

THIRD-PARTY RISK MANAGEMENT IN THE TIME OF DORA: The challenge for the sell-side

IN ASSOCIATION WITH


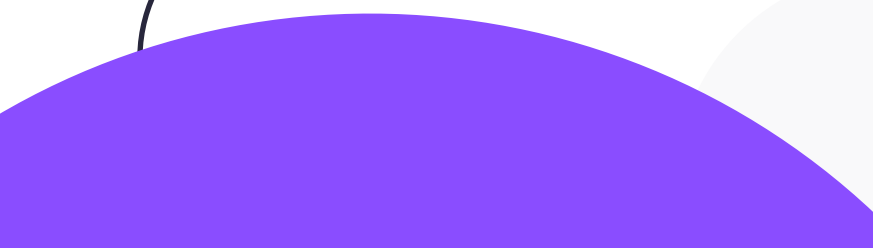



COMPASS PARTNERS
NAVIGATING FINANCIAL MARKETS



Table of Contents

PAGE 3	Introduction
PAGE 4	Introducing DORA
PAGE 6	Preparing for DORA
PAGE 9	Mapping relationships
PAGE 11	Monitoring relationships
PAGE 12	Reviewing relationships
PAGE 16	Exit strategies
PAGE 18	The future of TPRM



Introduction

The EU's incoming Digital Operational Resilience Act (DORA) is set to redefine how financial firms interact with their third-party suppliers. The regulation is intended to ensure that firms have the operational resilience to deal with cyber-attacks and other issues threatening the operations of their information and communications technology (ICT) stacks.

DORA will apply to over 20,000 EU regulated entities and has an extra-territorial impact for any firms with operations or activities in the EU. All Mifid II registered firms will be in scope for DORA.

For executives overseeing third-party risk management (TPRM), DORA is the latest in a web of guidelines and regulation that is exponentially increasing the complexity of the

role. For many firms, especially those on the buy-side, such as hedge funds and proprietary trading firms, DORA will be an entry point into formalised TPRM. However, it is one that is set to grow in complexity.

In order to understand how firms operational in derivatives and wider capital markets are preparing for DORA and their overall approach to TPRM, Compass Partners commissioned Acuiti to conduct a survey into the approaches and challenges they are dealing with.

This report focuses of the sell-side but also includes a look at how the asset management and proprietary trading communities are approaching the implementation of DORA. It is based on a survey of senior executives at 106 firms.

The key findings are:

- The complexity of third-party risk management has increased dramatically over the past three years, driven by evolving regulation and the increased risk of cyber attacks
- DORA is the most significant new regulation that firms are facing and over nine in 10 sell-side respondents said that they will have to make major changes to how they manage third-party risk to meet the requirements
- Awareness of DORA is concerningly low among the buy-side and proprietary trading communities, with little more than a year to go until implementation
- The top challenges firms are facing in preparing for DORA include the operational resources required; the criteria to analyse threats and getting information from vendors
- While a majority of sell-side firms already map third-party relationships across their firm, the number that map Nth party relationships, a key element of DORA, is much lower
- Few firms currently meet the full requirements of DORA with exit strategies for critical vendors, application to critical intra-group relationships and the frequency of reviews of third-party relationships key areas of weakness
- Almost 90% of firms are increasing investment in TPRM to meet the requirements of DORA and other regulations and many are considering outsourcing management and compliance on a managed service basis





Introducing DORA

The Digital Operational Resilience Act (DORA) is the EU's response to the growing risk that cyber-attacks and other operational disruptions pose to financial firms' technology infrastructure and the resilience of the markets they serve.

While DORA is currently the most significant new regulation facing firms, it is also part of a wider web of rules and guidelines such as the PRA SS1/21 (Ops Resilience), PRA SS2/21 (Outsourcing and TPRM), FCA SYSC 8.1, EBA Guidelines on Outsourcing Arrangements and FSB Consultative Document on Enhancing Third-Party Risk Management and Oversight.

DORA sets out extensive requirements for firms to monitor and improve their operational resilience and manage their third-party relationships. It also requires firms to implement robust risk management and contingency plans, to mitigate the risk of disruption to the services they provide clients and the wider market.

DORA covers five core areas: ICT risk management, ICT incident reporting,

Resilience testing, Third-party risk mapping and Information sharing. At its core is extensive mapping and information gathering requirements designed to enable firms to understand and mitigate risk. This paper focuses on that element of DORA, in the context of sell-side capital markets firms.

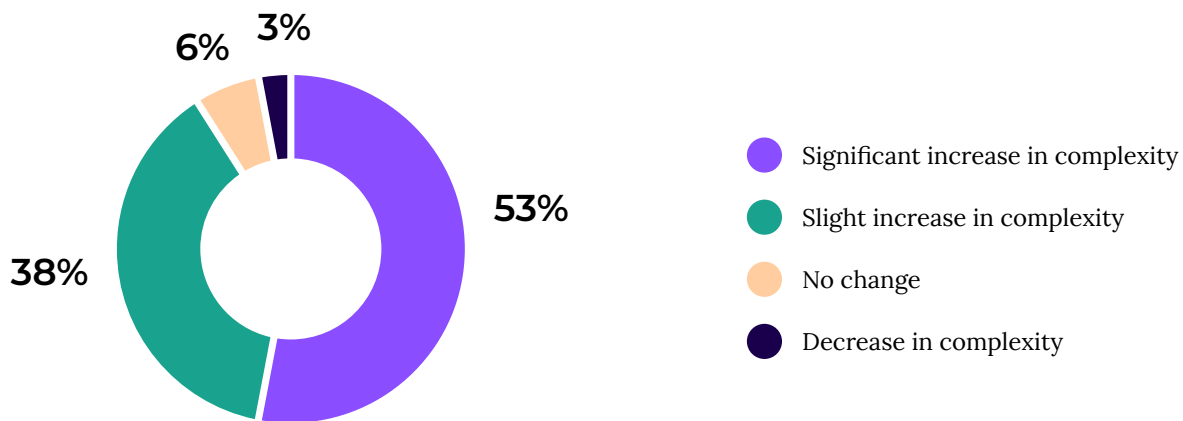
DORA comes off the back of a significant increase in complexity for third-party risk management on the sell-side. Over half of respondents to this study said that they had seen a significant increase in the complexity of third-party risk management.

