Deloitte.

The threats are real

Third Party Governance and Risk Management

Contents

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 organisations 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 organisations, 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 organisations 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 organisations. 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)
- Healthcare & Life Sciences (HLS)
- Business, Infrastructure and Professional Services (BIPS)

The majority of these organisations had annual revenues in excess of US$1 billion (approximately R14 billion). Additional insight was also obtained from subsidiaries of group organisations with some degree of decentralisation around third party management and others with lower annual revenues.

We hope this report will enable you to enhance your understanding of organisational 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 decentralisation and autonomy of operating units in organisations, disruptive technology and globalisation. 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 organisation.

1. Executive summary

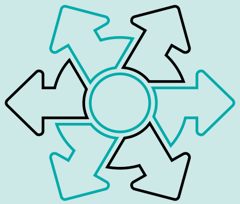
TPGRM is emerging as a board level focus area for many organisations in 2016. The survey results show how investment by organisations in TPGRM has increased year-on-year and that organisations are now in the process of either implementing or refining the existing implementation of TPGRM processes and 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 organisational commitment to managing third party risk achieves the intended objectives.

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

Third party ecosystem
The emerging strategic perspective, together with the severity of consequences of third party related incidents, is compelling organisations to swiftly "catch-up" in upgrading the maturity of their TPGRM processes – to create, as well as to protect, organisational 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 specialised skills and knowledge, innovation, process-improvement and other sources of sustainable competitive advantage) are now motivating organisations 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% of respondents feel that flexibility and scalability will be the top emerging driver for third party engagement.

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

Managing third party risk

As incidents relating to third parties continue to rise, organisations 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 decentralisation of operating units in organisations is starting to create challenges to a unified and consistent approach to TPGRM, driving organisations to mandate consistent third party management standards across their operating units and aspiring to increase their monitoring and assurance activities over third parties.

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

28% faced major disruption and...

11% 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 organisations, supported by increasing organisational 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 organisational commitment and high level governance framework.

Mind the execution gap

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

Delivery models

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

To in-source or outsource TPGRM?

58.4% of respondents are increasingly moving to a centralised in-house function to support third party management with only 8% to external provider-based models while as many as 33.6% 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 realised this has compromised organisational reputation, broken down business continuity and even attracted substantial penalties and regulatory enforcement action.

The threats are real

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

86.0% of respondents now mandate consistent third party standards across their operating units to manage these threats.

2. Key findings

The third party ecosystem

1. As dependence on third parties becomes increasingly critical, organisations 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 organisational 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. Organisational 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 organisations 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 organisations are mandating consistent third party governance standards amidst increasing decentralisation of operating units.

Technology and delivery models

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

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

3. The third party ecosystem

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

The survey demonstrates how organisations continue to rapidly enhance their dependence on global third party ecosystems (extended enterprise) to garner the benefits of collaboration. 73.9% of respondents believe that third parties will play a highly important (44.8%) or critical (29.1%) role in the year ahead, up from 60.3% a year ago.

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

1. Organisations 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.

2. 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".

3. 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".

4. The dependence on individual third parties will further increase as organisations 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% of respondents had integrated or optimised their TPGRM systems a year ago. The survey confirms that organisations are now being compelled to rapidly "catch-up" in taking a holistic and proactive approach to third party risk; 71.6% of respondents expect to be able to integrate and optimise their third party risk management system, including 16.5% of respondents aspiring to be "best-in-class" in a year or more.

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

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

Deloitte point of view

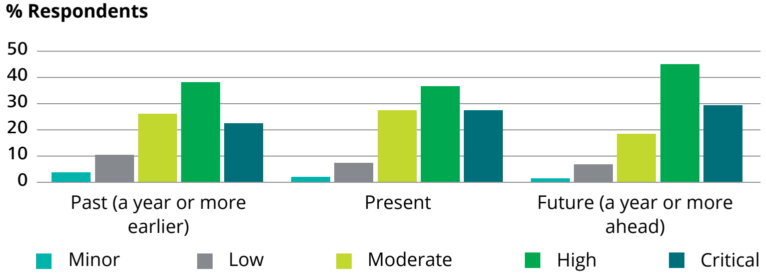
Organisational focus on third party risk has traditionally been reactive and dependent upon who is driving the activity. This has typically been procurement teams focused on suppliers and vendors, or brand and intellectual property (IP) protection functions focused on distribution channels and non-authorised manufacturers. Such a decentralised 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).

Organisations 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 organisational value. This covers all categories of third parties and all areas of risk, considering *operational risk* factors (e.g. performance, quality standards, delivery times, KPI/SLA measurement) with *reputational/financial risk* factors (e.g. labour 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 and Health & Safety compliance).

Deloitte recommends that organisations 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.

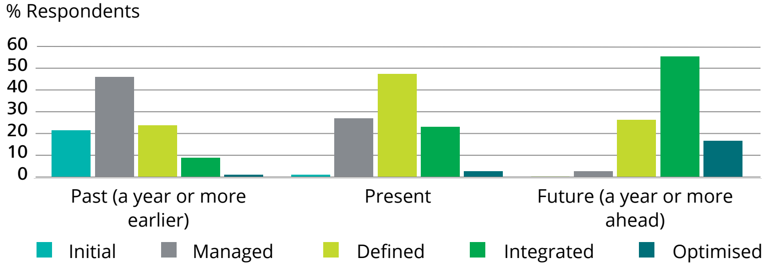
In addition, Deloitte specialists, who have significant experience of working with organisations undergoing similar transformations, consider respondent aspirations to be optimistic in their estimation of the time and effort required to achieve this organisational transformation. Given the diverse range of stakeholders, processes and technology impacted by this transformation, respondent organisations 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 programmes 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



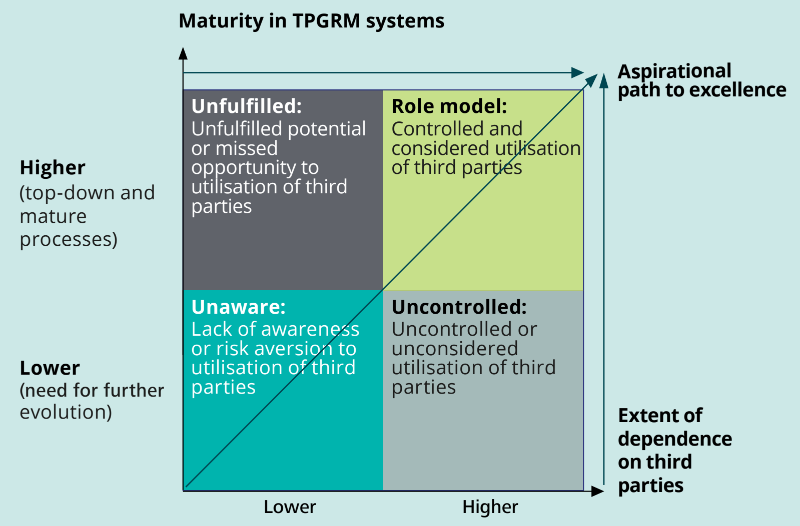
Maturity level definition:
Respondents rated the maturity of their organisation's approach to third party risk management based on the following elements:
- Structure of third party management organisation;
- Clarity of related roles and responsibilities;
- Stakeholder awareness and commitment to third 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.
Optimised: "Best in class" organisation – all of the elements addressed and evolved.

Treading the Aspirational Path to Excellence (by industry segment):

The survey reveals that organisations across the eight major industry segments are adopting varying stances in the extent of dependence on third parties, along a continuum ranging from a 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 organisations, grouped by industry segment, can be mapped to a two-by-two grid in the figure right. This grid can be used by organisations 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 maximise the opportunities through the third party ecosystem, while managing the related risks.

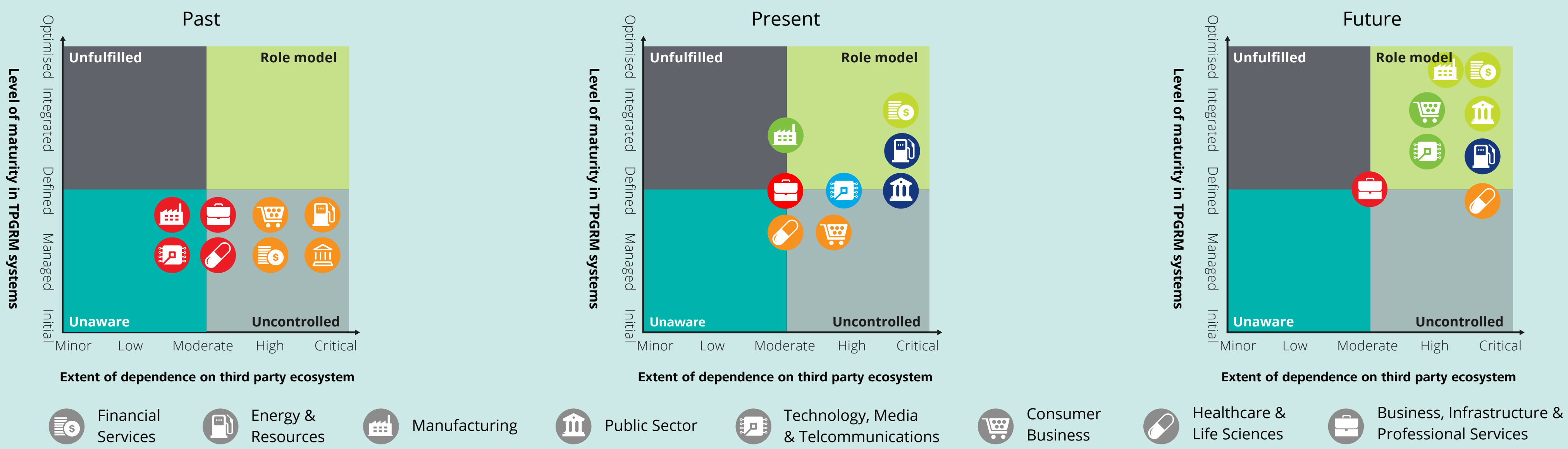


Dependance on third party ecosystem								
	BIPS	Consumer Business	E&R	FS	HLS	Manufacturing	TMT	Public Sector
Past	Moderate	High	Critical	High	Moderate	Moderate	Moderate	Critical
Present	Moderate	High	Critical	Critical	Moderate	Moderate	High	Critical
Future	Moderate	High	Critical	Critical	Critical	Critical	High	Critical

Level of maturity in TPGRM systems								
	BIPS	Consumer Business	E&R	FS	HLS	Manufacturing	TMT	Public Sector
Past	Managed	Managed	Managed	Managed	Managed	Managed	Managed	Managed
Present	Defined	Managed	Defined	Integrated	Managed	Integrated	Defined	Defined
Future	Defined	Integrated	Integrated	Optimised	Defined	Optimised	Integrated	Optimised

The Role Models: the "best-in-class" organisations 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 organisations 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 organisations would therefore be the best positioned to maximise the opportunities arising from the use of third parties as a valuable organisational asset. It is likely that these organisations 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 organisations 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 organisations are likely to face the greatest potential challenges to erosion of organisational value. Accordingly, they can be classed as the ***unaware;*** those who are likely to experience erosion in their profitability and organisational value which may threaten eventual survival. For such organisations 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 organisational value.

