Baringa
Brighter together

Operational Risk Survey 2019/20

An evolving risk landscape

About this survey

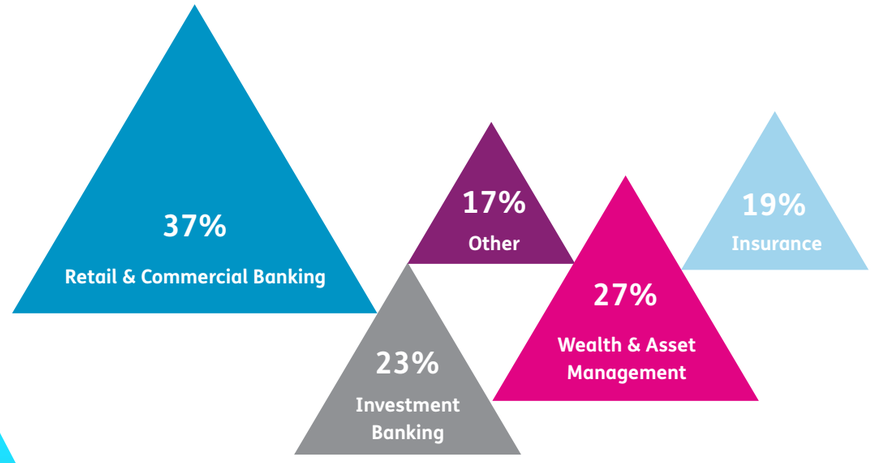
Following the success of our inaugural operational risk survey in 2018, Baringa launched the second iteration of the survey in Q4 2019. Once again, we invited firms across the financial services industry to provide their views on the state of operational risk management within their organisations and the challenges ahead.

The survey contained 33 questions, a number of which were also included in the survey last year, facilitating analysis of year-on-year movements and trends. The survey was carried out via form responses and through direct conversations with respondents, which has enhanced the depth of insight the survey has been able to provide this year.

The survey results contain data provided by 32 firms across the financial services industry. Almost 40% of respondents are in retail and commercial banking, and a further 27% in wealth and asset management services. Approximately 75% of responses relate solely to the UK and EMEA, with remaining respondents also answering questions on the basis of APAC and the Americas. This indicates that there may still be some way for firms to go to implement a truly global operational risk management framework.

The survey data can be analysed by sector, business activity and size of firm, allowing comparison versus peer organisations. We can help you benchmark your own firm against this data. For more information, please contact us via OpRisk@baringa.com.

Figure 1: Business activities undertaken by respondents



Executive summary

Now in its second year, Baringa Partners' annual operational risk survey explores firms' views on their key risks, the effectiveness of risk appetite statements and Management Information (MI), challenges around taxonomies and Risk and Control Self Assessments (RCSAs), and areas of future focus.

Firms are upskilling teams in specialist skills

The results indicate that firms' operational risk management frameworks are maturing. Firms are scaling back the size of their operational risk teams, and instead focussing on increasing the skills and experience of the team. They are engaging in targeted recruitment of individuals with cyber and resilience expertise. This reflects the fact that information security risk (including cyber) was the highest-ranked risk across the respondent group, with third party risk coming in second.

Automation and data analytics are the future

The single biggest area of investment that we have heard from market respondents is around increasing the speed and accuracy of reporting on operational risk. Although firms have reported improvements in their data management and reporting since last year, they are still spending a disproportionate amount of time on data collection. Utilising tools such as automation and data analytics will provide firms with the capacity to focus on where they can add the most value – interpreting and analysing the data.

Engaging the business remains a challenge

Risk assessments are evolving, as firms increasingly employ both causal and impact taxonomies, in addition to their risk taxonomies. Firms are also adopting more dynamic, trigger-based RCSAs, rather than the standard scheduled cycle of updates across the whole risk and control estate. These positive signs suggest firms are becoming more proactive and thoughtful in their risk management. However, firms continue to struggle to engage the business and make the RCSA output meaningful and useful. Data visualisation techniques and tools have been employed by other industries to tackle this problem, and financial services firms may wish to explore using similar techniques, if they aren't already.

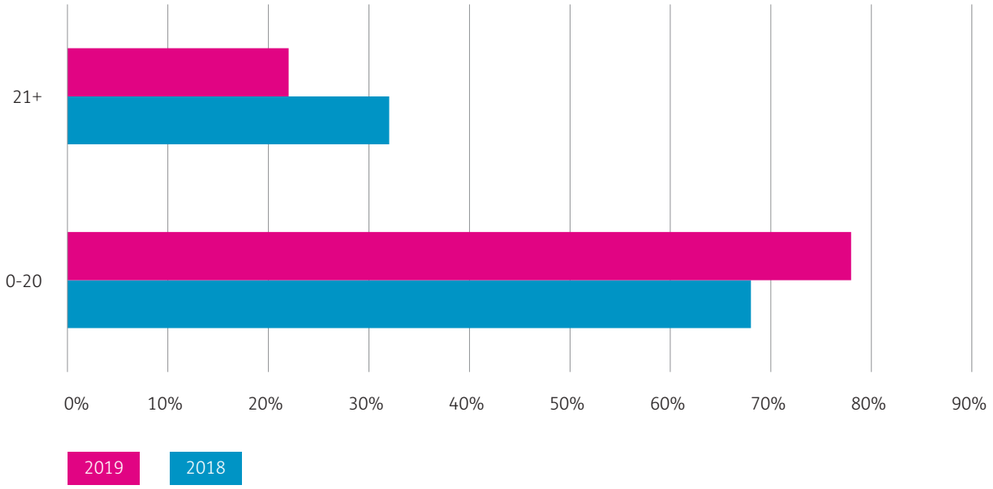
The future will see firms continuing to balance business as usual (BAU) and regulatory change

