

# Improving third-party risk management

A joint study between ORIC International and McKinsey & Company



## FOREWORD

We're pleased to present the findings of our study, conducted jointly by ORIC International and McKinsey, into third party supplier management.

This is a topic at the forefront of our industry and we trust these insights will provide a meaningful step towards defining the major challenges and potential solutions within this important area.

As outsourcing in financial services increases, so does business complexity and we're already seeing heightened expectations from regulators, both in the UK and internationally. In the UK, the PRA have raised the stakes for insurers' responsibilities for outsourcing, by proposing a Prescribed Responsibility for outsourced operational functions and activities.

Against this backdrop, good market practices continue to evolve and (re)insurance and investment firms must expand their efforts to ensure risk management processes remain effective, not only to meet the regulatory agenda, but also to protect the interests of both customers and stakeholders. Therefore, a key output of this study is an essential maturity diagnostic that can be used to benchmark your firms' third party risk management approach and identify opportunities to enhance existing practices.

We'd like to thank the firms from across the financial services industry, both within and outside of our member base that participated in this study. In acknowledgement of their generous participation, a more detailed report has been made available exclusively to them.

We'd also like to thank our supply chain management working group for their contribution to this study, their collective knowledge, experience and insights have helped to inform the best practice set out within. Future issues for consideration by this group include the development of standard approaches to segmentation, cyber and GDPR.

If you'd like to find out more about our work please get in touch. We look forward to hearing from you.

Best wishes,



Caroline Coombe  
(CEO, ORIC International)



Michael Bartholomeusz  
(Chair, Supply Chain Management Working Group  
& Deputy Chairman, ORIC International)

## EXECUTIVE SUMMARY

Third-party risk management is increasingly important for (re)insurance and investment firms, many of which are turning to outsourcing for an array of technology and other services. Outsourcing is helping firms become more efficient, but it is also leading to challenges, including a recent increase in regulatory action for breaches such as poor supervision.

In light of increased scrutiny and to boost oversight, a number of (re)insurance and investment firms have instigated reviews of their third-party risk management frameworks. With programmes set to continue for the next years, ORIC International and McKinsey have joined forces to benchmark progress and explore best-practice models.<sup>1</sup>

Our research highlights good practices across the industry, but also certain areas of weakness. Those include a lack of common standards, and often a case-by-case approach to third-party risk management, in a diverse range of systems, policies and approaches used by firms. Also, coverage varies across the industry with some firms focusing on as few as ten counterparties, while others monitor several thousand – and much of this variation cannot be explained by size differences between the firms in question. Finally, the survey reveals a lack of completeness in oversight frameworks, with the most intense focus often falling on third-party selection and onboarding, while elements of the ongoing monitoring of established third-party relationships often receive much less attention.

Outsourcing has become an established way of working for (re)insurance and investment firms, and we expect it will continue to play an important role in the years ahead. Hence, organisations should adopt strategies that reflect a systematic approach and help build a comprehensive framework. Based on our research, we recommend four actions:

- Design an explicit third-party and/or supplier risk management framework, including a definition of ownership, governance and articulation of risk appetite that will lead to alignment among internal stakeholders.
- Extend the scope to all third parties and apply risk-based segmentation to determine the level of control required.
- Apply a proactive and comprehensive approach to third-party risk management, including ongoing monitoring and escalation processes.
- Invest in IT tools, like data management systems, end-to-end workflow tools and analytics to increase efficiency of and ensure consistency in the process.

On a cross-industry basis, we see an opportunity to define common third-party risk management standards, which will set a course for a more secure and efficient future. They could also bring benefits such as an increase in cybersecurity and improved data management.

---

<sup>1</sup> From autumn 2016 to spring 2017, ORIC International and McKinsey surveyed more than 30 (re)insurance and investment firms (members as well as non-members of ORIC International).

# BENCHMARKING RISK MANAGEMENT FRAMEWORKS

In recent years, third-party risk management has become a primary concern for (re)insurance and investment firms, amid increased outsourcing against a backdrop of rising costs, digitisation and low interest rates, which have put downward pressure on margins. While there are many benefits driving outsourcing, e.g., increased efficiency and scale, it naturally also increases the level of risk and complexity of third-party relationships. Coupled with increased lengths of agreements, on average five to seven years, the need for ongoing performance management becomes that much greater.

Financial and reputational risks have increased with more outsourcing, and regulators have focused on how companies manage their relationships with third parties, in some cases leading to tighter regulation. The first to increase regulatory scrutiny in this area were the US with a regulatory paper on third-party risk management as far back as 2002, albeit only for banks<sup>2</sup>. UK initiatives include the FCA review of outsourcing in general insurance and the PRA's extension of the Senior (insurance) Managers regime to include a Prescribed Responsibility for outsourcing<sup>3</sup>. In Europe, Solvency II regulates how insurers maintain access to and control over outsourced activities.<sup>4</sup> Further requirements have emerged in particular areas, e.g., GDPR<sup>5</sup> in IT outsourcing. Fines imposed in the UK and US show that (re)insurance and investment firms will be held accountable for outsourced activities, and firms have been fined for breaches including insufficient oversight of third parties.

