Executive summary

Baringa Partners’ Operational Risk Report explores the top operational risks and resulting key themes in the financial services industry today.

The results show a wide range of management tools are currently deployed and highlight clear areas for development and improvement, particularly around the use of risk self-assessments and Key Risk Indicators.

Faced with growing regulatory pressures, shrinking budgets and increasingly sophisticated cyberattacks, functions are becoming more resourceful in their efforts to keep critical processes and services up and running.

Senior executives, including heads of operational risk, directors, and group leaders at the world’s biggest asset management, banking and insurance firms also noted the challenge and opportunity of balancing rapid technological change with heightened regulatory expectations.

Communication, transparency, and fostering a top-down culture of corporate responsibility and ethical conduct are considered the best ways to move business forward, but survey responses indicate these changes are difficult to execute in the short term.

Operational risk teams clearly understand they must better utilise resources and improve the flow and quality of information to management, as this allows for more effective decision-making at C-suite and board level, as well as strengthening the feedback loop.

Against this backdrop, we have identified several key challenges which we believe firms could benefit from addressing:

- Transforming management information and associated governance
- Improved controls rationalisation
- Implementing a single IT operational risk system of record
- Capturing and strengthening risk culture
- Adopting/improving controls automation

Baringa Partners’ Operational Risk Report explores the top operational risks and resulting key themes in the financial services industry today.
The key challenges identified are explored in this report across the following four topics:

1. **Management information and governance**

   More than three quarters of firms are prioritising more targeted and streamlined management information (MI) by 2021, and 58% say their organisation does not have a forward view of risk. There are clear opportunities to refine existing metrics and develop new MI that really focuses on the risks firms are trying to measure, and to review the forums where this information is absorbed, ensuring it is fit for purpose.

2. **Risk and control libraries**

   Standardisation of risks and controls continues to be a challenge for firms, in part driven by the lack of clarity over the level at which controls should be specified. Meanwhile, 86% of firms have integrated conduct risk into their operational risk frameworks, which brings efficiencies but also brings challenges around managing the different governance frameworks supporting these two risks.

3. **Assessing risks and controls**

   The lack of a single IT architecture continues to impact on the efficiency of the Risk and Control Self Assessment process, and is an area firms are investing in going forward. At the same time, risk executives are trying to move on from older box-ticking compliance methods to strengthen the risk culture inside their organisations.

4. **Future developments**

   With cyber risk the top operational risk for 64% of respondents, and the regulatory focus on this over the last year, it is not surprising that operational resilience is a key priority area for firms over the next two years. The continuing regulatory burden also means firms are looking to process automation in order to create capacity and increase efficiency going forward.
About this survey

In Q4 2018, Baringa Partners surveyed 30 financial services firms, including retail banks, investment banks, asset and wealth managers, and insurance firms, to take the pulse of risk management and consider strategies to help businesses better manage risk and realign priorities to improve risk culture.

The firms surveyed provided services across multiple business lines and jurisdictions. As a result, the size of their Operational Risk functions varied considerably, from less than 10 to as many as 600.

Business activities undertaken by respondents

Bar chart showing the distribution of business activities undertaken by respondents.

Business activities performed by firms surveyed

Bar chart showing the distribution of business activities performed by firms surveyed.

The survey contained 31 questions across the following six categories: about the organisation; risk identification and reporting; processes and tools; assessment of risks and controls; and future challenges.

The questions recorded detailed information, for example on the size of operational risk teams, top operational risks and associated Key Risk Indicators, risk and control libraries, the Risk and Control Self Assessment framework, operational risk capital calculation methodologies and key areas of improvement over the next two years.

Our goal in launching this survey was to kick-start the debate and formulate an agenda for improving the future function of operational risk. By highlighting strengths and weaknesses of the current strategies, we hope this report can help executives plan for the future and think about new solutions to help their firms advance.

The data can be analysed by sector, business activity and size of firm, allowing comparison versus peer organisations.