This has been driven by a wide range of factors, from increased regulation to the heightened risk of cyber-attacks. These factors have emerged amid a proliferation of vendor relationships, as markets have grown in sophistication and complexity.

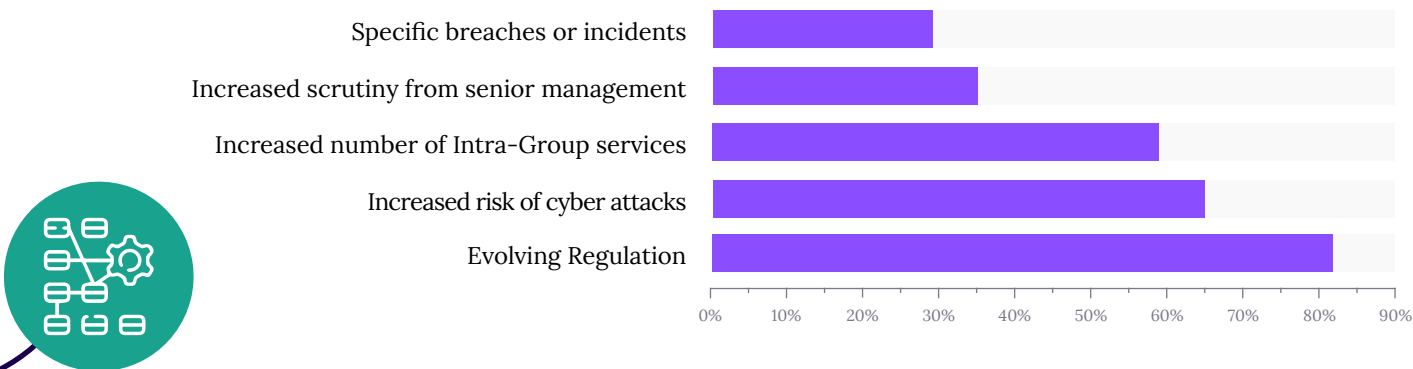
In addition to the move to cloud-based delivery and subsequent need to monitor several core hosting environments, these factors have created exponential increases in the complexity of third-party risk management.



Overall, how has the complexity of third-party risk management changed for your organization over the past three years?



What are the biggest factors in the increase in complexity?



This increase in complexity is only set to increase with DORA, which puts new responsibilities onto firms to map and monitor their third-party relationships. In many ways, DORA codifies practices that have been in

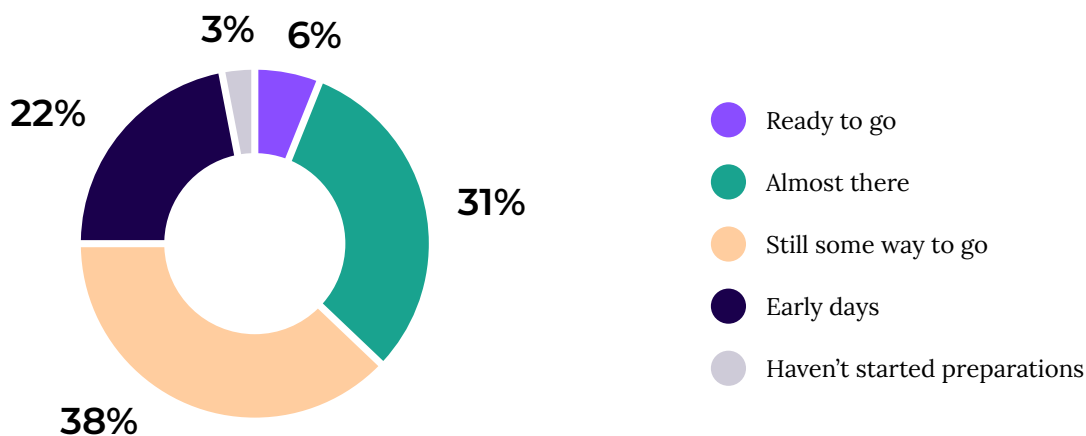
place across many sell-side firms. However, it is prescriptive in its approach and for most sell-side firms will require significant changes to how TPRM currently operates – both in terms of processes and team structures.

Preparing for DORA

Dora is set to apply as law from January 17, 2025. The survey found that most sell-side institutions were in progress with their preparations for DORA although, as would

be expected considering the timeframe to implementation, a majority had a long way to go before they were ready for implementation.

How prepared is your organization for the implementation of DORA?