In light of increased scrutiny, (re)insurance and investment firms are reviewing their third-party risk management frameworks. ORIC International, the world's leading provider of specialist operational risk resources, benchmark services and thought leadership for the insurance, reinsurance and investment

management sectors, has joined forces with McKinsey to benchmark the quality and robustness of those frameworks and explore best practices (Exhibit 2).

More than 30 (re)insurers and investment firms joined the survey. Participants included members of ORIC International and non-members, from across lines of business and varying from local players to global leaders (Exhibit 1). While the majority of answers came from firms based in the UK, Germany and France, several of them have an international, often global reach.

Based on McKinsey's experience, the most successful third-party risk management frameworks achieve excellence in nine dimensions: scope, segmentation, due diligence, control systems, scorecards and risk assessments, governance, organisation, policy framework as well as tools and data (Exhibit 2).

There are best practices for each dimension:

- **Scope.** Firms should establish a comprehensive inventory of third-party relationships including outsourcing partners, suppliers of goods and services (including third-party administrators), distribution partners, group-internal relations (associates, affiliates, joint ventures) and important fourth parties (sub-contractors).
- **Segmentation.** Segmentation of third parties should be risk-based and refreshed regularly to efficiently allocate resources to relationships posing the highest risk. It should directly tie into a tailored approach for on-going risk monitoring.
- **Due diligence.** Onboarding and due diligence tests should be based on carefully designed rules, including an assessment of compliance with relevant regulations. Specific due diligence tests may be performed. Also, onboarding teams should be put in place for medium-sized to large institutions to identify risks based on materiality criteria.
- **Control systems.** Control systems should include comprehensive lists of risks, escalation triggers essential for the success of audit routines and scorecards to monitor risk. Best practice is to have a master register of escalation trigger-points and their risk weights in each category relevant to all firms. That can then be adapted to the particular circumstances of individual suppliers.

2 OCC BULLETIN 2002-16 – Bank Use of Foreign-Based Third-Party Service Providers

3 In CP8/17, PRA proposes creating a new PRA Prescribed Responsibility in respect of outsourced operational functions and activities. This would normally be allocated to the newly established PRA Senior Insurance Management function (SIMF) of the Chief Operations function (SIMF24).

4 Delegated authority: outsourcing in the general insurance market (June 2015)

5 General Data Protection Regulation

EXHIBIT 1  
Share of survey participants by size and line of business

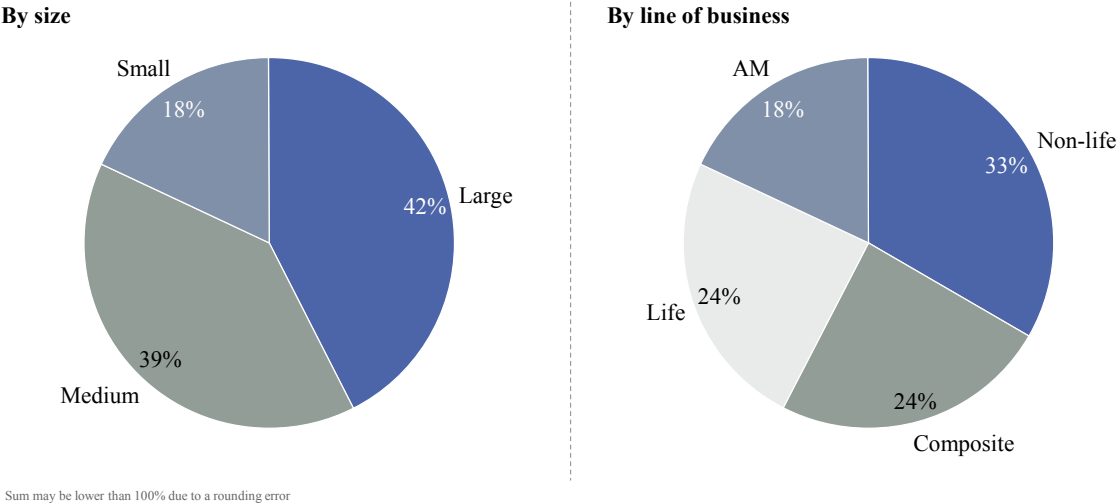
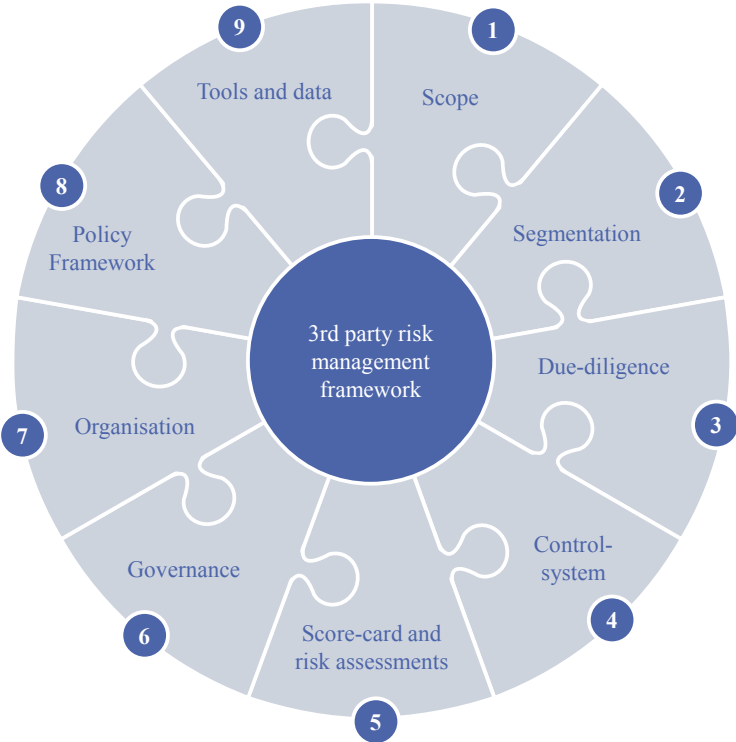