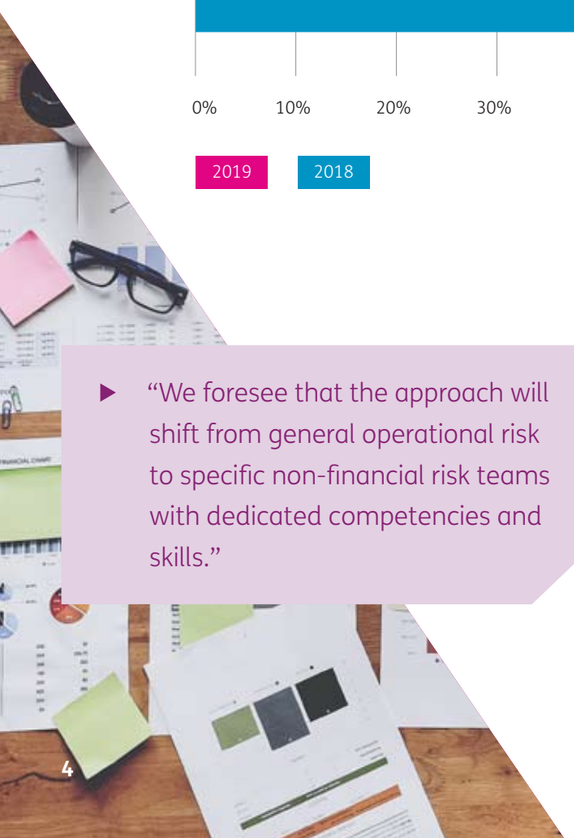
As we look ahead to the next two years, the main priority for half of respondents is continuing to refine their operational risk framework to address new regulatory requirements. Operational resilience, outsourcing and climate risk are all key areas of regulatory focus, but firms should also consider other emerging areas such as digitalisation and the ethics of artificial intelligence. At the same time, firms are also looking to implement more BAU enhancements around their processes, documentation, and systems. Balancing these competing requirements in an era of tight budgets and constrained resources will no doubt continue to prove a challenge for firms.

Operational risk organisation

Given the wide variety of respondents, the size of operational risk functions yet again varied considerably across the population surveyed. There was some indication of a scaling down of operational risk teams versus last year, but broadly results suggest a degree of stability across the operational risk organisations of participating firms.

Figure 2: Size of respondents' operational risk teams

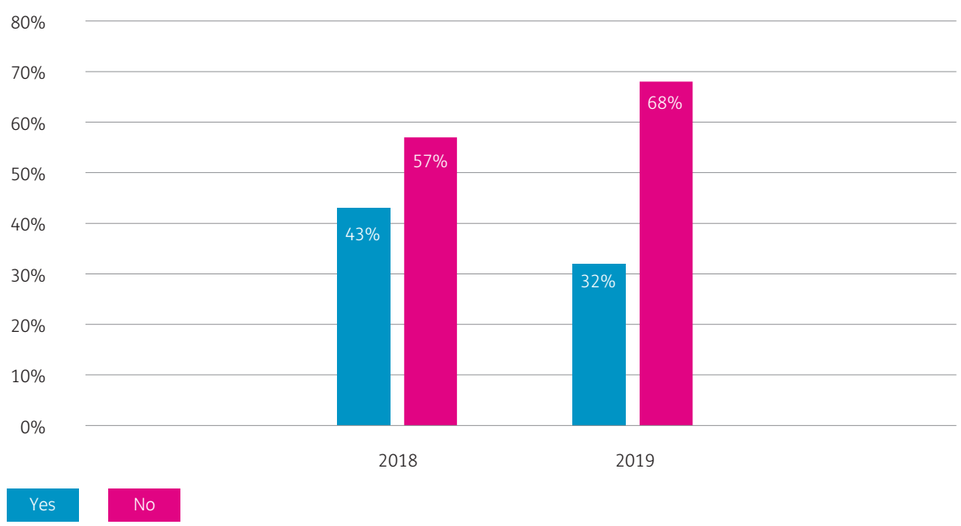




> "We foresee that the approach will shift from general operational risk to specific non-financial risk teams with dedicated competencies and skills."

Almost 70% of firms were not anticipating any material changes in the size of their operational risk teams in the next 18 months. That relative stability is a reflection of hiring undertaken over the past 18-36 months to bolster the operational or non-financial risk presence in many organisations.

Figure 3: Percentage of respondents expecting material changes to the size of their operational risk team over the next 18 months



In terms of the composition of operational risk teams, **nearly 80% of firms felt that they had sufficient skills and knowledge in the team** to provide effective challenge to the business. Nonetheless, several respondents noted that they were looking to further increase the expertise and experience of the team. This included building capability in areas of current regulatory focus, particularly around operational resilience and cyber risk.

From an organisation set-up perspective, **almost 70% of firms reported that they had a first-line operational risk team in place.** The nature of these teams varied considerably, with three broad models reported across respondents:

- Dedicated first-line teams focused on operational risk
- First-line teams focused on multiple risk types, including operational risk
- First-line teams focused on specific specialist sub-risks, e.g. financial crime or IT risk

Whilst a first-line risk team can help bridge the gap between the business and second line, firms should ensure that this doesn't result in the business relinquishing responsibility for identification, assessment and monitoring of risks in the process. First-line teams should act as a conduit between the business and second line, and help embed the risk framework, rather than acting as risk and control owners.