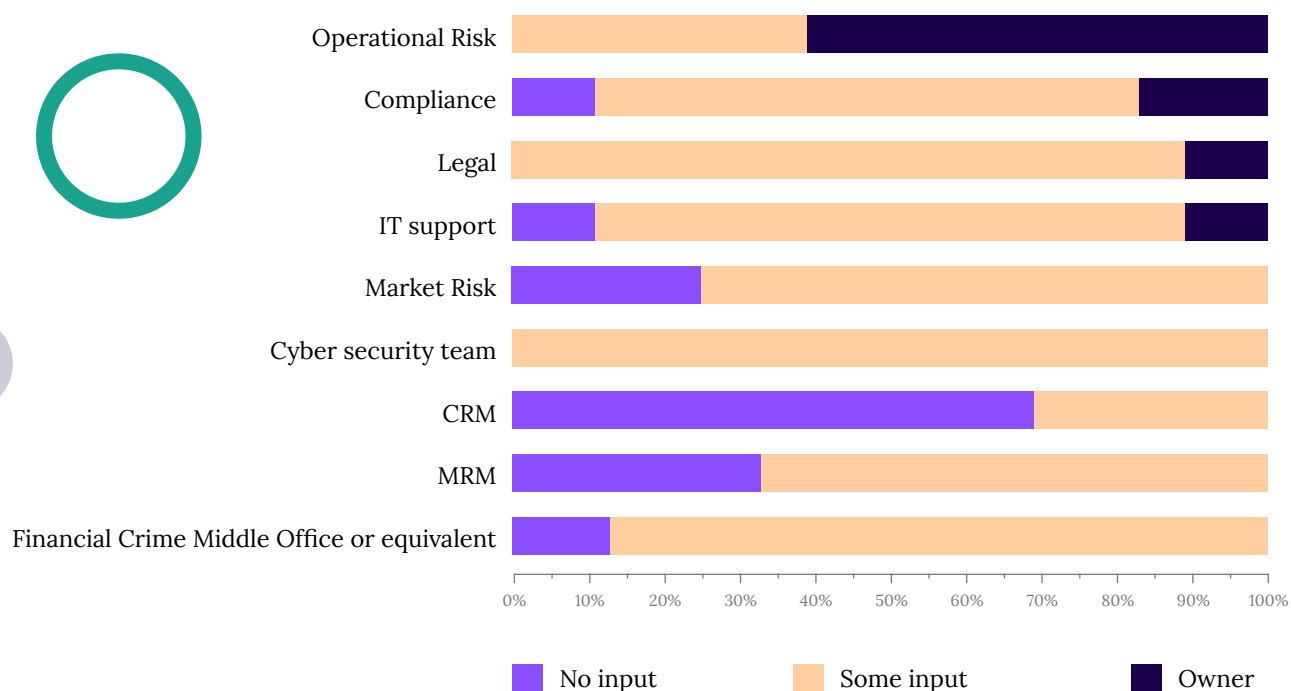
While DORA builds on existing protocols and processes, 94% of respondents said that they were having to make changes to how they manage third-party risk in order to meet the requirements.

A key issue from the outset, particularly for large sell-side institutions, has been which department takes the core responsibility for

the implementation of DORA. At most firms, TPRM historically has been spread across various different teams with no one specific owner.

DORA changes this and most firms will now require a new team structure to take ownership or at the very least a formalisation of responsibilities.

Which departments in your organization are currently responsible for TPRM as part of their function?



This survey found that operational risk departments were the most likely owners of TPRM within large sell-side institutions. However, there is clearly significant

fragmentation over decision-making at many organisations – creating a risk that implementation of DORA can fall through the gaps.

The top 5 challenges for the sell-side in preparing for DORA:

- 1** Operational resources required
- 2** Understanding the criteria to analyse threats
- 3** Getting information from vendors
- 4** Assessing vendor relationships
- 5** The cultural shift from a reactive to a proactive approach



Respondents to the survey reported multiple challenges in preparing for DORA, with the operational resources required the top challenge for most respondents.

Proprietary trading firms and asset managers

For proprietary trading firms with operations or trading activities in the EU, the immediate challenge posed by DORA is one of awareness.

In the most recent Acuiti Proprietary Trading Expert Network report, a survey of over 100 senior proprietary trading executives from the global market, 80% of respondents based in Europe said either that they did not know they were impacted or that their firm wasn't impacted.

With DORA applying to all Mifid II investment firms, almost all proprietary trading firms in Europe will come into scope of the regulation.

Of those firms that were in the process of implementing DORA, the biggest challenge was the scale of operational resources required to prepare. Additional challenges included getting information from vendors, understanding the criteria to analyse critical vendor relationships and the costs of implementation.

Awareness among asset managers was stronger but they share similar challenges. Getting information on vendors was the top challenge for asset managers followed by the operational resources required to get ready.

“80% of respondents based in Europe said either that they did not know they were impacted or that their firm wasn't impacted.”



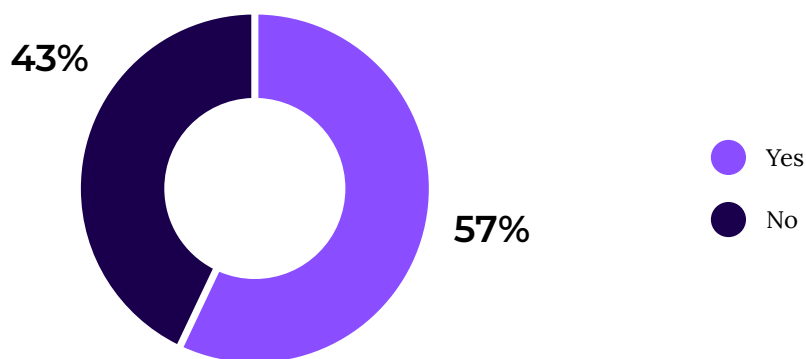


Mapping relationships

While many elements of DORA will replicate existing processes such as extensive penetration testing and due diligence on

vendors, the new regulation codifies and creates harmonised standards for how firms must map, monitor and report relationships.