EXHIBIT 2  
Third-party risk management framework



- **Scorecards and risk assessments.** Based on a comprehensive inventory of risks, scorecards can help monitor compliance with regulations and performance relative to metrics. Scorecards should have the appropriate level of detail, and highlight metrics that can be aggregated to an executive level report. Supplier performance and behaviour should be continuously monitored, e.g., via on-site audits. The frequency and scope of performance monitoring and assessments can be differentiated based on segmentation, e.g.:  
 “[In our firm, we use] monthly KCI/KRI/risk appetite reporting, monthly engagement with key third-party meetings across three lines of defence. Concerns flagged on risk watch list and escalated to ExCo and board risk committee where sufficiently serious.” – Risk manager at small general insurer on their ongoing monitoring and review of 3rd parties/suppliers
- **Governance.** Effective governance means establishing a natural owner for third-party risk management and ensuring he or she has appropriate powers. Governance can be either centralised, decentralised or a mixture of both. Centralised governance typically leads to coherent application of standards, while decentralised governance is shaped mostly by business units. Escalation frameworks are necessary to resolve disagreements and challenges. Contingency plans are formulated to deal with failure or degradation of critical third-parties.
- **Organisation.** Firms should align their third-party risk management with their divisional and geographic setups and governance structures. There should be clearly defined roles and responsibilities, especially regarding due diligence, onboarding, auditing and segmentation.
- **Policy framework.** Policy frameworks provide guidance for all business units and functions. They should also clearly define a risk appetite assessment. A robust policy framework includes:
  - An overarching third-party risk management policy to establish minimum standards and a firm-wide control framework
  - Third-party risk policies and procedures for functions, including compliance, finance and procurement
  - Regional policies tailored to local regulatory and legal requirements.
- **Tools and data.** Commercially available data as well as workflow, monitoring and reporting tools tailored to the firm support third-party risk management processes for accountability across all three lines of defence. The tools should perform three functions:
  - Track and monitor data
  - Aid workflow within and across business units
  - Give managers the right information to build an accurate picture of risk in near real time.

---

“[IN OUR FIRM, WE USE] MONTHLY KCI/KRI/RISK APPETITE REPORTING, MONTHLY ENGAGEMENT WITH KEY THIRD-PARTY MEETINGS ACROSS THREE LINES OF DEFENCE. CONCERNS FLAGGED ON RISK WATCH LIST AND ESCALATED TO EXCO AND BOARD RISK COMMITTEE WHERE SUFFICIENTLY SERIOUS.” Risk manager at small general insurer on their ongoing monitoring and review of 3rd parties/suppliers

# PERFORMANCE SELF-ASSESSMENT

The survey results and discussions we held with industry participants have shown that many firms have strong risk management frameworks for outsourcing, and most have significant capabilities in all dimensions of the third-party risk management framework.<sup>6</sup> However, the maturity and scope of these frameworks is uneven, and firms perform better in some areas than others. Across the more than 30 participants, the tools and data segment is rated lowest, with roughly only half of them stating they have those elements mostly in place (Exhibit 3).

