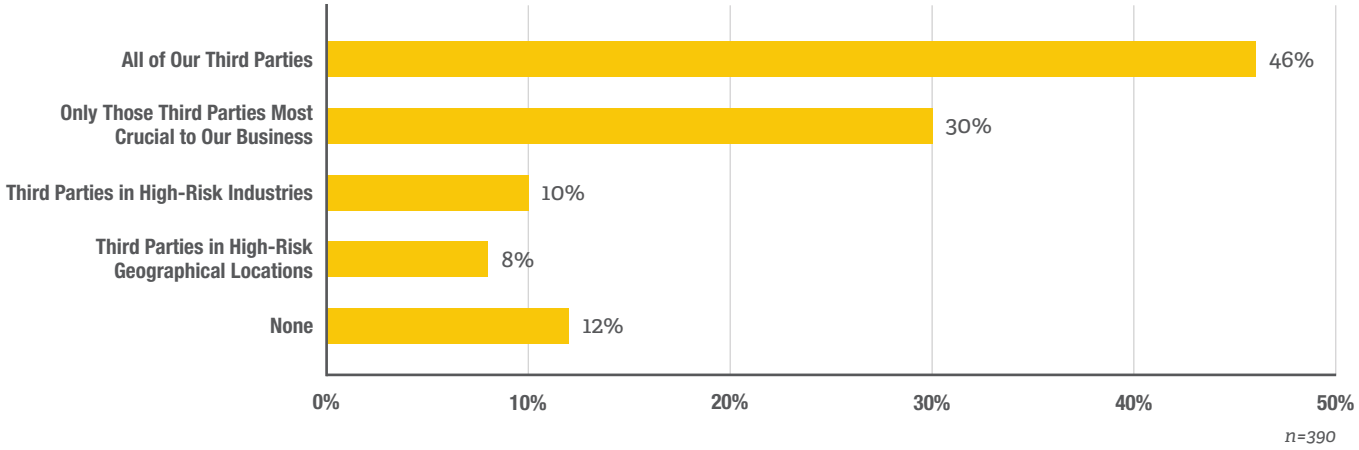
The FCPA Guide states that, "[C]ompanies should have an understanding of the business rationale for including the third party in the transaction. Among other things, the company should understand the role of and need for the third party and ensure that contract terms specifically describe the serviced to be performed." (FCPA Guide, page 60)

Organizations that do not require clearly defined business rationale prior to engagements are at greater risk of using third parties more likely to engage in misconduct or bribery. Engaging third parties without reasonable business justification who violate the law or the organization's policy is hard to defend.

Additionally, the FCPA Guide also reminds organizations that the U.S. Department of Justice and the SEC expect that "…the [engaging] company has informed third parties of the company's compliance program and commitment to ethical and lawful business practices… and has sought assurances from third parties, through certification and otherwise, of reciprocal commitments. These can be meaningful ways to mitigate third-party risk." (FCPA Guide, page 60)

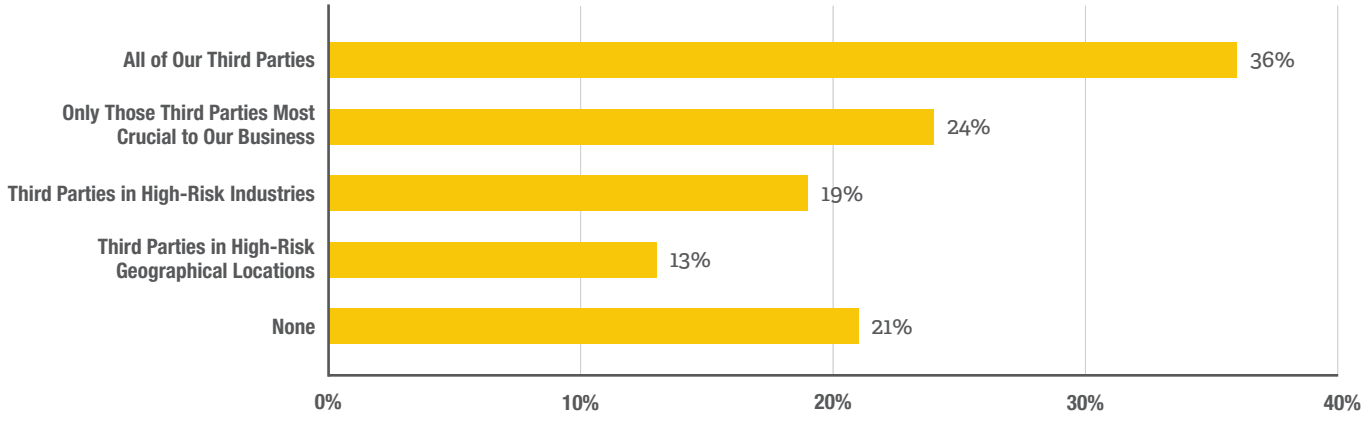
Certifications and training on the organization's code of conduct helps ensure that the third party is aligned with the organization's position and expectations when it comes to complying with the law and particularly the organization's policy on bribery and corruption prevention.

On Which Third Parties Does Your Organization Define Business Rationale for the Engagement?



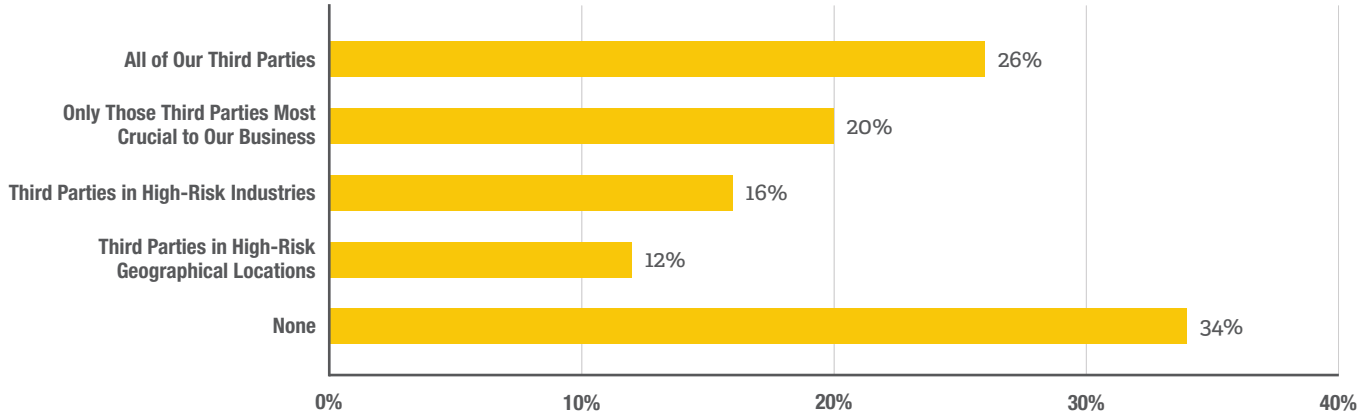
n=390

On Which Third Parties Does Your Organization Require Completion of a Questionnaire for Initial Onboarding?



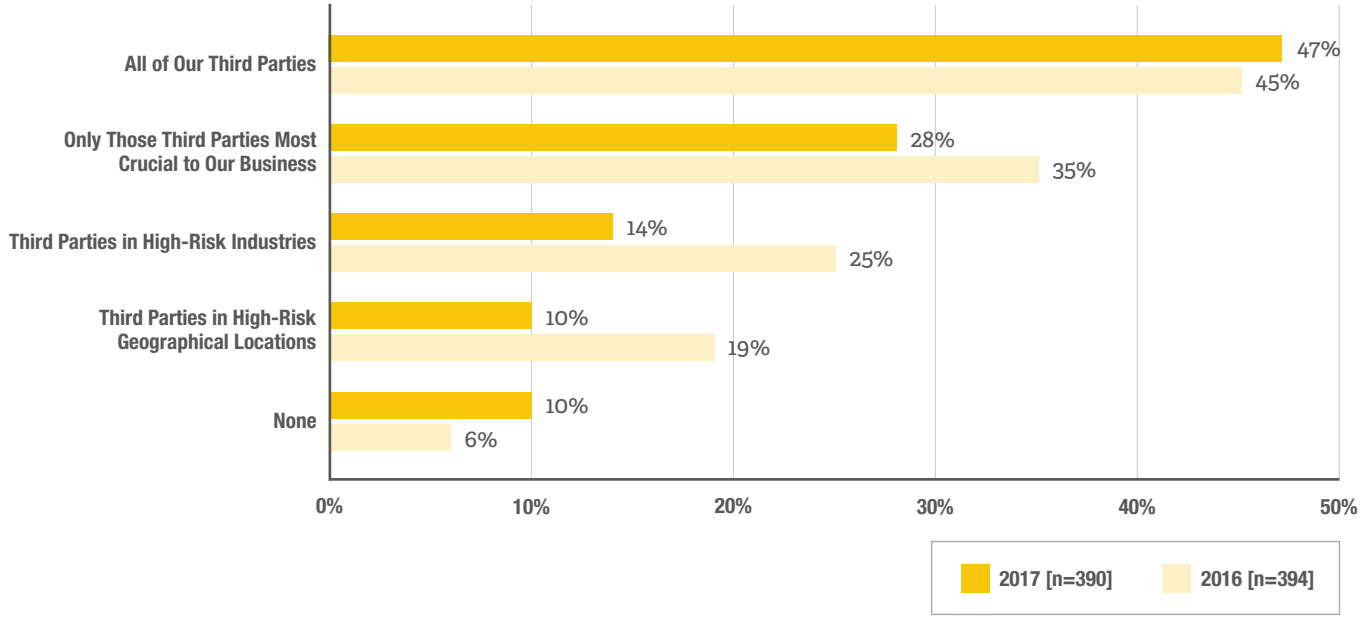
n=390

On Which Third Parties Does Your Organization Train on Your Code Of Conduct & Require Attestation?