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

Organisations that have a higher dependence on third parties in their aspiration for higher organisational 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, organisations that will continually remain ***ufulfilled*** 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 10.

As can be seen, organisations across all the industry segments are treading this aspirational path of excellence, some quicker than others, with those in the Business and Professional Services (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 drivers for third party engagement are progressively shifting from a focus on cost to a focus on value, reflecting organisational recognition of the strategic opportunity that third parties can create for them.

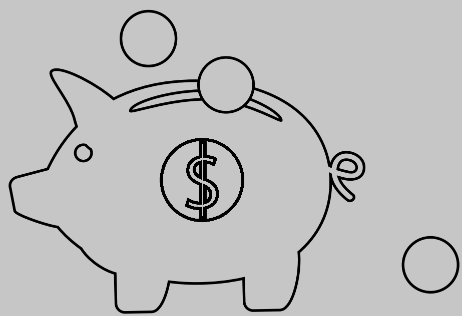
The survey reconfirms how new and emerging strategic drivers for third party engagement such as strategic agility, competitive advantage, innovation and performance improvement, are being focused upon to enhance organisational value.

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% of respondents consider this to be a key future driver, down from 57.1% a year ago.

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

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

With regard to services provided by the third party ecosystem, as many as 20.5% 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 9.0% a year ago. In addition, 21.8% of respondents expect third parties to be a source of competitive advantage (up from 10.3% a year ago).

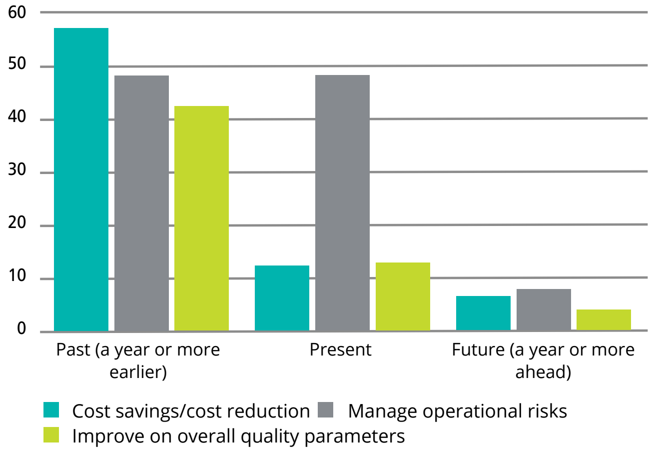


Cost savings/cost reduction is rapidly losing its dominance as the most significant traditional driver for third party engagement with only 42.3% of respondents considering it a key future driver, down from 57.1% a year ago.

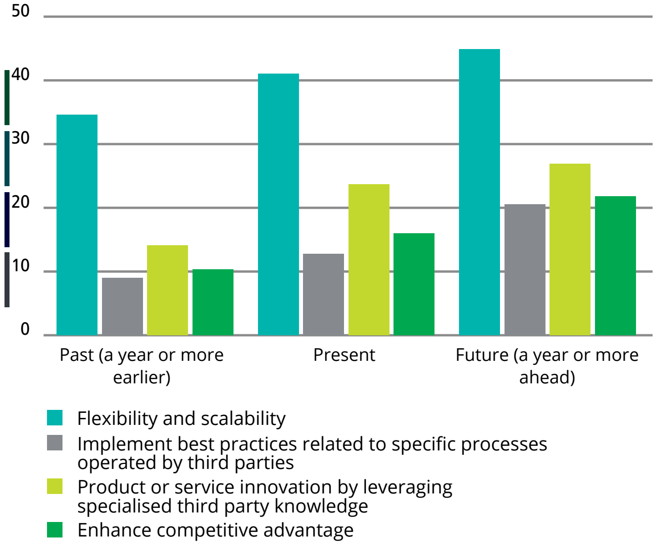
44.9% see the need for organisational agility characterised by flexibility and scalability (up from 34.6% a year ago) to be the strongest emerging value-driver for future third party engagement.

Changing drivers for third party engagement

Traditional drivers
% of Respondents



Emerging drivers
% of Respondents



Deloitte point of view

The increasing recognition of the strategic opportunity that third parties can create for organisations resonates with Deloitte's experience that effectively governed third party relationships can be a significant source of organisational 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 organisations are now able to effectively benefit from third parties as their knowledge partners, or even as trusted advisors, to catalyse organisational innovation, provide strategic insights and feature on organisational advisory boards.

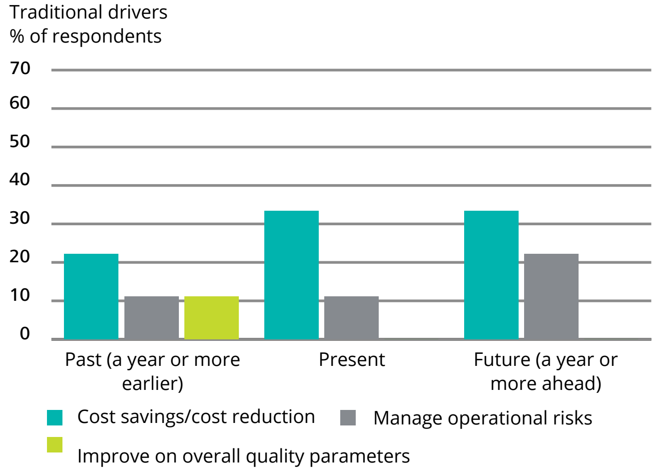
Deloitte believes those organisations that have a good handle on their third party business partners, can not only avoid the punitive costs and reputational damage, but stand to gain competitive advantage over their peers out performing them by an additional 4-5% ROE (which, in the case of Fortune 500 or FT500 companies can mean additional EBITA in the range of US$ 25-500 million: R350 million-R7 billion). 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.

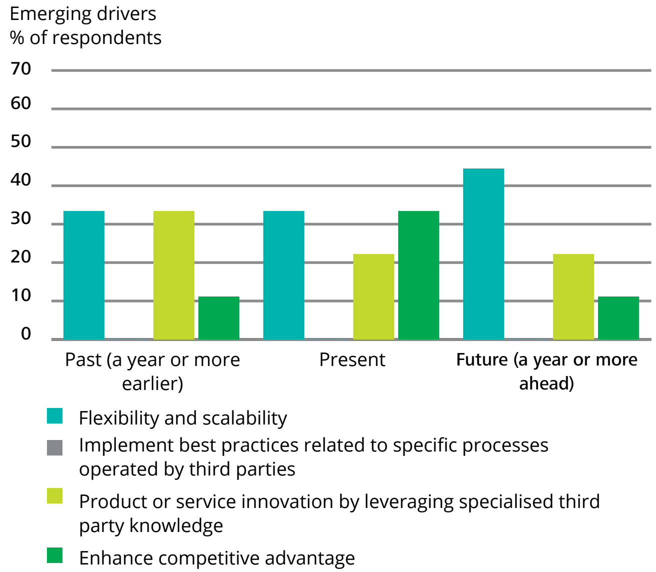
Survey results by industry segment

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 Consumer Business segment, with 57.1% of respondents focused on cost savings a year or more ahead rapidly decreasing to 28.6% a year or more ahead. On the other hand, organisations in the Business, Infrastructure and Professional Services (BIPS) segment aspire to continue to increase their focus on cost savings (22.2% of respondents a year or more ago to 33.3% a year or more ahead).