The different segments in the insurance sector generally perform in line with each other. However,

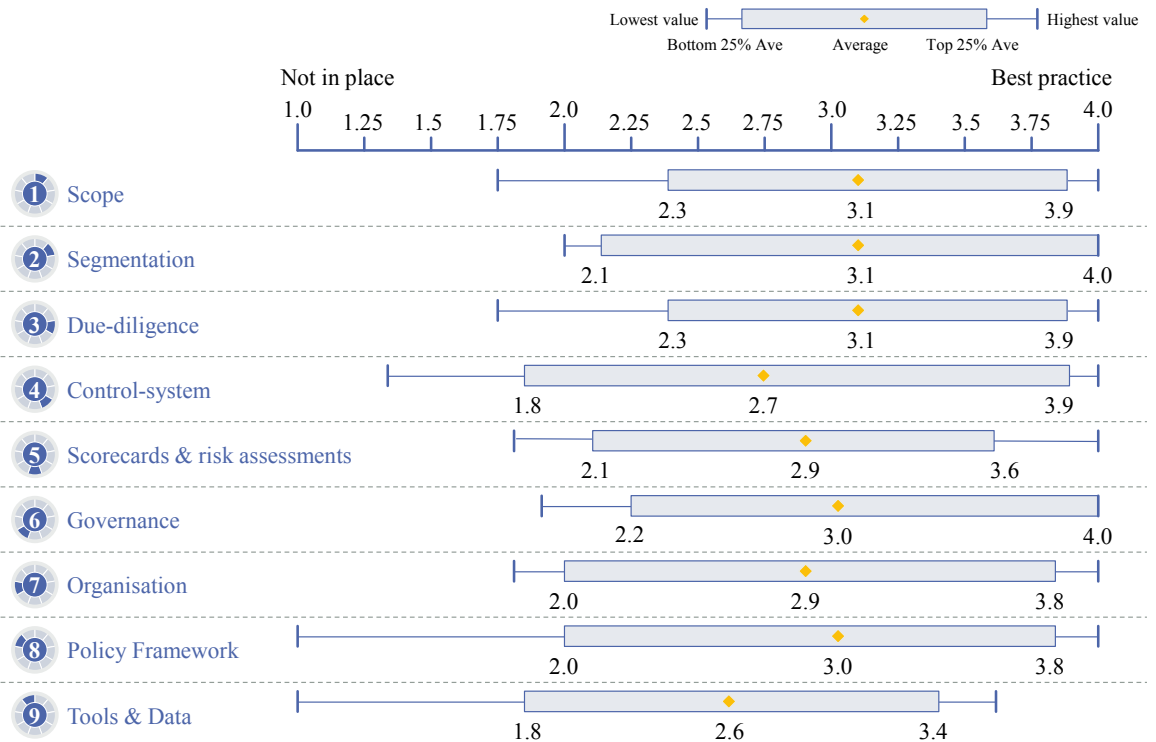
composite insurers emerge as outperformers on most framework elements and particularly in the scope of their coverage, segmentation, governance and tools and data.

Our analysis shows three trends:

- Across the industry, there are only few common standards in third-party risk management.
- Most firms do not have an overarching third-party risk management framework. Instead, they rely on case-by-case evaluations as well as a variety of systems, policies and approaches.
- Coverage varies enormously, with some firms assessing only ten third parties while others consider several thousand – and much of this variation is not explained by size differences between the firms in question.
- Frameworks are mostly focused on selection and onboarding. There is much less focus on ongoing risk management once third-party relationships are in place.

<sup>6</sup> Assessment was derived from 49 statements of best practices with which participants did “strongly agree” (score of 4), “agree” (score of 3), “disagree” (score of 2) or “strongly disagree” (score of 1). “Strongly agree” indicates that the organisation is already applying the best practice, whereas “strongly disagree” indicates that the framework has not yet been implemented.

**EXHIBIT 3**  
Risk management performance across nine metrics



SOURCE: Insurance 3rd Party/Supplier Risk Management Survey

**LACK OF COMMON STANDARDS**

Third-party risk management practices vary significantly across the (re)insurance and investment industries. Some of this is due to organisational differences, but there is a broader absence of commonly observed best practices. For example, the composition of teams conducting due diligence and onboarding varies enormously from firm to firm.