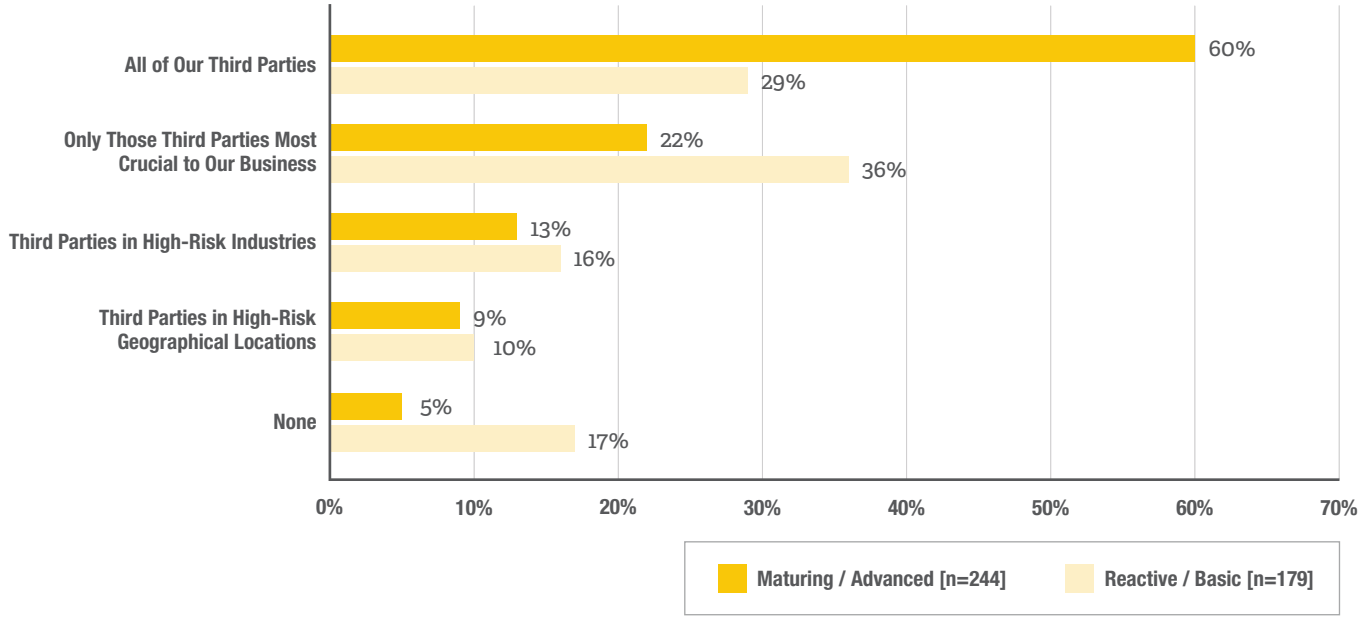


n=390

On Which Third Parties Does Your Organization Screen Prior to Engagement?



On Which Third Parties Does Your Organization Screen Prior to Engagement?



Monitoring Third Parties

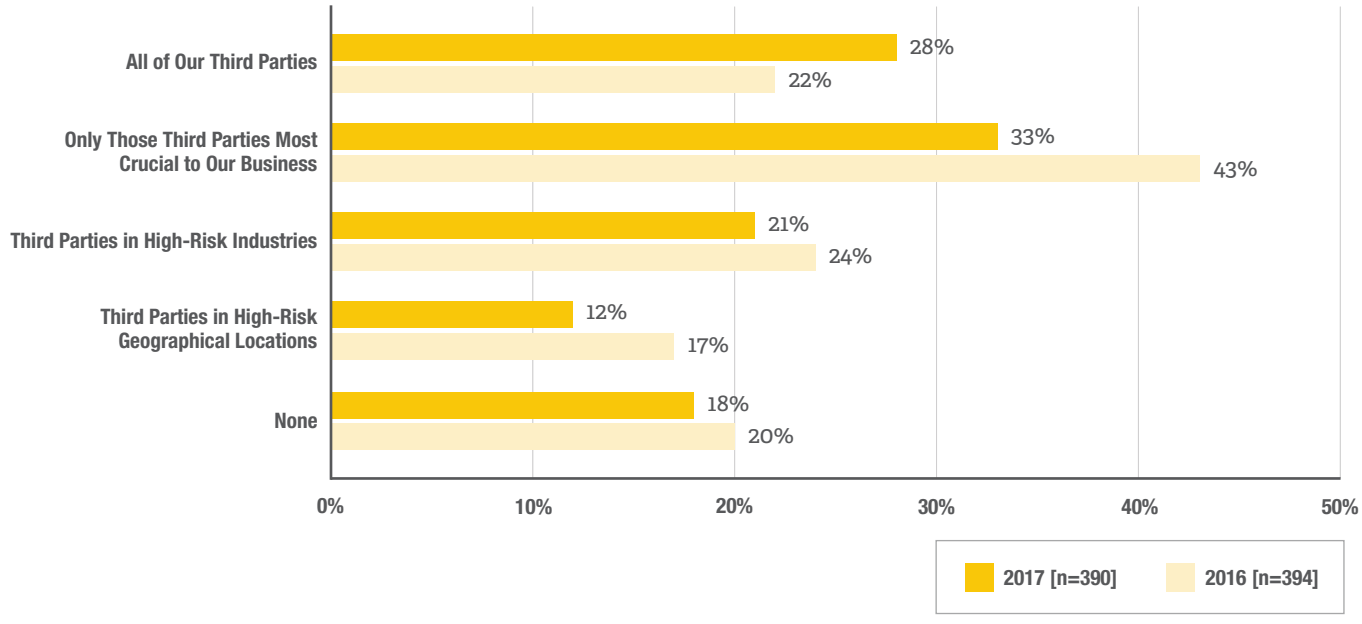
Findings: Consistent with 2016 findings, most organizations (66%) only monitor select third parties continuously throughout the lifecycle of the engagement.

- While a third of organizations with *Reactive/Basic* programs monitor those most crucial to their business, almost a third do not continuously monitor third parties. Among *Maturing/Advanced* programs, the vast majority (92%) continuously monitor third parties, including more than a third (37%) that monitor all third parties.
- Organizations that use automated systems are more likely to continuously monitor all third parties than those not using automated systems (41% vs. 23%).

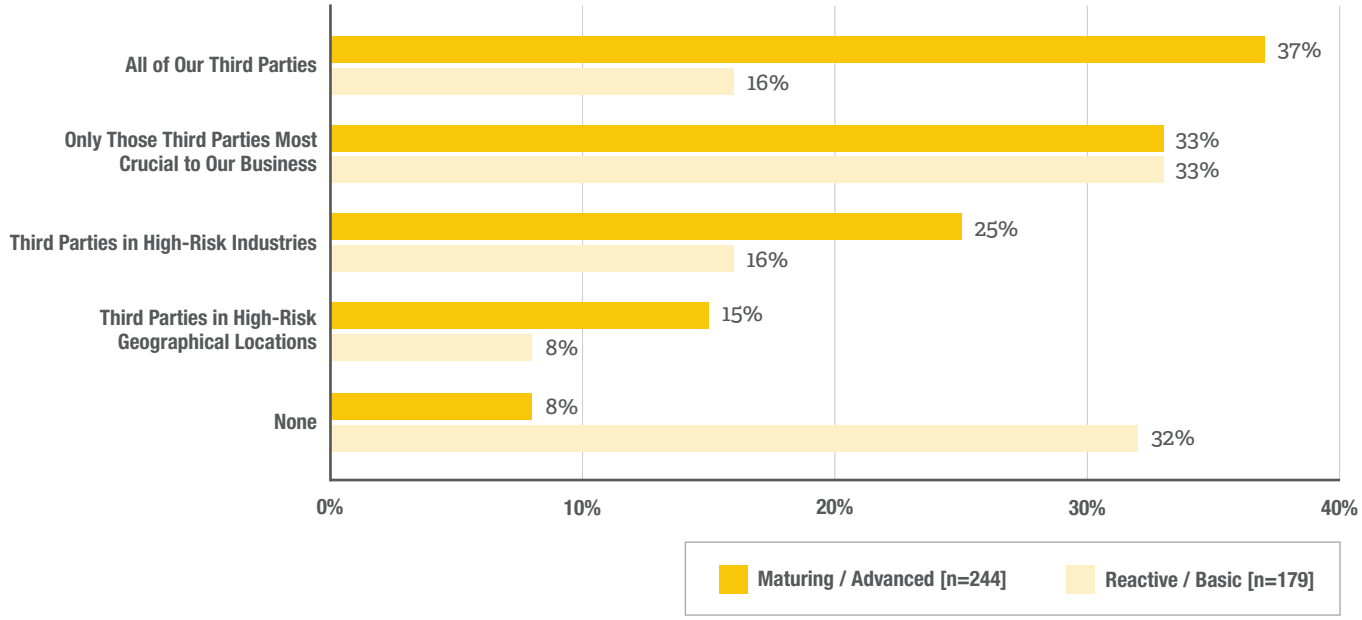
Analysis: The FCPA Guide and recent *Evaluation of Corporate Compliance Programs* criteria includes "ongoing monitoring and auditing" of the efficacy of their third-party risk management program. This includes conducting periodic reassessment of the status and risks each third party represents and adjusting the risk factors and third-party engagement where changes in status warrant it. Without ongoing monitoring, misconduct which occurs after the initial due diligence and engagement may go unnoticed or not be addressed until the organization hears from a regulator.