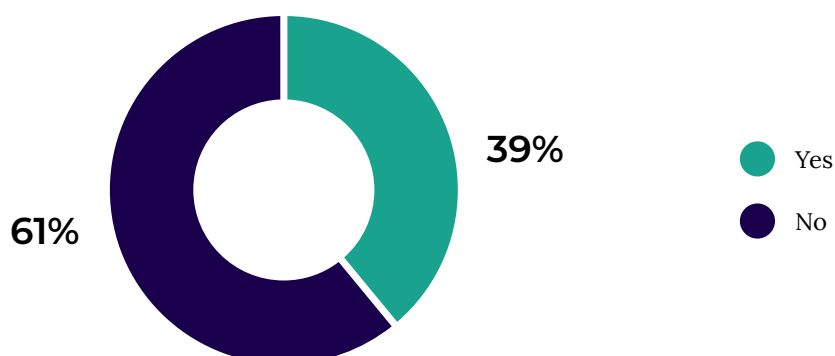
Do you have a centralised map of all your third-party relationships and associated services?



Almost half of respondents to the survey did not currently have a centralised map of all third-party relationships and associated services. Mapping of third-party relationships is essential to understanding concentration risk and the extent of impact across a firm

that issues with a key supplier would cause. While mapping direct relationships is relatively straightforward for a firm once resources and attention is applied to it, DORA also requires firms to map nth party relationships – i.e. their suppliers' suppliers.

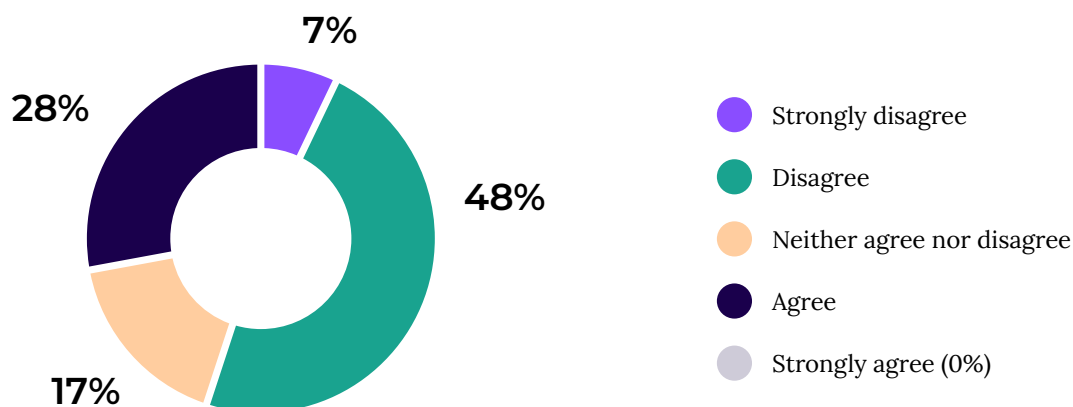
Does your mapping cover Nth party relationships?



While over half of respondents had mapped their third-party relationships, under 40% had successfully mapped nth party ones. A key challenge for mapping and monitoring nth party

relationships is gaining the information from vendors. Over half of respondents disagreed that vendors were good at providing the information that is asked of them.

Vendors are typically good at providing the information we ask of them with regards to TPRM



In defence of the vendors, DORA is a significant operational burden for them as well as their clients, especially for the larger vendors. Vendors need to isolate exactly which services and software are used by each client and then provide a map of their relationships

relevant to that software and those services. Many vendors have had to hire significant numbers of additional staff to meet the demands of DORA and it will inevitably take time before they are fully prepared for the extent and level of client requests.





Monitoring relationships

Mapping and understanding the scope and extent of both direct and nth party relationships is essential under DORA. The legislation also imposes strict standards for monitoring and reviewing those relationships.

A key definition within DORA is that of a critical supplier. This definition is based on a number of factors, including the nature and importance of the services provided by the vendor to the firm, the level of reliance that firm has on the vendor and the impact that any disruption would have on the firm's customers and financial markets as a whole.

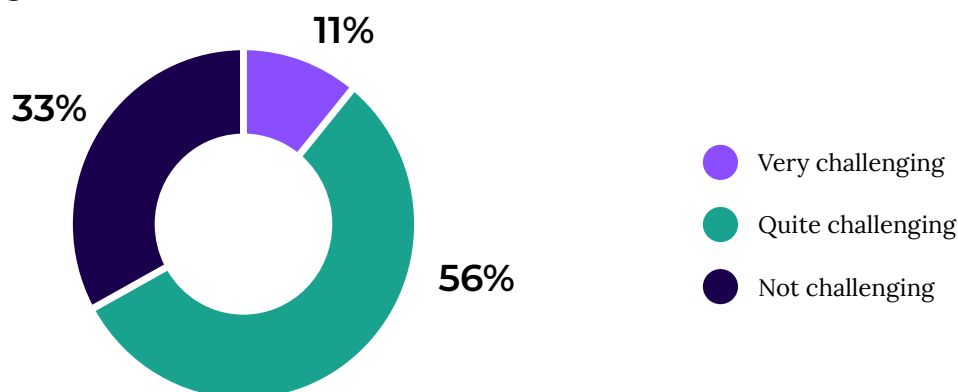
Another dimension that firms will have to consider is the criteria against which such relationships should be evaluated. These include the volume and complexity of the services provided by the vendor, the degree to which it is integrated into a firm's processing systems and processes, the extent of the firm's

reliance on that vendor and the impact any disruption would have on the firm's finances and reputation.