**CASE-BY-CASE EVALUATION**

Many firms manage third-party risk case by case or with numerous systems, policies and frameworks. While this addresses most of what is required for an effective third-party risk management, it does not provide a comprehensive and consistent framework. Thus, firms risk failing to capture the full lifecycle and range of third-party relationships, which may create inefficiencies, blind spots and inconsistencies, e.g.:

“[We do] not yet have a central third-party policy that defines roles and responsibilities; instead these are

covered by a number of policies. As such there are areas of responsibility overlap and minor gaps which are resolved by close interaction.” – Risk manager at medium-sized general insurer

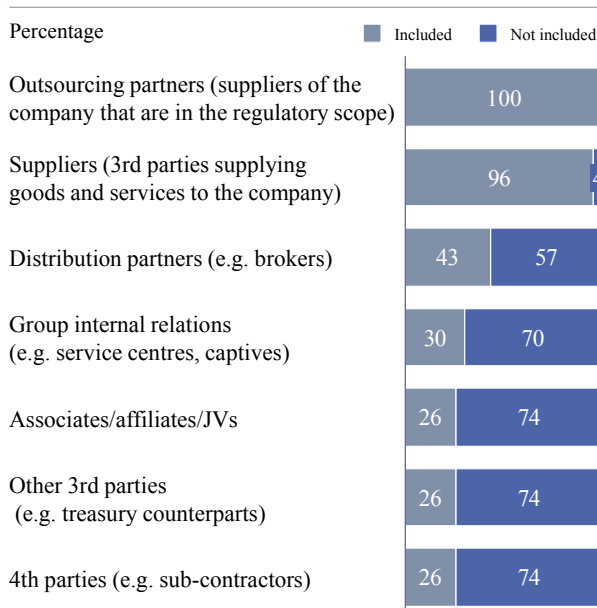
**VARYING COVERAGE**

The most striking variation in coverage concerns the scope of third-party risk management frameworks. Counterparts of firms in our survey range from around ten to several thousand – and much of this is neither explained by differences in size nor by differences in business activity. For example, generally life insurers and smaller firms assess fewer numbers. Most institutions only include suppliers in their framework managing third-party risk, excluding distribution partners, captives, associates, affiliates etc. and some apply additional limitations, such as size, geography or their counterparts’ business activities (Exhibit 4). Additionally, few companies apply a stringent segmentation approach.

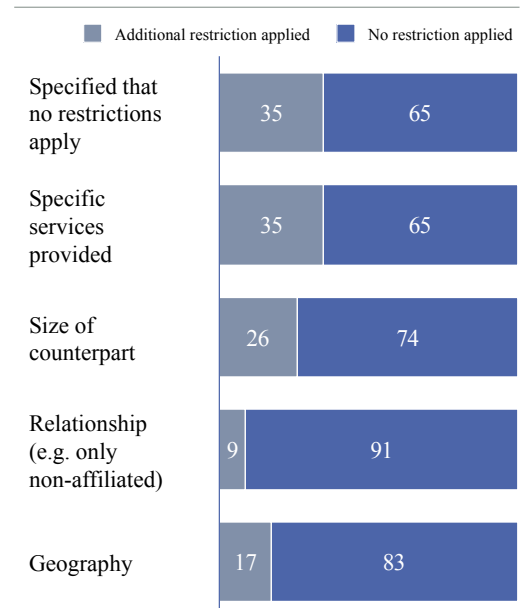
EXHIBIT 4

Types of counterparties in third-party risk management

**Question:** Which counterparts are covered by your framework for 3rd party/ supplier risk management?



**Question:** Are there any other restrictions you place on inclusion of counterparts in your framework for 3rd party/supplier risk management?





---

“[WE DO] NOT YET HAVE A CENTRAL THIRD-PARTY POLICY THAT DEFINES ROLES AND RESPONSIBILITIES; INSTEAD THESE ARE COVERED BY A NUMBER OF POLICIES. AS SUCH THERE ARE AREAS OF RESPONSIBILITY OVERLAP AND MINOR GAPS WHICH ARE RESOLVED BY CLOSE INTERACTION.” Risk manager at medium-sized general insurer

#### **MAIN FOCUS ON SELECTION AND ONBOARDING**

Firms tend to focus their risk management on the selection of third parties, including due diligence and onboarding. Continuous monitoring is less common and in some cases missing altogether.

The initial due diligence is one of the most important elements of third-party risk management. However, over-reliance on it leaves firms vulnerable to deterioration in third-party performance, as well as concentrations, e.g., through mergers between suppliers. Furthermore, third parties may bypass the review process if they are erroneously deemed not to be material or if they only become material later in the relationship.

## RECOMMENDATIONS AND THE ROAD AHEAD

Given the issues surfaced by our research, many (re) insurers and investment managers would benefit from establishing a common set of standards and a more systematic and comprehensive approach to third-party risk management framework. This will provide a holistic, end-to-end view of third-party risks and enable (re)insurers and investment firms to be more effective and efficient in managing those risks.

Based on our research, organisations should focus their efforts on four areas:

- Formulate an explicit third-party risk management framework, including a clear definition of ownership and governance, standardised workflows and an articulation of risk appetite in respect of third parties, aimed at creating alignment among internal stakeholders
- Extend the scope to all third parties and apply risk-based segmentation to determine the level of control required
- Put in place a proactive and comprehensive approach to third-party risk management, including ongoing monitoring and escalation processes  
Invest in IT tools like data management systems, end-to-end workflow tools and analytics to increase efficiency of and ensure consistency in the process.