Changing drivers for third party engagement (% of respondents)

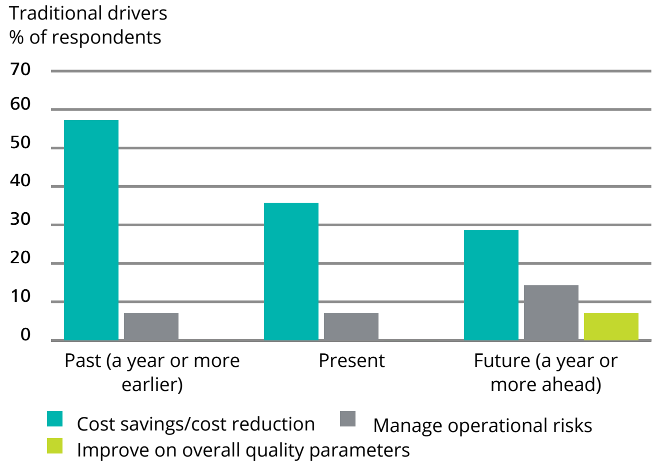
BIPS

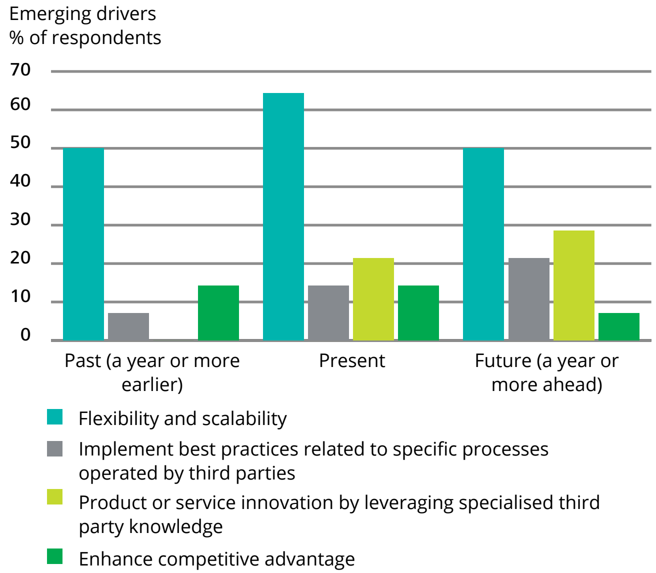




Changing drivers for third party engagement (% of respondents)

Consumer business



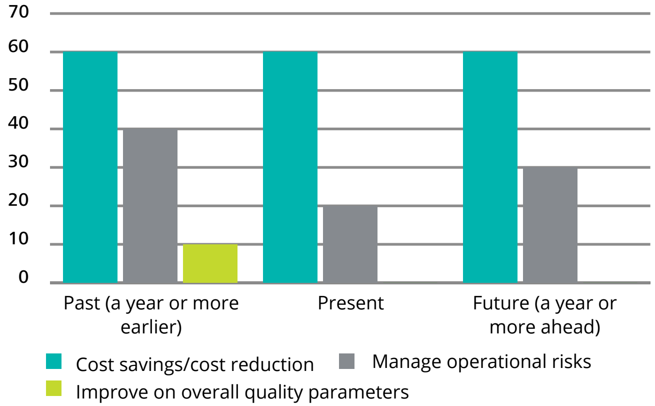


Survey results by industry segment

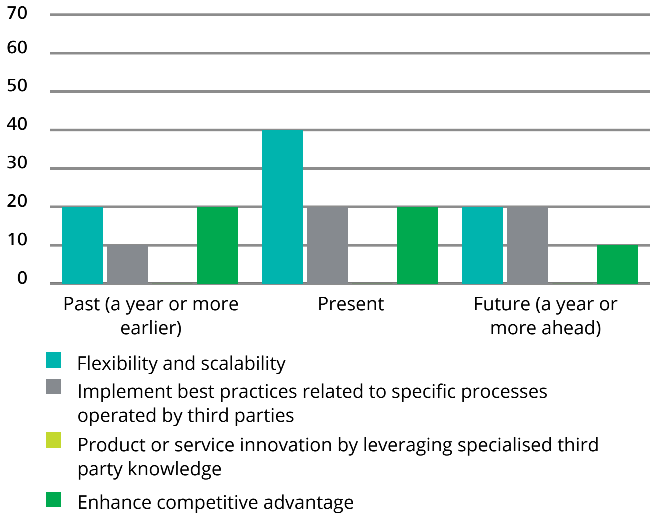
Changing drivers for third party engagement (% of respondents)

Energy & Resources

Traditional drivers
% of respondents



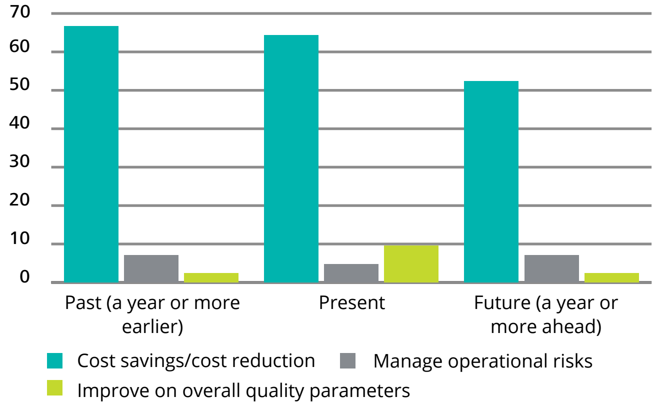
Emerging drivers
% of respondents



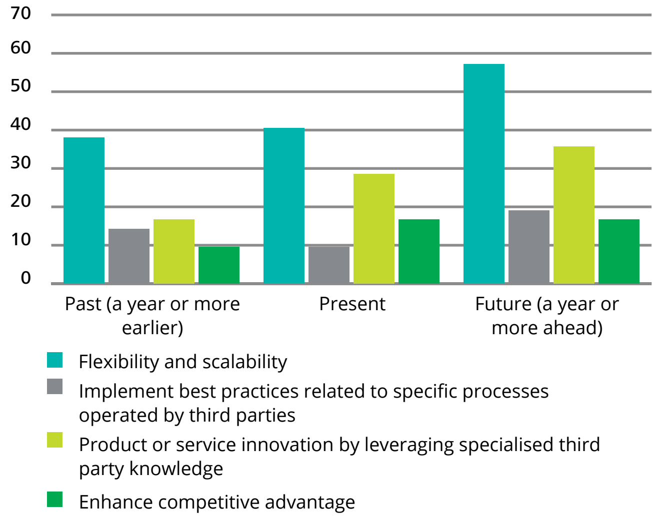
Changing drivers for third party engagement (% of respondents)

Financial services

Traditional drivers
% of respondents



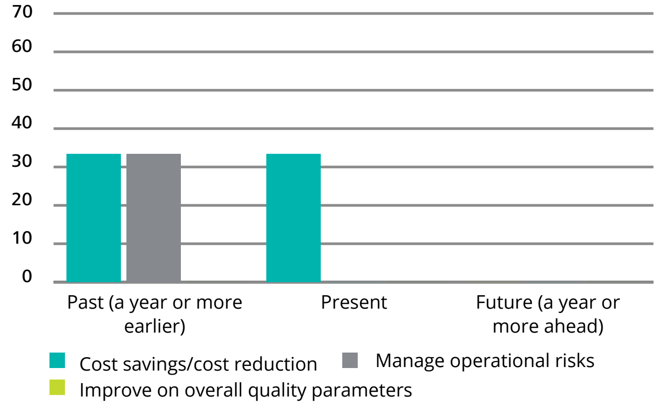
Emerging drivers
% of respondents



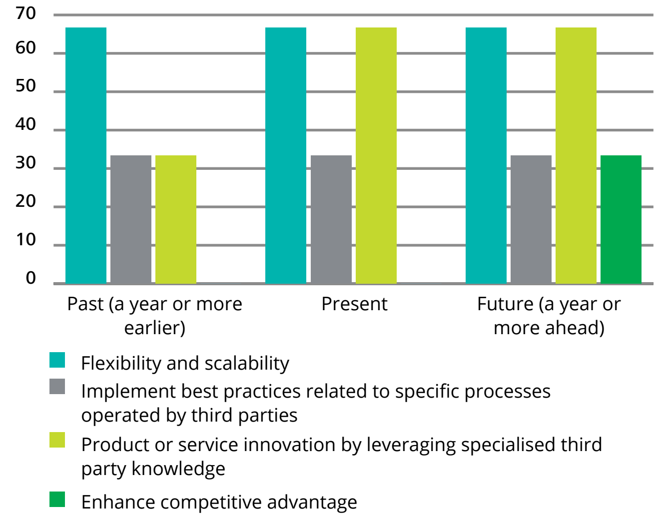
Changing drivers for third party engagement (% of respondents)

Health & life sciences

Traditional drivers
% of respondents



Emerging drivers
% of respondents

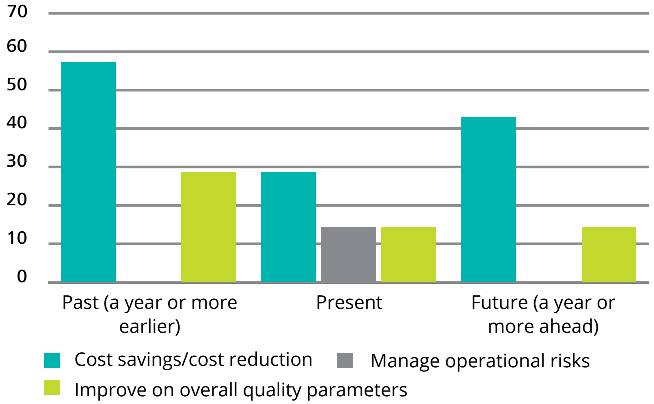


Survey results by industry segment

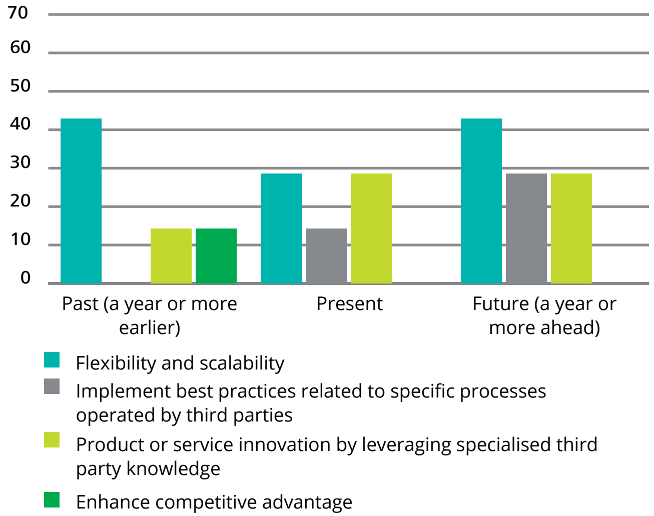
Changing drivers for third party engagement (% of respondents)