Best practices indicate an inclusive and consistent program through which all third parties are continuously monitored for risk on a daily basis. This allows organizations to quickly respond to changes in status and reevaluate engagements when necessary.

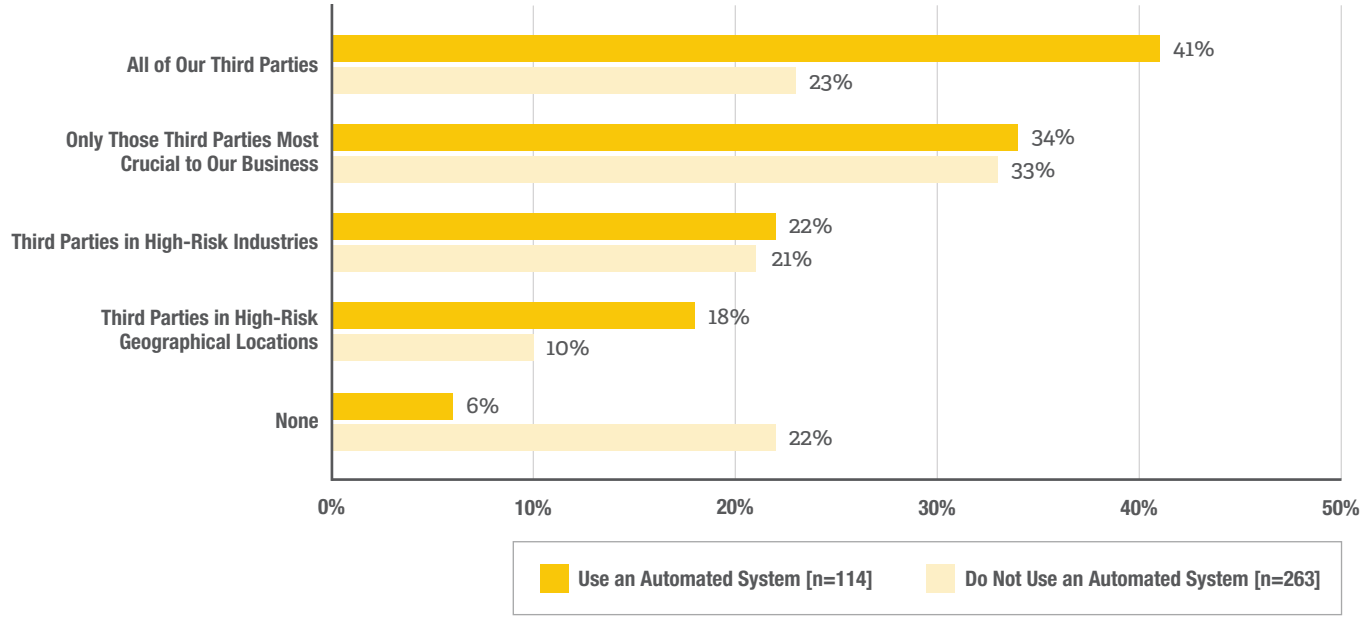
On Which Third Parties Does Your Organization Continuously Monitor Throughout the Engagement Lifecycle?



On Which Third Parties Does Your Organization Continuously Monitor Throughout the Engagement Lifecycle?



On Which Third Parties Does Your Organization Continuously Monitor Throughout the Engagement Lifecycle?



Approach to Discovering "Red Flags"

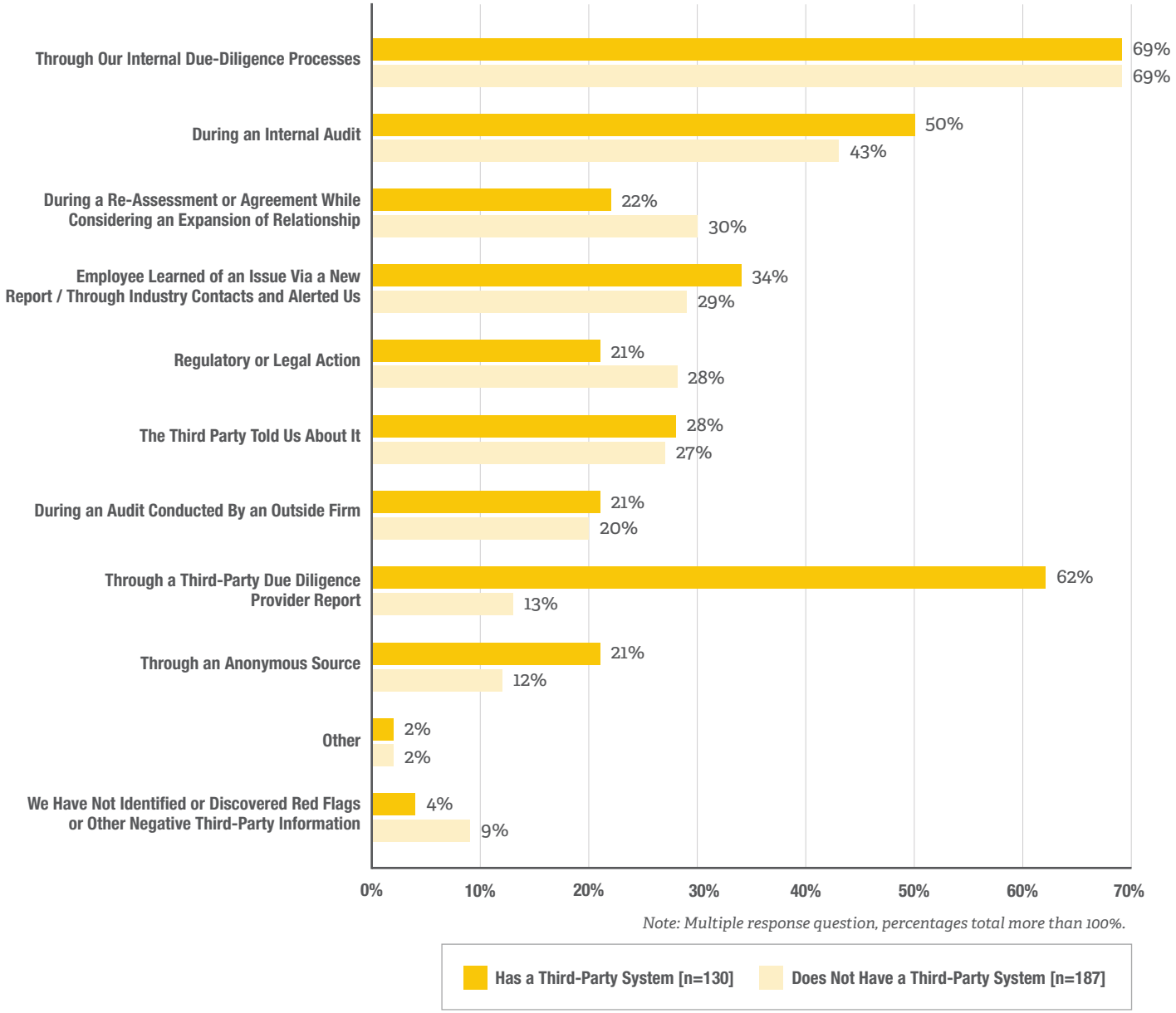
Findings: Most organizations have uncovered third party "red flags." While they are often discovered through multiple channels, most organizations identified them through their internal due diligence processes (65%).

Analysis: The number of respondents identifying red flags through internal due diligence processes may indicate a general maturity trend in internal audits and processes. It is less important how the red flag is discovered than how it is resolved. The Evaluation of Corporate Compliance Programs specifically addresses whether red flags were "identified from the due diligence of the third parties involved in the misconduct and how were they resolved?"

Accordingly, once red flags have been identified, a reasoned, risk-based and documented response needs to happen. The presence of a red flag does not mean that a third party must be rejected any more than the absence of red flags or negative information means a third party will not engage in misconduct. However, once a red flag is identified, prompt action should be taken to understand the nature of the risk and whether or not it can be satisfactorily mitigated.