A major issue for the sell-side today is defining critical relationships. Some examples are clear. A payment provider for a bank or cloud provider in which large parts of the ICT infrastructure is hosted, for example, clearly represent a critical supplier.

However, when it comes to the granular processes within a firm's operations, the distinctions are less clear cut. Disruption to a core clearing system, for example, could be mitigated by a back-up, reducing the reliance on the vendor and meaning that the relationship is not critical. But if that vendor also provided a front office and risk management system then the impact of all services going down at the same time would render that supplier a critical supplier.

How challenging do you find it to identify critical relationships within your third-party mapping?



For these reasons, two-thirds of respondents to the survey said that they found it challenging to identify critical relationships within third-party mapping.

Reviewing relationships

Designating a vendor as critical also requires a different set of monitoring processes. Respondents to the survey said that once a critical vendor had been identified, the most

common additional steps that they currently deployed were an increased depth of audit, a greater depth of functional reviews and increased frequency of the audit.

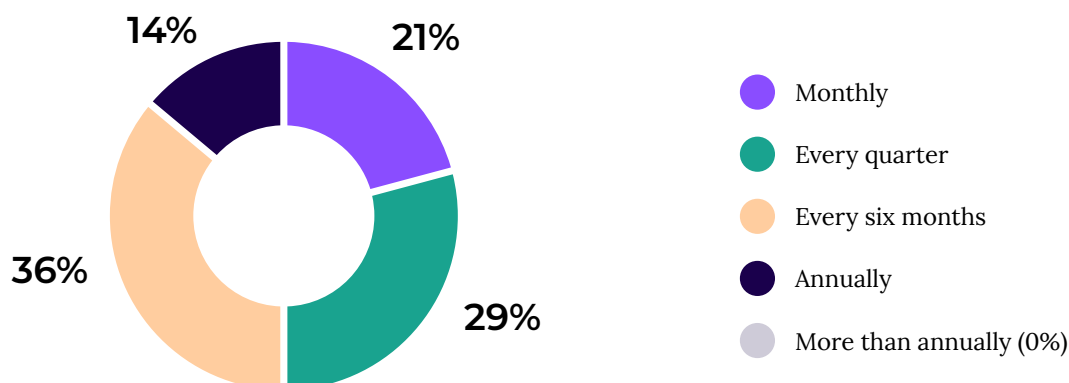
Once a relationship has been identified as critical, what additional steps do you take to monitor that vendor?

- 1** Increased depth of audit/due diligence processes
- 2** In depth functional reviews (IT, Compliance, legal etc)
- 3** Increased frequency of audit/due diligence processes
- 4** Requirement of additional documentation
- 5** On-site reviews
- 6** Performance reviews

DORA sets out requirements to monitor critical suppliers on a quarterly basis to identify and mitigate risks. Currently only half of respondents

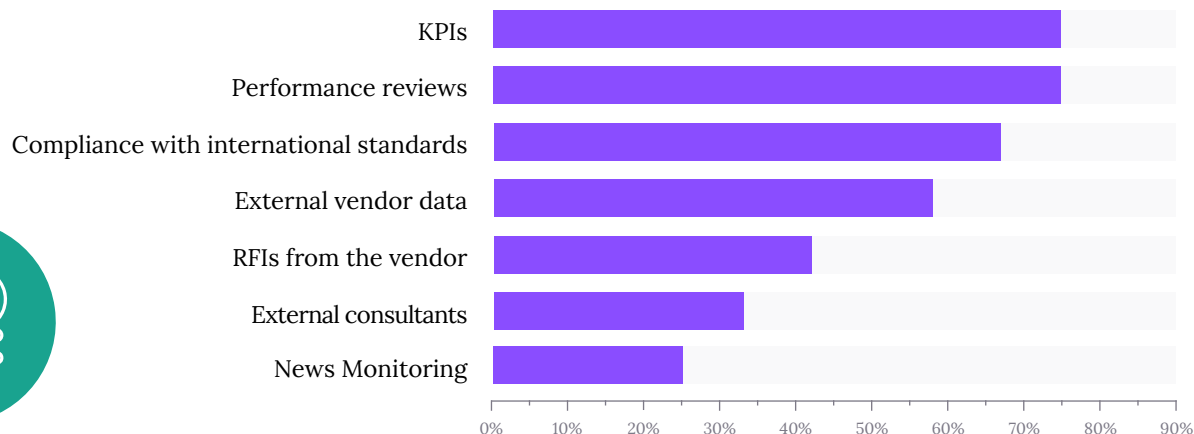
reviewed their critical relationships quarterly, suggesting that significant changes to the review process was necessary.

How regularly do you review your critical third-party vendor relationships to evaluate risk?



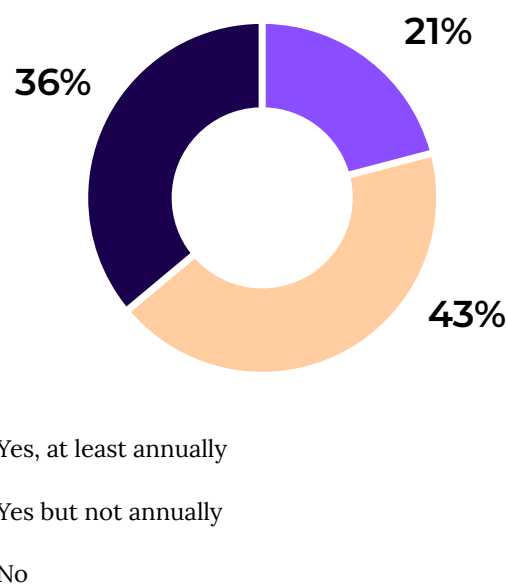
Most respondents relied on inhouse information when conducting their monitoring of critical relationships, with three quarters of firms setting KPIs and conducting performance reviews.