Baringa offers a benchmarking service against this data – for more information please contact us via OpRisk@baringa.com to discuss.
Management information and governance

Improving the quality and flow of management information allows business leaders to make more informed decisions, better forecasts, and gives a clear view on how much progress has been made. Operational risk executives recognise the importance of improving this process.

Improving the delivery of crucial information on risk management to boards in the coming 18 months is a major priority for 78% of the firms surveyed.

For some firms that may mean streamlining metrics so that management are able to focus on those that really matter. Our survey showed respondents had varying levels of Key Risk Indicators that they track – from less than 10 to over 50. Too many metrics can increase the risk that management do not interpret key messages and take necessary associated action.

Some firms may need to be more transformational across their metric suite. They must begin this process by firmly establishing the key questions they are trying to answer from their management information (MI), and then determine appropriate assessment factors based on these questions, rather than just looking at available data points, or in some cases pieces of data in isolation.

Hand-in-hand with this, organisations need to challenge the governance around their MI to ensure that the right MI goes to the right forums. Almost all participants reported that operational risk MI is being consumed by multiple forums across their organisation. Escalation thresholds for metrics need to be set at the right level for each committee, to ensure that metrics are escalated to the appropriate forum at the right time and each layer of governance serves a robust purpose, rather than repeating or recycling the same metrics and thresholds for all forums.

Key Risk Indicators (KRIs) tracked by firms

This chart shows the proportion of respondents monitoring the indicated number of KRIs

<table>
<thead>
<tr>
<th>Number of KRIs</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-10</td>
<td>50%</td>
</tr>
<tr>
<td>11-25</td>
<td>45%</td>
</tr>
<tr>
<td>25-50</td>
<td>40%</td>
</tr>
<tr>
<td>50+</td>
<td>35%</td>
</tr>
<tr>
<td>75+</td>
<td>30%</td>
</tr>
<tr>
<td>100+</td>
<td>25%</td>
</tr>
<tr>
<td>150+</td>
<td>20%</td>
</tr>
<tr>
<td>200+</td>
<td>15%</td>
</tr>
<tr>
<td>250+</td>
<td>10%</td>
</tr>
<tr>
<td>300+</td>
<td>5%</td>
</tr>
<tr>
<td>350+</td>
<td>0%</td>
</tr>
</tbody>
</table>

0-10 11-25 25-50 50+
However, metrics are meaningless unless a firm has adequately defined its appetite, against which it will measure itself. Whilst the majority of firms had risk appetite statements that were set by the Board and which were supported by relevant metrics, 50% of respondents noted that their risk appetite statements did not link to the firm’s strategy or to the actual underlying risk the firm faced, and did not provide a forward looking view of risk.

“How to distribute risk appetite across multiple [diverse] businesses who share the same infrastructure is false precision” said one respondent.

<table>
<thead>
<tr>
<th>Risk appetite statement observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statements are set by the board</td>
</tr>
<tr>
<td>Statements utilise both qualitative and quantitative components</td>
</tr>
<tr>
<td>Statements are specific to the risk profile of the organisation</td>
</tr>
<tr>
<td>Statements are monitored by senior management on a regular basis</td>
</tr>
<tr>
<td>Statements are monitored by relevant KRIs</td>
</tr>
<tr>
<td>Statements are cascaded through the organisation</td>
</tr>
<tr>
<td>Statements clearly link to the underlying risk rather than being performance indicators</td>
</tr>
<tr>
<td>Statements provide a clear link with the firm’s strategy</td>
</tr>
<tr>
<td>Statements provide a forward-looking view of risk</td>
</tr>
<tr>
<td>Statements are embedded into business decision-making</td>
</tr>
</tbody>
</table>

This chart shows respondents’ level of agreement with the indicated statements.

0% 20% 40% 60% 80% 100%

- Strongly agree
- Agree
- Disagree
- Strongly disagree
2 Risk and control libraries

Disparate systems and libraries are driving inefficiencies in assessment of risks. Firms need to standardise where possible, as problems will exacerbate as firms look to integrate conduct risk and operational risk.

In 2010 the Institute of Operational Risk suggested that firms consider establishing a central operational risk repository to provide a central common risk event and key control library. Whilst this has been an area of development for banks over the last few years, around half of firms surveyed reported ongoing struggles in this area.