Manufacturing

Traditional drivers
% of respondents



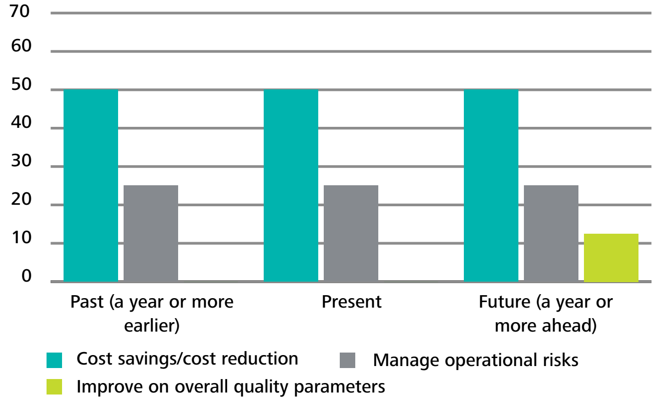
Emerging drivers
% of respondents



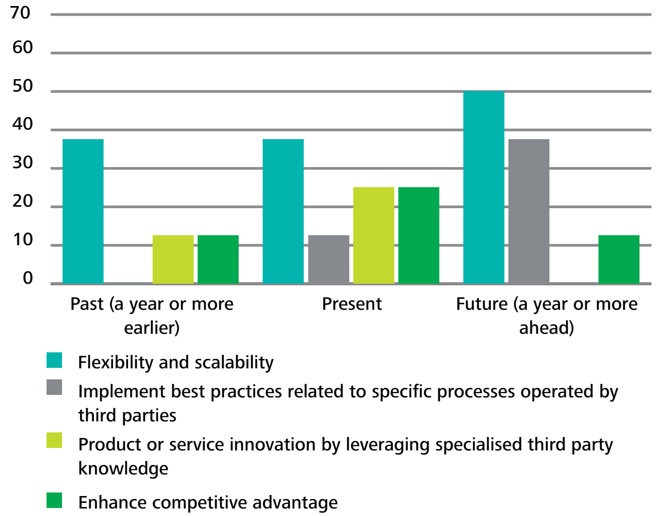
Changing drivers for third party engagement (% of respondents)

Public sector

Traditional drivers
% of respondents



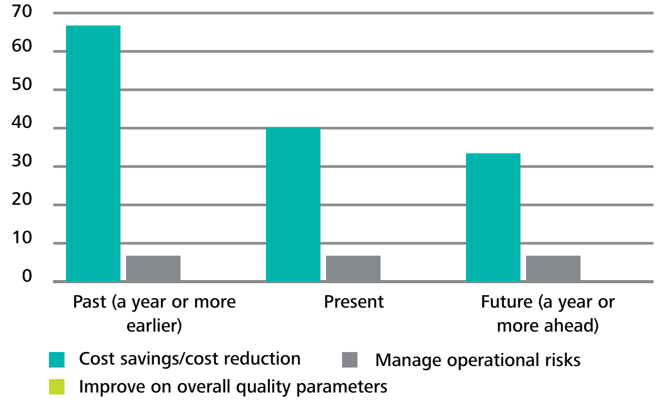
Emerging drivers
% of respondents



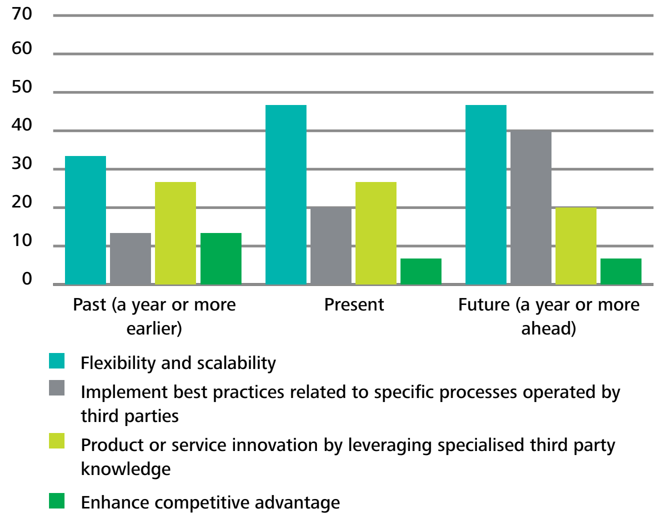
Changing drivers for third party engagement (% of respondents)

TMT

Traditional drivers
% of respondents



Emerging drivers
% of respondents



4. Managing third party risk

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 realised, this has compromised organisational 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 organisation. 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. 87% of respondents have faced a disruptive incident associated with third parties in the last 2-3 years, out of which 28% faced major disruption and 11% experienced a complete third party failure – reducing their confidence in the related governance and risk management processes.

26.2% of respondents have suffered reputational damage arising from third party action in the last 2-3 years, while 23.0% have ended up being non-compliant with regulatory requirements with 8.7% of these respondents facing a fine or financial penalty as a result of this non-compliance. Another 23.0% of respondents have experienced financial or transaction-reporting errors, 20.6% have dealt with a situation where sensitive customer data has been breached through third parties and 10.3% have actually lost revenue.

87% of respondents have faced a disruptive incident associated with third parties in the last 2-3 years, of which 28% faced major disruption and 11% 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 behaviour	3
Breakdown in supply chain due to failure of third parties	4
Financial fraud or exposure created by third party behaviour	5
Failure of financial viability of third party impacting delivery	6

Impact of third party incidents actually faced by respondents

26.2%	23.0%	23.0%	20.6%	10.3%
Reputational damage	Financial or transaction reporting errors	Non-compliance with regulatory requirements	Breach of sensitive customer data	Lost business

Deloitte point of view

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

Deloitte believes that the Financial Services 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 life sciences and healthcare, chemicals, food and retail etc., together with global regulation such as the US Foreign Corrupt Practices Act (FCPA) impacting all industries, irrespective of where the related organisations 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 (R27 million-R692 million), while action under global legislation such as the US FCPA can be far higher, touching US$ 0.5–1 billion (R7 billion-R14 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% in the three days after the announcement, where direct harm to customers and investors is involved. This of course is in addition to the significant reputational damage that an organisation will incur.

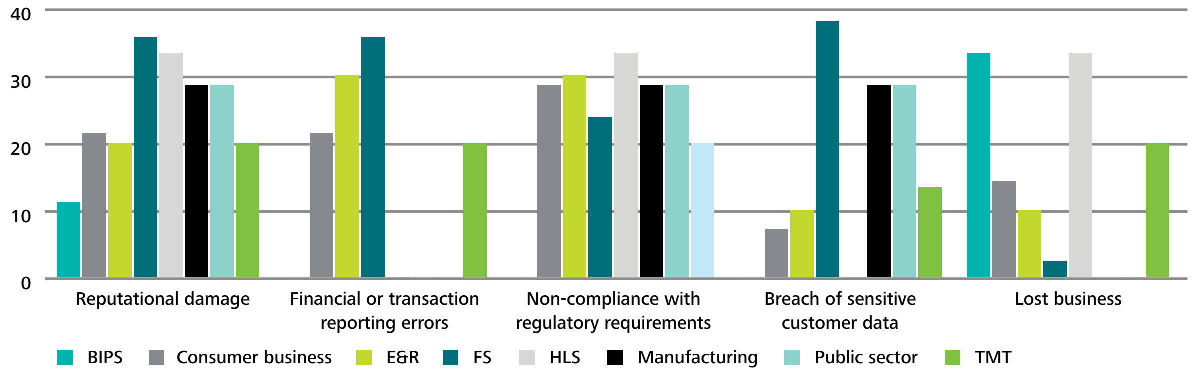
Survey results by industry segment

The survey reveals that concerns around the breakdown in their service supply chain features higher amongst organisations engaged in Business, Infrastructure and Professional Services (BIPS) as well as those in Healthcare and Life Sciences (HLS), 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 Consumer Business, Technology Media and Telecom (TMT) and Manufacturing industries while Public Sector 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, organisations in the BIPS segment (33.3% of respondents) as well as in Healthcare and Life Sciences (33.3% 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 organisations have faced a comparatively lower impact of regulation and loss of customer data.

Impact of third party incidents actually faced by respondents

Nature of third party incident (% of respondents)



Top third party related risks ranked in order of criticality

Risk areas	BIPS	Consumer business	E&R	FS	HLS	Manufacturing	Public sector	
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 behaviour	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 behaviour	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

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

Organisations 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% of respondents. 57.1% of respondents are stepping up their assurance activities over third parties as their key initiative to reduce third party risk.

Respondents recognise 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 Defence”, 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 organisation to address the most significant areas of concern.

Enhancing the rigour 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% and 38.7% of respondents respectively.