### FORMULATE AN EXPLICIT THIRD-PARTY RISK MANAGEMENT FRAMEWORK

A failure to design and implement an explicit third-party risk management framework may obscure potential gaps and overlaps between existing policies and procedures. Conversely, a clear framework ensures a balance between risk and commercial factors, increasing the effectiveness of risk management. (Re)insurers and investment managers should consider three key actions:

- Incorporate third-party risk management into overall risk appetite and limits, which will set the tone from the top and establish clear mechanisms for business lines and key stakeholders to identify and manage risks. Some areas may require qualitative expressions of risk appetite and limits (e.g., compliance level), while others may be measured quantitatively (e.g., minimal credit rating).

- Implement clear governance and escalation processes, providing structured forums and interfaces for stakeholders, including business lines, operational risk, compliance, finance, procurement and IT. This will break through silos and enable balanced and joined-up decision making. Mandate a committee to be responsible for third-party risk, with processes defined end to end.
- Standardise third-party risk management workflows across the organisation, including for the composition and scope of responsibility of due diligence and onboarding teams.

### EXTEND THE SCOPE TO ALL THIRD PARTIES AND APPLY RISK-BASED SEGMENTATION TO DETERMINE THE LEVEL OF CONTROL REQUIRED

While regulators often only require a risk management process for material outsourcing partners, experience has shown that third parties outside the regulatory scope can be the source of significant risk, e.g., reputational risk.

(Re)insurers and investment managers should take a close look at their exposures and design a segmentation framework that enables a comprehensive view of their dealings with all third parties, even if some counterparts will only be monitored minimally, to ensure that all material third-party risks are identified and managed.

### APPLY A PROACTIVE AND COMPREHENSIVE APPROACH TO THIRD-PARTY RISK MANAGEMENT, INCLUDING ONGOING MONITORING AND ESCALATION PROCESSES

Third-party risk must be monitored through the relationship lifecycle, not just at the onboarding stage. Ongoing monitoring should capture material changes after the third party has been onboarded and limit the implications of potential failures in the due diligence process. It should also help to ensure third parties continue to fulfil the firm's needs and abide by contractual arrangements.

Monitoring should be tailored to third-party risk profiles, e.g., periodic reviews for high-risk counterparties, ongoing management information for key third parties.

### INVEST IN IT TOOLS, LIKE DATA MANAGEMENT SYSTEMS, END-TO-END WORKFLOW TOOLS AND ANALYTICS

Automated tools can help firms organise data more effectively, identify breaks and failures, analyse trends and patterns as well as support consistent and efficient work routines. Resources may include:

- A *central repository* and data management system that enables an overview of relationships and aggregation of risk exposures, as well as deep dives into individual third-party relationships
- An *end-to-end workflow tool* to minimise breaks and duplication between teams, leveraging digitisation to increase process effectiveness and efficiency
- *Robust analytics capabilities*, including data visualisation tools to help monitor behaviours and enable a more proactive approach.

In addition to the actions taken by individual firms, the industry as a whole should improve third-party risk management. This might mean to agree on common standards and industry best practices. Both sides in a third-party relationship benefit from clear requirements and limitations, e.g., regarding data access, reporting expectations and contract terms.





Firms should also review systems and processes to address data management and cybersecurity, which are rightly attracting a significant amount of attention following numerous cases of cyberattacks. To protect customers and themselves as well as to reassure regulators, (re)insurers and investment firms should ensure that their systems and the systems of related third parties are up to standard


### CONCLUSION

Third-party risk management is increasingly important for (re)insurance and investment firms as well as the regulators supervising them. Our survey and research have shown that while firms have made good progress. However, there is still room for improvement, especially in ensuring that:

- Firms have an effective third-party risk management framework
- All third parties are covered with an effective segmentation approach in place
- There is adequate focus on ongoing, post-onboarding monitoring and management of third parties
- Third-party risk management processes are supported by adequate tools.

