Deloitte.

Third-party governance and risk management
The threats are real

Extended enterprise risk management global survey 2016

Risk powers performance.

Contents

Letter from Owen Ryan

Foreword 1

Executive summary 2

- Key findings 5
- The third-party ecosystem 6
- Managing third-party risk 16
- Third-party governance 23
- Technology and delivery models 29

About the authors 33

Global third-party governance & risk management contacts 34

Risk powers performance.

Risk has traditionally been viewed as something to be minimized or avoided, with significant effort spent on protecting value. However, we believe that risk is also a creator of value and, approached in the right way, can play a unique role in driving business performance.

Take third-party relationships. As the extended enterprise grows and becomes more complex, the ability to manage third-party relationships becomes even more critical to success. Organizations that hesitate to expand their ecosystem, for fear of the risks it can create, will likely be overtaken by organizations that boldly decide to seize the value of third-party relationships, confident in their ability to effectively identity and manage the accompanying risks.

This report includes recent research that highlights opportunities and challenges encountered by organizations in their approach to:
• The third-party ecosystem
• Managing third-party risk
• Third-party governance
• Technology and delivery models

Today's leading organizations are those that have learned how to protect their value through risk management. Tomorrow's leaders will be those that recognize the opportunity for risk to also create value. Deloitte's Risk Advisory professionals around the world can guide you on that journey and help you transform your organization into a place where risk powers performance.

To learn more, please visit us at www.deloitte.com/risk.

Regards,

Owen Ryan
Global Risk Advisory Leader

Foreword

Welcome to our 2016 global survey on Third-party Governance and Risk Management (TPGRM). In this survey, we provide the results from over 170 organizations on the key issues and trends impacting their approaches to managing and mitigating third-party risk.

The results show that TPGRM is starting to rapidly mature in many organizations, not just to enable enterprise-wide visibility of the risks that third-parties present, but, more importantly, to be able to exploit the full spectrum of opportunity that the extended enterprise can create for them.

This report reflects the survey responses of over 170 senior members of management from a variety of organizations across all industries. The respondents were typically responsible for governance and risk management around third-parties, including Chief Finance Officers, Heads of Procurement/Vendor Management, Chief Risk Officers, Heads of Internal Audit and those leading the Compliance and Information Technology (IT) Risk functions in organizations. The respondents represented eight major industry segments covering:

- Financial Services (FS)
- Energy & Resources (E&R)
- Manufacturing (MF)
- Public Sector (PS)
- Technology, Media and Telecommunications (TMT)
- Consumer Business (CB)
- Life Sciences & Health Care (LSHC)
- Business, Infrastructure and Professional Services (BIPS)

The majority of these organizations had annual revenues in excess of US$1 billion. Additional insight was also obtained from subsidiaries of group organizations with some degree of decentralization around third-party management and others with lower annual revenues.

We hope this report will enable you to enhance your understanding of organizational positioning in relation to your peer group across a number of key issues that span the management of third-parties and related risks in a rapidly-changing context, e.g. increasing decentralization and autonomy of operating units in organizations, disruptive technology and globalization. The peer group perspective should also assist you in strategic decision-making around evolving issues such as emerging delivery models and technology infrastructure for third-party risk management. This, in turn, is intended to help you not merely manage third-party risk, but also highlight the opportunity that third-parties create for your organization.

Executive summary

TPGRM is emerging as a board level focus area for many organizations in 2016. The survey results show how investment by organizations in TPGRM has increased year over year and that organizations are now in the process of either implementing or refining the existing implementation of TPGRM processes and frameworks.

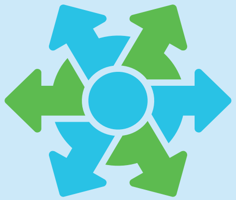
At the same time the survey reveals significant gaps in the tools, technology, and underlying processes that must be addressed to ensure that the emerging organizational commitment to managing third-party risk achieves the intended objectives.

Deloitte believes that the increasing frequency of third-party incidents, negatively impacting organizational reputation, earnings, and shareholder value, is currently the single-most compelling driver for organizations to invest in TPGRM.

Third-party ecosystem

The emerging strategic perspective, together with the severity of consequences of third-party related incidents, is compelling organizations to swiftly "catch up" in upgrading the maturity of their TPGRM processes – to create, as well as to protect, organizational value.

The results of the survey demonstrate how a renewed set of drivers, which are directly aligned to long-term value-creation (such as business agility, access to specialized skills and knowledge, innovation, process-improvement and other sources of sustainable competitive advantage), are now motivating organizations to rapidly enhance the management of risks within their global third-party ecosystems. The desire to achieve short-term cost savings remains an important consideration, but is diminished in relative importance.



44.9 percent of respondents feel that flexibility and scalability will be the top emerging driver for third-party engagement.

55.1 percent of respondents aspire to have integrated third-party risk management systems in a year or more, with 16.5 percent aspiring to be "best-in-class."

Managing third-party risk

As incidents relating to third-parties continue to rise, organizations are becoming more and more concerned about any disruption to customer service this can create or any regulation this may breach, given the growing severity of the related punitive action by regulators, and customers. At the same time, increasing decentralization of operating units in organizations is starting to create challenges to a unified and consistent approach to TPGRM, driving organizations to mandate consistent third-party management standards across their operating units and aspiring to increase their monitoring and assurance activities over third-parties.

87 percent of respondents have faced a disruptive incident with third-parties in the last 2-3 years of which...

28 percent faced major disruption and...

11 percent experienced a complete third-party failure.

Third-party governance

It is encouraging to see third-party risk starting to feature consistently on the board agenda in the more forward-looking organizations, supported by increasing organizational awareness and commitment to this issue. However, the survey reveals a wide "execution gap" resulting from the inability of supporting tools, technology, and processes to achieve intended results, despite the organizational commitment and high level governance framework.

Mind the execution gap

94.3 percent of respondents have only low to moderate levels of confidence in the tools and technology used to manage third-party risk and 88.6 percent have a similar level of confidence in the quality of the underlying risk management processes, despite significantly higher levels of confidence in organizational commitment and governance frameworks – creating the execution gap.

Delivery models

As the demands of TPGRM keep increasing, the majority of organizations are investing in centralized in-house functions to support the management of third-party risk, with a smaller proportion of organizations moving to external service-provider based models. A significant minority remain undecided on their future course of action.

To insource or outsource TPGRM?

58.4 percent of respondents are increasingly moving to a centralized in-house function to support third-party management with only 8 percent to external provider-based models while as many as 33.6 percent are unsure about their future direction.

Reputation on the line

As businesses take the concept of the extended enterprise to new levels, the survey confirms how third-parties are exposing businesses to new risks such as the threat of high profile customer service disruption and other major business failures. Where these risks have been realized has compromised organizational reputation, broken down business continuity, and even attracted substantial penalties and regulatory enforcement action.

The threats are real

26.2 percent of respondents have suffered reputational damage, 23 percent of respondents have been non-compliant with regulatory requirements and 20.6 percent have experienced breach of sensitive customer data – all arising out of third-party actions.

86 percent of respondents now mandate consistent third-party standards across their operating units to manage these threats.

Key findings

The third-party ecosystem

1. As dependence on third-parties becomes increasingly critical, organizations are being compelled to rapidly "catch up" in enhancing the maturity of their TPGRM processes.

2. The drivers for third-party engagement are progressively shifting from a focus on cost to a focus on value, reflecting organizational recognition of the strategic opportunity that third-parties can create for them.

Managing third-party risk

3. Third-party risk incidents are on the increase with customer service disruption and regulatory breach being considered the top risks.

4. Increased monitoring and assurance activity over third-parties is believed to significantly reduce third-party risk.

5. Organizational commitment to third-party risk management is not supported by confidence in the related technology and processes.

Third-party governance

6. Third-party risk is starting to feature consistently on board agendas with CEO/board-level responsibility in the more progressive organizations or those operating in highly regulated environments.

7. Visits to third-party locations are considered the most effective method to gain assurance over third-party management.

8. Most organizations are mandating consistent third-party governance standards amidst increasing decentralizations of operating units.

Technology and delivery models

9. Existing technology platforms for managing third-parties are considered inadequate.

10. Organizations are in the process of deciding between centralized in-house models and external service-provider based models for third-party monitoring.

The third-party ecosystem

01 As dependence on third-parties becomes increasingly critical, organizations are being compelled to rapidly ‘catch up’ in enhancing the maturity of their TPGRM processes.

The survey demonstrates how organizations continue to rapidly enhance their dependence on global third-party ecosystems (extended enterprise) to garner the benefits of collaboration. Nearly 74 percent of respondents believe that third-parties will play a highly important (44.8 percent) or critical (29.1 percent) role in the year ahead, up from 60.3 percent a year ago.

Survey respondents believe that this increasing dependence on third-parties arises from four key drivers:

- Organizations have now gone far beyond the traditional focus on leveraging third-parties in their direct supply chain (suppliers and vendors), with an increasing proportion of third-parties in sales, distribution, and support services, in addition to alliance and joint venture partners. The increasing use of new technologies (such as the cloud and cloud-based applications) that facilitate collaboration and enable businesses to enhance their virtual boundaries, will further accelerate this trend;

- Secondly, the nature of the tasks being executed through third-parties is becoming more critical than ever before, thus increasing the severity of consequences on disruption or failure. In the words of one respondent, “third-parties are increasingly carrying out activities traditionally carried out by direct employees, in particular interacting with customers”;

- Thirdly, respondents believe that the pursuit of lower costs will continue to drive businesses to “continue to identify and work with high quality but lower cost vendors and other third-parties in emerging markets”;

- Finally, the dependence on individual third-parties will further increase as organizations choose to work with a smaller number of global strategic partners in an environment where consolidation activity is ongoing within the third-party marketplace.

Against this backdrop, only 9.5 percent of respondents had integrated or optimized their TPGRM systems a year ago. The survey confirms that organizations are now being compelled to rapidly “catch up” in taking a holistic and proactive approach to third-party risk; 71.6 percent of respondents expect to be able to integrate and optimize their third-party risk management system, including 16.5 percent of respondents aspiring to be “best-in-class” in a year or more.

73.9 percent of respondents believe that third-parties will play a highly important or critical role in the year ahead, up from 60.3 percent a year ago.

Against this backdrop, only 9.5 percent of respondents had integrated or optimized their TPGRM systems a year ago. Organizations are rapidly catching up, with 71.6 percent respondents expecting to be integrated and optimized in a year or more, including around 16.5 percent aspiring to be “best-in-class.”

Deloitte point of view

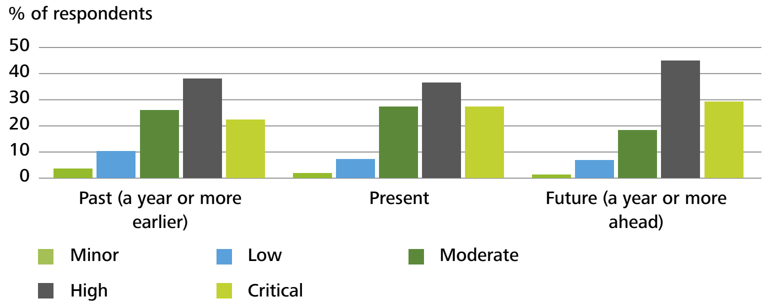
Organizational focus on third-party risk has traditionally been reactive and dependent upon who is driving the activity. This has typically been procurement teams focused on suppliers and vendors, or brand and intellectual property (IP) protection functions focused on distribution channels and non-authorized manufacturers. Such a decentralized approach to risk has led to micro-focus on risk areas that interest certain parts of a business or certain functions (for example, operational performance from a supply chain perspective or information security from a corporate security angle).

Organizations are only now starting to depart from this siloed approach and take a board and leadership-led holistic, proactive approach to risk as a source of organizational value. This covers all categories of third-parties and all areas of risk, considering *operational risk* factors (e.g. performance, quality standards, delivery times, key performance indicators (KPI)/service level agreements (SLA) measurements)) with *reputational/financial risk* factors (e.g. labor practices, an understanding of financial health, appropriate charging mechanisms, and adherence to these) and *legal/regulatory risks* (e.g. compliance with bribery regulations, awareness of global industry standards as they apply to third-parties, environment, health and safety compliance).

Deloitte recommends that organizations look at all risks (as highlighted above) across the third-party ecosystem in a consistent manner and do so in such a way that does not over-burden third-parties. In particular, adaptive risk management questionnaires should be used so that third-parties are not overwhelmed with questions and requests for evidence.

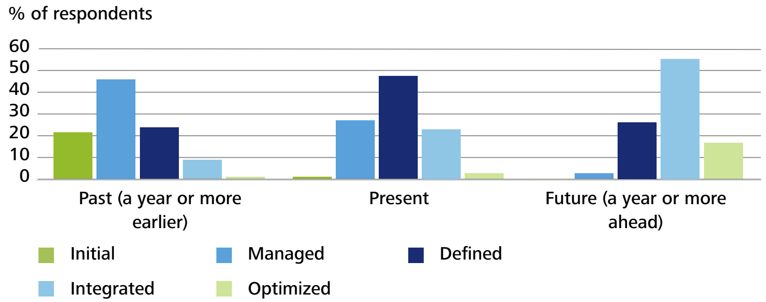
In addition, Deloitte specialists, who have significant experience of working with organizations undergoing similar transformations, consider respondent aspirations to be optimistic in their estimation of the time and effort required to achieve this organizational transformation. Given the diverse range of stakeholders, processes and technology impacted by this transformation, respondent organizations who believe that they would be able to substantially complete their transformational journey in the next year, may actually take much longer to do so and such programs typically span a 2-3 year timeframe.