Firms should also ensure that the roles and responsibilities of the first-line and second-line risk teams are clearly defined to avoid inefficiencies and duplication. The teams should work with, rather than against, each other, to embed risk management into the business. Consistent training and tools across the two teams can help to facilitate this.

> "There is a 1b team, but they are quite inconsistent. Relationship historically has been really bad – massive friction between the teams."

Operational risk identification and appetite

Understanding of the operational risk landscape and its many nuances continues to evolve across the full breadth of the financial services industry. The increasingly granular understanding of the nature of risks and how they come to bear is driving greater sophistication in the way in which they are mitigated and reported on an ongoing basis.

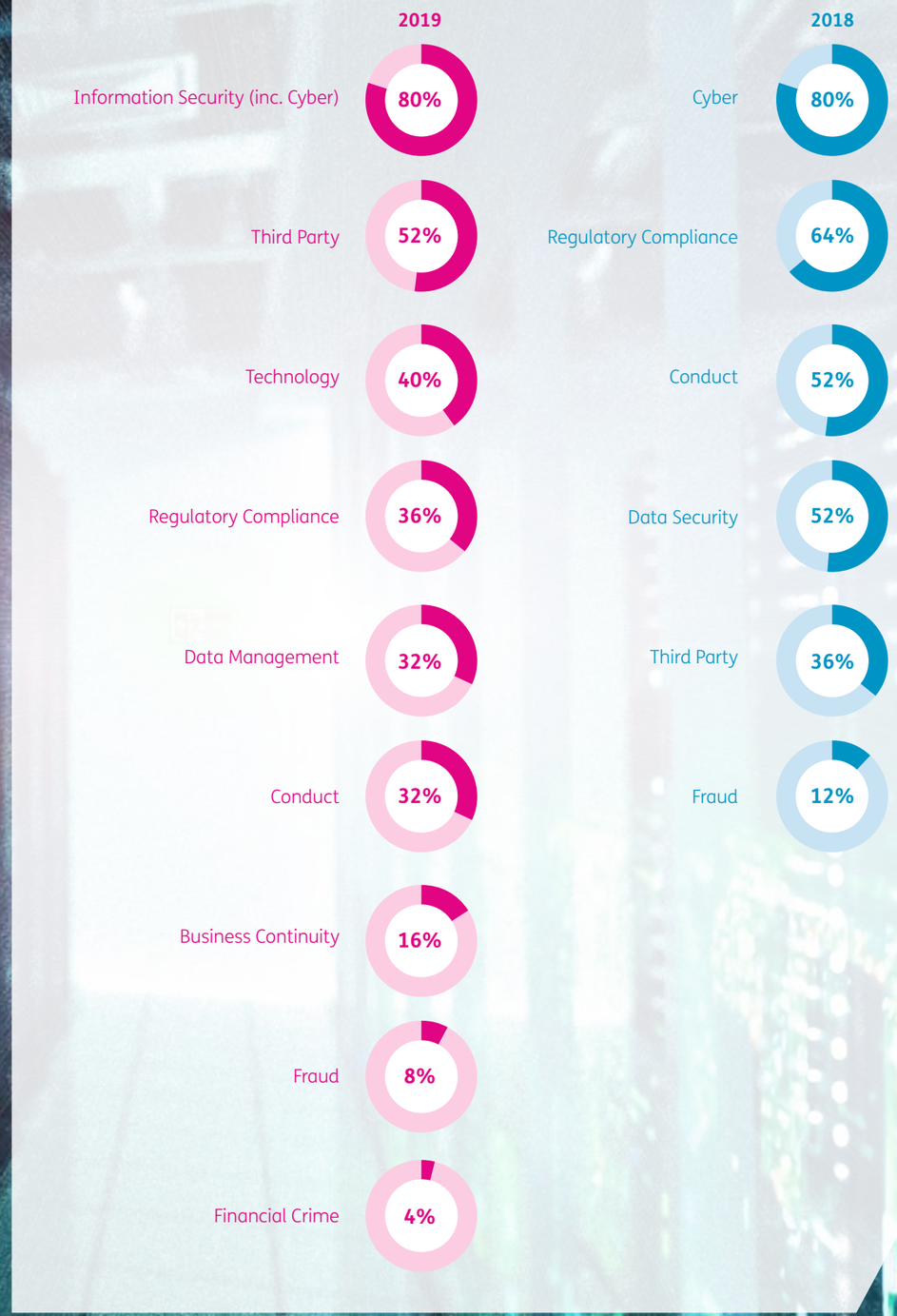
> "[Risk appetite statements] are considered in decision making, but most are backward looking, so impact on decision making is mostly related to remediation or to projected impact of proposed business developments."

Comparing responses to last year's findings, it is clear that operational resilience related risks have increasing prominence on the radar of most firms, with **80% of firms highlighting information security as their top operational risk, and 52% highlighting third party risk**. This comes as no surprise given the increased regulatory focus on operational resilience. However, information security, third party and technology risks are not just the biggest identified risks because of regulatory mandates. These threats are being realised with the greatest frequency across the financial services landscape. In part this is due to their complexity and the speed with which they can evolve. It is also a reflection of the magnitude of their potential impact and the challenge of implementing preventative controls, particularly as firms move towards more agile and digital environments. As the provision of financial services continues its shift to a technology-driven, partner-enabled ecosystem, more potential points of weakness emerge. That proliferation, and the potential implications of a complete failure of service provision, poses one of the greatest challenges for operational risk teams.