What sources of information do you use for your monitoring?



Two thirds of respondents also performed on-site reviews of key vendors but only a fifth did so on an annual basis.

Do you perform on site reviews of critical vendors?



“It is imperative that performance and KPI monitoring is streamlined and efficient. This process is becoming increasingly cumbersome for sell side firms and increases burden on the vendors. This is expected to continue as regulation increases and also considers “Nth Party” relationships”

Neil McDonald, managing partner,
Compass Partners

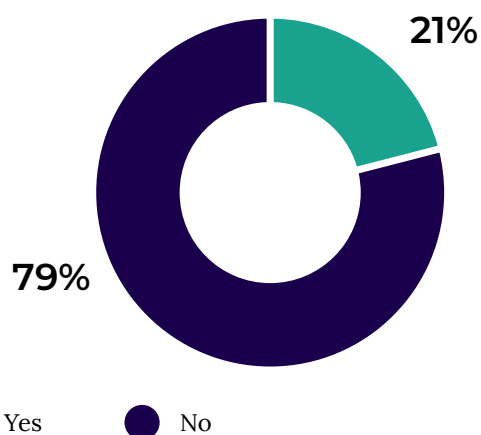
For larger firms, there is also the question of how to treat intra-group outsourcing. Regulators' position on intra-group services has caused some confusion since proposals for DORA were released. Many financial firms

operating structures' include entities that provide services such as IT or HR exclusively to the wider group. This confusion could be why just a fifth of firms held intra-group outsourcing to the same standards as they do third-parties.

"Interestingly, recent communication from EU based regulators have mandated the same robust processes for intra-group as they do external providers. This has meant that firms with a EMEA footprint are having to consider substitutability, KPI monitoring and exit planning for their intra-group outsourcing."

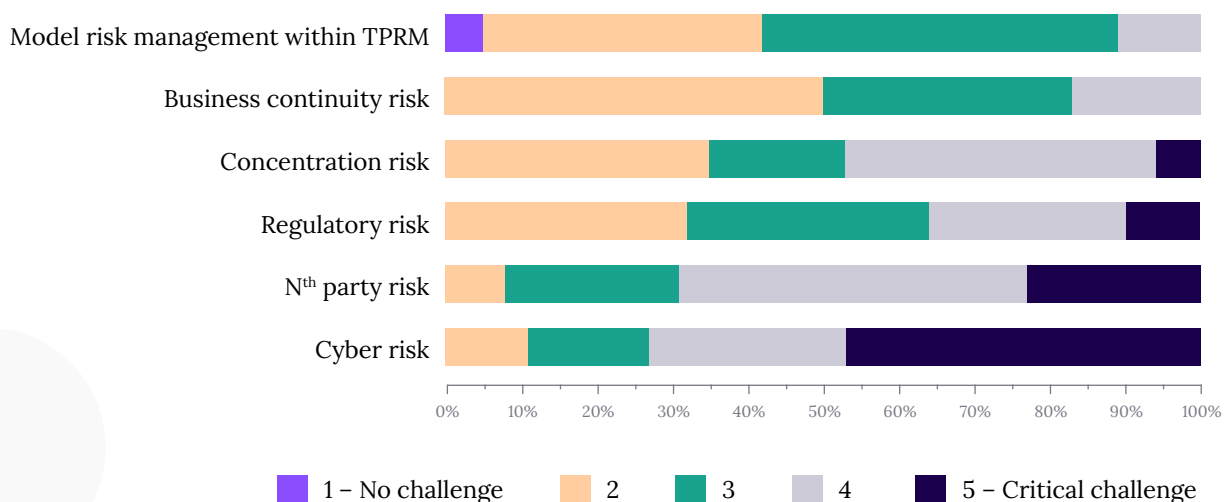
Neil McDonald, managing partner,
Compass Partners

Do you hold intra-group outsourcing to the same standards as third-party?



For most respondents to this study, nth party risk and cyber risk were the two most challenging areas to keep on top of. However, concentration risk was also a key concern.

How challenging do you find the following risks to manage when it comes to third party relationships?



Concentration risk has been elevated over the past decade by a wave of consolidation across the capital markets technology sector. This was initially welcomed by most in the market as it enabled firms to simplify vendor relationships and, in some instances, reduce costs by consolidating services with providers.

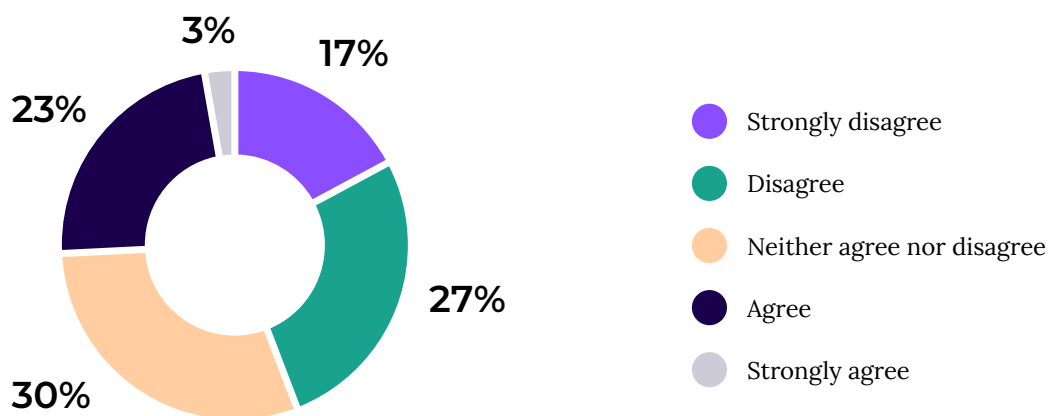
However, the price of that simplification was increased concentration risk, which is coming sharply into focus with the introduction of DORA.