Increasing dependence on third-party ecosystem



Dependence based on critical factors including number of third-parties, criticality, proportion of businesses involved, etc.

Increasing maturity of TPGRM systems



Maturity level definition:
Respondents rated the maturity of their organization's approach to third-party risk management based on the following elements:

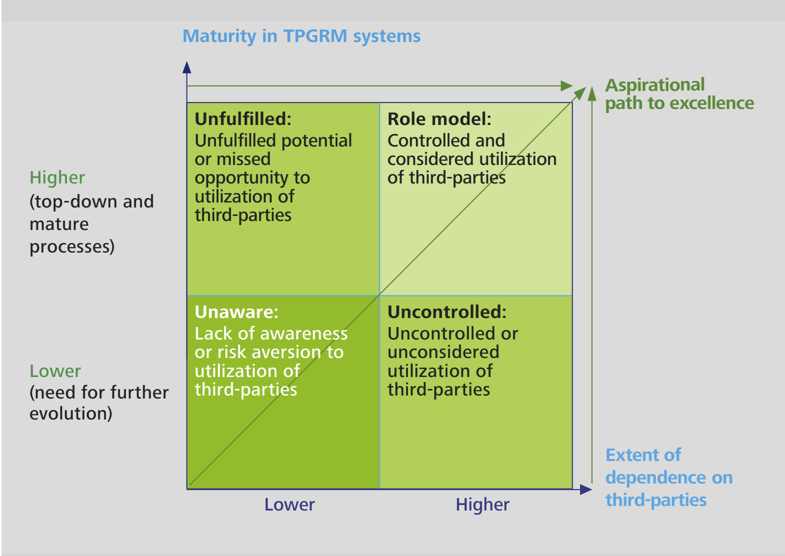
- Structure of third-party management organization;
- Clarity of related roles and responsibilities;
- Stakeholder awareness and commitment to third-party risk management;
- Skills, bandwidth and competence in management of third-parties; and
- Process and supporting technology for third-party risk management.

Rating:
Initial: None or very few of the elements addressed.
Managed: Some of the elements addressed with limited effort.
Defined: Consideration given to addressing all the elements with room for improvement.
Integrated: Most of the elements addressed and evolved.
Optimized: "Best-in-class" organization – all of the elements addressed and evolved.

Treading the aspirational path to excellence (by industry segment):

The survey reveals that organizations across the eight major industry segments are adopting varying stances in the extent of dependence on third-parties, along a continuum ranging from lower to a higher level of dependence. On a second dimension, they are at varying levels of maturity in their risk and governance approach to third-parties.

Based on the above two criteria – the extent of dependence on third-parties, and the maturity of governance processes – these organizations, grouped by industry segment, can be mapped to a two-by-two grid in the figure right as set out in our TPGRM whitepaper in 2015. This grid can be used by organizations to understand their current positioning as a first step to developing plans for reinventing themselves as the role models (upper right-hand quadrant) who, as explained below, are able to maximize the opportunities through the third-party ecosystem, while managing the related risks.



Dependance on third-party ecosystem

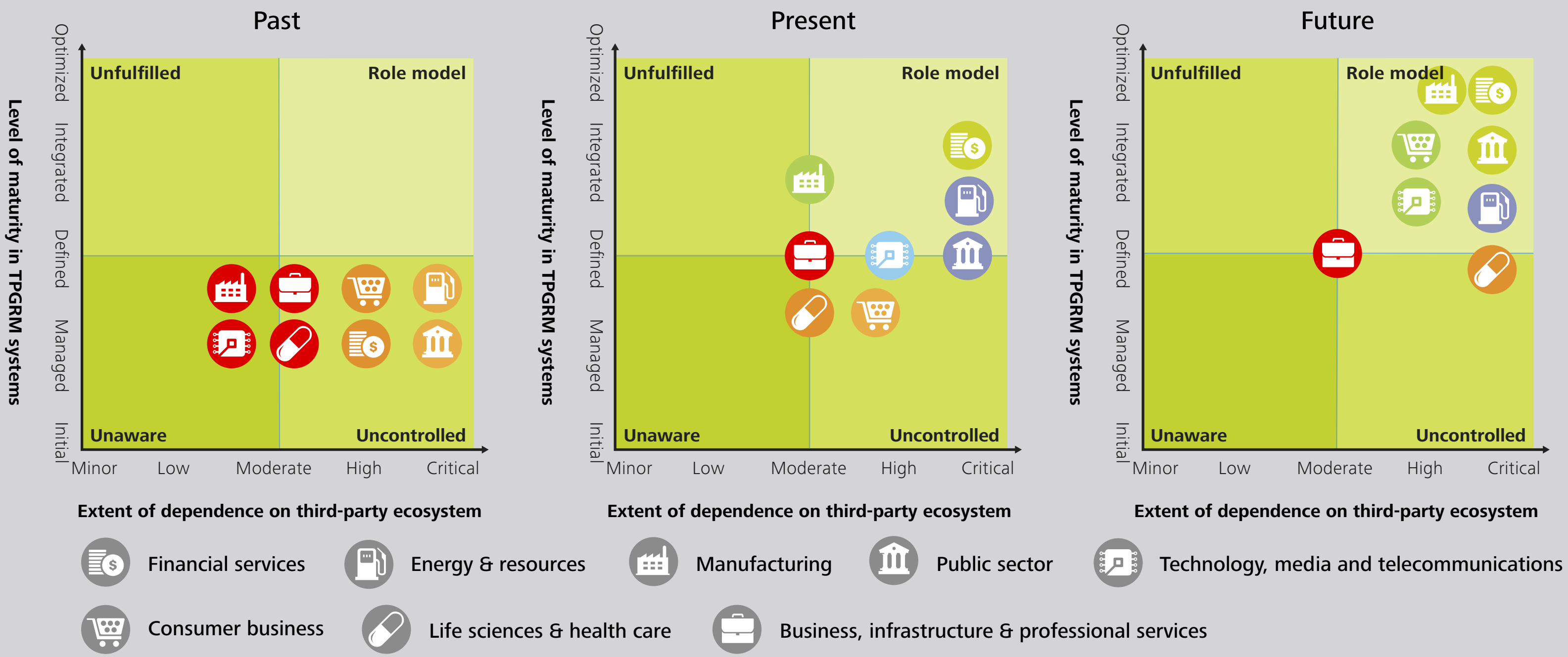
	BIPS	CB	E&R	FS	LSHC	MF	TMT	PS
Past	Moderate	High	Critical	High	Moderate	Moderate	Moderate	Critical
Present	Moderate	High	Critical	Critical	Moderate	Moderate	High	Critical
Future	Moderate	High	Critical	Critical	Critical	Critical	High	Critical

Level of maturity in TPGRM systems

	BIPS	CB	E&R	FS	LSHC	MF	TMT	PS
Past	Managed	Managed	Managed	Managed	Managed	Managed	Managed	Managed
Present	Defined	Managed	Defined	Integrated	Managed	Integrated	Defined	Defined
Future	Defined	Integrated	Integrated	Optimized	Defined	Optimized	Integrated	Optimized

The role models: The "best-in-class" organizations are clearly those that are able to leverage their third-party ecosystem more extensively with a higher planned dependence on them. They are also the organizations that are in a more mature stage of implementation of the related governance and risk management mechanisms, implemented top-down from the board and C-suite. These organizations would therefore be the best positioned to maximize the opportunities arising from the use of third-parties as a valuable organizational asset. It is likely that these organizations will involve third-parties in higher value processes, considering and managing a greater level of risks in a dynamic, agile and innovative way in their pursuit of business value.

Treading the aspirational path to excellence



Diametrically opposite them are the organizations that continue to have limited use of the third-party ecosystem and have also not implemented or matured in their implementation of governance mechanisms and practices. Such organizations are likely to face the greatest potential challenges to erosion of organizational value. Accordingly, they can be classed as the ***unaware;*** those who are likely to experience erosion in their profitability and organizational value which may threaten eventual survival. For such organizations it is likely that any limited use of third-parties would be focused on lower value generating and less risky activities. They may still face several threats and hazards in these limited pursuits of organizational value.

Organizations that have a higher dependence on third-parties in their aspiration for higher organizational value, without the requisite evolution in governance mechanisms to give them the required control, are likely to be unable to manage the various threats they face as they engage with their third-party ecosystem and can be considered ***uncontrolled.***

Finally, organizations that will continually remain ***unfulfilled*** are those that have limited leverage of third-parties despite maturing in governance mechanisms and practices. They are likely to be perpetually facing significant opportunity loss, leading eventually to threats of value erosion and survival challenges.

This aspirational path to excellence across the key industry segments, as revealed by the survey, is set out on page 9.

As can be seen, organizations across all the industry segments are treading this aspirational path of excellence, some quicker than others, with those in the BIPS segment transitioning the slowest. This is a reflection of the nature of their businesses around service-delivery, rather than product delivery. Accordingly, they do not have a “product-based” supply or distribution chain and therefore tend to involve third-parties at a significantly lower level than other product-based industries.

The ‘best-in-class’ organizations are those that are able to leverage their third-party ecosystem more extensively. They are also the organizations that are in a more mature stage of implementation with related governance and risk management mechanisms.

The third-party ecosystem (cont.)

02 The drivers for third-party engagement are progressively shifting from a focus on cost to a focus on value, reflecting organizational recognition of the strategic opportunity that third-parties can create for them.

The survey reconfirms how new and emerging strategic drivers for third-party engagement such as strategic agility, competitive advantage, innovation, and performance improvement, are being focused upon to enhance organizational value.

Traditional drivers

As previously stated, the pursuit of cost savings continues to remain one of the key factors driving the increasing dependence on third-parties. At the same time, the survey reveals that increasing use of third-parties is not about cost-reduction alone. The survey reveals that cost saving/cost-reduction is rapidly losing its dominance as the most significant traditional driver for third-party engagement. Only 42.3 percent of respondents consider this to be a key future driver, down from 57.1 percent a year ago.

Other traditional drivers such as the need to reduce operational risk through the involvement of third-parties (12.2 percent of respondents a year ago) or improve overall quality parameters (6.4 percent of respondents a year ago) are also declining or remaining unchanged in relative importance, as reflected by 12.8 percent and 3.8 percent of respondents, respectively, considering the above as key future drivers.

Emerging drivers

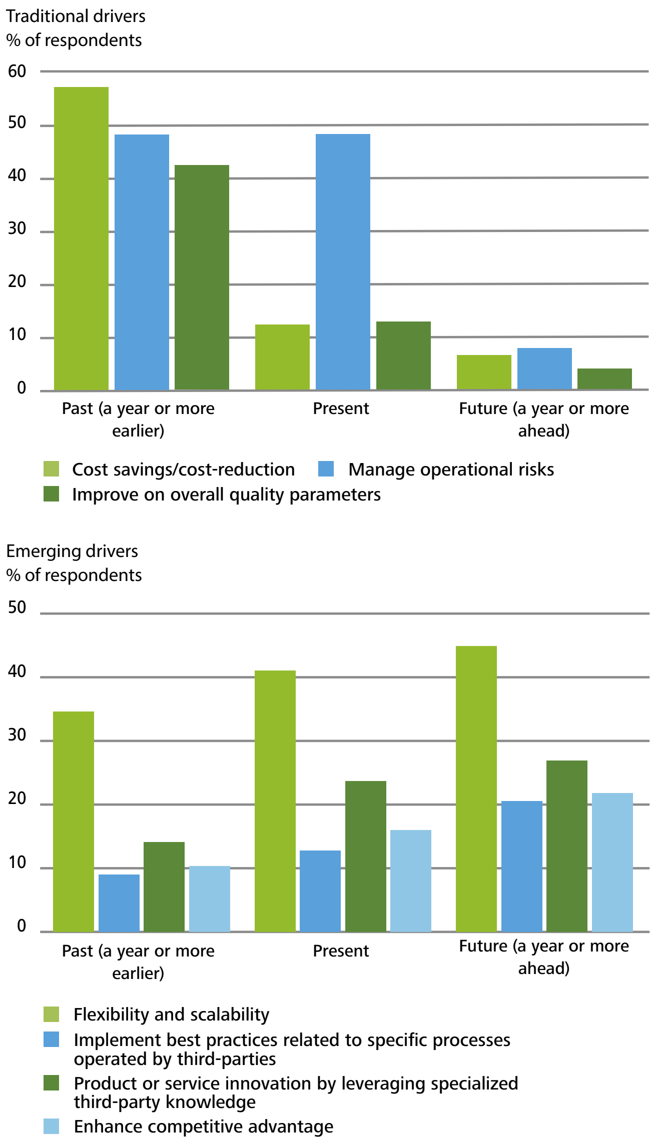
Emerging drivers for engaging third-parties that reflect an increasing focus on organizational value-enhancement are increasingly becoming more significant. The survey reveals that organizational agility, characterized by the need for flexibility and scalability, is emerging as the most powerful value-driver for future third-party engagement (44.9 percent of respondents, up from 34.6 percent a year ago). Similarly, the opportunity to bring in product or service innovation by leveraging specialized knowledge or skills from third-parties is also rapidly enhancing its dominance as a key future driver (26.9 percent of respondents, up from 10.3 percent a year ago).

With regard to services provided by the third-party ecosystem, as many as 20.5 percent of respondents are expecting to improve their performance from the implementation of best practices related to specific processes operated by third-parties, representing a significant increase from 9 percent a year ago. In addition, 21.8 percent of respondents expect third-parties to be a source of competitive advantage (up from 10.3 percent a year ago).

Cost savings/cost-reduction is rapidly losing its dominance as the most significant traditional driver for third-party engagement with only 42.3 percent of respondents considering it a key future driver, down from 57.1 percent a year ago.