Given the increasing level of inherent risk across the landscape, it is of value to note the way in which firms are managing that risk profile within their risk appetite framework. The survey responses clearly indicate that while firms continue to struggle in determining the appropriate level at which to set risk appetite statements, some consistent fundamentals are in place across participants. Specifically, risk appetite statements are being set by the board, they contain a mix of both qualitative and quantitative components, and they are appropriately supported by Key Risk Indicators (KRIs).

Despite having these core components in place, organisations are still struggling to develop a forward looking view of risk and to embed risk appetite into decision making. These features are critical to developing a more proactive and dynamic approach to operational risk management.

Figure 4: The top operational risks highlighted by respondents

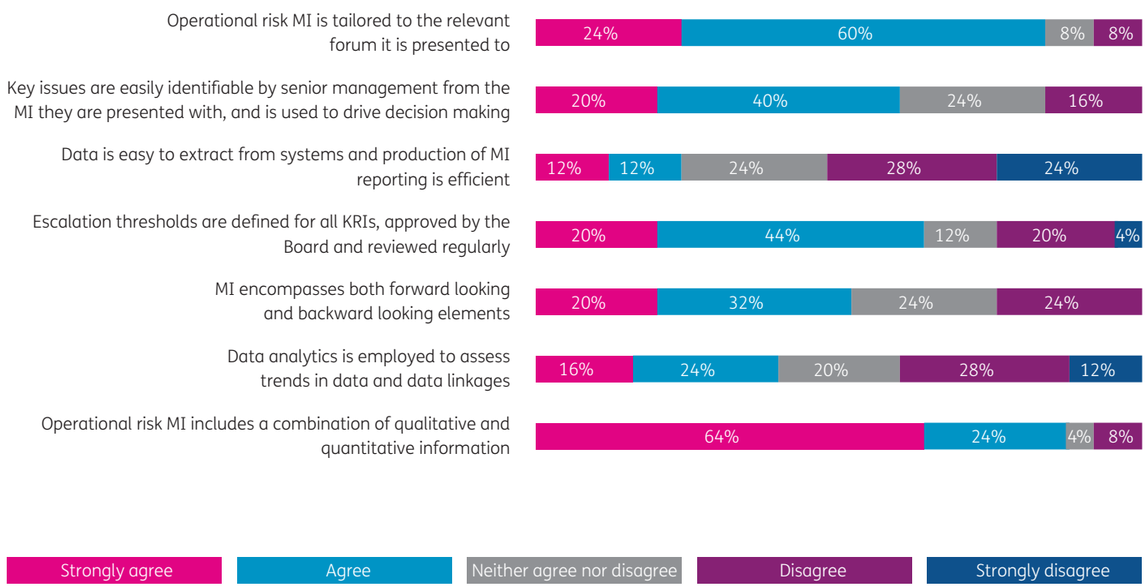


Operational risk data capture and reporting

Overall, our survey provides a broadly positive view of data management and reporting capabilities within participating firms. A number of respondents noted that their data management capability had improved significantly over the last year. Respondents are generally comfortable with their ability to tailor their data to relevant audiences and governance forums – an improvement versus last year's position. They are also saying that the MI that is being produced contains a good mix of both quantitative and qualitative information that can be used to drive insight into key issues.

Data management challenges are not unique to operational risk within financial services, but there is a fundamental reality that the capture of incident or event data is absolutely critical to developing the forward looking view of risk discussed earlier in the report. **52% of respondents felt that MI encompasses both forward and backward looking elements**. Given the point highlighted earlier around risk appetite statements not providing a forward looking view of risk, this suggests a disconnect between the two; are risk appetite statements and risk MI really focused on the key risks the firm cares about?

Figure 5: Respondents' views on how operational risk MI flows through the organisation



The data also highlights that what is tracked in the form of KRIs varies significantly across the surveyed firms, with the number of KRIs reported ranging from less than 10 to more than 1000. Undoubtedly there is some variance in what firms consider a true KRI, and it is evident that the differing size and scale of participants is an influential factor. Nevertheless, the range of responses shows just how significant the difference is in what firms are tracking.

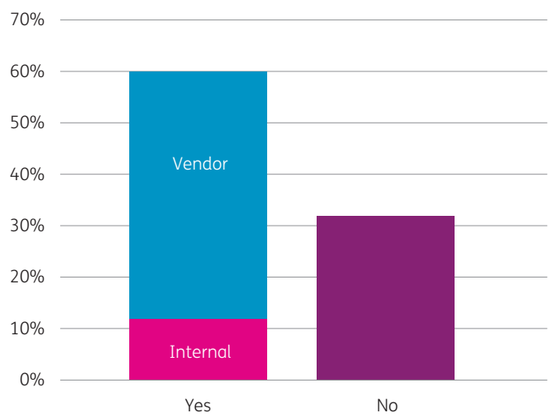
With so many KRIs, it begs the question as to whether management is really able to understand what the information is telling them and respond appropriately. Similar to our recommendations last year, we urge firms to think about the data they need, rather than just looking at the data they have.

The main data management concern appears to be the actual process to collate MI and derive insights on trends and linkages. There is a sense that operational risk teams spend a disproportionate amount of time and effort putting data together for reporting purposes – time that could be better spent on more active risk management or control development. This is a bit surprising as 68% of respondents have a single system for capturing risks, events and controls. This should be reducing reporting time, but seems not to be. This may be because the system is not configured to produce reports in the right format or at the right level of aggregation. Or it may be because data quality issues mean the data needs cleansing or reviewing before being reported, e.g. to interpret free text entries.

> "So many metrics. Useful for management but not consumable by the board."

> "The volume of data and complexity of extraction and correlation makes identifying trends challenging. However, considerable effort is being exerted to transform data so it offers greater insights."