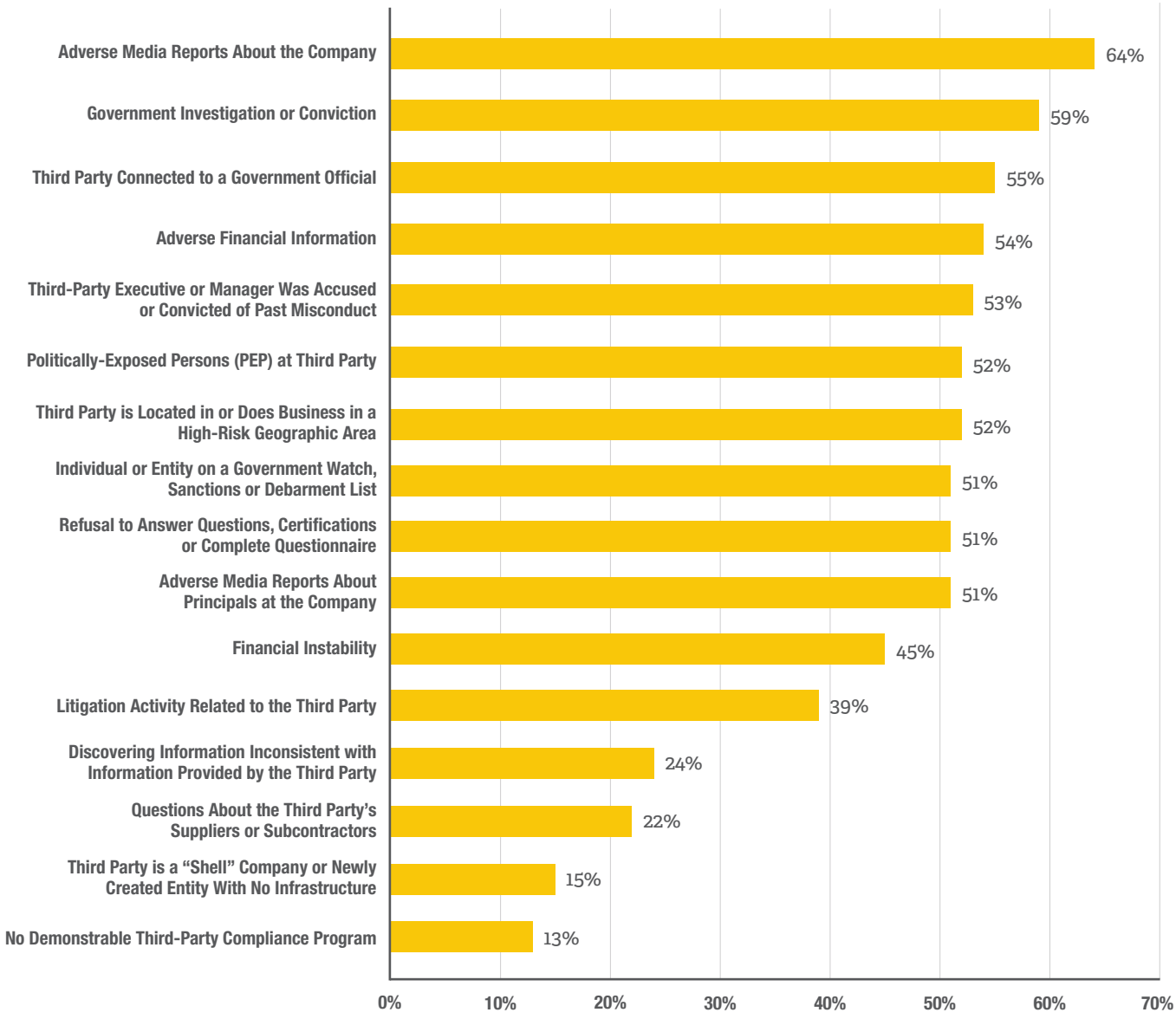
Automated or third-party risk management systems may be more successful at identifying red flags through the use of sophisticated algorithms which search thousands of databases to provide information and source documents.

How, If at All, Have You Identified or Discovered Red Flags or Other Negative Third-Party Information?



Note: Multiple response question, percentages total more than 100%.

What Types of "Red Flags" Would Your Third-Party Due Diligence System Typically Return?



Note: Multiple response question, percentages total more than 100%. n=125

Legal & Regulatory Issues

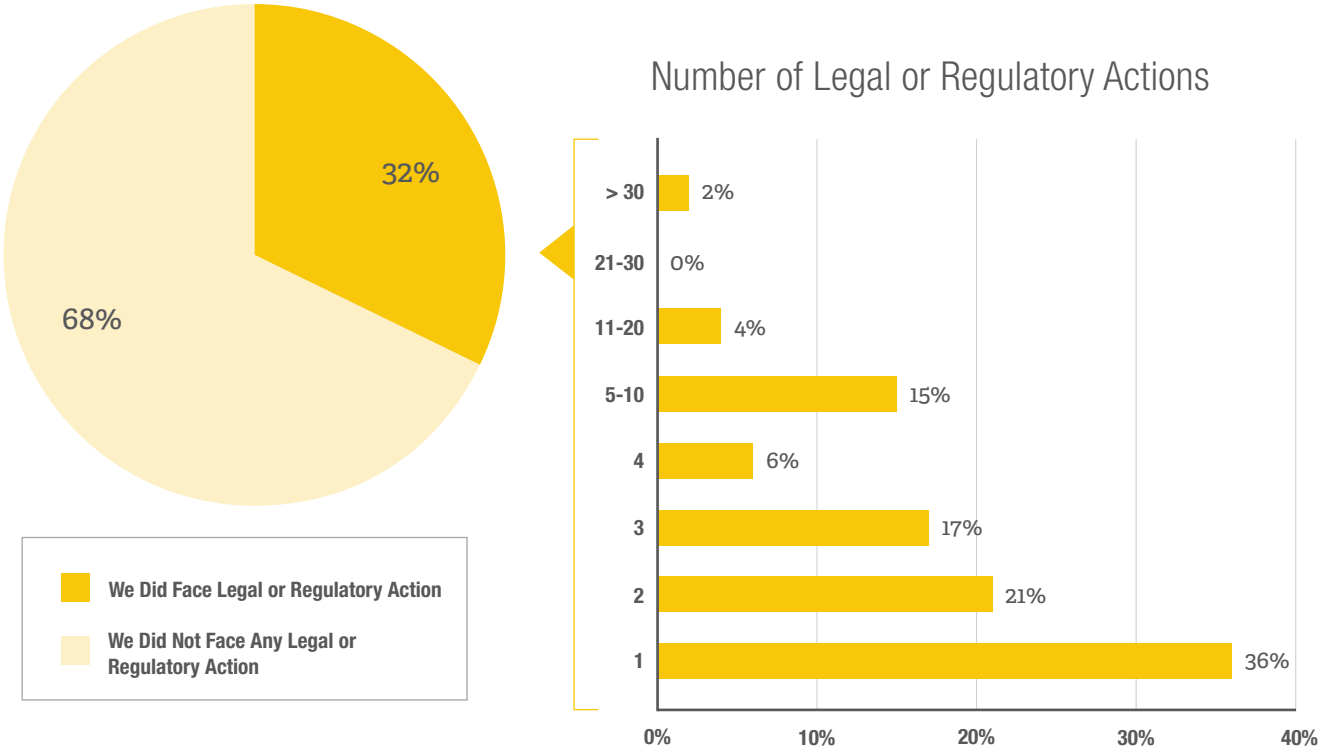
Findings: More than two thirds of organizations have not faced legal or regulatory action in the past 3 years. Among those who did, more than half (57%) faced one or two actions. The proportion of organizations reporting five or more legal actions declined (21% in 2017 from 31% in 2016).

Organizations that continuously monitor all third parties fared better than those that do not (24% faced regulatory or legal action compared to 35% of organizations that do not continuously monitor all third parties).

- Organizations that have not faced legal action in the past 3 years are more likely to indicate that they continuously monitor all of their third parties throughout the engagement lifecycle (32% vs. 21% of organizations that have faced legal action).
- Organizations that have faced legal action tend to:
  - Be larger (41% of organizations employing more than 5,000 people vs. 26% of those employing fewer)
  - Engage with more third parties (36% of those engaging 100 or more vs. 21% engaging fewer)
  - Have *Reactive* programs (46% faced legal action, vs. 29% of *Basic* and *Mature* programs and 30% of *Advanced* programs)

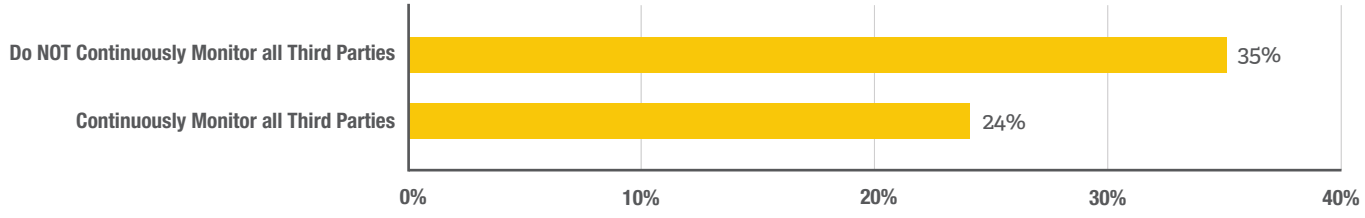
Analysis: Continuous monitoring seems to be a relevant factor in lowering legal and regulatory actions. This makes sense as organizations that continuously monitor third parties have a higher likelihood of identifying potential red flags or issues early and either addressing the issue through an investigation, mitigation or termination of the third party. This early response will lessen the chance that a misstep grows into misconduct and a resulting lawsuit or a regulatory action.

How Many Times in the Past Three (3) Years Did Your Organization Face Legal or External Regulatory Action Where a Third Party Came Under Review as Part of the Action or Defense?



Pie chart [n=320]. Bar graph [n=117]. Note: Totals may not add up to 100 percent due to rounding.

Faced Legal Action by Third-Party Monitoring Activities



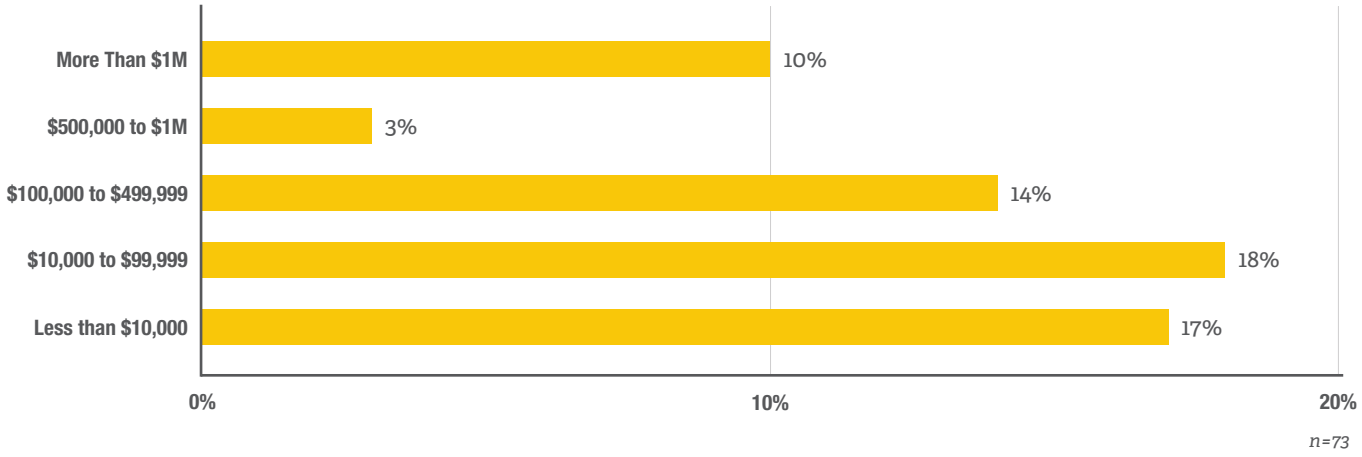
Do NOT Continuously Monitor all Third Parties, n=265. Continuously Monitor all Third Parties, n=105.