44.9 percent see the need for organizational agility characterized by flexibility and scalability (up from 34.6 percent a year ago) to be the strongest emerging value-driver for future third-party engagement.

Changing drivers for third-party engagement



Deloitte point of view

The increasing recognition of the strategic opportunity that third-parties can create for organizations resonates with Deloitte's experience that effectively governed third-party relationships can be a significant source of organizational value. This can arise, for example, from product or service innovation, expansion to new markets and access to skills and capabilities not available internally, including the capability to operate with greater agility. In addition, some organizations are now able to effectively benefit from third-parties as their knowledge partners, or even as trusted advisers, to catalyze organizational innovation, provide strategic insights, and feature on organizational advisory boards.

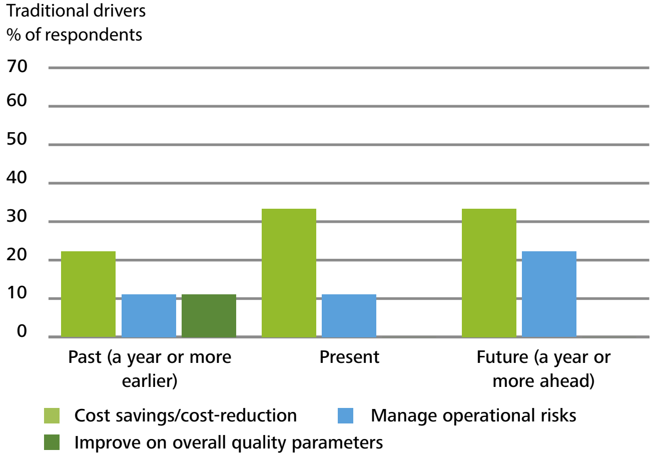
Deloitte believes those organizations that have a good handle on their third-party business partners, can not only avoid the punitive costs and reputational damage, but stand to gain competitive advantage over their peers out performing them by an additional 4-5 percent return on equity (ROE) (which, in the case of Fortune 500 or FT500 companies can mean additional earnings before interest, taxes, and amortization (EBITA) in the range of US$25-500 million). Academic researchers concur with this view. When stakeholders can appreciate improvements in governance, controls, and risk management that upgrade their long-term expectations, equity values will rise.

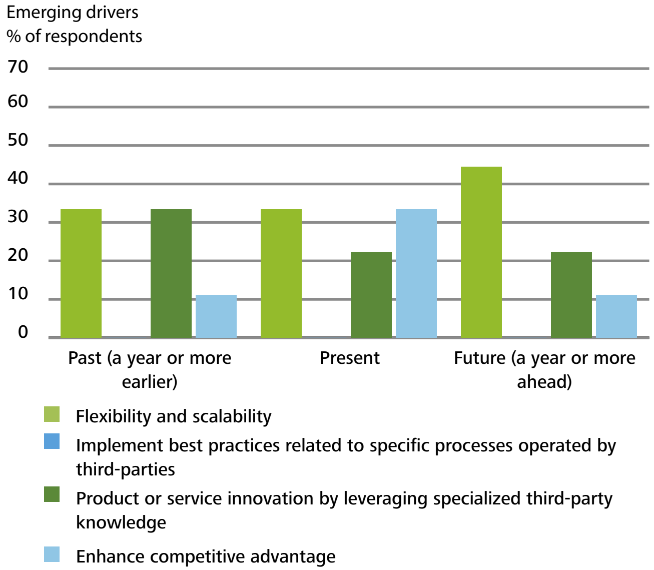
Survey results by industry segment

The increasing importance of emerging drivers over traditional drivers for third-party engagement persists as a general trend across most of the industry segments. This trend is probably the most dominant in the CB segment, with 57.1 percent of respondents focused on cost savings a year or more ahead rapidly decreasing to 28.6 percent a year or more ahead. On the other hand, organizations in the BIPS segment aspire to continue to increase their focus on cost savings (22.2 percent of respondents a year or more ago to 33.3 percent a year or more ahead).

Changing drivers for third-party engagement

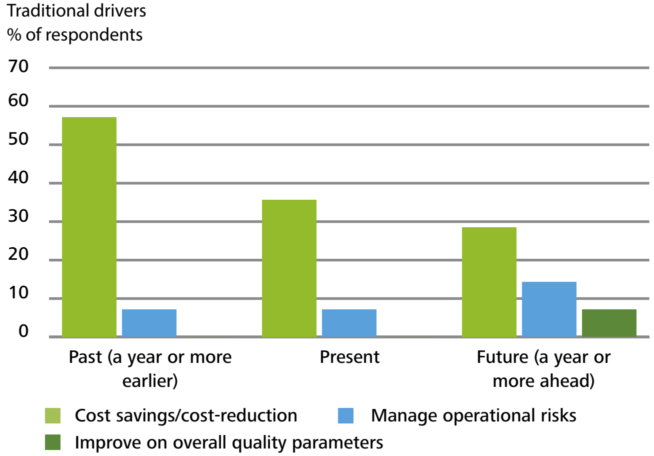
Business, infrastructure and professional services

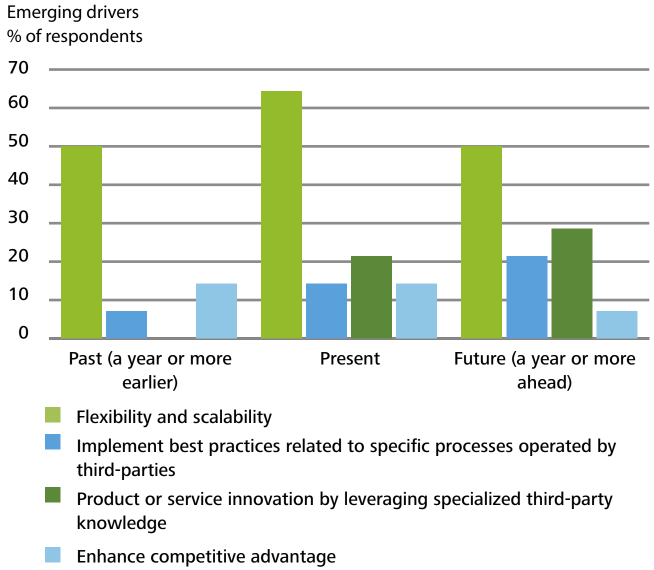




Changing drivers for third-party engagement

Consumer business



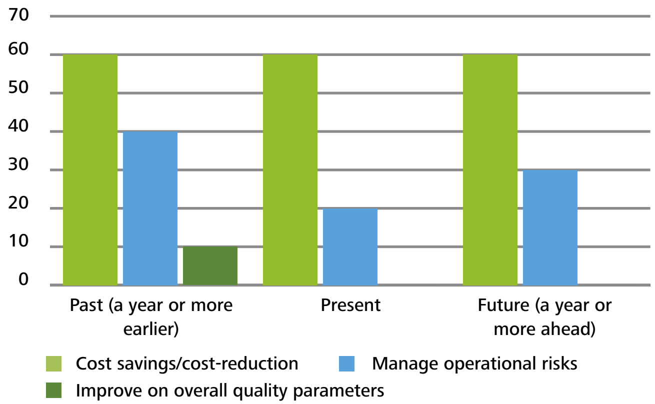


Survey results by industry segment

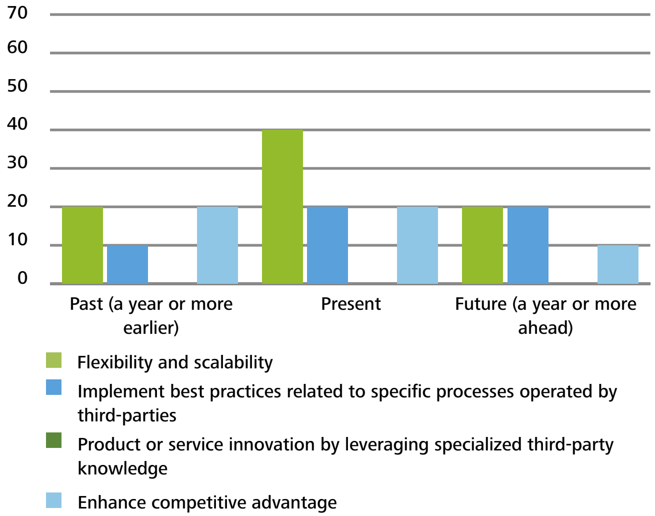
Changing drivers for third-party engagement

Energy & resources

Traditional drivers
% of respondents



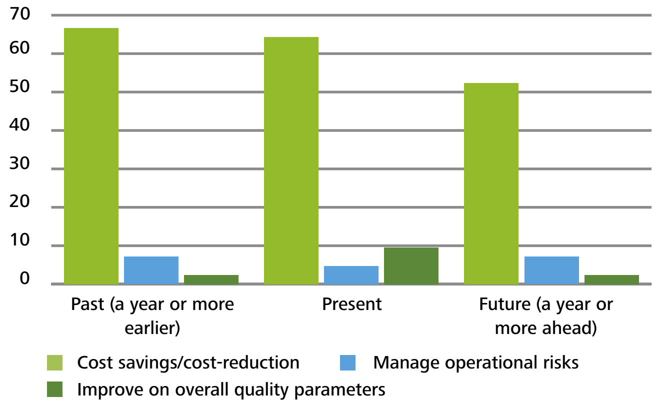
Emerging drivers
% of respondents



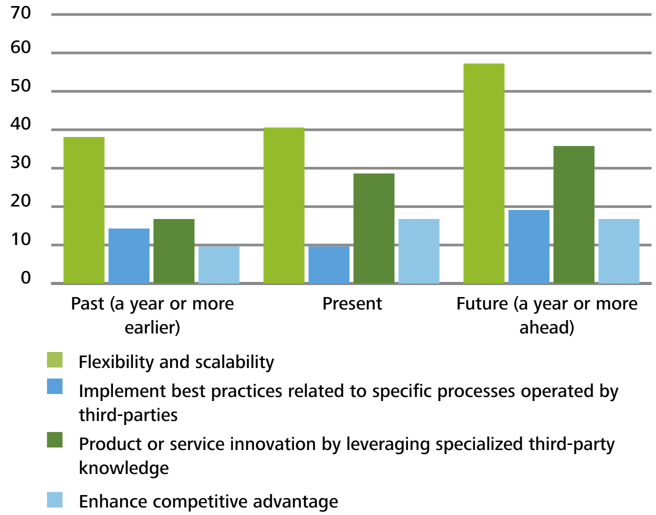
Changing drivers for third-party engagement

Financial services

Traditional drivers
% of respondents



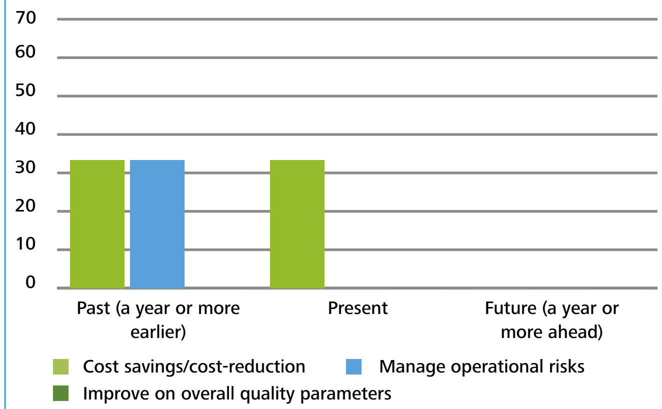
Emerging drivers
% of respondents



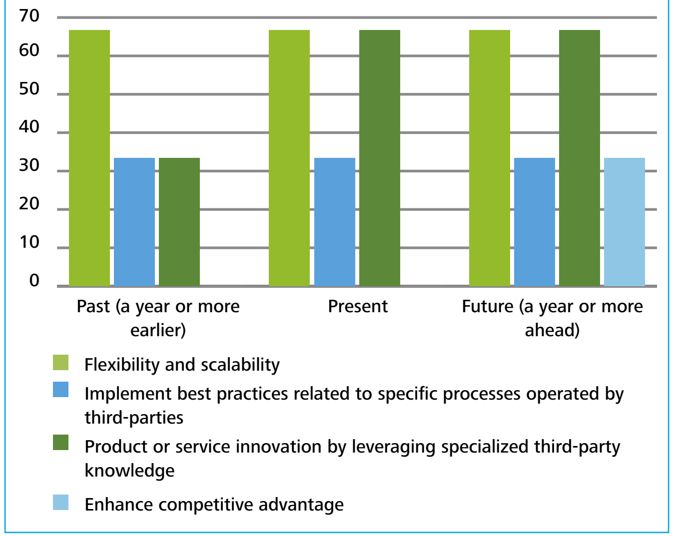
Changing drivers for third-party engagement