Figure 6: Percentage of respondents who have a single system for recording operational risks, controls and incidents



In reality, it seems that such systems are not yet configured to deliver the analytical capability that firms truly desire, and a number of firms reported that they were employing manual techniques to analyse trends and themes in the data. Given much-heralded advances in artificial intelligence (AI) and other forms of advanced analytics, we would certainly expect a change in this picture in the coming years. Indeed, a number of respondents highlighted that they had projects in flight to employ analytics tools in the future.

Risk and control taxonomies

Risk and control taxonomies represent a critical foundation of an operational risk framework, regardless of the size, shape or scale of the organisation it is intended to support. These taxonomies can provide a central reference point for both the first and second lines of defence to reinforce their identification of relevant risks and controls across the business, provided that they are combined with clear guidance and explanation of what the risks mean. They also provide the basis for consistent ongoing monitoring and reporting.

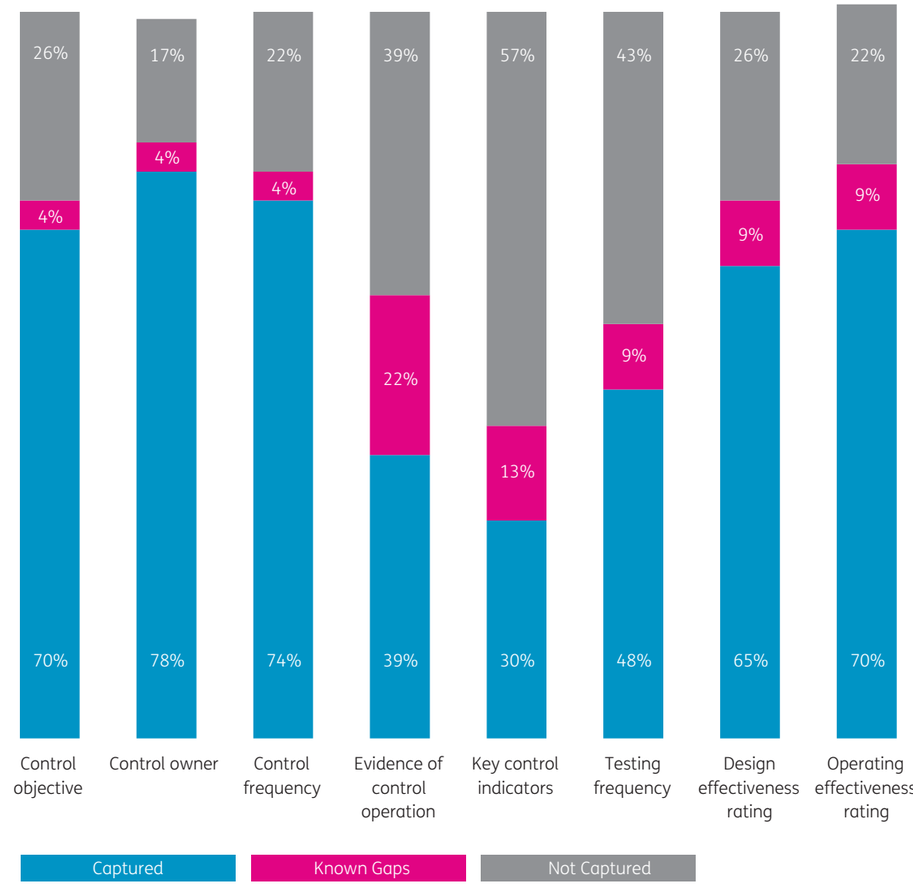
> "Op risk is not well defined enough....lot of work to help 1st line understand what op risk is."

That said, there is a reasonable counter-argument that over-reliance on a taxonomy can lead to a 'tick box' mentality that reduces the need for the first line in particular to really explore and challenge their understanding of risks and associated controls. Nevertheless, we would suggest that an effective culture of active review and challenge must start from a place of common understanding, provided by a common risk language and standardised taxonomy. Indeed, this need was a driving force behind the work of the operational risk association, ORX, over the last year to develop their new operational risk reference taxonomy [1].

It is therefore somewhat surprising to note that **46% of the surveyed population still do not have a standardised risk and control library in place**. In the absence of this infrastructure, risk assessment can become a much less structured discipline, leading to an increased threat of inappropriate control design or definition. The majority of respondents have a risk taxonomy in place, and over half of respondents also employ causal and impact taxonomies in addition to their reference taxonomy. Instead, it is the standardised controls taxonomy that continues to elude many firms. With some firms reporting the number of controls in the thousands, a standardised taxonomy or library plays an important role in enabling firms to provide an aggregate view of the effectiveness of their controls and avoid duplication of assessments and testing.

[1] https://managingrisktogether.orx.org/research/operational-risk-horizon-2019

Figure 7: Factors captured within respondents' controls documentation

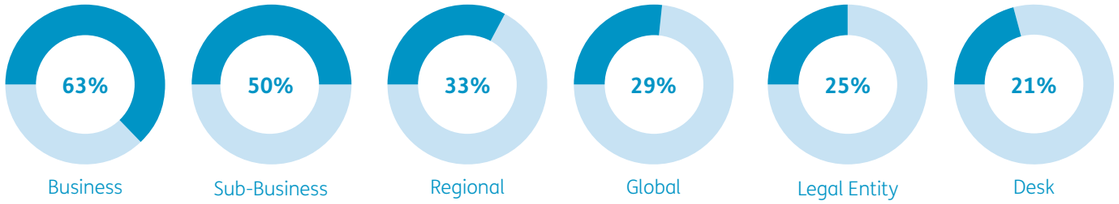


While challenges remain regarding the controls taxonomy or library, there are some clear and encouraging trends in controls documentation. We see that fundamental attributes such as control objective, owner and frequency are routinely captured, alongside design and operating effectiveness ratings. While we would certainly still encourage firms to spend time thinking about how to incorporate evidence of control operation and associated Key Control Indicators (KCIs) into their documentation, the overall picture here is positive.