# APPENDIX 1 | DETAILED SURVEY RESULTS BY FRAMEWORK DIMENSION

	<p><b>Third-party/supplier scope.</b> Based on participants' responses, the industry seems to have adequate practices in place to determine the third parties/suppliers within scope, despite significant variation in the actual types of third parties included in the framework (not only does the type and number of third parties vary widely among participants, limiting factors, such as size, service provided and geography are also frequently applied).</p> <p>Establishing a single repository of third-party relationships and contracts that is broadly accessible seems to be particularly challenging. Many participants noted the problem of several legacy systems. There are also issues with ensuring access for relevant employees. Finally, there are different practices regarding the location of the repository: some firms use the legal function, others procurement or a decentralised system in which department managers keep records.</p>
	<p><b>Third-party/supplier risk segmentation.</b> The industry seems to have adequate practices in place in relation to segmentation of third parties. However, participants' comments indicate there are issues with the comprehensiveness and practical application of segmentation. For example, one participant noted that only material outsourcing relationships were assigned a risk level, while another participant did not split material relationships into different risk levels. Additionally, answers to the annual segmentation review were the broadest, indicating a wide range of practices.</p>
	<p><b>Third-party due diligence and onboarding.</b> The industry seems to have adequate practices in place regarding third-party due diligence and onboarding. However, the descriptions of the teams responsible for and involved in due diligence and onboarding, as well as the materiality criteria, show significant differences in practices applied. For example, many firms use an ad-hoc group instead of a dedicated due diligence team. Participants also noted that different due diligence teams are needed to evaluate different third-party relationships.</p> <p>The teams most frequently involved in due diligence are the relationship-holding business unit, risk, compliance, IT, data security and procurement. If the relationship-holding business unit is not involved in due diligence, then the procurement function usually is. A similar substitution is visible between risk and compliance.</p> <p>Several firms use the same composition for due diligence and onboarding teams (about a third of participants). The most common participants in the onboarding group, aside from the relationship-holding business unit, are procurement, legal and data security.</p>
	<p><b>Control systems in third-party risk management frameworks.</b> The industry has defined key escalation triggers and assigned adequate controls. However, the majority do not seem to have a centralised repository of controls and escalation triggers and many do not regularly update these.</p> <p>Several partial solutions seem to be in place, e.g., escalation triggers defined, but only for material outsourcing relationships, or a centralised repository that only includes contract terms.</p>

	<p><b>Scorecards and risk assessment of third parties.</b> Most firms regularly review on-the-ground third-party operations, monitor compliance of third parties with applicable regulation and undertake reviews in a rule-based manner. Fewer firms use comprehensive scorecards.</p> <p>Some firms use a more advanced risk-based approach for scheduling reviews and some build rule-based reviews into the third-party contract. However, there are also firms that rely solely on the self-assessment of third parties.</p>
	<p><b>Governance of third-party relationships.</b> The industry seems to have adequate practices in place regarding third-party risk governance. The least common practice in this segment seems to be contingency planning for degradation or non-delivery of third parties.</p> <p>Most firms seem to use a risk committee for third-party risk management, while some firms also leverage operational committees and executive committees for risk management decisions. The use of a specialised committee to handle third-party/supplier risk is uncommon (about a third of participants mentioned one).</p> <p>Despite most firms having adequate practices in place, several participants cited challenges in this area. These include a sole focus on material outsourcing, inconsistencies and lack of regular reporting. Follow-up interviews also did not confirm whether third-party/supplier risks are explicitly included in the assessment of other risks.</p>
	<p><b>Organisation of the third-party risk management framework.</b> Most firms have clearly defined rules for handling third-party/supplier risk without gaps in the division of responsibilities. However, there seems to be issues regarding overlaps in the division of responsibilities and interfaces between units.</p> <p>Some participants pointed out that overlapping responsibilities were intentional to ensure coverage. However, since most firms that had overlapping responsibilities also acknowledged gaps in the division of responsibilities, it is unclear whether this is always the case.</p>
	<p><b>Policies in place regarding third-party relationships.</b> The industry seems to have adequate practices in place regarding third-party/supplier risk management policies. There are, however, significant differences between firms, ranging from all best practices being fully observed to participants' qualitative comments indicating that while most best practices are included in the policy framework, often the inclusion is only implicit, with no specific reference to third parties/suppliers.</p>
	<p><b>Tools for third-party risk management and access to third-party data.</b> Adherence to best practice was the lowest in this area. Most firms have a clear owner of third-party data and arrangements for access to the data. However, most firms do neither have a clear and easily accessible workflow tool (almost three-quarters of participants) nor a comprehensive database of third-party exposures and risks, accessible by all relevant parties (more than two thirds of participants).</p> <p>Some participants noted that new tools for third-party/supplier risk management are being implemented, addressing some of the challenges.</p>