Life sciences & health care

Traditional drivers
% of respondents



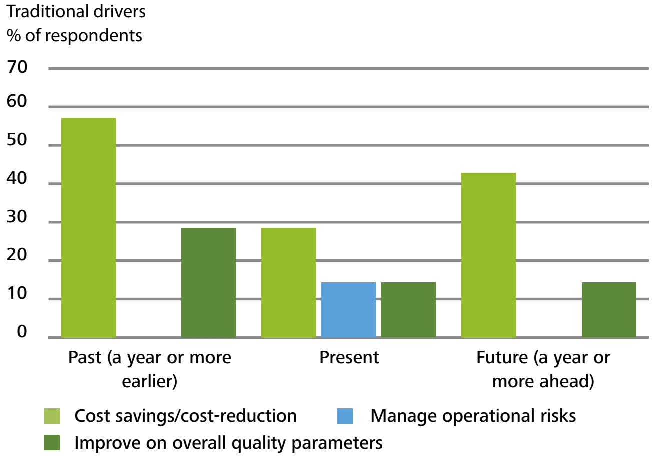
Emerging drivers
% of respondents

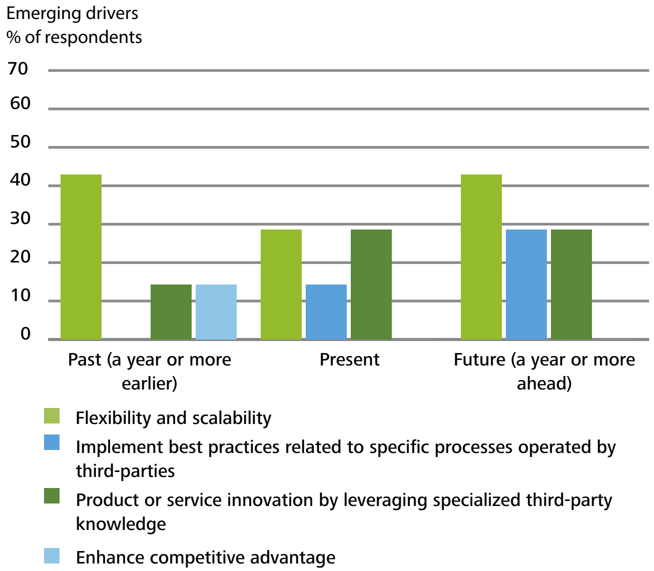


Survey results by industry segment

Changing drivers for third-party engagement

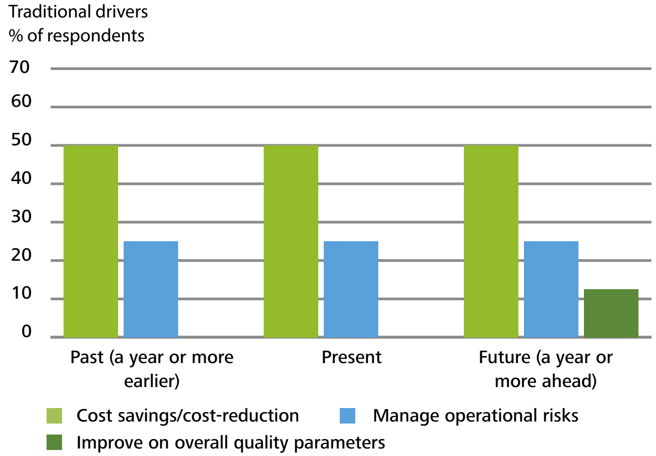
Manufacturing

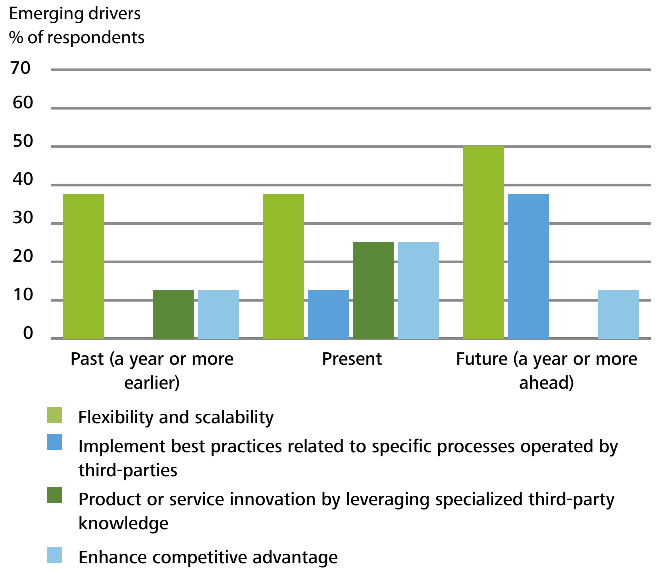




Changing drivers for third-party engagement

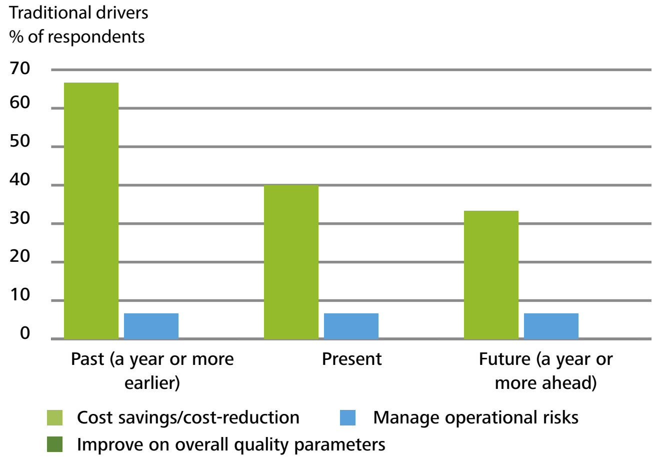
Public sector

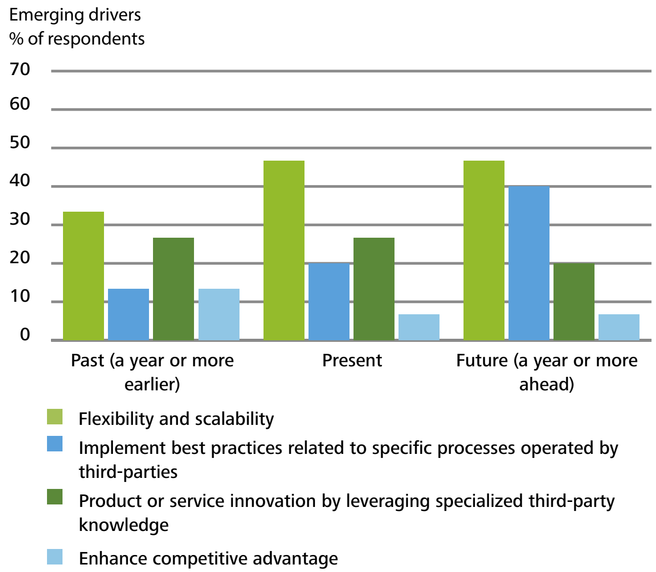




Changing drivers for third-party engagement

Technology, media and telecommunications





Managing third-party risk

03 Third-party risk incidents are on the increase with customer service disruption and regulatory breach being considered the top risks.

As businesses take the concept of the extended enterprise to new levels, the survey confirms how third-parties are exposing businesses to new risks such as the threat of high profile customer service disruption and other major business failures. Where these risks have been realized, this has compromised organizational reputation, broken down business continuity, and even attracted substantial penalties and regulatory enforcement action.

Respondents consider disruption in client service due to third-party action as the most critical risk, closely followed by the breach of regulation or law by third-parties being attributed to their organization. Reputational damage, supply-chain breakdown, financial fraud/exposure caused by third-party action also feature on the list of critical risks. In addition, respondents are anxious about any failure in financial viability of a third-party that can impact their ability to deliver.

The threats arising from the actions of third-parties are real. Eighty-seven percent of respondents have faced a disruptive incident associated with third-parties in the last 2-3 years, out of which 28 percent faced major disruption and 11 percent experienced a complete third-party failure – reducing their confidence in the related governance and risk management processes.

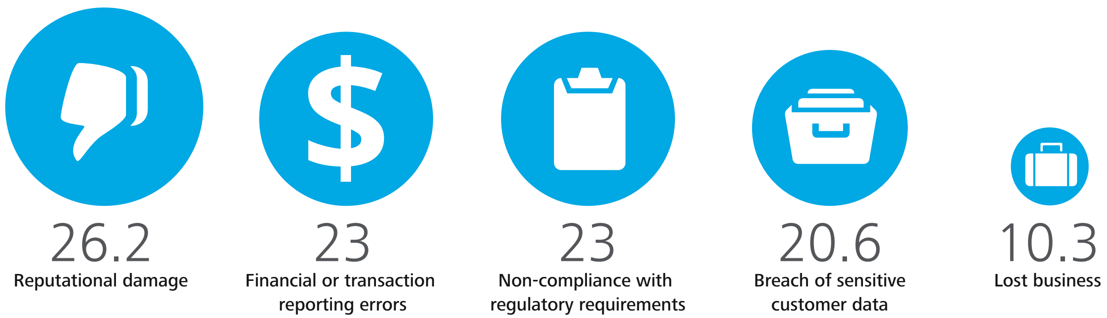
Slightly more than 26 percent of respondents have suffered reputational damage arising from third-party action in the last 2-3 years while 23 percent have ended up being non-compliant with regulatory requirements with 8.7 percent of these respondents facing a fine or financial penalty as a result of this non-compliance. Another 23 percent of respondents have experienced financial or transaction-reporting errors, 20.6 percent have dealt with a situation where sensitive customer data has been breached through third-parties, and 10.3 percent have actually lost revenue.

87 percent of respondents have faced a disruptive incident associated with third-parties in the last 2-3 years, of which 28 percent faced major disruption and 11 percent complete third-party failure – reducing their confidence in the related governance and risk management processes.

Top areas of third-party engagement risk, ranked in order of criticality

Risk areas	Rank
Disruption in customer service due to third-parties	1
Breach of regulation or law through third-party action	2
Reputational damage arising from third-party behavior	3
Breakdown in supply chain due to failure of third-parties	4
Financial fraud or exposure created by third-party behavior	5
Failure of financial viability of third-party impacting delivery	6

Impact of third-party incidents actually faced by respondents (% of respondents)



Deloitte point of view

The severity of consequences of negative actions by third-parties on organizational reputation, earnings and shareholder value is currently the single-most compelling driver for organizations to invest in either implementing or refining TPGRM processes and frameworks.

Deloitte believes that the FS sector will continue to dominate industry-specific regulation around the world impacting the use of third-parties, which is expected to get more rigorous. Similar regulation however, is also expected to grow in other industry sectors such as LSHC, chemicals, food and retail, etc., together with global regulation such as the US Foreign Corrupt Practices Act (FCPA) impacting all industries, regardless of where the related organizations are headquartered.

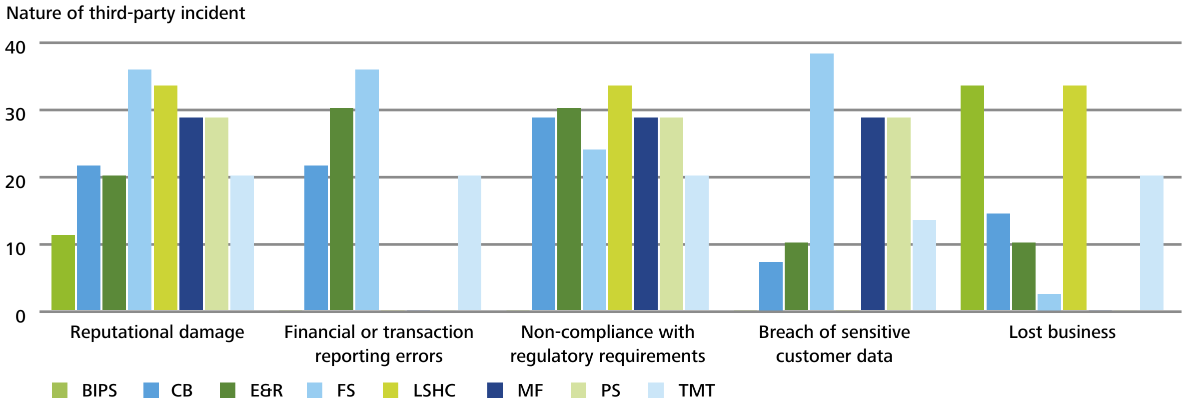
Deloitte estimates that the failure by large multinational businesses to appropriately identify and manage third-parties can lead to fines and direct compensation costs or other revenue losses in the range of US$2–50 million, while action under global legislation such as the US FCPA can be far higher, touching US$0.5–1 billion. This point of view resonates with academic research which has established that punishment by regulators causes losses to shareholders that are, on average, 10 times the size of the fine itself and negatively impacts share prices by an average of 2.55 percent in the three days after the announcement, where direct harm to customers and investors is involved. This is in addition to the significant reputational damage that an organization will incur.

Survey results by industry segment

The survey reveals that concerns around the breakdown in their service supply chain features higher amongst organizations engaged in BIPS as well as those in LSHC, compared to respondents from other industry segments, given the nature of their business. Similarly, concern around fraud by third-parties ranks higher than others for CB, TMT and MF industries, while PS undertakings appear to be most perturbed about failure in financial viability of their third-parties.

In terms of the related impact of third-party incidents, organizations in the BIPS segment (33.3 percent of respondents) as well as in LSHC (33.3 percent of respondents) appear to have faced revenue losses arising from third-party-related failures but with significantly lower experience of financial or transaction errors. Additionally, BIPS organizations have faced a comparatively lower impact of regulation and loss of customer data.

Impact of third-party incidents actually faced by respondents (% of respondents)



Top third-party related risks ranked in order of criticality

Risk areas	BIPS	CB	E&R	FS	LSHC	MF	PS	TMT
Disruption in customer service due to third-parties	4	3	1	1	4	3	2	6
Breach of regulation or law through third-party action	4	6	3	2	3	3	3	5
Reputational damage arising from third-party behavior	1	4	4	4	1	2	4	3
Breakdown in supply chain due to failure of third-parties	1	2	5	3	1	6	5	4
Financial fraud or exposure created by third-party behavior	6	1	2	5	6	1	6	1
Failure of financial viability of third-party impacting delivery	3	5	6	6	5	5	1	2

Managing third-party risk (cont.)