This survey suggests that, while the market remains split on the pros and cons of vendor consolidation, the balance is tipping away from consolidation. 26% of respondents thought that streamlining relationships was more important than vendor consolidation risk, while 43% thought the opposite.

“Whilst there is commonality in how sell side firms are reporting concentration risk, the market is yet to see clear regulation in this area and how concentration risk is reported and managed differs across sell side firms.”

Neil McDonald, managing partner,
Compass Partners

Streamlining vendor relationships for operational efficiency is more important than vendor concentration risk





Exit strategies

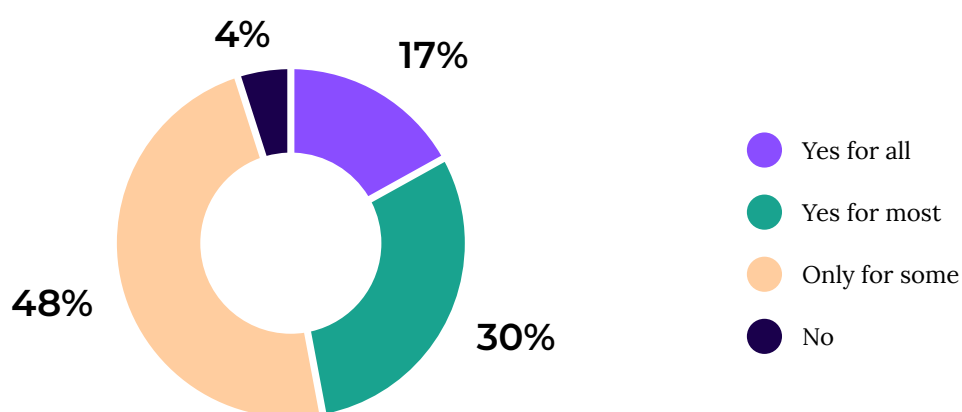
DORA requires financial entities to have exit strategies in place for all of their critical and material relationships. These exit strategies need to be designed to minimise the risk of disruption to the firm's operations and to protect its customers in the event that a vendor relationship is terminated. Exit strategies must be tested on a regular basis to ensure that they are effective and up-to-date.

Executives that took part in this study reported significant difficulty in establishing effective exit strategies for all their relationships. Much of the challenge comes from the circumstances in which the exit is required. If a relationship is terminated with a sufficient notice period, it would be relatively

straightforward to plan for the implementation of a replacement system with another vendor. However, if there was a sudden termination to a relationship this would be a significant challenge for critical vendors and require an entirely different exit plan.

Aside from having a back-up system for all processes, which for most firms would represent an unacceptable cost, there are no clear answers for firms on how to establish effective exit strategies across all vendor relationships. For that reason, only 17% of respondents had an exit strategy in place for all of their critical and material vendor relationships, with almost half having one in place only for some.

Do you have exit strategies in place for your critical and material vendor relationships?



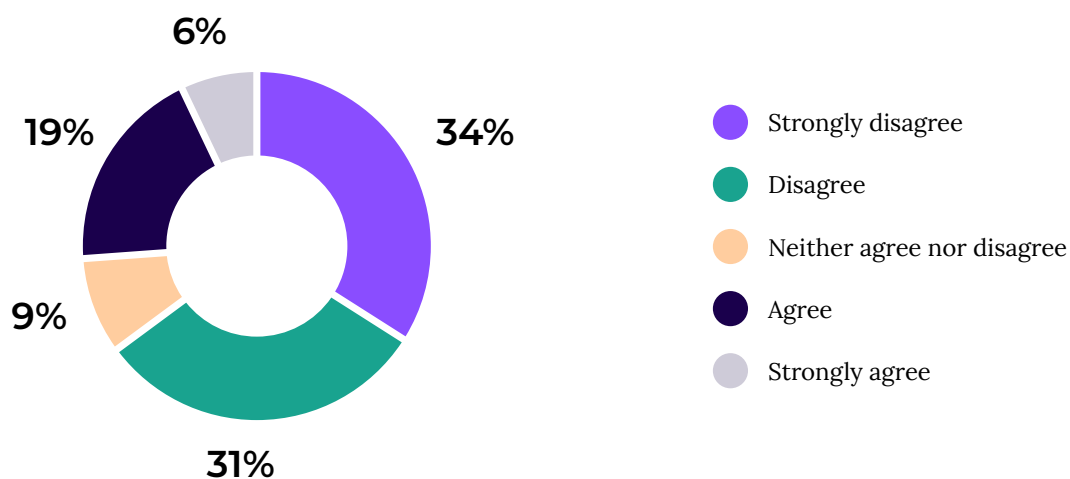
At the same time, 25% of respondents said that having no exit strategy in place for some critical relationships was an acceptable risk – a view that is likely to reduce as firms approach implementation of DORA.

“While 25% of survey respondents said not having an exit strategy in place for some critical firms is an acceptable risk, EMEA based firms are required to have exit strategies in place for critical vendors and also consider “soft” and “hard” exits, as well as test hard scenarios. The findings of this survey indicate that sell side firms are behind the curve in this regard.”