Cost of Legal & Regulatory Incidents

Findings: Organizations using third-party systems are more inclined to agree that their third-party due diligence program significantly reduced their legal, financial and reputational risk, compared to those who do not (73% vs. 53%). In terms of average cost per incident, while more than a third of respondents don't know, 27 percent indicate average costs per legal or regulatory incident to be in excess of $100,000.

Analysis: With many organizations reporting cost per incident at more than $100,000, legal and regulatory fees alone can often justify the use of an automated system to reduce legal, financial and reputational risk.

Average Cost per Incident



4: Best Practices in Third-Party Risk Management Program Performance

How do you assess program effectiveness?

Findings: The top approaches used to assess effectiveness of third-party due diligence programs are periodic risk assessments (47%) and audits (46%). Just over 20 percent of organizations indicate they do not assess program effectiveness.

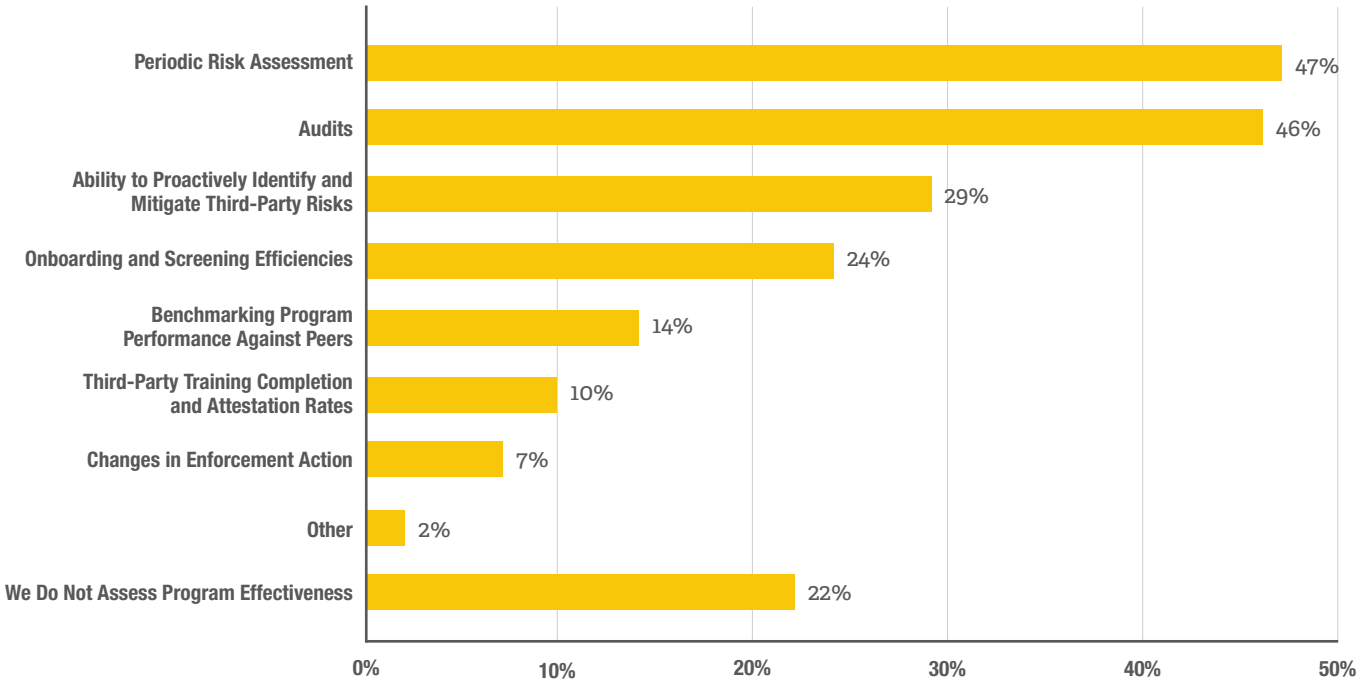
- Organizations with *Maturing/Advanced* programs are more likely to assess the effectiveness of their program using the following approaches:
  - Periodic risk assessments (56% vs. 36% of *Reactive/Basic* programs)
  - Onboarding and screening efficiencies (32% vs. 13%)
  - Ability to proactively identify and mitigate third-party risks (36% vs. 19%)
  - Third-party training completion and attestation rates (13% vs 6%)
  - Audits (53% vs. 36%)
  - Benchmarking program performance against peers (20% vs. 6%)
- Almost half of organizations with *Reactive* programs (48%) and more than a third of those with *Basic* programs indicate they do not assess their program's effectiveness (compared to only 11% of *Maturing* and 8% of *Advanced* programs).

Analysis: A high percentage of *Maturing* and *Advanced* programs use periodic risk assessments and audits to assess effectiveness. This best practice ensures the program is working as intended and can also be an early warning sign for gaps or opportunities to improve.

It is surprising that 22 percent of respondents do not measure effectiveness using any means. You can't improve what you can't measure. The strongest compliance programs will be able to rely on data, metrics and outcomes to measure effectiveness and apply resources accordingly.

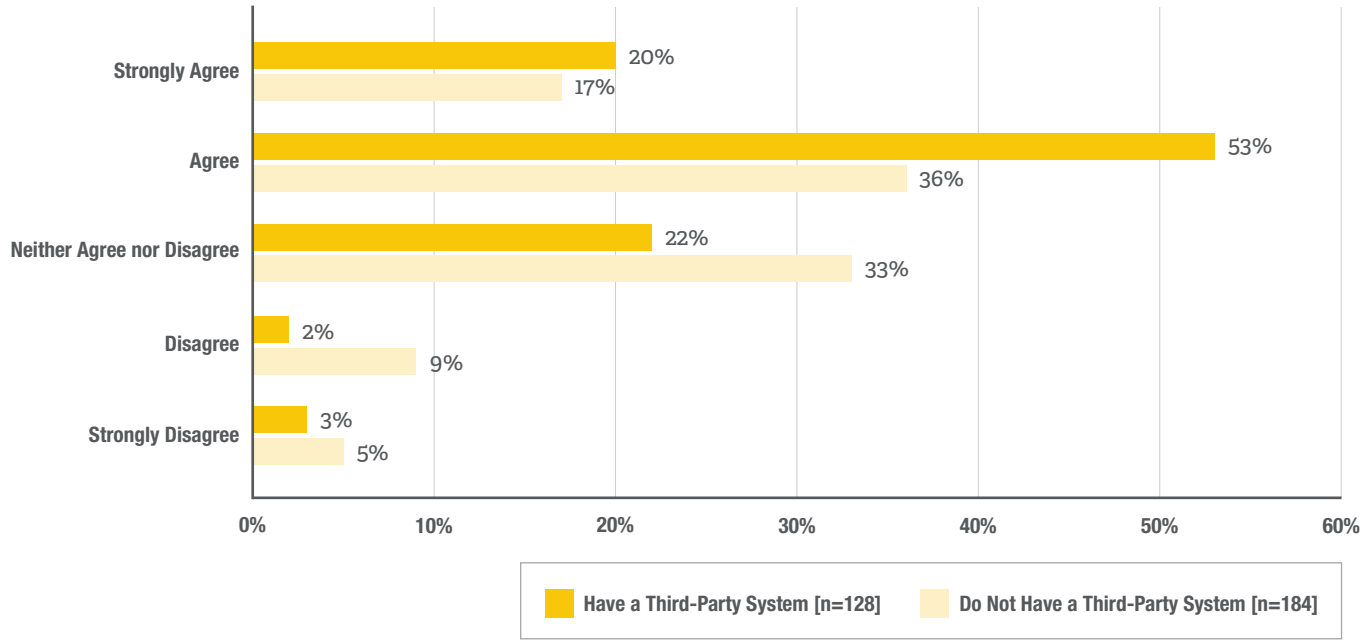
Best Practices in Third-Party Risk Management Program Performance Continued

How Do You Assess the Effectiveness of Your Third-Party Due Diligence Program?