04 Increased monitoring and assurance activity over third-parties is believed to significantly reduce third-party risk.

Organizations are undertaking a number of key initiatives to address the risks that the increased use of third-parties creates for them. Enhanced monitoring of third-parties appears to be the top initiative in this regard, being taken up by 59.7 percent of respondents. Just over 57 percent of respondents are stepping up their assurance activities over third-parties as their key initiative to reduce third-party risk.

Respondents recognize that stakeholders across various levels and functional areas (for instance, business owners, supply chain teams, and compliance groups) have a role to play in these monitoring and assurance activities. Each of these players brings a unique set of perspectives and skills to risk management, which can be an invaluable asset to the business. In keeping with the principle of the “Three Lines of Defense,” they perceive the need to be able to orchestrate their activities to ensure that there is complete clarity on respective roles and responsibilities. This ensures that limited risk management resources are deployed effectively across the organization to address the most significant areas of concern.

Enhancing the rigor of disciplined contracting, ‘business case articulation and due diligence’ for third-parties are some of the other key risk-reduction initiatives being taken up by 44.5 percent and 38.7 percent of respondents respectively.

59.7 percent of respondents are enhancing their monitoring activities and

57.1 percent are increasing their assurance activities over third-parties as their key initiative to reduce third-party risk.

Risk reduction initiatives taken up by respondents (% of respondents)

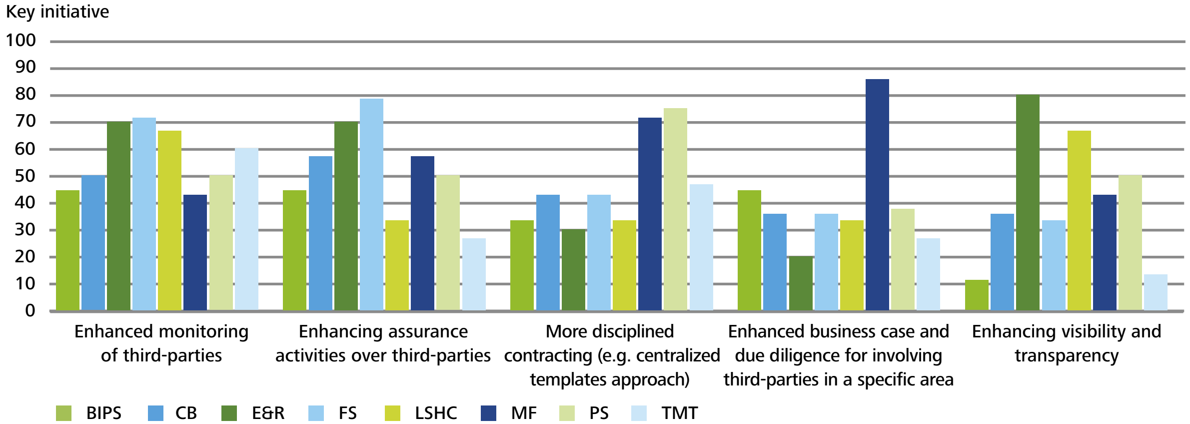
59.7	57.1	44.5	38.7	36.1
Enhanced monitoring of third-parties	Enhancing assurance activities over third-parties	More disciplined contracting (e.g. centralized templates approach)	Enhanced business case and due diligence for involving third-parties in a specific area	Enhancing visibility and transparency

Survey results by industry segment

The survey results indicate that the prioritization of initiatives to reduce third-party risk vary by industry segment. The following industries have prioritized other initiatives over enhanced assurance and monitoring of third-parties:

- Energy and Resources (E&R): Enhancing visibility and transparency (80 percent of respondents)
- Life Sciences & Health Care (LSHC): Enhancing visibility and transparency (66.7 percent of respondents)
- Manufacturing (MF): Enhancing business case and due diligence (85.7 percent of respondents) followed by more disciplined contracting (71.4 percent of respondents)
- Public Sector (PS): More disciplined contracting (75 percent of respondents)
- Technology, Media and Telecommunications (TMT): More disciplined contracting (46.7 percent of respondents)

Key initiatives associated with third-parties (% of respondents)



Deloitte point of view

Deloitte's experience indicates that organizations have been benefiting from assurance and monitoring activities by being able to identify and remediate significant unseen risks such as non-compliance with anti-bribery legislation, lack of appropriate physical and IT security, and over-charging compared to contractual rates (in the range of 3-10 percent of total spend). Only now are organizations expanding their third-party monitoring and assurance activities to cover all risks and all third-party types, having previously focused on a particular type of risk or a sub-section of third-parties.

The organizational clamor for increasing monitoring and assurance-related activities around third-parties demonstrates growing organizational realization that the implementation of controls to manage third-party risks is not a one-time activity. Given the dynamism in the external environment as well as within their extended enterprise, organizations must continually ensure that changing conditions have not made these controls out-of-date. In addition, more and more organizations are starting to appreciate the need to continually evaluate the effectiveness of these controls to reconfirm that they are working effectively, using various monitoring mechanisms.

In particular, the lack of organizational confidence in the tools and technology used for third-party management, resulting in absence of reliable data in this area which is described in a subsequent section of this report, reinforces the need for "other organizational assurance mechanisms" to obtain comfort on third-party management.

Managing third-party risk (cont.)

05 Organizational commitment to third-party risk management is not supported by confidence in the related technology and processes.

Survey respondents have indicated varying levels of organizational confidence in the different domains of TPGRM. Organizational confidence appears to be the highest in the level of awareness of various stakeholders in third-party risk management processes and their commitment to managing third-party risk. Just over 78 percent of respondents have expressed a moderate to high level of confidence in this domain.

Closely related to stakeholder awareness is the clarity with which the ownership of related risk management activities is known to those tasked with the performance and oversight of the framework. As many as 77.9 percent of respondents have expressed a moderate to high level of confidence. This high level of confidence also extends to the organization of third-party risk management as well as the skills, competence, and training of the relevant individuals.

However, higher levels of confidence are not mirrored in the related tools, technology, and processes. For instance, organizational confidence is the lowest in the areas of tools and technology, monitoring mechanisms and the quality of processes to support third-party risk management with as many as 94.3 percent, 93.5 percent, and 88.6 percent respondents respectively expressing moderate to low levels of confidence in these domains.

Organizational confidence appears to be the highest in the awareness and commitment to managing third-party risk, with

78.1 percent of respondents expressing a moderate to high level of confidence in this domain of third-party risk management. However, organizational confidence is the lowest in the areas of tools and technology, monitoring mechanisms and the quality of processes to support third-party risk management, with as many as 94.3 percent, 93.4 percent and 88.6 percent respondents respectively expressing moderate to low levels of confidence in these domains.

Domains of third-party risk management where confidence is moderate to high (% of respondents)

78.1
Awareness and commitment to managing third-party risk

77.9
Clarity of roles and responsibilities

73.9
Skills competence and training

73.2
Organization of third-party risk management

Domains of third-party risk management where confidence is moderate to low (% of respondents)

94.3
Tools and technology used for risk management

93.5
Management and monitoring mechanisms

88.6
Quality of third-party risk management processes

78.9
Disciplined escalation framework

Survey results by industry segment

Analysis of the survey results indicates that there is divergence amongst respondents across industry segments in the TPGRM domains where the survey has revealed an overall higher level of confidence associated with them. For instance, only 50 percent of respondents from PS have moderate to high levels of confidence in the manner in which third-party risk management is organized, the clarity of roles and responsibilities, together with related skills competence and training. This is significantly lower than the other industry segments, implying that PS organization may require stronger levels of accountability amongst its senior officials responsible for third-party risk management. Further, respondents within the BIPS industry segment as well as CB have indicated lower levels of confidence in awareness and commitment around third-party risk management, with only 44.4 percent and 57.1 percent respondents having moderate to high confidence levels respectively.

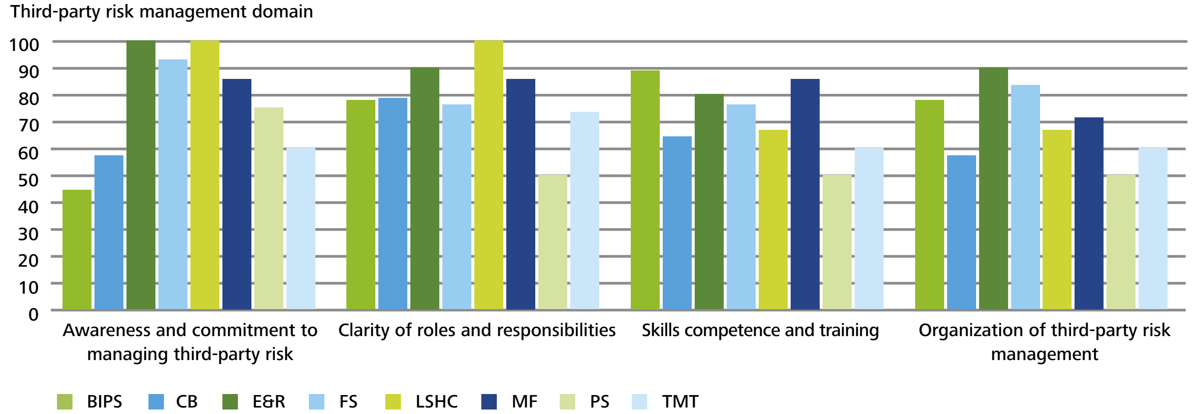
Deloitte point of view

Deloitte perceives an emerging "execution gap" in TPGRM. This gap is the result of organizational commitment not being supported by the ability of the related tools, technology, and processes to achieve intended results.

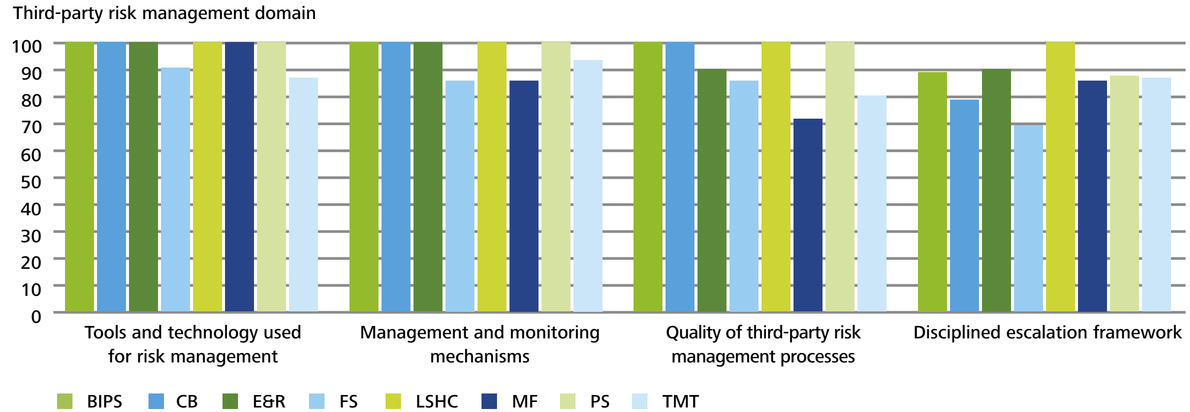
In spite of the overall strategy and governance framework having been put in place in a larger number of respondent organizations, there is more to do in strengthening third-party risk management tools and technology, together with the underlying processes and monitoring mechanisms.

Addressing this execution gap would go a long way in reducing the potential for failure, while augmenting organizational capability to maximize the opportunities from their third-party ecosystem.

Domains of TPGRM where confidence is moderate to high (% of respondents)



Domains of TPGRM where confidence is moderate to low (% of respondents)



Third-party governance

06 Third-party risk is starting to feature consistently on the board agendas with CEO/board-level responsibility in the more progressive organizations or those operating in highly regulated environments.

With the increasing strategic importance of third-parties, the survey demonstrates how TPGRM is rapidly becoming a board and top leadership-level issue. Being viewed for decades as an operational-level issue rather than a board or top leadership issue, this rethinking now presents a transformational opportunity for the more progressive organizations leveraging their extended ecosystem.

The survey reveals that the ultimate accountability for third-party risk management resides in the CEO or member(s) of the board in 46.6 percent of respondents. This is in addition to other members of the C-suite such as the Chief Procurement Officer (CPO), the Chief Risk Officer (CRO), and the Chief Finance Officer (CFO) being ultimately responsible for third-party risk in a further 16.9 percent, 9.3 percent, and 5.1 percent of respondents, respectively.

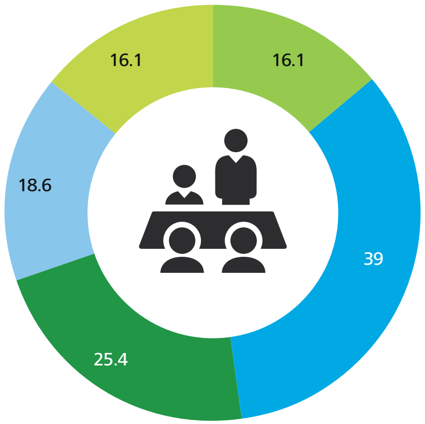
Third-party risk features consistently on the board agenda in 39 percent of respondents with varying levels of urgency, but with critical urgency in a further 16.1 percent of respondent organizations, representing the more progressive organizations and those that operate in highly regulated environments.

However, third-party risk is still discussed reactively in 25.4 percent of respondents, only in response to third-party incidents, while a further 18.6 percent of organizations engage in this boardroom discussion only intermittently, with a low level of importance. This indicates that this transformational thinking is still to make a substantial impact on a number of organizations where regulatory pressures are lower, or in those organizations that are yet to experience the negative consequences of a major third-party-related risk incident.

Third-party risk features consistently on the board agenda in

39 percent of respondents with varying levels of urgency, but with critical urgency in a further 16.1 percent of respondent organization. Ultimate accountability for third-party risk management resides in the CEO or member(s) of the board in 46.6 percent of respondent organization.