59.7% of respondents are enhancing their monitoring activities and

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

Risk reduction initiatives taken up by respondents

59.7%
Enhanced monitoring of third parties

57.1%
Enhancing assurance activities over third parties

44.5%
More disciplined contracting (e.g. centralised templates approach)

38.7%
Enhanced business case and due diligence for involving third parties in a specific area

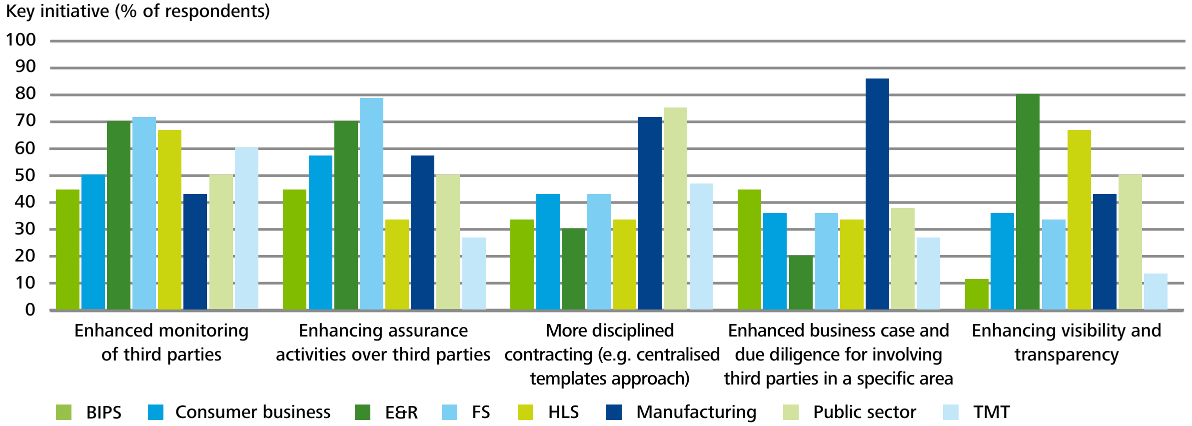
36.1%
Enhancing visibility and transparency

Survey results by industry segment

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

- Energy and Resources (E&R): Enhancing visibility and transparency (80.0% of respondents)
- Healthcare and Life Sciences (HLS): Enhancing visibility and transparency (66.7% of respondents)
- Manufacturing: Enhancing business case and due diligence (85.7% of respondents) followed by more disciplined contracting (71.4% of respondents)
- Public Sector (PS): More disciplined contracting (75.0% of respondents)
- Technology Media and Telecommunications (TMT): More disciplined contracting (46.7% of respondents)

Key initiatives associated with third parties



Deloitte point of view

Deloitte experience indicates that organisations 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% of total spend). Only now are organisations 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 organisational clamour for increasing monitoring and assurance-related activities around third parties demonstrates growing organisational realisation 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, organisations must continually ensure that changing conditions have not made these controls out-of-date. In addition, more and more organisations 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 organisational 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 organisational assurance mechanisms” to obtain comfort on third party management.

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

Survey respondents have indicated varying levels of organisational confidence in the different domains of TPGRM. Organisational 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. 78.1% 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% of respondents have expressed a moderate to high level of confidence. This high level of confidence also extends to the organisation 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, organisational 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%, 93.5% and 88.6% respondents respectively expressing moderate to low levels of confidence in these domains.

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

78.1% of respondents expressing a moderate to high level of confidence in this domain of third party risk management. However, organisational 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%, 93.4% and 88.6% respondents respectively expressing moderate to low levels of confidence in these domains.

Domains of third party risk management where confidence is moderate to high

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%
Organisation of third party risk management

Domains of third party risk management where confidence is moderate to low

94.3%
Tools and Technology used for risk management

93.5%
Management and monitoring mechanisms

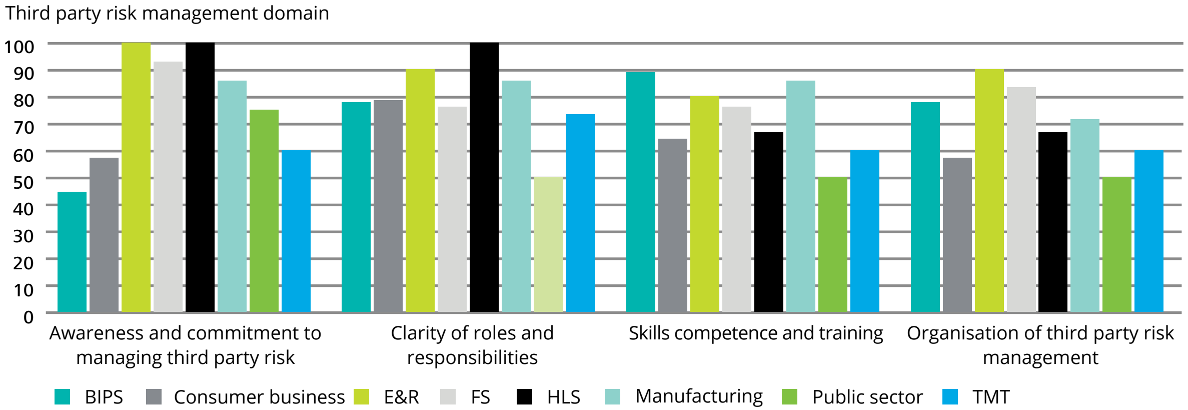
88.6%
Quality of third party risk management processes

78.9%
Disciplined escalation framework

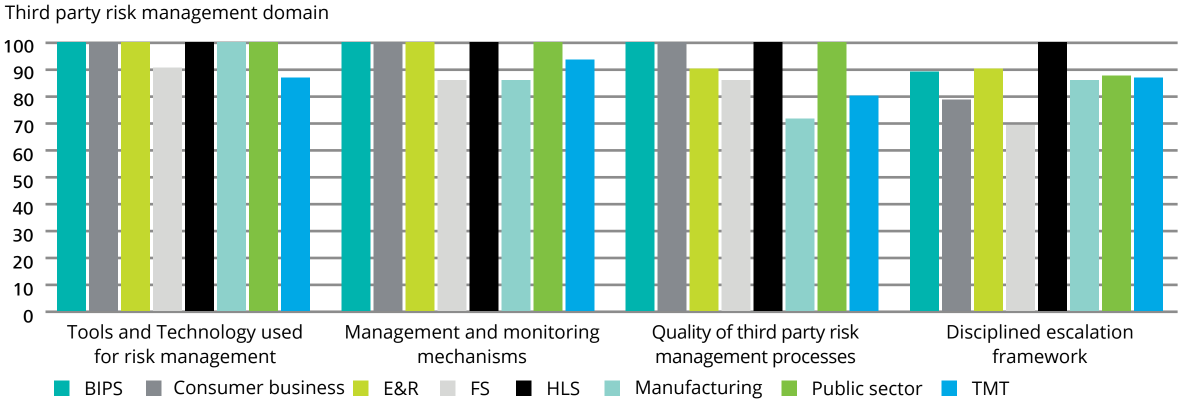
Survey results by industry segment

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% of respondents from Public Sector (PS) have moderate to high levels of confidence in the manner in which third party risk management is organised, the clarity of roles and responsibilities, together with related skills competence and training. This is significantly lower than the other industry segments, implying that Public Sector organisations may require stronger levels of accountability amongst its senior officials responsible for third party risk management. Further, respondents within the Business, Infrastructure and Professional Services (BIPS) industry segment as well as Consumer Business have indicated lower levels of confidence in awareness and commitment around third party risk management, with only 44.4% and 57.1% respondents having moderate to high confidence levels respectively.

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



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



Deloitte point of view

Deloitte perceives an emerging “execution gap” in TPGRM. This gap is the result of organisational 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 organisations, 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 organisational capability to maximise the opportunities from their third party ecosystem.

5. Third party governance

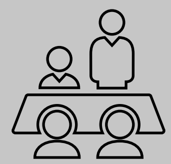
Third party risk is starting to feature consistently on the Board agendas with CEO/Board-level responsibility in the more progressive organisations or those operating in highly regulated environments.

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 organisations 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% 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%, 9.3% and 5.1% of respondents, respectively.

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

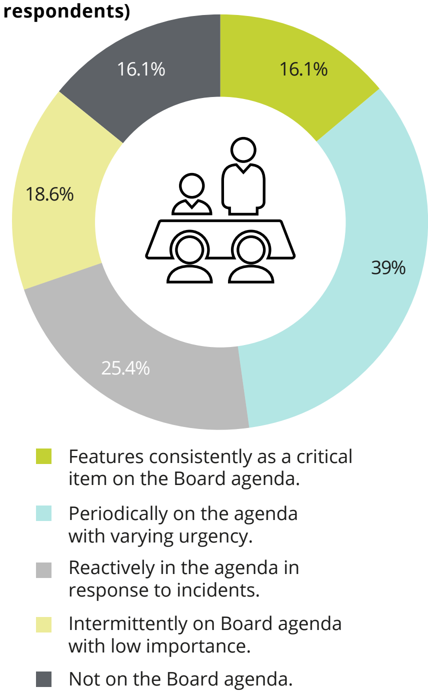
However, third party risk is still discussed reactively in 25.4% of respondents, only in response to third party incidents, while a further 18.6% of organisations engage in this Boardroom discussion only intermittently, with a low level of importance. This indicates that this transformational thinking is still to make a substantial impact on a number of organisations where regulatory pressures are lower, or in those organisations 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% of respondents with varying levels of urgency, but with critical urgency in a further 16.1% of respondent organisations. Ultimate accountability for third party risk management resides in the CEO or Member(s) of the Board in 46.6% of respondent organisations.

Third party risk on the Board agenda (% of respondents)

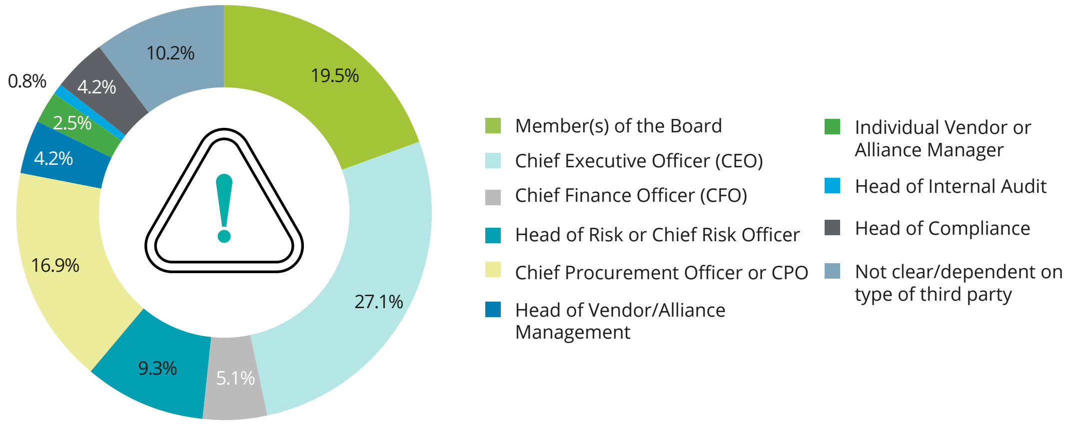


Deloitte point of view

The survey results echo the growing organisational 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 maximising 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.