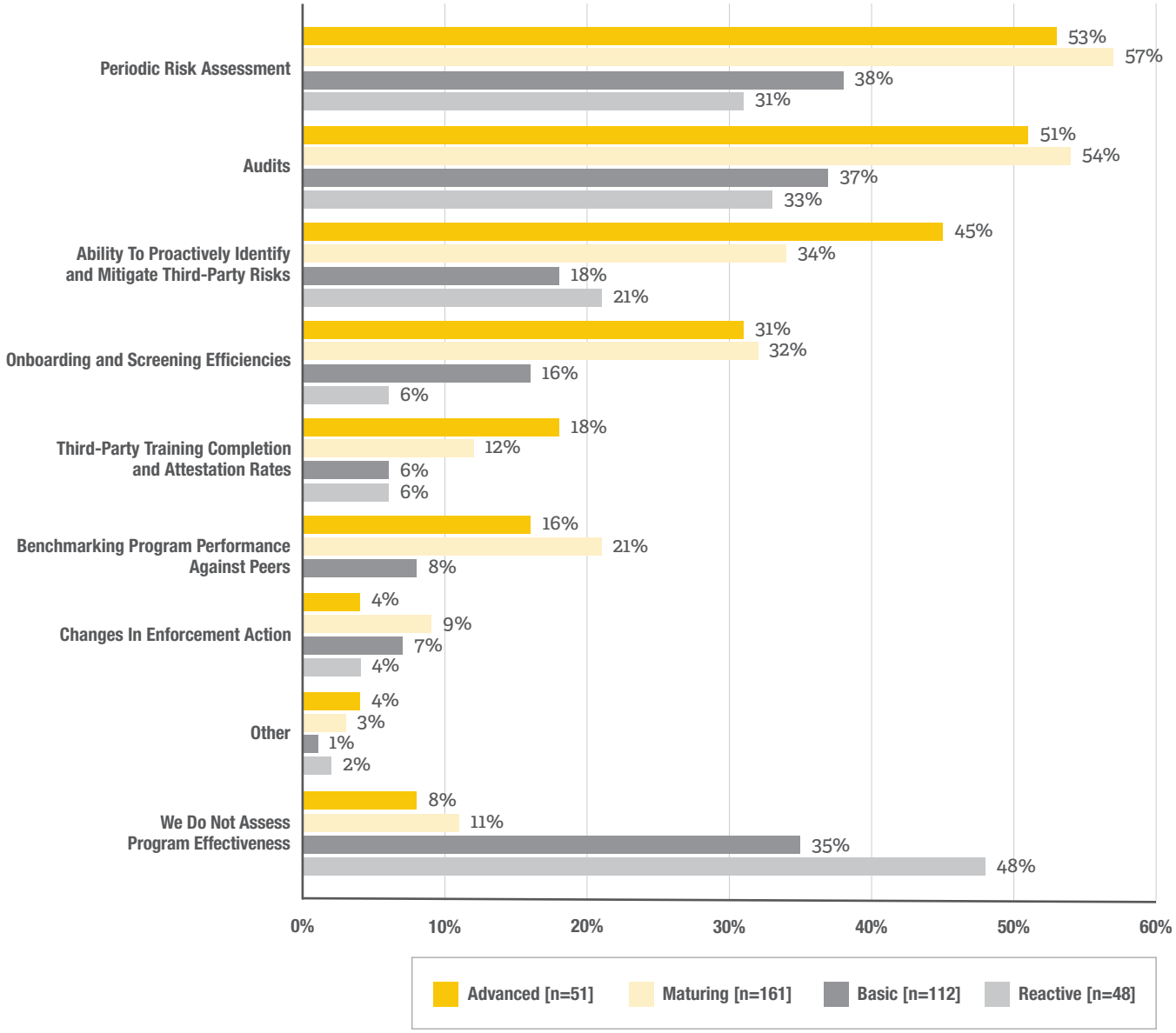


Select Up To 3 Primary Methods. n=371

Level Of Agreement: Our Third-Party Due Diligence Program Significantly Reduces our Legal, Financial and Reputational Risks



Methods of Assessing Third-Party Due Diligence Program by Program Maturity



Program Performance

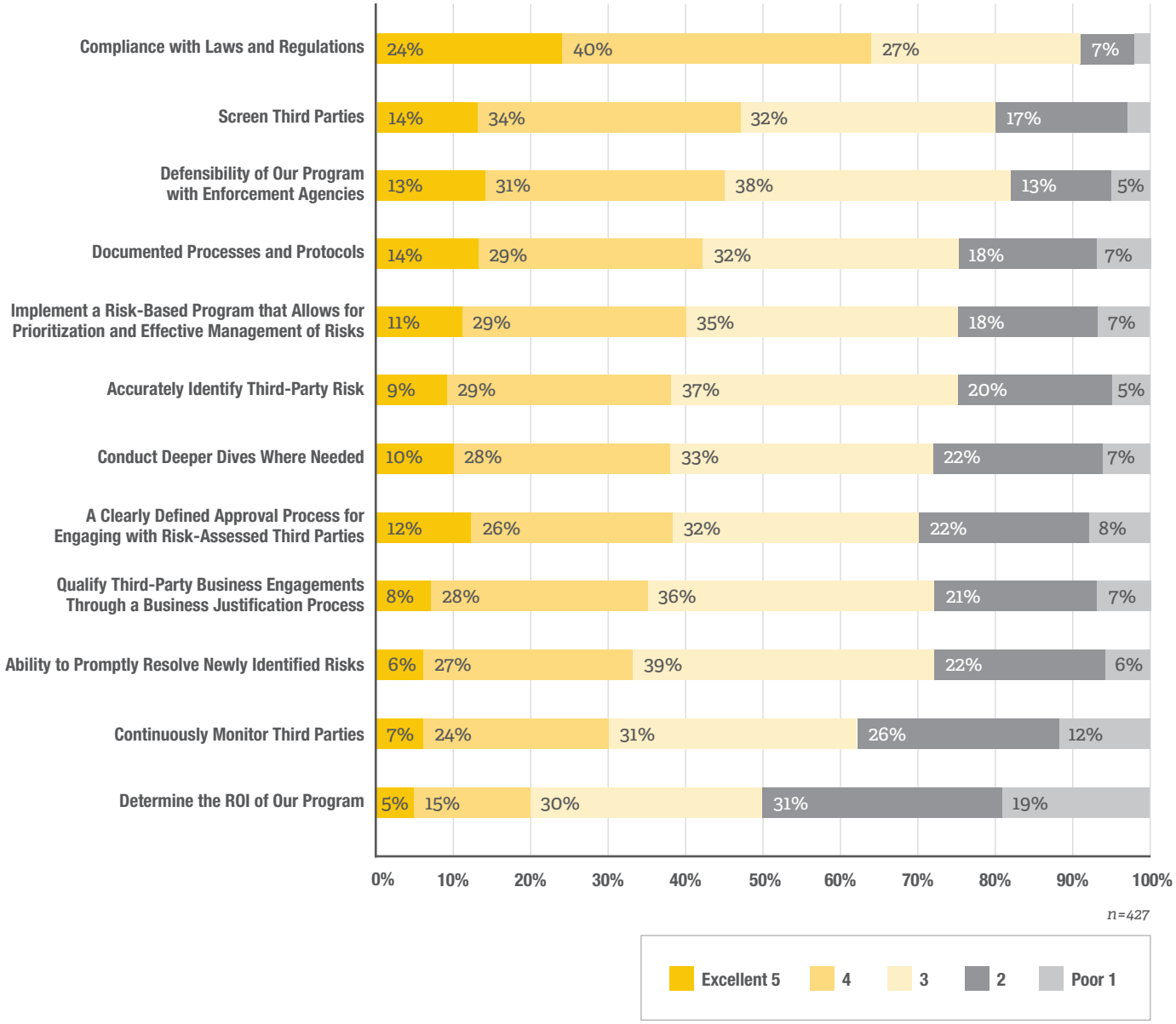
Findings: While most organizations consider themselves to be doing a good job complying with laws and regulations (64% rate themselves a 4 or 5 on a scale of 1 to 5), there is much room to improve other aspects of their third-party risk management programs. Fewer than half of organizations self-rated high performance on other aspects of their program. Determining ROI and conducting continuous monitoring of third parties appears to be particularly challenging. Half of organizations indicate they are poor (1 or 2 on a scale of 1 to 5) when it comes to determining ROI, and 38 percent when it comes to continuous monitoring.

- Across all aspects of program execution, performance significantly improves with maturity. Across all aspects of program execution, organizations that use automated systems perform significantly better, especially when it comes to screening third parties.
- With the exception of determining program ROI, prompt resolution of newly identified risks, and accurately identifying new risks (areas where most organizations are experiencing some challenges), organizations that use a third-party due diligence provider perform significantly better on execution. In particular, they excel at implementing a risk-based program that allows for prioritization and effective management of risks, screening third parties and documenting processes and protocols.
- Overall program ratings correlate with program maturity level, use of third-party due diligence providers and use of automated technology.