Third-party risk on the board agenda (% of respondents)



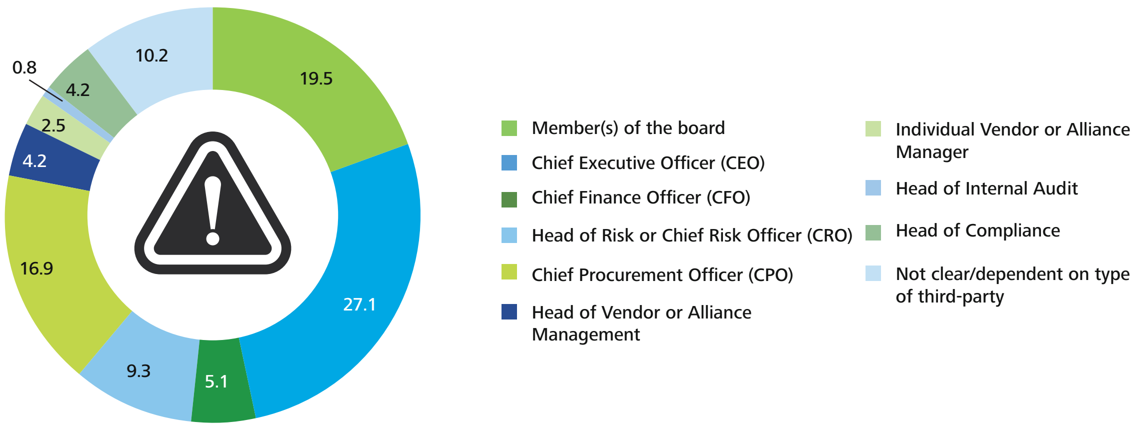
- Features consistently as a critical item on the board agenda
- Periodically on the agenda with varying urgency
- Reactively in the agenda in response to incidents
- Intermittently on board agenda with low importance
- Not on the board agenda

Deloitte point of view

The survey results echo the growing organizational acceptance of the need for enhanced accountability for third-party risk management at their board and the C-suite level to ensure the explicit linkage of risk and strategy in maximizing the opportunities from their third-party ecosystem. Following the financial crisis, key regulators/governance bodies now agree on the board's central role in approving and monitoring strategy, in keeping with their fiduciary duties to shareholders. The board therefore needs to understand the risks and ensure appropriate risk management, which would further enable them to strike a better balance between risk oversight, growth, performance, and strategy.

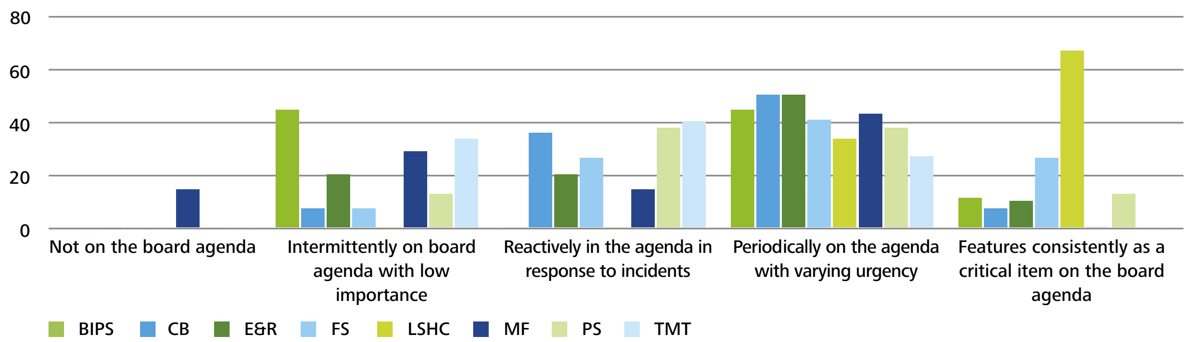
Deloitte further believes that board and C-suite ownership and oversight of TPGRM is critical to be able to exploit the opportunities and manage the risks from third-parties efficiently and effectively. This also facilitates multiple stakeholder buy-in at the functional level.

Level of ultimate accountability for risk management (% of respondents)



The survey results indicate divergence in the MF and BIPS industry segments where a significantly large proportion of respondents do not have third-party risk management featuring in their board agenda at all or only intermittently (MF 42.9 percent of respondents in total; BIPS 44.4 percent). On the other hand, the LSHC industry segment appears to have third-party risk featuring most consistently as a critical item on the board agenda with 66.7 percent of respondents in this category.

Third-party risk on the board agenda (% of respondents)



Third-party governance (cont.)

07 Visits to third-party locations are considered the most effective method to gain assurance over third-party management.

The survey reveals that respondents obtain assurance over third-party management activities through a combination of methods, some of which are more popular or effective compared to others.

Visiting third-party locations periodically based on risk assessments appears to be the most popular method for gaining assurance over third-party management activities, with 69.5 percent of respondents making such on-site visits.

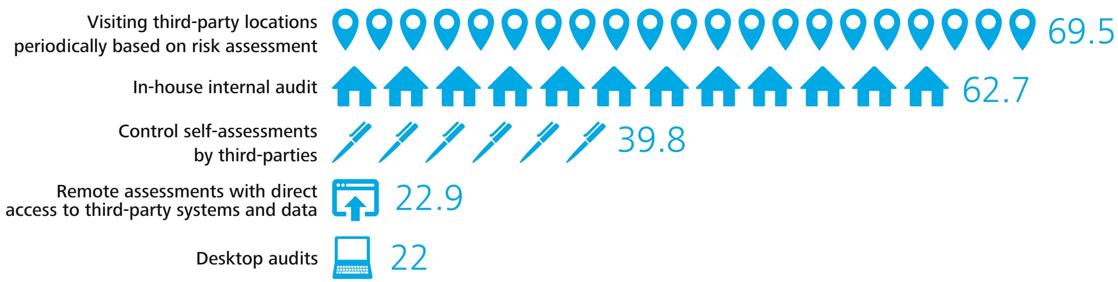
In-house internal audit reviews represent the second most popular and effective method of gaining third-party assurance, practiced by 62.7 percent of respondent organizations. In addition, controls self-assessments by third-parties, remote assessments with direct access to third-party systems/data, and desktop audits represent the other key assurance methods, although not considered as effective as on-site reviews or in-house internal audit procedures.

Use of contractors or outsourced internal audit providers to perform third-party audits are is also rapidly gaining popularity as effective methods for obtaining assurance over third-party management.

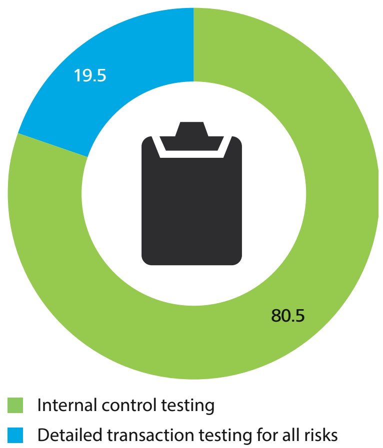
Some respondents have expressed their dependence on external audits and service provider audits under SSAE16/ISAE3402 standards. However, most of these audits cover the risk of material financial statement misstatements only and may not address the wider set of strategic, operational, reputational, legal, and regulatory risks that a best-in-class framework should holistically and proactively address. They may also not cover the specific obligations contained in organizations contracts with its third-parties.

69.5 percent of respondents periodically visit third-party locations based on risk assessment as the most effective way of gaining assurance over third-parties. However, internal controls testing drives the approach to such assurance in the vast majority of cases (80.5 percent) with the other 19.5 percent driving their approach through detailed transaction testing.

Most effective methods of gaining assurance over third-party management (% of respondents)



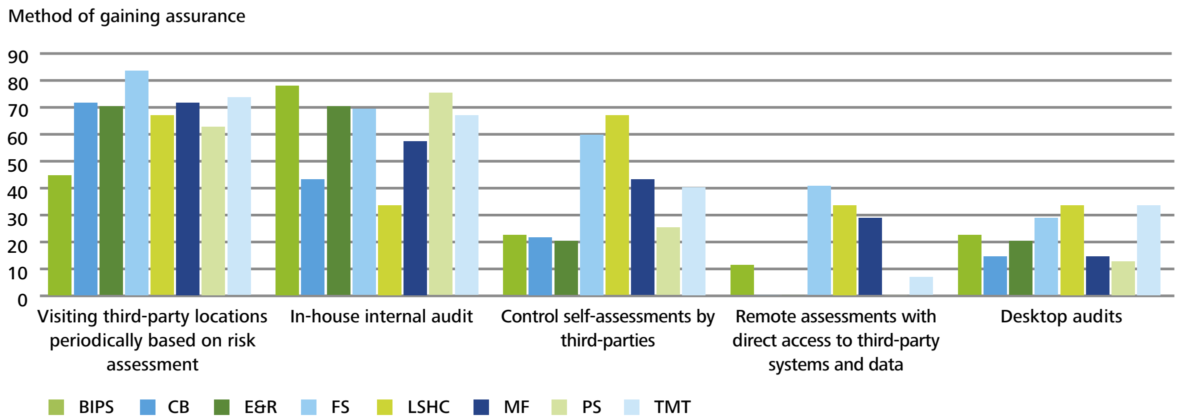
What drives the approach to on-site third-party reviews? (% of respondents)



Survey results by industry segment

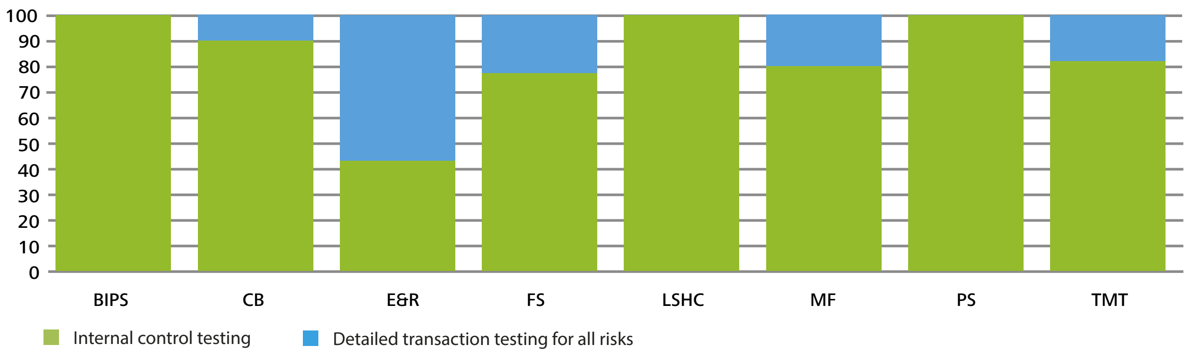
There is a fair degree of consistency in the methods of gaining assurance on third-party activity across the industry segments, all of whom rely heavily on risk-based visits to third-party locations as well as in internal audit procedures, as indicated below:

Dominant methods of gaining assurance over third-party management (% of respondents)



During these periodic risk-based on-site reviews, the proportion of respondents relying on internal controls testing, rather than detailed transaction testing across all risks is the highest in BIPS, LSHC, and PS where the level of detailed transaction testing appears to be insignificant, with the sole focus being on internal controls. On the other hand, E&R organization seem to be doing the most detailed transaction testing, with 57.1 percent of respondents adopting this approach.

What drives the approach to on-site third-party reviews? (% of respondents)



Deloitte point of view

Deloitte's experience in the area of TPGRM indicates that the growing complexity of third-party risks requires a holistic and deep understanding across a diverse group of organizational stakeholders, as well as disparate groups of third-parties in the extended enterprise. This results in the utilization of a combination of methods for gaining assurance over third-party management, striking a balance between efficiency and effectiveness. Visits to third-party locations is identified by respondents as being the most effective method of gaining assurance, further recognizing the relational impact that this creates.

However, it is interesting to note that internal controls testing drives the approach to on-site third-party reviews in more than 80 percent of cases, with detailed transaction testing for all risks driving the approach in less than 20 percent of cases. There is clearly room for improvement here to adopt a review approach, based on increasing the extent of detailed transaction testing supported by available data that would significantly improve the quality of assurance obtained. Deloitte specialists believe that reversing the mix with 20 percent of controls testing and 80 percent of transaction testing should be the benchmark that organizations should strive to attain in this area. This would provide evidence based assurance around the operating effectiveness of a control as opposed to relying on an assessment of it's design.

Third-party governance (cont.)

08 Most organizations are mandating consistent third-party governance standards amidst increasing decentralization of operating units.

A decentralized organization is one where the decision-making authority does not vest in a central group or individual, but is dispersed across business units and divisions to achieve divisional flexibility with which to react to local environmental and operational contingencies.

The survey confirms that global organizations are increasingly being managed through degrees of decentralization across their various operating units and entities. Nearly 76 percent of respondents today have a partial through to a high degree of decentralization, reflecting a potential challenge to a holistic and unified approach to third-party risk management.

As many as 86 percent of respondents mandate common third-party standards to ensure a consistent approach to third-party risk management across decentralized and often diverse business units.