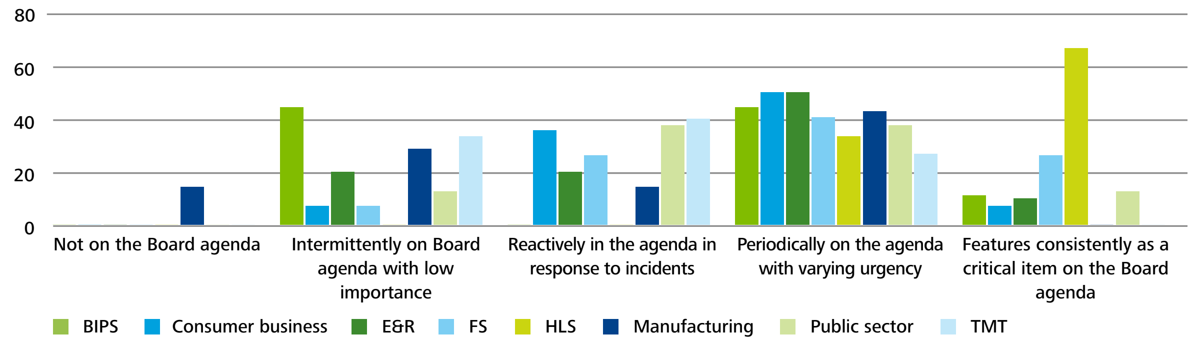
Deloitte further believes that Board and C-suite ownership and oversight of TPGRM is critical to be able to exploit the opportunities and manage the risks from third parties efficiently and effectively. This also facilitates multiple stakeholder buy-in at the functional level.

Level of ultimate accountability for risk management (% of respondents)
Ultimate accountability for third party risk management



The survey results indicate divergence in the Manufacturing and Business, Infrastructure and Professional Services (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 (Manufacturing: 42.9% of respondents in total; BIPS 44.4%). On the other hand, the Healthcare and Life Sciences (HLS) industry segment appears to have third party risk featuring most consistently as a critical item on the Board agenda with 66.7% of respondents in this category.

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



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% of respondents making such on-site visits.

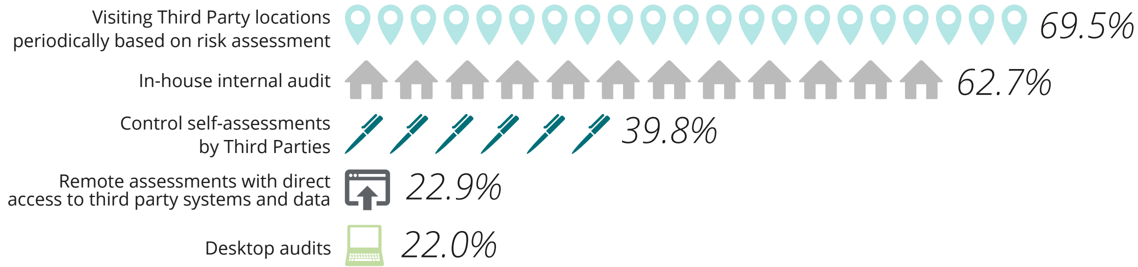
In-house internal audit reviews represent the second most popular and effective method of gaining third party assurance, practiced by 62.7% of respondent organisations. In addition, controls self-assessments by third parties, remote assessments with direct access to third party systems/data and desktop 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 is also rapidly gaining popularity as effective methods for obtaining assurance over third party management.

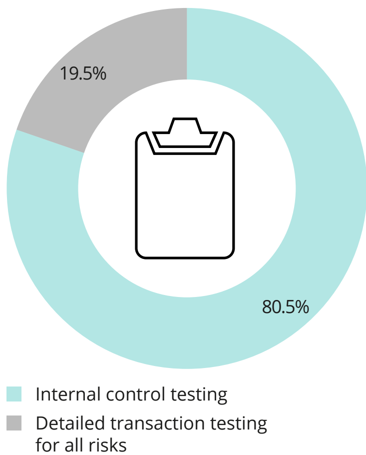
Some respondents have expressed their dependence on external audits and service provider audits under SSAE16/ISAE3402 standards. However, most of these audits cover the risk of material financial statement misstatements only and may not address the wider set of strategic, operational, reputational, legal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

69.5% 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%) with the other 19.5% driving their approach through detailed transaction testing.

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



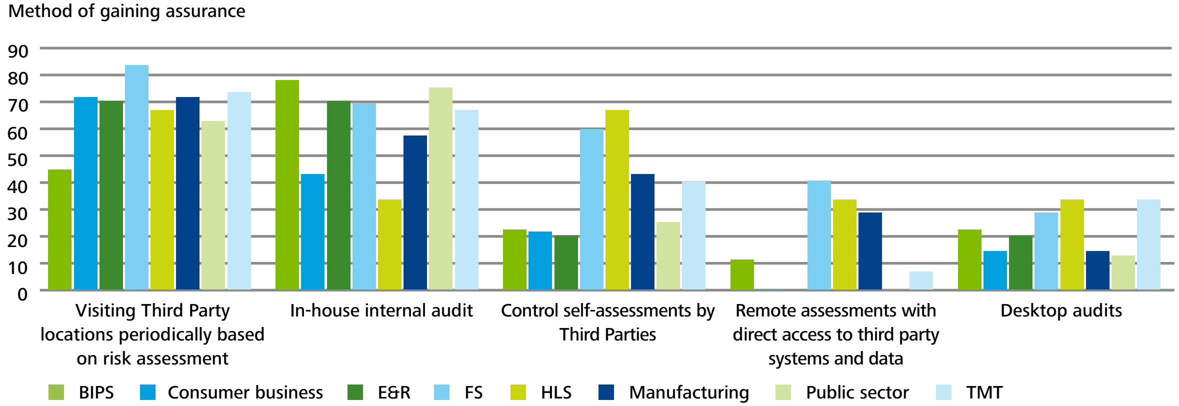
What drives the approach to on-site third party reviews?



Survey results by industry segment

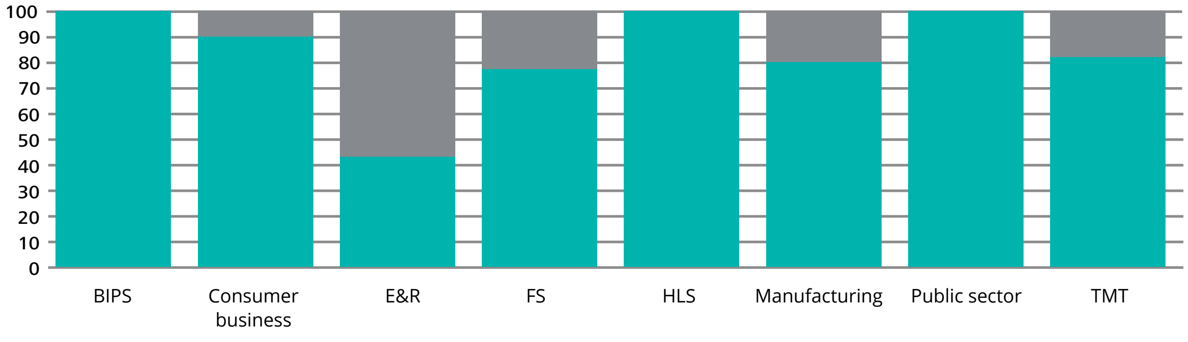
There is a fair degree of consistency in the methods of gaining assurance on third party activity across the industry segments, all of whom rely heavily on risk-based visits to third party locations as well as in internal audit procedures, as indicated below:

Dominant methods of gaining assurance over third party management



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 Business, Infrastructure and Professional Services (BIPS), Healthcare and Life Sciences (HLS) and Public Sector (PS) where the level of detailed transaction testing appears to be insignificant, with the sole focus being on internal controls.
On the other hand, Energy & Resources (E&R) organisations seem to be doing the most detailed transaction testing, with 57.1% of respondents adopting this approach.

What drives the approach to on-site third party reviews?



Deloitte point of view

Deloitte 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 organisational stakeholders, as well as disparate groups of third parties in the extended enterprise. This results in the utilisation 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 recognising 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% of cases, with detailed transaction testing for all risks driving the approach in less than 20% 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% of controls testing and 80% of transaction testing should be the benchmark that organisations 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.

Most organisations are mandating consistent third party governance standards amidst increasing decentralisation of operating units.

A decentralised organisation 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 organisations are increasingly being managed through degrees of decentralisation across their various operating units and entities. 75.5% of respondents today have a partial through to a high degree of decentralisation, reflecting a potential challenge to a holistic and unified approach to third party risk management.

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

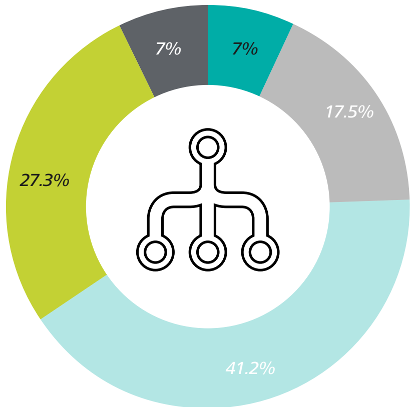
The survey also reveals that the general trend is to have a combined approach to formulating these standards, representing a mix of existing industry-specific (e.g. HIPAA standards for safeguarding of personal identifiable or private information for patient data handled or managed by third party service providers) or generally accepted functional standards (ISO 22301 standard for business continuity in relation to business processes operated by third parties), supplemented by organisation-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% of respondents today have a partial through to a high degree of decentralisation, reflecting a potential challenge to a holistic and unified approach to third party risk management. However,

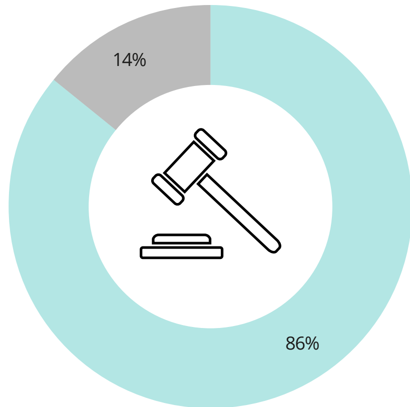
86.0% (the vast majority of these organisations) mandate common third party standards to ensure a consistent approach across business units.