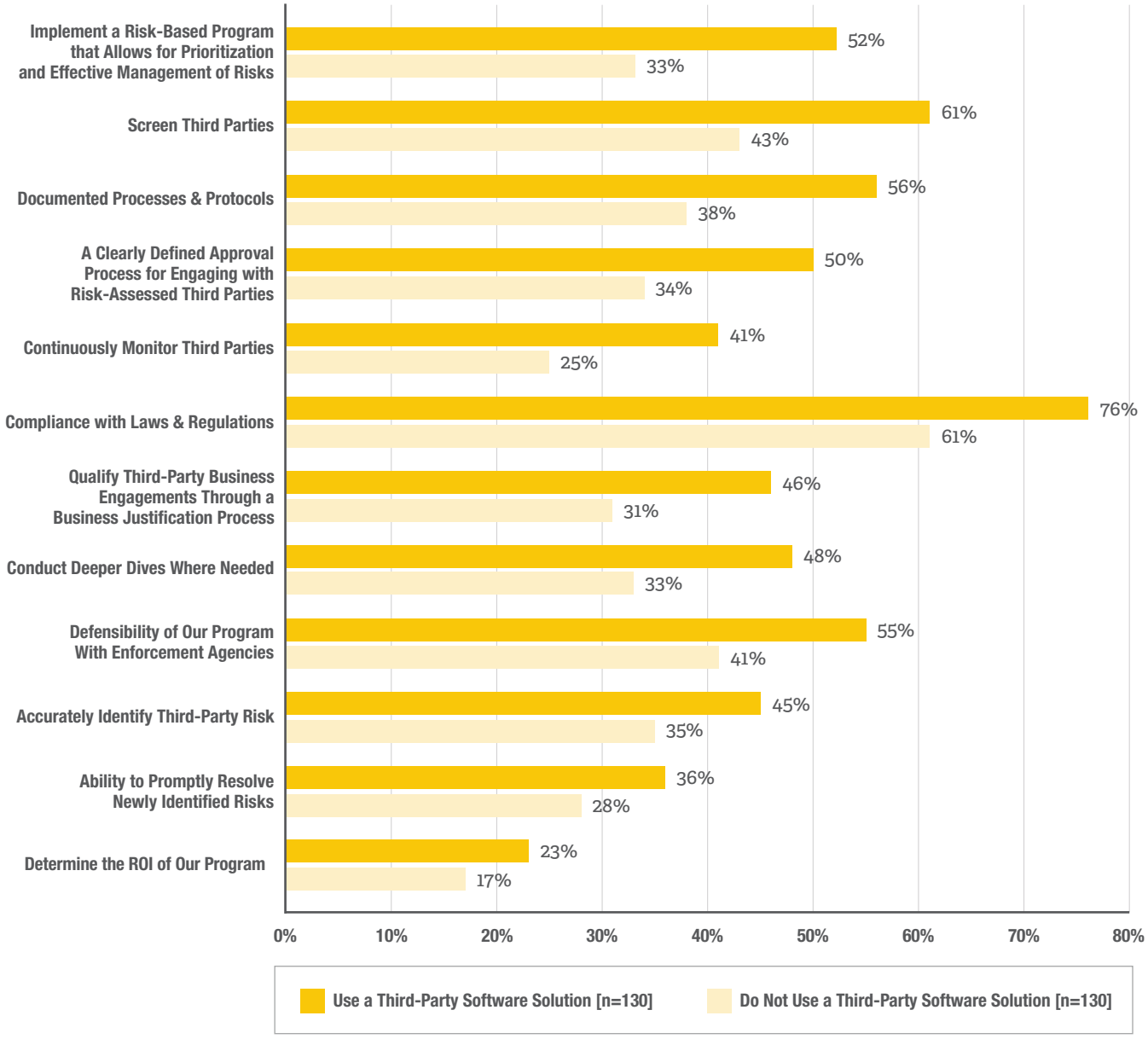
Analysis: When we asked respondents to rank program effectiveness against 12 program elements, those who rated their programs most effective either a 4 or 5 were also users of third-party or automated software. Compliance with laws and regulations (81%), screening third parties (74%) and defensibility with regulators (64%) had the highest performance ratings, but all elements rated higher.

This suggests that higher levels of effectiveness and performance are benefits of using a purpose-built third-party software solution instead of trying to execute these elements internally.

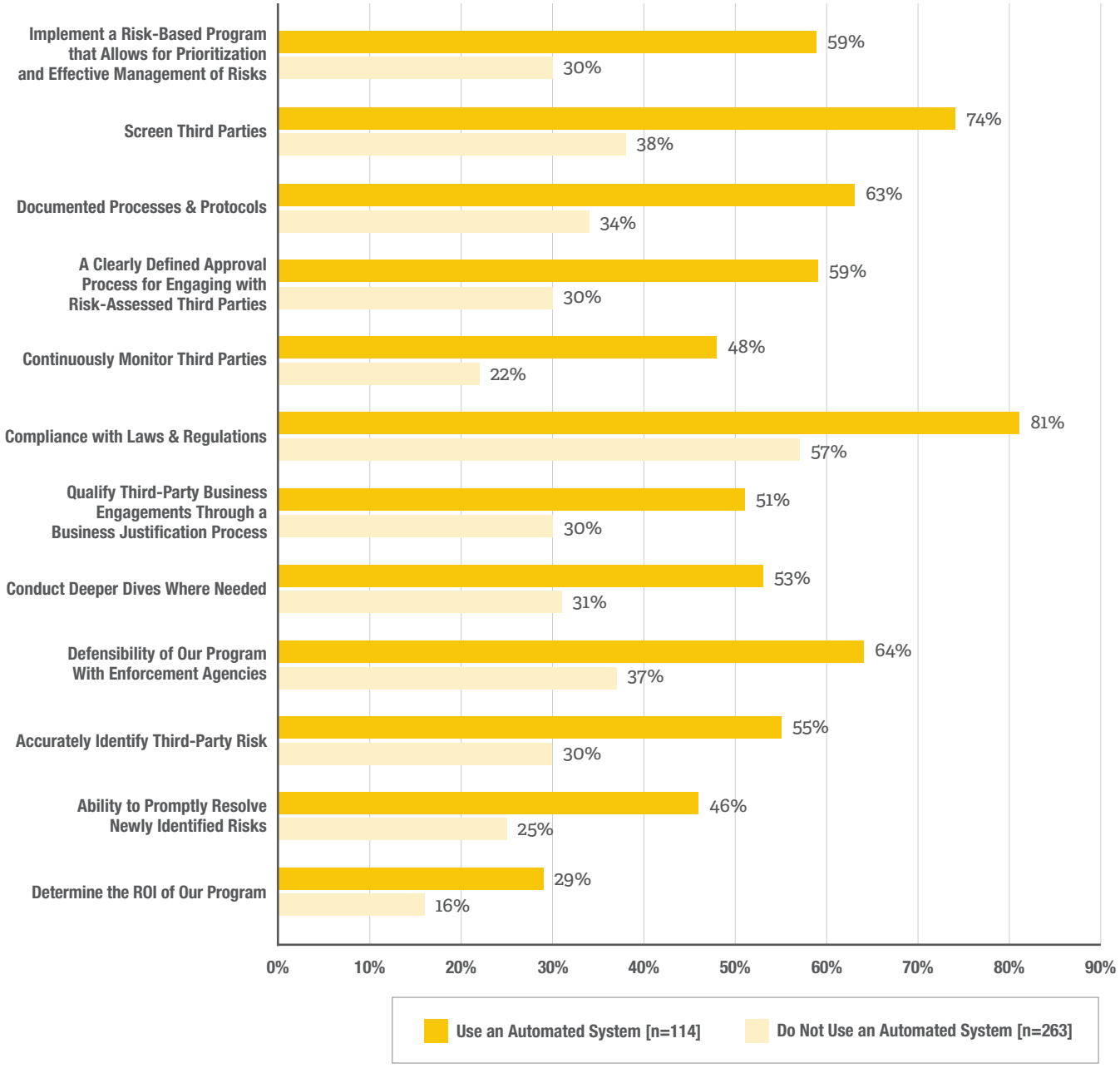
Please Rate Your Organization's Execution on the Following Aspects of Your Third-Party Risk Management Program



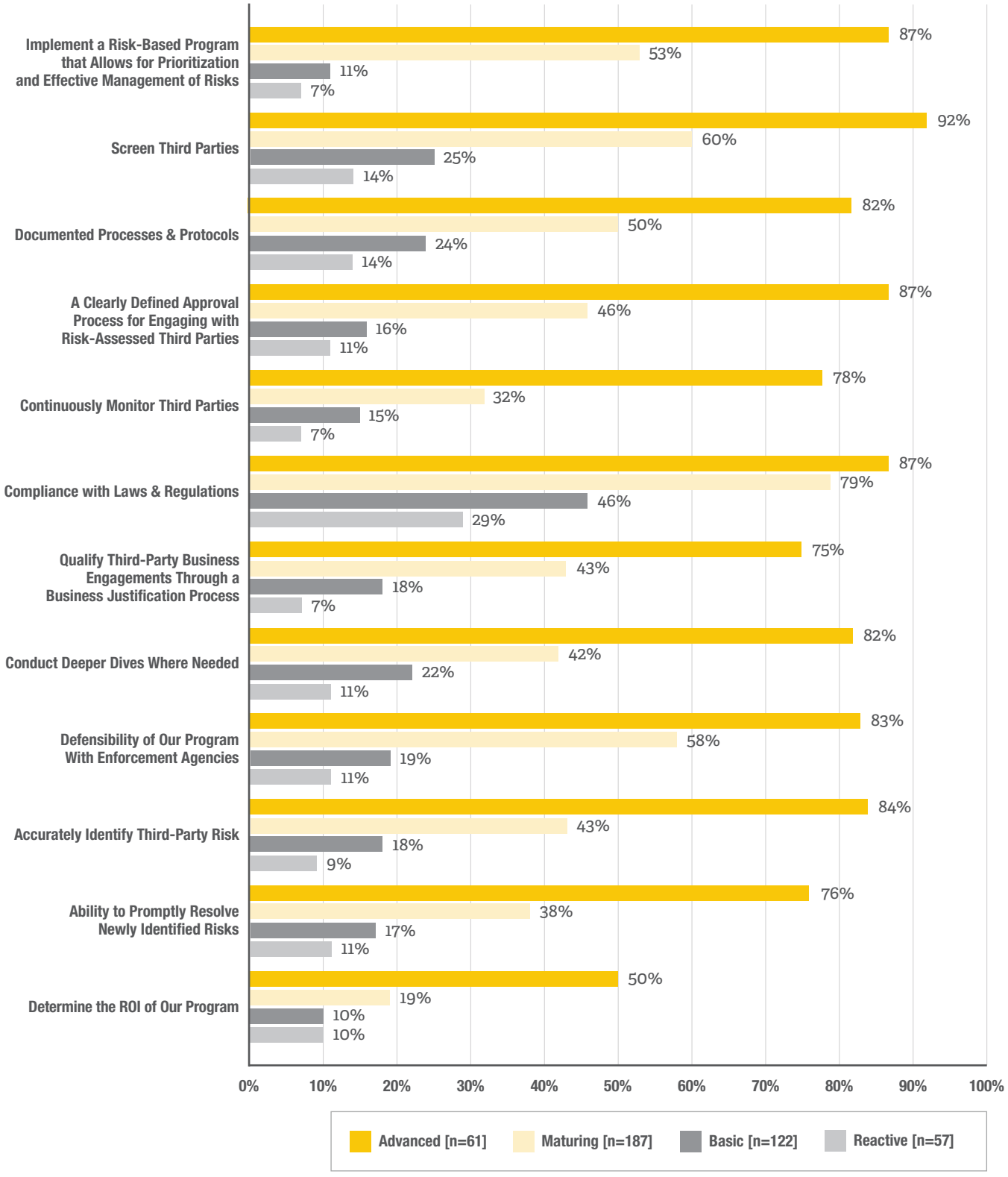
Top 2 Box (Rating of 4 or 5 Out of 5) by Use of Third-Party Software Solution