## APPENDIX 2 | MATURITY DIAGNOSTIC FORM

		<b>BASIC PRACTICE</b>	<b>COMMON PRACTICE</b>	<b>BEST PRACTICE</b>
1	Scope	Only the most important relationships are managed for risk	Inventory covering most external relationships; third-party relationships are identified, but not always centralised in a single repository	A comprehensive central inventory of third parties is established, including outsourcing partners, suppliers of goods and services, distribution partners, group-internal relations, associates/affiliates/JVs, other third parties and important fourth parties (sub-contractors)
2	Segmentation	Critical third parties are selected mostly by size of exposure	Third parties are grouped into high, medium and low importance as well as segmented by exposure and risk assessment (value of contract, expert panel assessment of risks)	Segmentation is risk-based and directly linked to monitoring activities. It is regularly reviewed by an expert group and includes qualitative and quantitative risk assessment across all risk dimensions
3	Due Diligence	Risk management capabilities of third parties are assessed; the supervisor is notified in case of material outsourcing	Rigorous due diligence by team representing most stakeholders; assessment is standardised to some extent. Multiple risk factors are identified and scored	Onboarding and due diligence tests are based on carefully designed rules. Specific due diligence tests are performed if triggered and specialised onboarding teams are in place (for medium-sized to large institutions), trained to identify risks based on materiality criteria. Multiple risk factors are identified and scored
4	Control-system	Some escalation triggers are defined, e.g., breach of SLA. There is no formalised risk framework	Lack of comprehensive or centralised repository of key risks; key escalation triggers are defined and controls are assigned to them	Control systems include comprehensive lists of risks and escalation trigger-points. Triggers are updated regularly and collected in a central depository, along with corresponding controls
5	Scorecards & Risk assessment	The compliance of third parties with applicable regulation is monitored	Third-party operations in critical dimensions are regularly reviewed (e.g., information security) and internal metrics defined	Comprehensive scorecards to help monitor compliance with regulation and performance relative to internal metrics; third-party performance and behaviour is continuously observed to limit risks, including on-site audits where meaningful

		<b>BASIC PRACTICE</b>	<b>COMMON PRACTICE</b>	<b>BEST PRACTICE</b>
6	Governance	Third-party risk is implicitly addressed through other risk types. In addition, there is at least one committee covering third-party risks (as well)	A specialised committee, e.g., focused on operational risks, has a mandate to look into third-party risks, along with escalation mechanisms, reporting and documentation. Governance is typically mandated within business units	Definition of a clear owner with decision-making powers; escalation frameworks to defined committees are in place. Contingency plans are formulated to deal with failure or degradation of critical third-parties
7	Organisation	Roles regarding third-party risk management are only loosely defined	Roles and responsibilities regarding third-party risk management are clearly defined for most essential steps in the process (e.g., between onboarding and monitoring). Large regional differences are often observed	Alignment of third-party risk management with the divisional and geographic setup of the organisation; instituted communication between groups involved in third-party risk management; clear roles and accountability are defined for third-party risk management, especially due diligence, onboarding, auditing and segmentation
8	Policy framework	Third-party risk is covered by policies that are regularly reviewed	Third-party risk is explicitly addressed by firm policies	A robust policy framework includes: i) a global third-party risk management policy to establish a firm-wide control framework and minimum standards, ii) individual policies for functions relevant to third-party risk management, including compliance, finance, procurement, and iii) regional policies tailored to the relevant jurisdiction's regulatory and legal requirements. The third-party risk policy is aligned with other risk policies in the firm, which explicitly mention third-party risk where appropriate
9	Tools & data	Third parties provide regular reports	Access to data stored at third parties is ensured, even if a third party ceases to operate	Third-party risk management is implemented with an end-to-end workflow tool, accessible by all relevant parties and integrated with adjacent platforms. All third-party risk data is stored in a central depository

## AUTHORS

### **Daniel Mikkelsen**

Senior Partner  
McKinsey & Company

### **Angelika Reich**

Partner  
McKinsey & Company

### **Emily Yueh**

Partner  
McKinsey & Company

### **Caroline Coombe**

Chief Executive  
ORIC International

### **Michael Bartholomeusz**

Deputy Chair  
ORIC International, and  
experienced former Chief Risk Officer

**Lead researchers:** Alexandra Mabey (ORIC International), Daniel Kaposztas (McKinsey & Company)

The authors would also like to thank Ulf-Erik Lett and Vasiliki Stergiou for their contributions.

\* \* \* \*

Founded in 2005, ORIC International is the leading operational risk consortium for the global (re)insurance and asset management sector. It is a not-for-profit organisation that facilitates the anonymised and confidential exchange of operational risk intelligence between member firms, providing a diverse, high quality pool of quantitative and qualitative information on relevant operational risk exposures. ORIC International provides industry benchmarks, undertakes leading-edge research, sets trusted standards for operational risk and provides a forum for members to exchange ideas and best practices. It has 40 members with accelerating growth globally.

McKinsey & Company is a global management consulting firm that has been serving leading businesses, governments, non-governmental organizations, and not-for-profits for more than a 90 years. McKinsey operates as a global partnership owned by 1,400 plus partners united by a strong set of values, focused on client impact. McKinsey comprises more than 12,000 consultants and nearly 2,000 research and information professionals.