Increasing degree of decentralisation in respondent organisations



- Highly centralised
- More centralised than decentralised
- Partly decentralised
- More decentralised than centralised
- Highly decentralised

Mandating third party standards



- Organisations that mandate standards for third parties
- Organisations that DO NOT mandate standards

Survey results by industry segment

The degree of decentralisation appears to be the highest in the following industries. A high proportion of respondents in these industries consider their organisation to be more decentralised than centralised or to be highly decentralised:

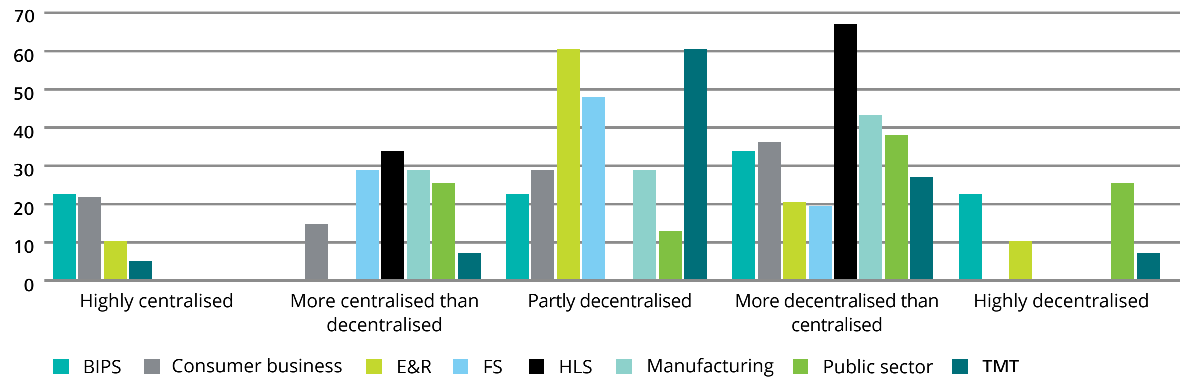
- Healthcare and Life Sciences (HLS) (66.7% of respondents),
- Public Sector (62.5% of respondents)
- Business Infrastructure and Professional Services (BIPS) (55.6% of respondents)
- Manufacturing (42.9%).

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

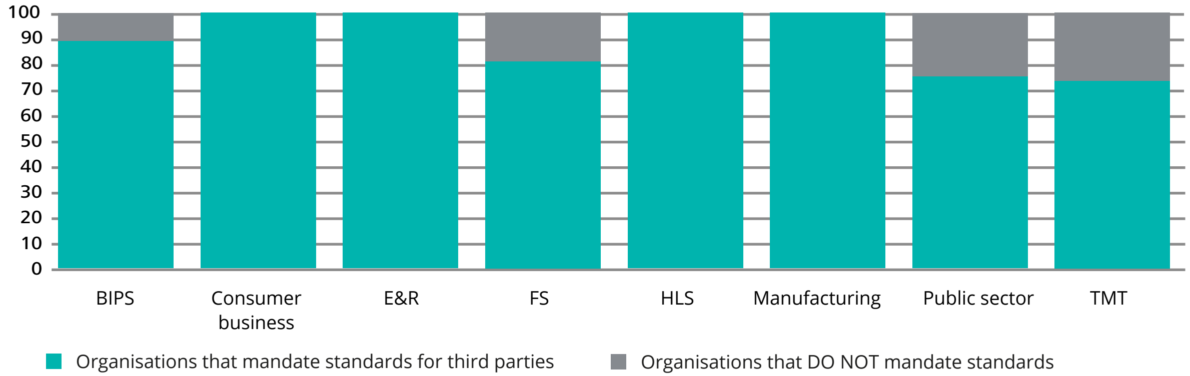
Deloitte point of view

TPGRM is clearly evolving as a crucial organisation-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 decentralisation. The survey results portray organisational 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 decentralisation in respondent organisations (%)



Mandating third party standards (%)



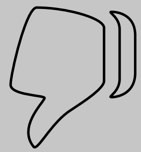
6. Technology and delivery models

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

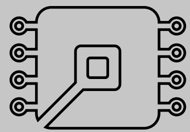
Organisational confidence in tools and technology is the lowest across all the domains of third party risk management, with 56.1% respondents rating their confidence level as low and another 38.2% respondents rating their level of confidence as moderate.

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. Whie 29.8% of respondents utilise their ERP platform for third party risk management, the remaining 70.2% 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 organisational 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 organisation, operating with a partial or high degree of decentralisation.

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.

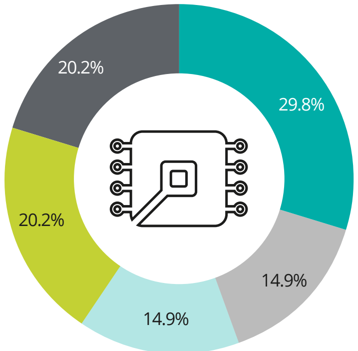


Confidence in tools and technology is the lowest across all the domains of third party risk management, with **56.1%** respondents rating their confidence level as low and another 38.2% respondents rating their confidence as moderate.



29.8% of respondents utilise their ERP platform for third party risk management while the remaining 70.2% 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.

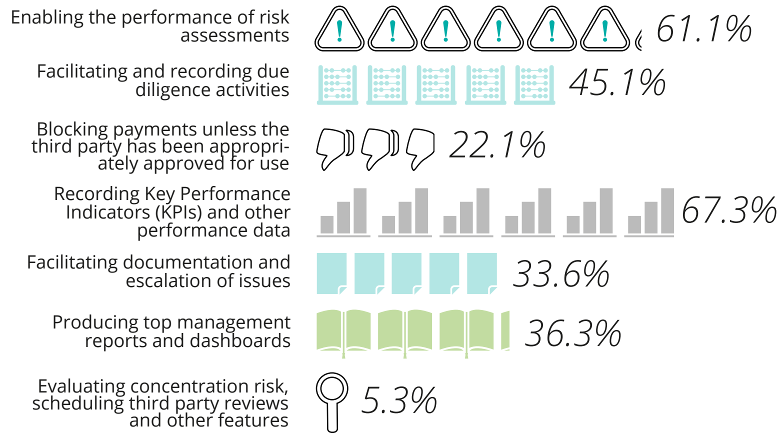
Technology platforms used for third party management



- ERP platform (e.g. SAP, Oracle module)
- Generic risk software package (not specific to third party management): An 'off the shelf' solution tailored to the organisation (e.g. Archer, Open Pages)
- Third party management software package: An 'off the shelf' solution tailored to the organisation (e.g. Hiperos)
- Bespoke software: software package specifically coded for third party risk management at your organisation
- Multiple platforms, typically a combination of bespoke, packaged and manual/unknown

■ ERP platform (e.g. SAP, Oracle module)

Desired functionality of third party software



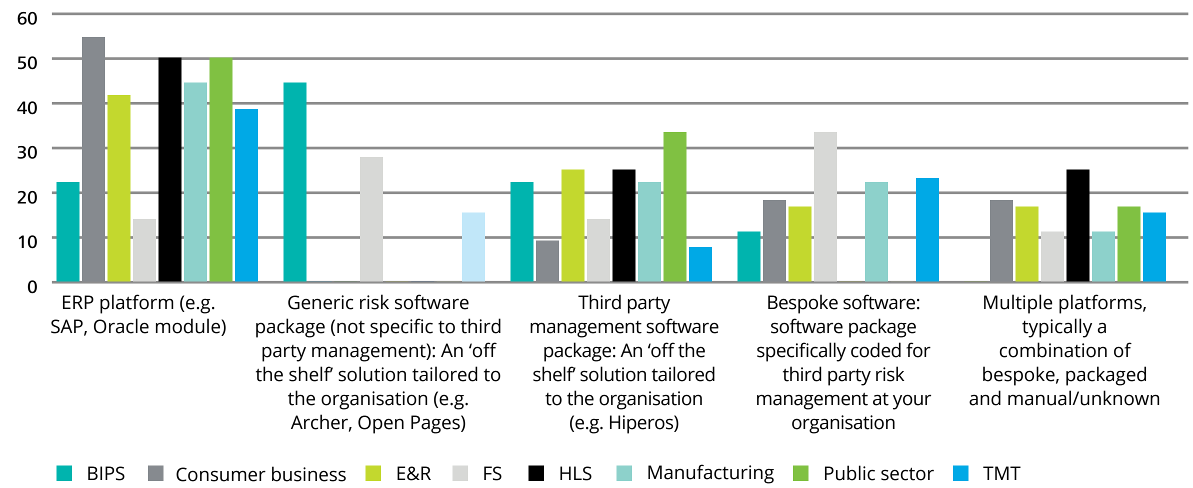
Survey results by industry segment

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 Consumer Business, Energy & Resources, Healthcare & Life Sciences, Manufacturing and Public Sector as tools to help manage third party risk.