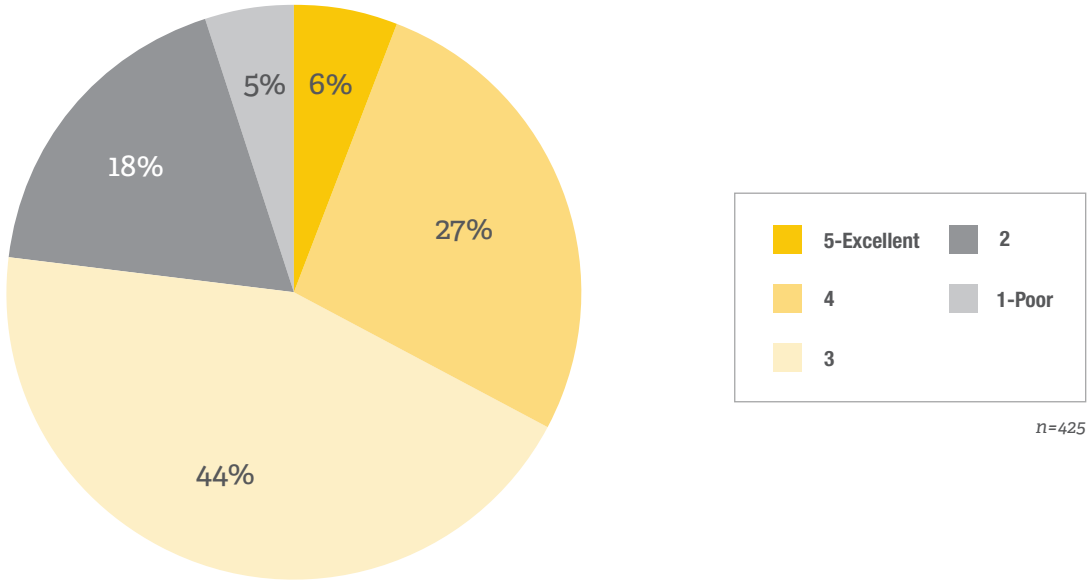
Top 2 Box (Rating of 4 or 5 Out of 5) by Use of Automated Systems



Top 2 Box (Rating of 4 or 5 Out of 5) by Program Maturity

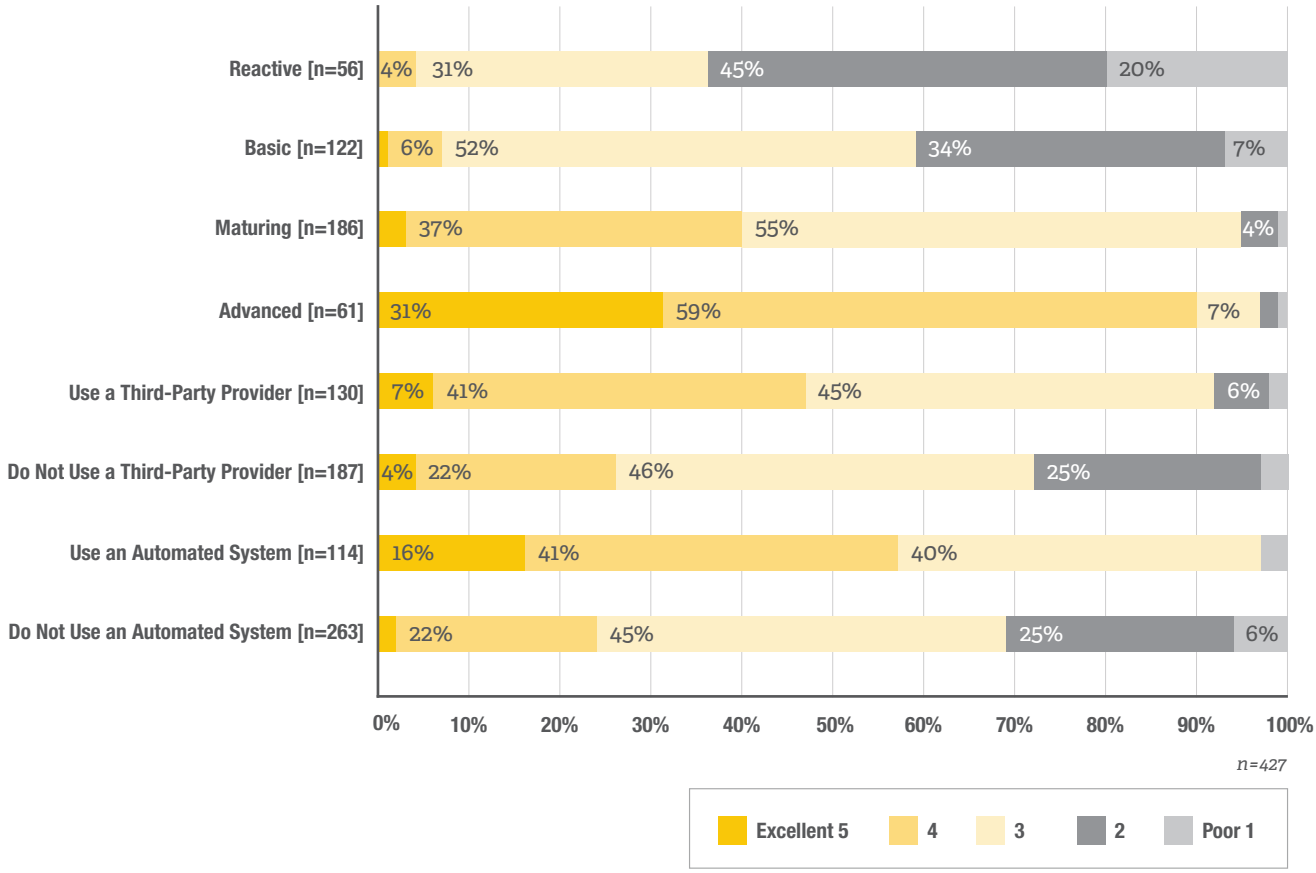


How Would You Rate Your Third-Party Risk Management Program Overall?



n=425

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



n=427


NAVEX GLOBAL®
The Ethics and Compliance Experts

CONCLUSION & KEY TAKEAWAYS

In this, our third consecutive report on third-party risk management, we see positive trends in terms of organizations working to follow regulatory guidelines and global regulations that address bribery, corruption and third-party engagements.

- Comparing 2017 to 2016, we see an increase in the percentage of programs planning to grow program expenditures (41% versus 33%). This is a positive trend which recognizes the value of investing in a third-party program.
- *Maturing* and *Advanced* programs more fully embrace the guidance of the FCPA, UKBA and other laws and regulations, yet they are still the minority. These programs benefit from a risk-based, educated approach to managing their third-party risks.
- Protection from legal and financial risk (69%) and reputational risk (45%) as well as complying with laws (63%) continue to be the top three objectives of third-party programs. This shows a positive focus on program objectives versus a more bottom line focus on reducing litigation and fines (8%). Focusing on these top objectives will definitely improve the latter.
- Our report shows that investments in program maturity may reflect a desire to get ahead of enforcement actions. We saw that 46 percent of those respondents with *Reactive* programs faced legal action in the last three years where less than 30 percent of those with *Basic*, *Maturing* and *Advanced* programs faced legal or regulatory enforcement actions over the same time period.
- There is still room for improvement when it comes to assessing program effectiveness. Although no single methodology can identify all strengths and gaps within a program, it is clear that programs employing third-party management systems and automation are more likely to demonstrate effectiveness.
- As with past years, organizations that rank their programs as highly effective in all 12 effectiveness categories also indicate that they use third-party automation or software. This alone is a strong indicator of ROI to support exploring and purchasing a third-party platform.

Key Takeaways

The power of this report is in seeing how best practice programs deliver better performance. A risk-based program, as defined by current regulations and guidance, helps ensure improved outcomes. Best practices include applying program diligence and consistency across all third parties, defining business justification for engagements, educating third parties on expectations and your code of conduct, continuously monitoring higher risk third parties, and applying due diligence analysis when and where its warranted.

Effectively managing large numbers of relationships and adapting associated risk management efforts for individual third parties as the FCPA Guide suggests can be exceptionally challenging. The reality is, the status of a third-party engagement can change at any time due to internal and external forces – and your due diligence program must be able to adapt as it happens. As this report shows, organizations using automated third-party management solutions to manage scale, scope and inevitable third-party status changes enjoy improved program performance across multiple measures. As automation delivers program precision and sophistication and an ability to measure and improve on performance, we view the discussion of whether to use an automated solution resolved.

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 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:

- Managing Policy, Compliance & Risk Through Effective Use of Technology & Software

White Papers:

- How to Automate Third-Party Due Diligence Monitoring: 10 Steps to Success
- Definitive Guide to Third-Party Risk Management
- What to Ask: Assessing Third-Party Risk Management Solutions

ABOUT THE AUTHOR

Randy Stephens

Vice President, 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.

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 12,500 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

AMERICAS

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

EMEA + APAC

Boston House, Little Green
Richmond, Surrey TW9 1QE
United Kingdom
info@navexglobal.com
www.navexglobal.co.uk
+44 (0) 20 8939 1650

PLEASE RECYCLE