Neil McDonald, managing partner, Compass Partners



No exit strategy for some critical vendors is an acceptable risk

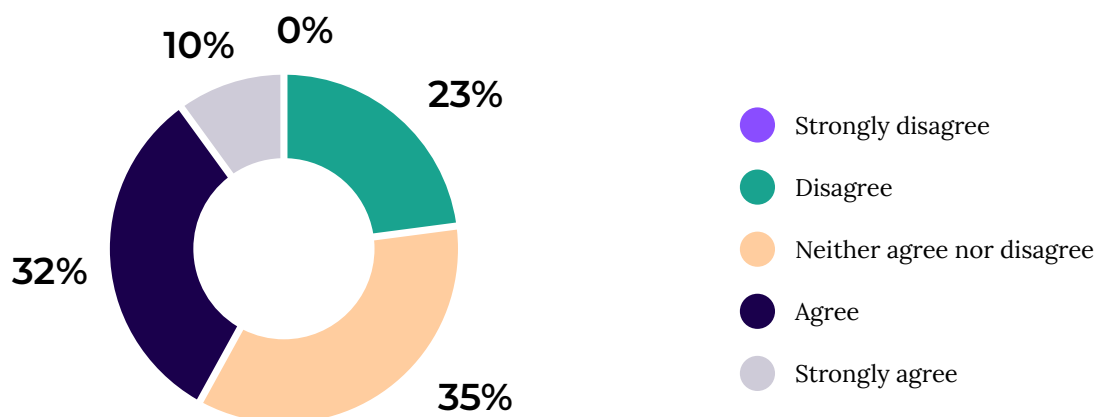


The future of TPRM

DORA will further accelerate an already changing landscape for how firms work with third-party vendors. A key question today is the impact that will have on firms' approaches

to outsourcing. For a significant proportion of the market, DORA and associated TPRM pressures are making them more inclined to build inhouse.

We are more inclined to build inhouse as a result of TPRM pressures



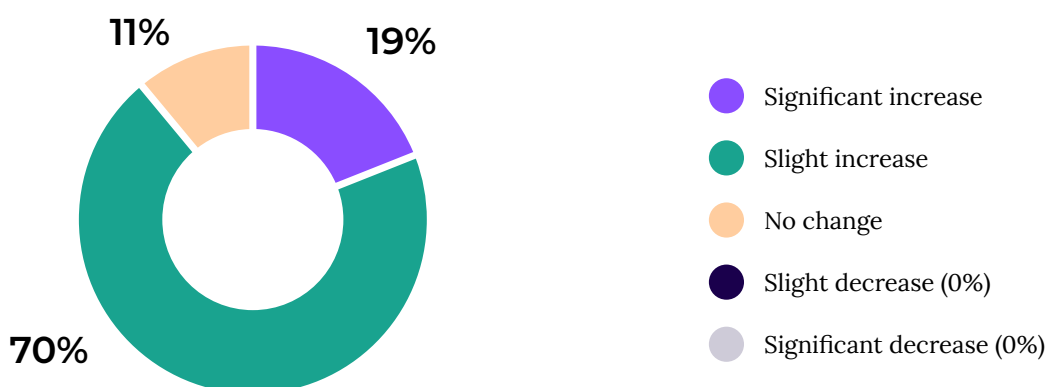
This will create separate challenges and threatens to reverse a long-term shift towards outsourcing that has enabled innovation and brought greater cost efficiency to financial markets. The rising complexity associated with TPRM is also likely to further drive consolidation among vendors and increase the barrier to entry for new firms, again potentially setting back innovation.

DORA is the latest strand in an ever-increasing web of complexity for third-party risk

management. The rising threat of cyber-attacks combined with increased complexity of internal monitoring and audit requirements is exponentially increasing the challenge for firms to keep on top of best practice and regulatory requirements.

As a result, respondents to the survey are expecting to significantly increase investment in TPRM. Overall 89% of respondents expect an increase in investment, with 19% planning a significant increase.

How do you expect your organisation's investment in TPRM to change over the next five years?



One alternative to investing internally is to outsource TPRM to a managed service provider. This was something that 74% of respondents were open to considering as a way of reducing cost and mutualising the process of information gathering and monitoring.

The survey found that for both proprietary trading firms and the sell-side, marshalling the required operational resources to prepare

for implementation was the biggest challenge. Firms are likely to look for support from consultants and managed services providers to share the burden and reduce costs.

This study found that firms have a long way to go in terms of getting their internal processes in place to meet the requirements of DORA. With little over a year to go until implementation, there is significant work to do.





About Compass Partners

Compass Partners is a boutique Managed Services Provider offering a comprehensive and outsourced approach to managing and supporting specific functions, processes, or systems with a focus on Operations, Risk Management and AML/KYC. In addition, we offer collaborative consultancy services to assist our clients in meeting their challenges

and goals in what is a constantly evolving market. The founding partners have combined over 40 years of experience in the Global Financial Markets specialising in TPRM, On-boarding, Trade Processing & Reconciliations, Customer Support, Business Development and Project Management.

What we do

Compass Partners possess in-house expertise in the fields of Operational & Digital Resilience, TPRM and Vendor On-boarding and the ongoing monitoring process. We are here to assist firms with the re-evaluation of their risk management strategies and Third Party framework helping them adapt to upcoming

regulatory changes efficiently. We also handle remediation projects across the inherent and residual third party risk lifecycle to ensure regulatory adherence and a consistent and coherent approach with your enterprise risk framework. For more information, contact:

neil.mcdonald@compasspartnersservices.com





0203 998 9190

acuiti.io

info@acuiti.io

Copyright © 2023 Acuiti. All rights reserved.