One of the drivers for this challenge that we have witnessed is the considerable variation in the number of controls in place at firms. On average firms reported 300-400 controls, but responses varied wildly from less than 100 to many thousands. What this highlights is the challenge in determining the appropriate level of granularity at which to specify controls. A control should be defined at a level that is meaningful, such that it clearly manages the risk that it is being assessed against.

In standardising controls, firms should also consider whether there is scope to rationalise their control environment. A number of tactical solutions have been implemented in recent years in response to regulatory findings or investigations, respondents report. Rather than looking at controls in isolation, reviewing the environment holistically may help identify areas for streamlining, such as measuring the balance of preventative versus detective controls, and considering whether having one negates the need for the other.

Integrating operational risk and conduct risk

Conduct risk has become one of the most important aspects of regulatory compliance in recent years as firms are increasingly pushed to develop new approaches to mitigation.

Although the total annual fines for banks by the Financial Conduct Authority (FCA) diminished in 2018 following the LIBOR-era spike, US regulators are showing no signs of leniency and the FCA is opening more investigations than ever.

Defining a clear boundary between operational risk and conduct risk issues has proved challenging. Given this, and the overlap in the control environment in managing these two risks, 86% of firms surveyed have integrated conduct risk into their operational risk framework.

Although integration can generate efficiencies, it can also provide challenges. A number of firms have developed Compliance-run conduct assessments, which can unnecessarily duplicate the existing Risk and Control Self Assessment process if the scope, purpose, timing and format of these assessments is not clearly defined at the outset.

Similarly, firms need to consider how the governance and reporting framework for conduct risk integrates with the risk framework more broadly in order to balance the need to avoid duplication with the need to be able to demonstrate the appropriate management and oversight of conduct risk to the regulators.
Assessing risks and controls

The time-consuming and overly complex nature of Risk and Control Self Assessments risks them becoming a tick box exercise rather than a genuine mechanism for firms to identify and manage the risks they are running.

Risk and Control Self Assessments (RCSAs) are utilised by all firms surveyed. Although there is considerable variation in the granularity and frequency at which these are performed across respondents, almost 100% of firms employ a standardised framework across their organisation.

However, respondents highlighted a number of challenges that they continue to face around this process, which limit their effectiveness. Survey data reveals the most common key challenges firms faced regarding the RCSA process are a varying granularity of risks and controls, the duplication of risk and controls and the RCSA process being time-consuming.

A single IT architecture for recording operational risk related data would go a long way to easing some of these challenges, and indeed a lack of such a system was explicitly called out by several respondents as the driver for some of these challenges. Unsurprisingly therefore, over half of respondents have committed to this project in the long term, with 51% of respondents citing system upgrades as a priority for the next 12 to 18 months.

However, firms need to ensure that they future-proof their IT investment by considering what additional data they may want to capture in the future, and how they would look to use this. Only 30% of firms surveyed currently have a clear mapping of regulations, policies, processes, risks, controls and events. Firms that are still working to build out this connected view should consider whether the systems and tools they are building will facilitate development of this picture in the future.
Risk culture

When designed well, the RCSA framework should provide a mechanism for the business to proactively self-identify their risks and determine how to appropriately mitigate them. This relies on the business engaging with the RCSA process, but it also relies on a strong risk culture to drive a quality engagement. Respondents highlighted this as an area of continual challenge.

Respondents raised concerns over the RCSA becoming a box-ticking exercise and the reluctance of the business to genuinely engage with the process and openly identify areas of concern.

To help address this, operational risk teams are highlighting the importance of actively engaging in the RCSA process to the business, both through training but also through internal campaigns that target engagement in risk.

As firms move away from just an annual cycle of RCSAs to a more dynamic and ongoing assessment of risks, this enhanced business engagement will become even more crucial. Firms may, therefore, wish to consider looking at ways to test their risk culture on a periodic basis, perhaps via specific risk culture surveys, to identify specific areas that need improving.