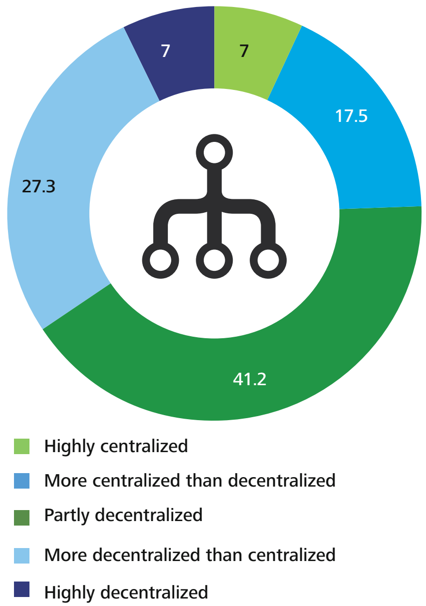
The survey also reveals that the general trend is to have a combined approach to formulating these standards, representing a mix of existing industry-specific (e.g. HIPAA standards for safeguarding of personal identifiable or private information for patient data handled or managed by third-party service providers) or generally accepted functional standards (ISO 22301 standard for business continuity in relation to business processes operated by third-parties), supplemented by organization-specific standards particularly in those areas where no such generally accepted standards exist.

Respondents have also indicated that the domains covered by these third-party standards are continually expanding and extending to areas such as code of conduct and ethics, regulatory compliance, minimum wage requirements, information security, and privacy etc.

75.5 percent of respondents today have a partial through to a high degree of decentralization, reflecting a potential challenge to a holistic and unified approach to third-party risk management.

86 percent (However, the vast majority of these organization) mandate common third-party standards to ensure a consistent approach across business units.

Increasing degree of decentralization in respondent organizations (% of respondents)



Mandating third-party standards (% of respondents)

Survey results by industry segment

The degree of decentralization appears to be the highest in the following industries. A high proportion of respondents in these industries consider their organization to be more decentralized than centralized or to be highly decentralized:

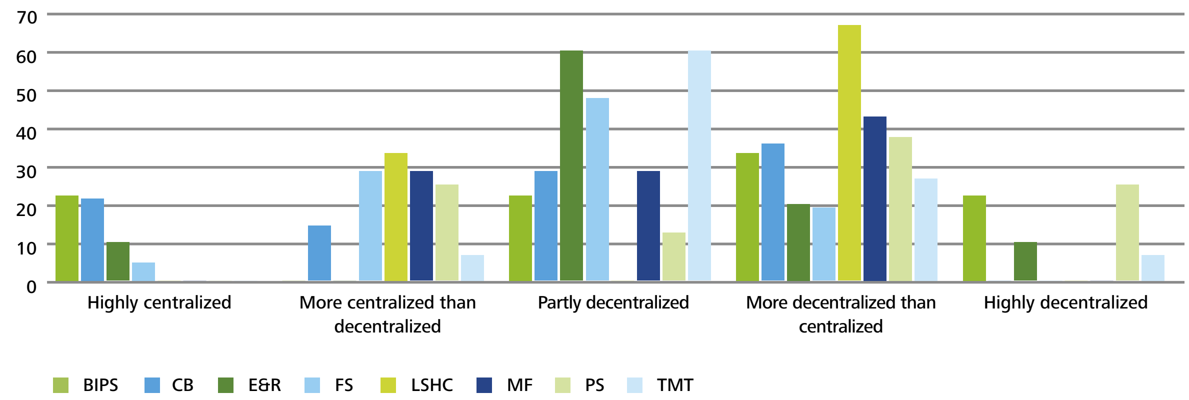
- Life Sciences and Health Care (LSHC): 66.7 percent of respondents
- Public Sector (PS): 62.5 percent of respondents
- Business Infrastructure and Professional Services (BIPS): 55.6 percent of respondents
- Manufacturing (MF): 42.9 percent of respondents

We do however, see consistency across all industry sectors in the way that organization mandate third-party standards to be applied across all business units and divisions.

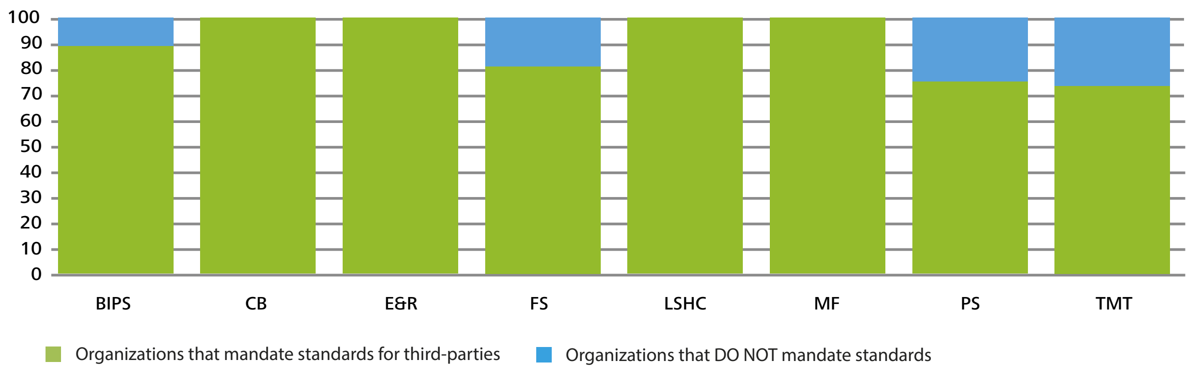
Deloitte point of view

Third-party governance and risk management is clearly evolving as a crucial organization-wide matter that cannot be left to the discretion of a divergent group of operational-level personnel in the multiple divisions of an institution that operates with a moderate to a higher level of decentralization. The survey results portray organizational response to maintain a holistic and unified approach to TPGRM through a consistent framework reinforced through the mandating of common third-party standards across a widening set of domains.

Increasing degree of decentralization in respondent organizations (% of respondents)



Mandating third-party standards (% of respondents)



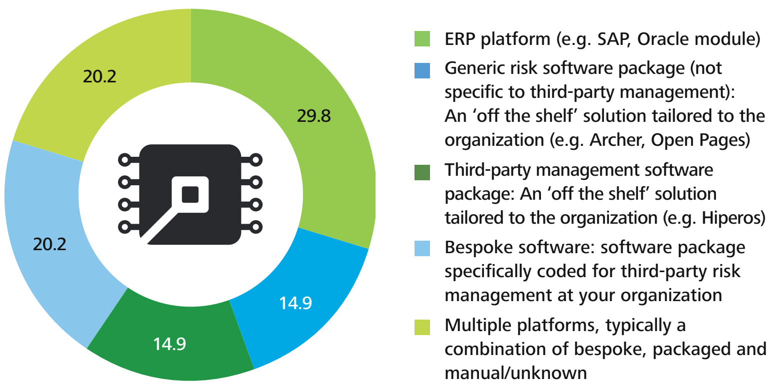
Technology and delivery models

09 Existing technology platforms for managing third-parties are considered inadequate.

Organizational confidence in tools and technology is the lowest across all the domains of third-party risk management, with 56.1 percent respondents rating their confidence level as low and another 38.2 percent respondents rating their level of confidence as moderate.

The survey provides further insight that there is no clear dominance of a particular type of technology or tool that respondents use for third-party risk management. While 29.8 percent of respondents utilize their enterprise resource planning (ERP) platform for third-party risk management, the remaining 70.2 percent represent a range of solutions including bespoke solutions, generic and third-party specific risk management software, and a combination of multiple systems, together with manual processes and spreadsheets. In many cases, respondents are challenged by the absence of organizational integration of the multitude of tools and technologies that may be used to manage different aspects of third-party risk, or even different types of third-parties across various parts of a large global organization, operating with a partial or high degree of decentralization.

Technology platforms used for third-party management (% of respondents)



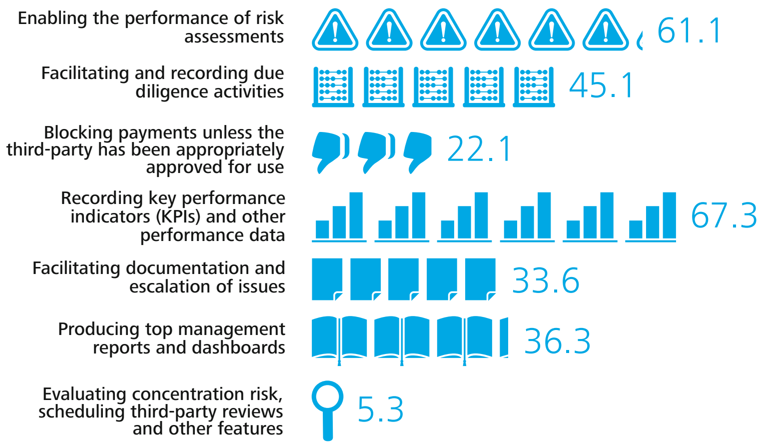
Confidence in tools and technology is the lowest across all the domains of third-party risk management, with

56.1 percent respondents rating their confidence level as low and another 38.2 percent respondents rating their confidence as moderate.

29.8 percent of respondents utilize their enterprise resource planning (ERP) platform for third-party risk management while the remaining 70.2 percent represent a range of solutions, including bespoke solutions, generic and third-party specific risk management software, and a combination of multiple systems, together with manual processes and spreadsheets.

Respondents are united in their desire for an integrated set of tools that would address as many of the dimensions of third-party risk management as possible.

Desired functionality of third-party software (% of respondents)



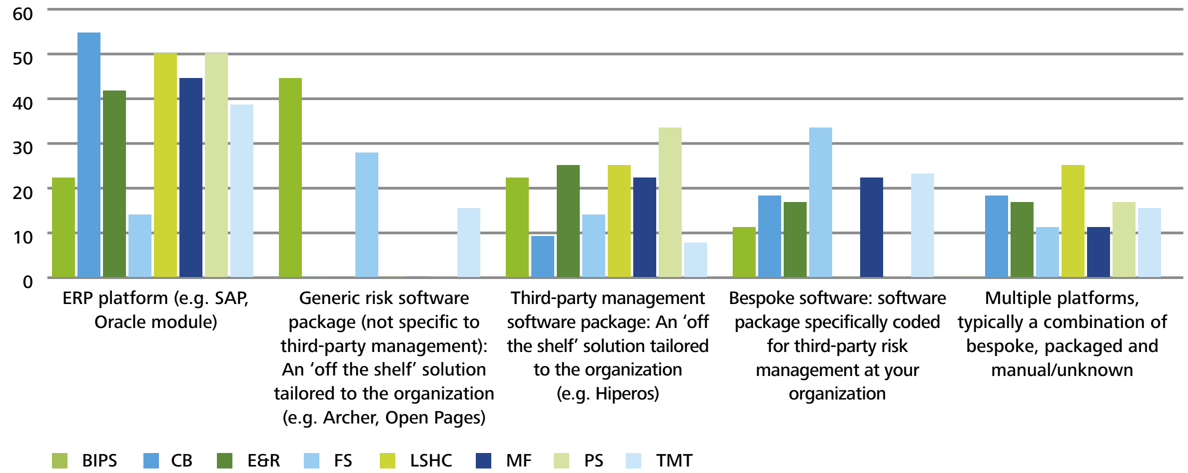
Survey results by industry segment

The results of the survey indicate a range of tool and technology solutions in use across all the industry segments, although generic risk management software platforms do not appear to be popular in CB, E&R, LSHC, MF, and PS as tools to help manage third-party risk.

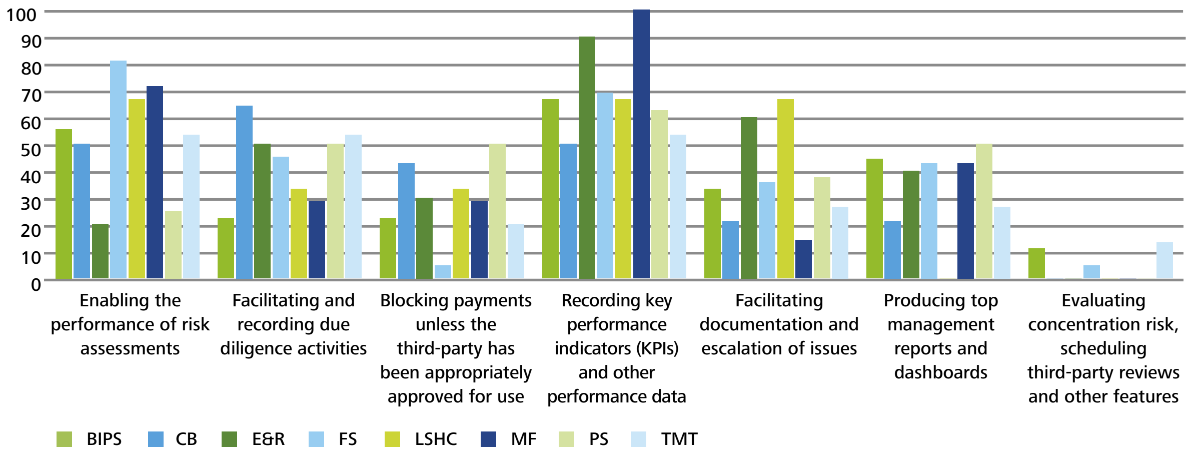
Deloitte point of view

There is no doubt that the lower level of organizational confidence in the tools and technology for TPGRM creates a burning platform to be addressed with urgency. The inadequacy of tools and technology reduces the effectiveness of reliable and timely data, adversely impacting organizational ability to make appropriate risk-informed decisions, as well as being able to implement optimized processes tailored to the type of product or service being outsourced. Deloitte's experience indicates that appropriate tools and technology can significantly reduce pre-contract, post-contract, and ongoing tracking/monitoring activities, thus making available time for risk management personnel to complete their third-party risk management activities timely and effectively.

Technology platforms used for third-party management (% of respondents)



Key software functionality (% of respondents)



Technology and delivery models (cont.)