RCSAs

The RCSA process is another core building block of the operational risk framework and it is positive to see that **88% of firms responding to our survey are embedding RCSAs in a consistent manner**. Nevertheless, we do see significant variance in the levels at which the RCSA is being conducted. The RCSA is most commonly carried out at the business or sub-business level, which makes sense given the variety of size and breadth of our respondents. Given the recent trend towards legal entity rationalisation it is surprising that we aren't seeing a greater tendency towards legal entity level RCSAs as a means for helping firms better understand and manage risks at entity level.

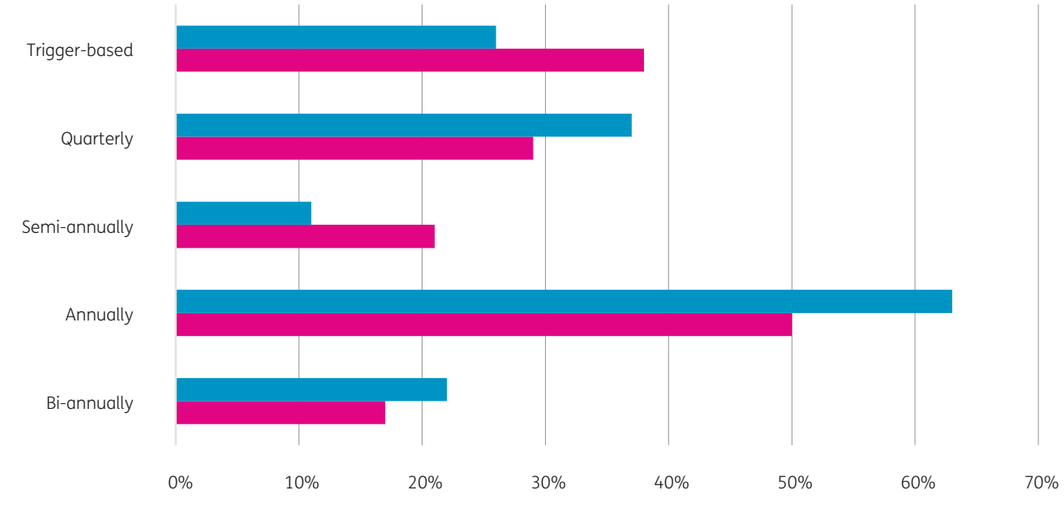
Figure 8: Level of granularity at which RCSAs are performed



The survey shows widespread acknowledgement of the value of mixed first and second line workshops in performing RCSAs. However, the level of facilitation required by the second line is something that should reduce over time. The increase in the number of firms using trigger-based updates is a very encouraging trend. This suggests firms are responding to events with rigour and, in some cases, are increasingly able to link KRI or KCI tolerances to the initiation of RCSAs. This is something that we are strong proponents of, particularly as it gets the business away from seeing an annual process as the only mechanism for raising issues. While we accept that a trigger-based approach relies on a degree of maturity in other aspects of operational risk infrastructure, it is a capability that we would encourage all firms to be working towards.

However, it is crucial that firms clearly and comprehensively define the triggers that would necessitate an update, and that there is sufficient monitoring by second line to ensure RCSAs are indeed updated if one of the triggers is breached. Otherwise, without a regular update cycle, firms risk their RCSAs quickly becoming out of date.

Figure 9: Frequency with which RCSAs are updated



As we saw in last year's survey, the time consuming nature and difficulties in engaging the business were highlighted by a number of respondents.

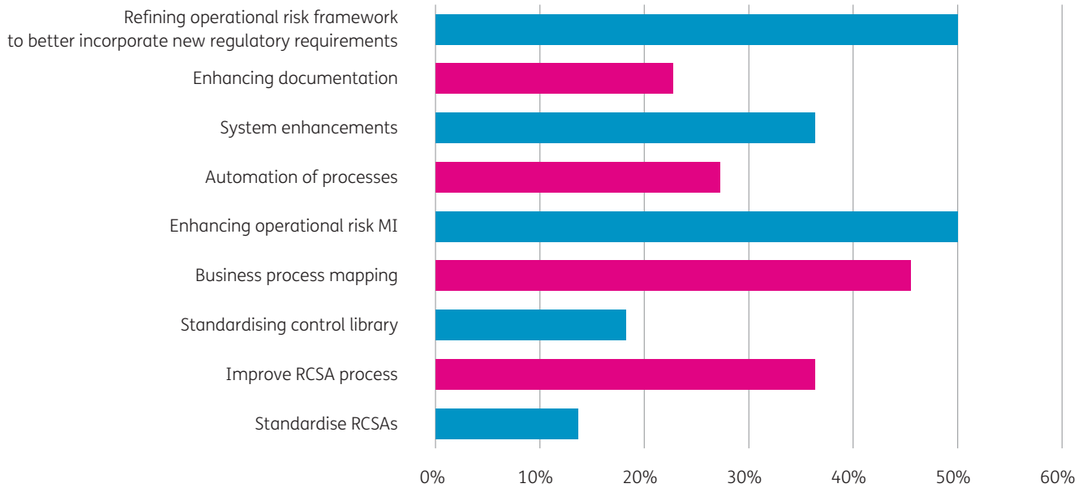
Much of this ties back to the earlier points around the absence of a standardised controls taxonomy resulting in RCSAs being performed at inconsistent levels of granularity and assessments being duplicated across multiple RCSAs. Importantly, a number of firms noted ongoing challenges around making RCSA outputs meaningful and useful. In our recent publication *Adopting cross-industry resilience practices; a guide for financial services* we noted that firms in the water industry are increasingly looking for more effective ways to visualise data. For instance, one firm has developed a dashboard that enables users to quickly see the key risks and level of controls in place across all of its sites. Similar data visualisation techniques could be employed when it comes to the output of RCSAs.