“The biggest challenge is getting across it is OK to have a high score and a willingness to show weakness, rather than downplaying risk,” said one respondent.
Future developments

Operational risk teams are remodelling themselves to protect the business from cyber risks, as they also contend with geopolitical shocks and further regulatory pressures.

Cyber risk has been an area of recent regulatory focus, with the Senior Managers and Certification Regime placing accountability for hacks or glitches on C-suite individuals. Last year the Bank of England set out that the Financial Policy Committee was establishing its tolerance for disruption of financial services from cyber incidents, and the European Banking Authority launched a consultation on its draft Guidelines on Information and Communication Technology and security risk management.

Top identified operational risks

This chart shows the proportion of respondents that recognised each risk type as a top concern.

As a result, it is perhaps no surprise that 64% of firms highlighted cyber as their top risk in 2018 and almost 50% of respondents ranked operational resilience as one of their top five priorities for the next two years. Those firms looking to expand their operational risk teams over the next 18 months noted cyber and operational resilience more broadly as the key skills that they are looking to develop in their teams.

Operational resilience cannot be achieved in isolation but instead needs to be embedded into existing operational capabilities, to allow an organisation to offer resilient services to its customers and other interested parties. Firms need to look more widely than just their technology, premises and operations, but also look at ensuring that resilience is embedded into discussions around business change, supplier management and data security. Resilience needs to be on the agenda at the top of the house, with the Board actively involved in discussions weighing up resilience vs cost, but this needs to permeate through the organisation. Firms need to ensure they have a culture that values behaviours that support resilient outcomes, and people with sufficient skills and knowledge to maintain resilience.
Over the last 18 months firms have had to contend with several overlapping regulatory initiatives, including MiFID II and the General Data Protection Regulation. In the face of such regulation, the ever-expanding control environment provides an opportunity to apply automation to high-frequency processes. Such automation was highlighted as a top five priority by over 50% of firms.

We have seen firms successfully implementing robotic process automation (RPA) across a number of different processes, including production of client disclosures, pre and post trade controls, transaction reporting and management information generation. Such automation can reduce costs and create capacity so that staff can focus on those tasks where they best add value, as well as reducing errors and ensuring more accurate and timely reporting.

Upcoming priorities for the next two years

This word map shows the level of prominence of upcoming operational risk related priorities as recognised by respondents.
Conclusion

Our inaugural survey highlighted a number of challenges that firms are facing across the financial services industry. Some of these challenges, for instance those around standardised risk and control libraries and the Risk and Control Self Assessment process, are ones that the industry has been grappling with for some time. However, the challenges have become more acute as firms are forced to balance existing requirements around operational risk with new regulatory demands around the management of conduct risk and operational resilience.

In light of these ongoing regulatory demands, growing cost pressure and an ever-expanding control environment, firms need to look for opportunities to streamline their processes and rationalise controls where possible, or risk duplication of effort. To this end, firms are investing in streamlining their IT architecture over the next 12 to 18 months, to provide a single IT system for managing operational risk – one that captures risks, controls, processes and events in a single place.

Firms are also looking at other avenues for driving efficiency, including the adoption of robotic process automation. Whilst process automation has been successfully implemented across a number of Front Office and Finance processes, to date we have seen little utilisation of automation by Risk teams.

Over the course of the next year it will be interesting to see how responses to the following develop:

▲ How will conduct management information evolve and what new ways will firms look to leverage to measure conduct?

▲ Will the costs of control continue to risk, or will firms rationalise their control environment?

▲ Will the management of operational risk and conduct risk continue to converge?

▲ What percentage of firms will have deployed a single IT system for the management of operational risk?

▲ How will firms’ risk culture evolve over time?

▲ How will Operational Risk functions leverage the benefits of automation?

We hope that you have found this summary report of interest. We will contact all survey respondents to arrange time to review their custom benchmark report. If your firm did not take part this year, and you would still like a benchmark report to be produced, then please do get in touch (OpRisk@baringa.com) and we will share with you a template in which to provide your offline survey responses for comparison.
About Baringa Partners

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. Brighter together.