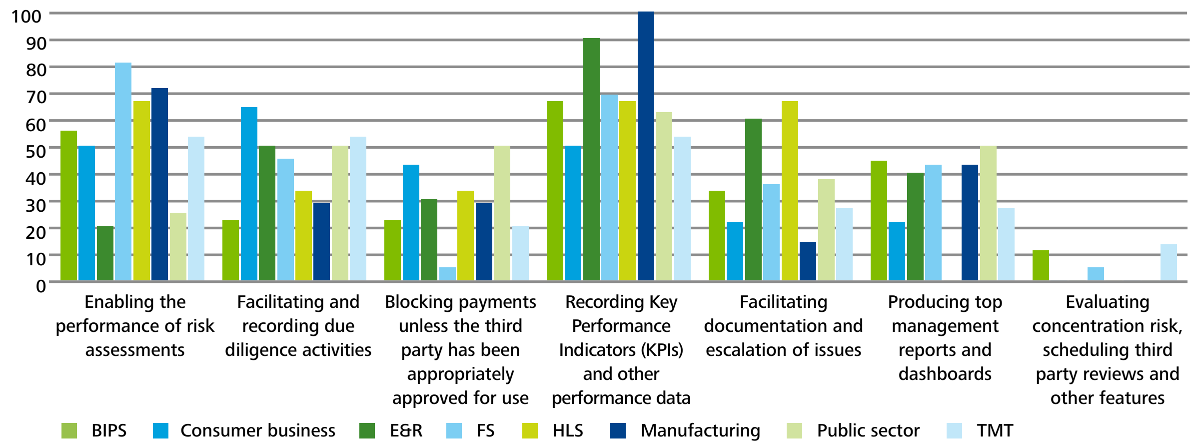
Deloitte point of view

There is no doubt that the lower level of organisational 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 organisational ability to make appropriate risk-informed decisions, as well as being able to implement optimised processes tailored to the type of product or service being outsourced. Deloitte 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 (%)



Key software functionality (%)



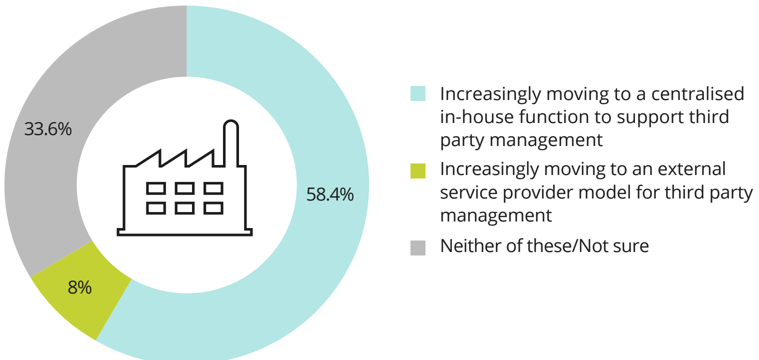
10/ Organisations are in the process of deciding between centralised in-house models and external service-provider based models for third party monitoring.

Establishing a centralised in-house function for third party management seems to be the approach that the majority of respondents are adopting, with 58.4% of respondents in this category. It is expected that this centralised function would cover most of the key activities related to third party management including ongoing risk assessments (80.3%); third party monitoring activities (80.3%) and co-ordination (56.1%); tracking remediation activities (57.6%) and ongoing monitoring requirements (50.0%). It would also be responsible for various administrative activities such as filing of contracts and amendments (48.5%), archiving evidence related to third party management (33.3%) and would assist in the implementation of third party contract termination plans (25.8%).

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

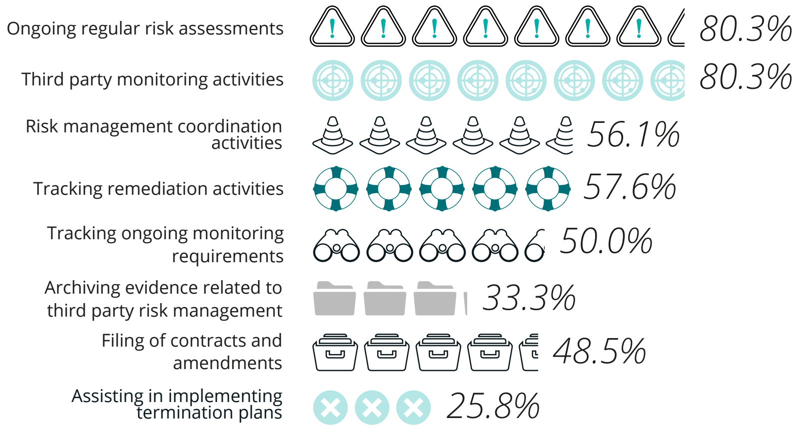
It should also be noted that as many as 33.6% of respondents are not yet clear on the future organisational choice of an in-house versus an external service provider model.

Organisations considering in-house versus external service provider-based third party risk management models



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

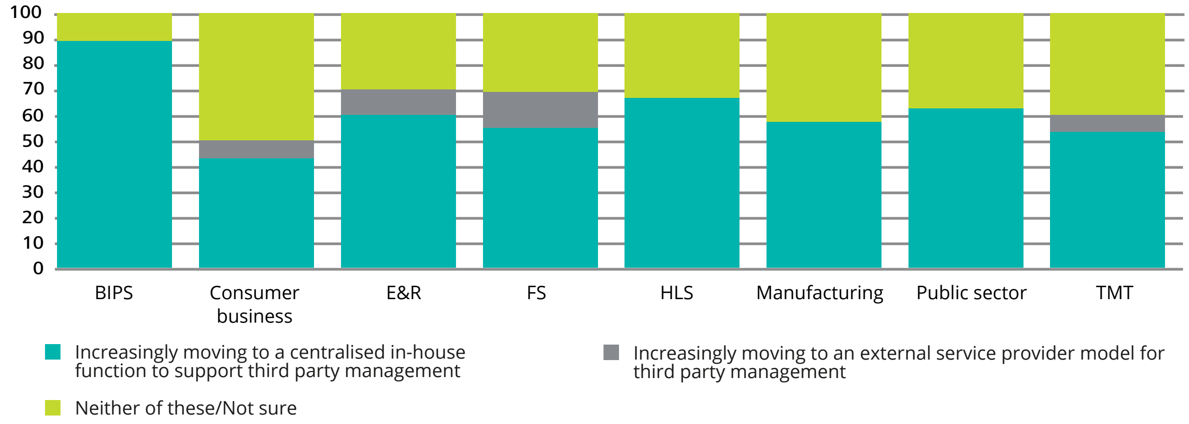
Expected functions of centralised in-house risk management team



Survey results by industry segment

The preference for moving to a centralised 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 Consumer Business, Manufacturing, Technology Media and Telecoms (TMT) and Public Sector industries with as many as 50%, 42.9%. 40% and 37.5% of respondents in this category.

Organisations considering in-house versus external service provider-based third party risk management models (%)

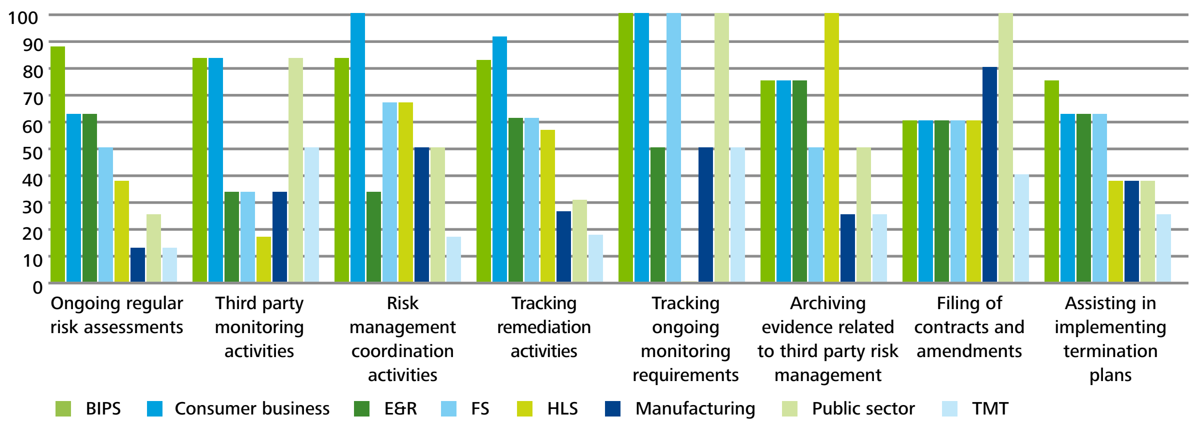


Deloitte point of view

The choice between a centralised 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 organisations moving to a centralised in-house function in this regard are primarily driven by the need to retain organisational control over this critical activity. This is enhanced by a better organisational understanding as well as the ability to manage a diverse group of stakeholders that an external provider may be unable to match.

Deloitte 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 organisations remaining undecided in this matter, although many of them are already working with contract staff to assist them in the related tasks.

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



Contacts

For more information, please contact

Southern Africa

Navin Sing
Managing Director:
Risk Advisory Africa
Mobile: +27 83 304 4225
Email: navising@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader:
Governance, Regulatory & Risk
Mobile: +27 82 415 8253
Email: dechivers@deloitte.co.za

Daniella Kafouris
Associate Director:
Risk Advisory Southern Africa
Mobile: +27 72 559 0360
Email: dkafouris@deloitte.co.za

East Africa

Julie Akinyi Nyangaya
Risk Advisory Regional Leader:
East Africa
Mobile: +254 72 011 1888
Email: jnyangaya@deloitte.co.ke

William Oelofse
Director:
Risk Advisory East Africa
Mobile: +254 20 423 0000
Email: woelofse@deloitte.com

West Africa

Anthony Olukoju
Risk Advisory Regional Leader:
West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director:
Risk Advisory West Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader:
Central Africa
Mobile: +263 772 234 932
Email: tsimon@deloitte.co.zm

Rodney Dean
Director:
Risk Advisory Central Africa
Mobile: +263 772 263 016
Email: rdean@deloitte.co.zm

About the authors

Kristian Park, DTTL, EMEA Leader, Contract Risk & Compliance
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 to Media 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 to manage their software licensing obligations – driving efficiencies and savings.

Sanjoy Sen is a Doctoral Research Scholar at Aston Business School, UK, specialising 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.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. J4012