> "The biggest challenge is to get the 1st line to assume ownership of their RCSAs and deliver in a timely manner."

Enhancements and emerging focus areas

Our survey concluded with a look to the future, seeking to understand how and where attention is being focused to enhance operational risk frameworks. A common theme is the ongoing refinement of the overall operational risk framework, both to take account of evolving regulatory requirements around conduct and operational resilience, but also to develop the maturity of the framework and its tools more generally.

Figure 10: Top areas of focus for improvement over the next 24 months



It is not surprising that operational risk MI and business process mapping also emerge as priority items going forward. Going through the pain of getting these building blocks right should create opportunity for more proactive, forward looking identification of risks and emerging threats.

We were particularly interested in understanding how emerging themes such as climate risk and operational resilience are being addressed and incorporated into the institutional approach to operational risk management.

Operational resilience and operational risk

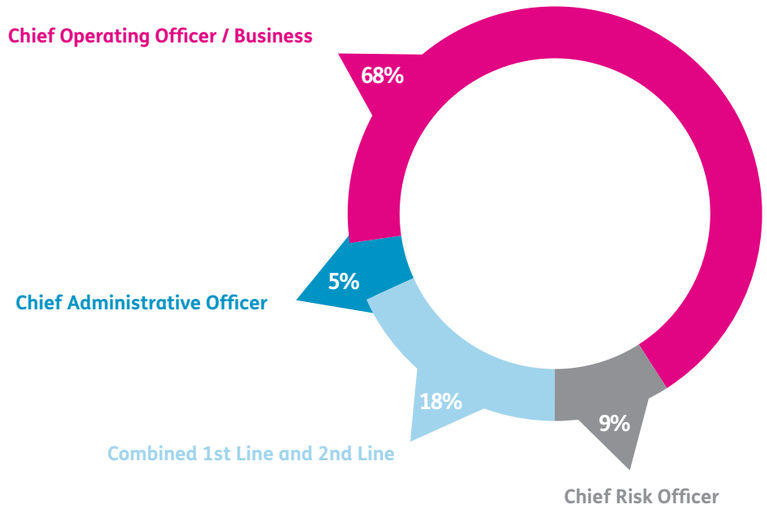
Almost 60% of firms reported that they are refining their operational risk framework to take account of changing requirements around operational resilience, or plan to do so. Given the clear guidance from the regulators that firms should be leveraging their existing frameworks for operational risk and business continuity, this is a positive development. This doesn't need to mean an overhaul of firms' risk frameworks, but rather a refinement to ensure that resilience is well integrated or embedded.

Operational resilience also slots neatly into the conventional three lines of defence model, with risks very clearly being identified and owned by the first line, and the second line facilitating robust oversight and challenge. Indeed, this is borne out by our survey, which consistently flags accountability for operational resilience as sitting with the COO.

However, this is not to say that operational resilience should be considered a mature discipline. There is certainly further work to be done in defining business services, mapping resources to assess resilience, and refining resilience monitoring. In all these aspects firms should consider the role of operational risk, and also what existing operational risk tools can be leveraged to assist with this. For instance, RCSAs can provide a helpful starting point in defining and mapping business services. From a taxonomy perspective, firms who employ impact taxonomies may wish to consider resilience as an additional impact factor, which may also help in extracting operational risk MI that has a resilience angle to it.

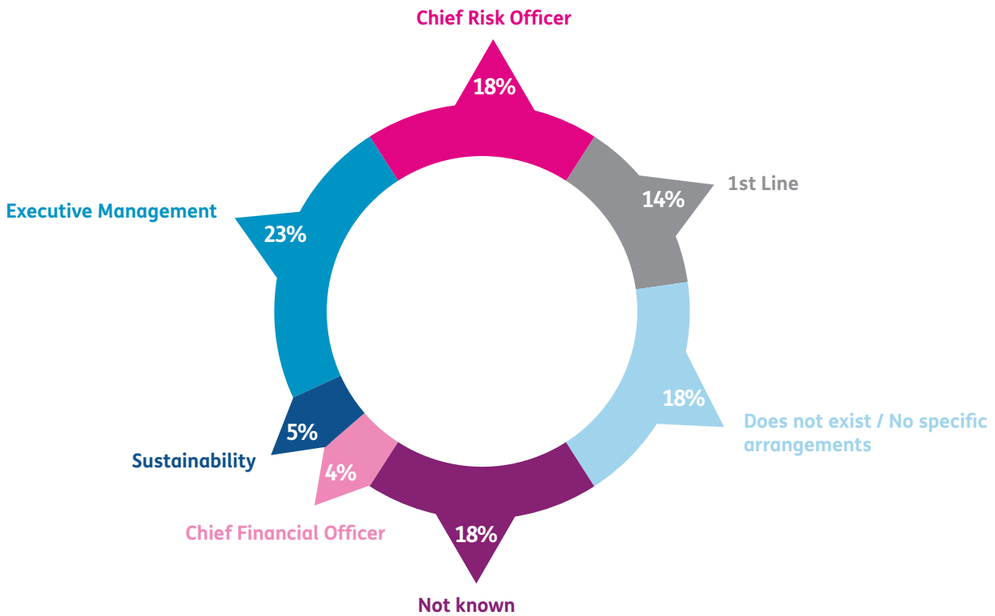
> "Resilience issues arise due to inconsistent application of the framework, so focus is driving this as opposed to needing fundamental framework changes."