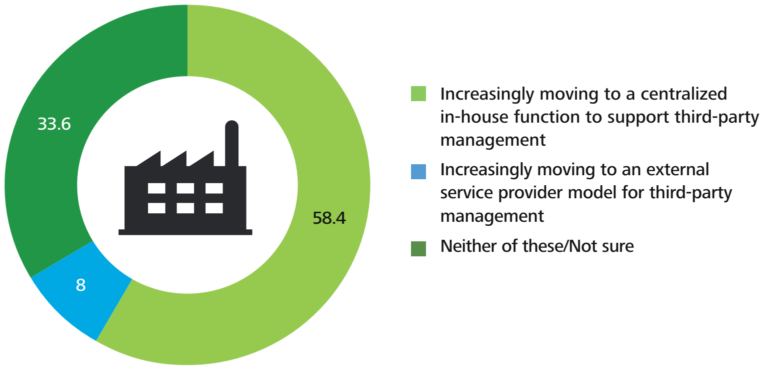
10 Organizations are in the process of deciding between centralized in-house models and external service-provider based models for third-party monitoring.

Establishing a centralized in-house function for third-party management seems to be the approach that the majority of respondents are adopting, with 58.4 percent of respondents in this category. It is expected that this centralized function would cover most of the key activities related to third-party management including on-going risk assessments (80.3 percent); third-party monitoring activities (80.3 percent) and co-ordination (56.1 percent); tracking remediation activities (57.6 percent) and on-going monitoring requirements (50 percent). It would also be responsible for various administrative activities such as filing of contracts and amendments (48.5 percent), archiving evidence related to third-party management (33.3 percent), and would assist in the implementation of third-party contract termination plans (25.8 percent).

There is a perception among some respondents that in-house models can adapt better to the needs of larger global organizations, particularly where diverse operating groups are involved, with varying degrees of decentralization.

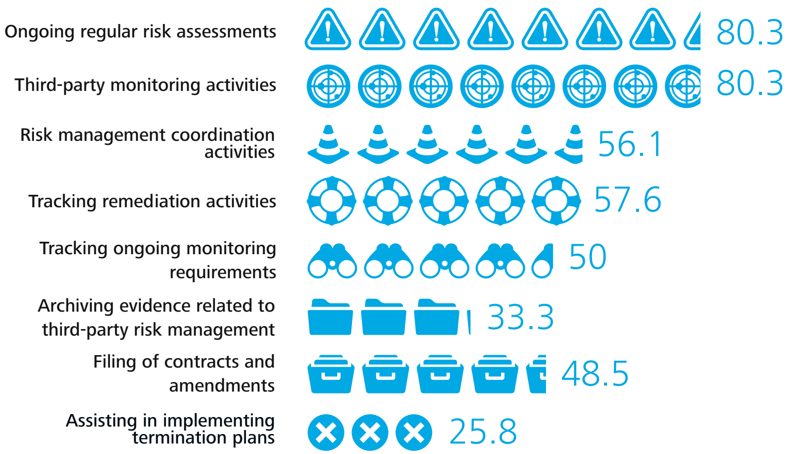
It should also be noted that as many as many as 33.6 percent of respondents are not yet clear on the future organizational choice of an in-house vs. an external service-provider model.

Organizations considering in-house vs. external service-provider based third-party risk management models (% of respondents)



While **58.4** percent of respondents are progressively moving to a centralized in-house function to support third-party risk management, as many as 33.6 percent of respondents are not clear on the future organizational choice of an in-house vs. an external service-provider model.

Expected functions of centralized in-house risk management team (% of respondents)



Survey results by industry segment

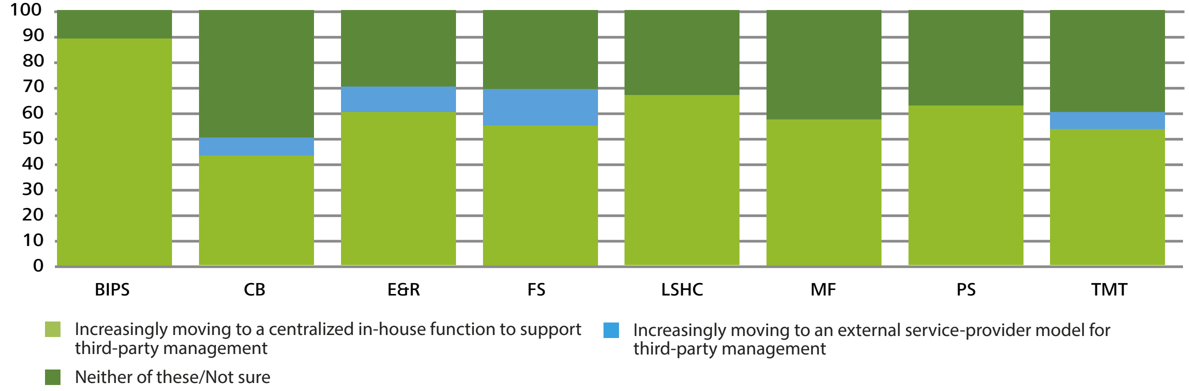
The preference for moving to a centralized in-house function for third-party risk management rather than to an external service-provider appears to be consistently higher across all industry segments as revealed by the following data. However, a very large proportion of respondents are undecided on this decision in the CB, MF, TMT, and PS industries with as many as 50 percent, 42.9 percent, 40 percent, and 37.5 percent of respondents in this category.

Deloitte point of view

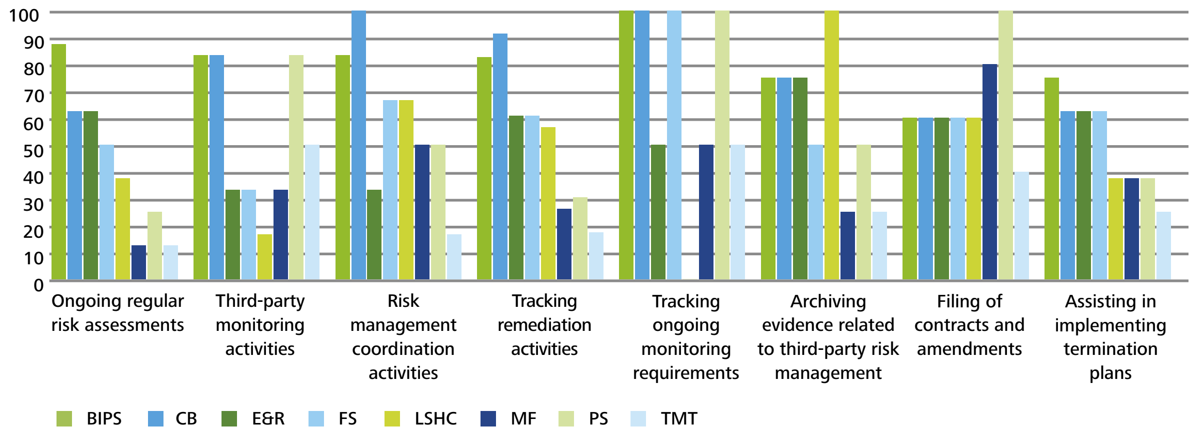
The choice between a centralized in-house model for TPGRM versus an external service-provider based model is a vital decision that can have far-reaching strategic consequences which need to be carefully considered and not undertaken recklessly. Deloitte believes that organizations moving to a centralized in-house function in this regard are primarily driven by the need to retain organizational control over this critical activity. This is enhanced by a better organizational understanding as well as the ability to manage a diverse group of stakeholders that an external provider may be unable to match.

Deloitte's experience further indicates that lack of understanding of their third-party ecosystem; together with inadequate knowledge of the marketplace of external providers, may be resulting in a significant proportion of organizations remaining undecided in this matter, although many of them are already working with contract staff to assist them in the related tasks.

Organizations considering in-house vs. external service-provider based third-party risk management models (% of respondents)



Expected functions of centralized in-house risk management team (% of respondents)



About the authors

Kristian Park, DTTL, Global Third-party Governance and Risk Management Leader
Kristian co-leads Deloitte's Global Third-party Governance and Risk Management team as well as the Contract Risk & Compliance team in the Europe, Middle East, and Africa region, helping clients with third-party risk, supply chain risk, and contract risk. He has worked across all industry sectors, from Life Sciences, Financial Services, Energy, Sports, Technology, Media and Telecommunications, and Consumer Business. As a UK based partner, Kristian focuses on Third-party Governance & Risk Management, working with clients to develop governance frameworks to identify and manage all types of third-party risks, looking at both process and technology solutions; performing inspections of third-party business partners on behalf of a client; and assessing third-party compliance with contractual terms and conditions. In addition, Kristian is responsible for Deloitte's UK Software Asset Management and Software Licensing teams and assists clients manage their software licensing obligations – driving efficiencies and savings.

Sanjoy Sen is a Doctoral Research Scholar at Aston Business School, UK, specializing in strategic governance related to third-party risk, having earlier worked as a partner at Deloitte and another global professional services firm. He has over 26 years of experience in risk and governance in the UK, Gibraltar, and various countries in the Middle East and in India. This includes assisting clients in strengthening their corporate governance mechanisms, establishing enterprise wide risk management frameworks to support governance mechanisms, and reviewing/addressing specific business and technology risks.

Global third-party governance & risk management contacts

Global third-party governance and risk management contact			
Kristian Park		krpark@deloitte.co.uk	+44 20 7303 4110
Regional contacts			
Americas	Kristina Davis	kbdavis@deloitte.com	+1 617 437 2648
APAC	Jimmy Wu	jimwu@deloitte.com.tw	+886(2)25459988
	Jansen Yap	jansonyap@deloitte.com	+65 6216 3119
EMEA	Kristian Park	krpark@deloitte.co.uk	+44 20 7303 4110
	Jan Corstens	jcorstens@deloitte.com	+3 22 800 2439
Country contacts			
EMEA			
Austria	Alexander Ruzicka	aruzicka@deloitte.com	+43 1 537 00 3701
Belgium	Jan Corstens	jcorstens@deloitte.com	+3 22 800 2439
Croatia	Ivica Perica	iperica@deloittece.com	+385 (91) 6778 091
Denmark	Thomas Brun	tbrun@deloitte.dk	+4 53 610 3571
Finland	Katariina Perkkio	kperkkio@deloitte.com	+35 820 755 5301
France	Marc Duchevet	mduchevet@deloitte.fr	+33 6 77 38 24 81
Germany	Andreas Herzig	aherzig@deloitte.com	+49 711 165 5460
Greece	Alithia Diakatos	adiakatos@deloitte.gr	+302106781100
Hungary	Zoltan Szollosi	zszollosi@deloittece.com	+36 (20) 910 7644
Ireland	Eileen Healy	ehealy@deloitte.ie	+353 214 907 074
Italy	Andrea Musazzi	amusazzi@deloitte.it	+39 3466805017
Luxembourg	Jan Corstens	jcorstens@deloitte.com	+3 22 800 2439
Netherlands	Jina Calmaz	JCalmaz@deloitte.nl	+31882881871
Portugal	Joao Frade	jfrade@deloitte.pt	+351 966304388
	Miguel Cunha	micunha@deloitte.pt	+351 962744629
Southern Africa	Justine Mazzocco	jmazzocco@deloitte.co.za	+27825507521
Spain	Oscar Martín	omartinmoraleda@deloitte.es	+34 914432660
Sweden	Michael Bernhardtz	mbernhardtz@deloitte.se	+46 73-397 10 66
Switzerland	Philipp Lanz	planz@deloitte.ch	+41 44 42 16 469
Turkey	Cuneyt Kirlar	ckirlar@deloitte.com	+90 533 281 98 49

United Kingdom	Kristian Park	krpark@deloitte.co.uk	+44 20 7303 4110
	Mark Bethell	mabethell@deloitte.co.uk	+44 20 7007 5913

Asia Pacific			
Australia	Brian Bogardus	bbogardus@deloitte.com.au	+61 2 9322 7049
China	Yvonne Wu	yvwu@deloitte.com.cn	+862161411570
Hong Kong	Hugh Gozzard	huggozzard@deloitte.com.hk	+ (852) 97461695
India	Porus Doctor	podoctor@deloitte.com	+91 9820069949
Japan	Masahiko Sugiyama	masahiko.sugiyama @tohmatsu.co.jp	09 09 809 6885
	Bruce Kikunaga	bruce.kikunaga@tohmatsu.co.jp	+819083477656
Korea	Min Youn Edward Cho	minycho@deloitte.com	+82-10-6361-2728
New Zealand	Aloysius Teh	ateh@deloitte.co.nz	64 21 544628
Philippines	Luisito Amper	lamper@deloitte.com	
Taiwan	Jimmy Wu	jimwu@deloitte.com.tw	+886(2)25459988
Singapore	Victor Keong	vkeong@deloitte.com	+6562248288
Indonesia	Deddy Setiady Koesmana	dkoesmana@deloitte.com	+62 21 29923100 x33555
Malaysia	Sin May Wong	sinwong@deloitte.com	+6012 212 6181
Thailand	Weerapong Krisadawat	wkrisadawat@deloitte.com	+66 26765700 x11706
Vietnam	Philip Chong	pchong@deloitte.com	+6562163113
Americas			
Argentina	Martin Carmuega	mcarmuega@deloitte.com	+54 11 4320 4003
Brazil	Patricia Muricy	pmuricy@deloitte.com	+55 21 3981 0526
Canada	Timothy Scott	tiscott@deloitte.ca	+1 416 643 8702
Chile	Christian Duran	chrduran@deloitte.com	+1 (562) 729-8286
LATCO	Maria Gabriela Castro	marcastro@deloitte.com	+58 212 2068570
	Esteban Enderle	eenderle@deloitte.com	+54 11 43202700
Mexico	Gema Moreno Vega	gmorenovega@deloittemx.com	+52 555 080 6324
United States	Walter Hoogmoed	whoogmoed@deloitte.com	+1 973 602 6517