Figure 11: Accountability for operational resilience across the respondent group



Climate risk and operational risk

Figure 12: Accountability for climate risk across the respondent group



Unlike with operational resilience, we continue to observe that climate risk is often addressed in pockets of an organisation, with only the biggest firms having developed a cohesive enterprise strategy. Ownership and accountability for climate risk is far more varied, and consequently so is the role for operational risk. However, it is an area that is developing quickly. The physical risks associated with climate change – increased flooding, wildfires and heat stress, for example – are increasingly seen as a cause of potential revenue disruption. It is important that firms identify these risks in their own facilities, and in their supply chains, to ensure that they can build climate resilience into their own operations. Specific analytics are becoming more prevalent within credit risk functions for assessing climate risks in lending books. In future surveys, we expect to see operational risk teams increasingly bringing these analytics across into the operational risk assessment process.

Conclusions

Our second operational risk survey has again highlighted the key trends around operational risk management. Positively, we have seen some maturing of firms' operational risk frameworks over the last year and stabilisation in firms' operational risk teams. However, firms continue to struggle with challenges around the RCSA process and in collating and analysing operational risk MI effectively. Firms are clearly investing in automation and data analytics as they are a key mechanism for assisting firms with these challenges.

Firms continue to balance BAU requirements with regulatory developments when assessing and developing their frameworks. The regulatory agenda around operational resilience in particular continues to drive a number of firms' priorities when it comes to operational risk. Many firms are looking to recruit resilience-related skill sets into their teams, and almost 50% of firms are focusing on business process mapping over the next two years (a key building block for assessing the resilience of a firm's services). Resilience-related risks are also front of mind for firms, with information security and outsourcing topping the leader board of key risks.

2020 promises to be another exciting year when it comes to operational risk management. The Bank of England, PRA and FCA are expected to publish their final policies on operational resilience in H2 2020. Combined with increasing expectations on firms around climate risk, and industry developments on the operational risk taxonomy, firms will continue to face operational risk management challenges.

Since participants completed this survey, the PRA has published a draft supervisory statement on outsourcing and third party risk management, to complement its policy proposals on operational resilience. As such, we expect firms to re-evaluate their plans and revisit their third party risk frameworks over the course of 2020.

We hope that you have found this summary report of interest. If your firm did not take part in the survey and you would like to benchmark your firm against our dataset, please email OpRisk@baringa.com.

Baringa Partners' operational risk capabilities

Baringa has deep subject matter expertise in operational risk, with a team that combines a mix of regulatory, industry and consulting experience.

Governance
We can design and review you target operating model for operational risk, including defining roles and responsibilities across the three lines of defence, drafting operational risk policies and procedures, and reviewing the effectiveness of committee structures

Risk Appetite
We can review and refine risk appetite statements and help you align your operational risk and business strategy to your risk appetite

Risk Identification & Definition
We can help you define distinct risk categories or taxonomies specific to your firm, supported by clear guidance

Risk & Control Assessment
We can develop or refine your risk assessment and controls assurance methodologies. We can also support you to perform RCSAs and controls testing across your business

MI & Reporting
We can review and streamline your operational risk metrics, and refine escalation thresholds. We can design clear and accessible management reports to support risk management

Event Management
We can support you in developing event/incident management tools, including supporting in vendor selection

Operational Risk Capital Assessment
We can review your capital modelling and allocation methodology, and review the embeddedness of capital into your business decision making

Risk Culture
We can undertake maturity assessments of your risk culture and help you define the behaviours and associated incentives to encourage good risk management. We can provide training to your risk teams, in order to upskill and educate your staff on their role in managing operational risk

For further information, please contact:

Salina Ladha
Director
– Finance, Risk and Compliance
+44 7971 049 625
Salina.Ladha@baringa.com

Stuart Cook
Partner
– Finance, Risk and Compliance
+44 796 811 1631
Stuart.Cook@baringa.com

About Baringa

Baringa Partners is an independent business and technology consultancy. We help businesses run more effectively, navigate industry shifts and reach new markets. We use our industry insights, ideas and pragmatism to help each client improve their business. Collaboration is central to our strategy and culture ensuring we attract the brightest and the best. And it's why clients love working with us.

Baringa launched in 2000 and now has over 700 members of staff and more than 65 partners across our five practice areas of Energy and Resources, Financial Services, Products and Services, and Government and Public Sector. These practices are supported by cross-sector teams focused on Customer & Digital; Finance, Risk and Compliance; People Excellence; Supply Chain and Procurement; Data, Analytics and AI; Intelligent Automation and Operations Excellence; and Technology Transformation. We operate globally and have offices in the UK, Germany, Australia, US, and the Middle East.

Baringa Partners have been voted as the leading management consulting firm for the second year in the Financial Times' UK Leading Management Consultants in the category energy, utilities and the environment. We have been in the Top 10 for the last 10 years in the small, medium, as well as large category in the UK Best Workplaces™ list by Great Place to Work®. We are a Top 50 for Women employer, and are recognised by Best Employers for Race.

Baringa
Brighter together

We'd love to hear from you

OpRisk@baringa.com

Headquarters: London (UK) | Belgium | Ireland | Germany | Australia | Singapore | UAE | USA |