The future of operational risk
Operational risk is important and increasing. But operational risk management is difficult. This intensification is happening at such a rapid pace that risk managers need to adapt faster than ever before. Many in the financial services industry have already made great strides in how they manage operational risk, but this will not be sufficient. Operational risk management is at an inflection point and needs a rethink.

ORX and McKinsey conducted a study to identify the strategic challenges that financial services firms must address if they are to manage operational risk more effectively. We asked CROs from 15 leading financial institutions a series of questions about operational risk in their organisations. We synthesised these discussions and – while our interpretation does not represent the views of any single CRO – given the broad consensus among participants on many issues, we believe it is an accurate reflection of the views of the group. The report is also informed by our broader conversations with the operational risk community and our experiences of working with financial services firms.

The results of the study show that the challenges facing operational risk management include reinventing the mandate for operational risk, generating dramatically better risk information, deploying analytics, adopting a better approach to controls, increasing skill levels and improving organisational risk culture. This report hopes to kick-start progress by articulating the challenges and framing how companies can think about solutions.

**Operational risk is increasingly important**

Ever since operational risk management emerged as a distinct discipline, its focus has been too sharply concentrated on firms’ ability (or inability) to calculate regulatory capital (at 99.9 percent over a one-year horizon) and on regulatory compliance. There has been too little proactive discussion about the growing importance of operational risk and how it can be managed better.

It is operational risk profiles that will change most in the next five to ten years, not credit or market risk.

There is little doubt that operational risk management needs to improve. The financial services industry is undergoing a profound change. Digitisation, automation, offshoring and outsourcing are overhauling how financial services companies operate in all areas of their business, and are combining to create an inflection point. It is operational risk profiles that will change most in the next five to ten years, not credit or market risk. Even the very act of change is a chance for firms to rethink risk management. “The change agenda is an opportunity to build the future risk profile,” explained another CRO.

Within the broad range of specific risks that fall under the heading of “operational risk”, our study shows that cyber risk is clearly the leading concern today – almost two-thirds of CROs cited it as a key risk driver – followed by conduct, compliance and outsourcing. Cyber risk cropped up in almost every conversation with CROs, and even those who were broadly comfortable with their overall risk profile were concerned: “In general, I feel we have good control over major operational risks, but with IT and cyber risk... we are scared,” said one.

Although day-to-day operational risk losses are declining at many institutions, 77 percent of all the CROs we surveyed said that operational risk is important (23 percent) or very important (54 percent) to their organisation. Several noted that it had been their principal
focus of late and this prioritisation shows no sign of abating. This is driven not just by
the potential for financial loss, but also by the perceived disproportionate impact that
operational risk events can have on reputation and on stakeholder relationships. Indeed,
despite losses falling, 62 percent of the CROs we surveyed believe operational risk will
increase as a proportion of their risk profile in the medium term, with just 8 percent
thinking it will fall.

If it was that easy...

Operational risk remains the “unloved child of risk management”, in the words of one CRO
we interviewed. Although senior management is dedicating more time to it, this does not
ease the burden on operational risk managers, who have to grapple with some peculiar
characteristics of operational risk, including:

- Its broad and multifaceted nature
- Its increasing interdependencies
- The opaque process through which firms take on operational risk
- The long time frames associated with both risk and mitigation
- The overhang of managing legacy events
- The high potential downsides and perception of limited upsides.

By contrast, most CROs and senior management have an intuitive understanding of what
drives risks that are more directly associated with revenue but are less experienced in the
complexity of operational risk. As one CRO explained, this is a problem because “you need
to know which questions to ask and which experts to call.”

In an attempt to overcome these challenges and respond to regulatory demands, CROs
have heavily invested in operational risk management in recent years. This has resulted
in stronger core frameworks that include risk assessments, metrics, reporting and capital
models. Most CROs feel their institutions have made good progress in designing and
implementing these frameworks. Some are also very focused on risk culture and feel their
institutions have made great strides here too.

Nevertheless, many of the CROs expressed real frustration that, despite all their efforts,
operational risk management still struggles to gain traction. The big challenge is to move
beyond theory and frameworks and actually get to grips with managing operational risk
more effectively. As one CRO put it “we are excellent at the textbook solution, but is that
solution reducing operational risk? I doubt it.” Only 30 percent of CROs feel that they have
good control of the most critical operational risks – such as cyber and IT risk, conduct
risk and financial crime risk – even though 70 percent believe they have good visibility of
those risks.

Step forward and step up: A new mandate and role

Amid a range of views on precisely what the operational risk function’s mandate and role
should be, two distinct ideas emerged on how it might evolve.

The first, and most frequently voiced, concerns the relationship between the first and
second lines of defence: the operational risk function needs to step forward and challenge
the business on key risk concerns. For many CROs, it also implies operational risk
managers rolling up their sleeves and getting involved in the day-to-day management of key risks and controls at the business level. This means generating and using real-time risk information and working on practical remediation. In the words of one CRO, “Operational risk needs to be the unpopular messenger – we have to enhance the level of challenge to the business in an increasingly complex environment.”

The second idea, voiced by a sizeable minority, focuses on the relationship between operational risk and other control functions and concludes that operational risk needs to step up and form an umbrella function for all operational risks, including those overseen by specialist teams outside the operational risk function (e.g. IT risks and compliance risks). This would give management a big-picture view of the risk profile, which would help prioritisation and make it easier to spot areas of concern.

Operational risk management needs to step forward and step up by engaging with the business and ensuring better coordination between different functions, such as operational risk, compliance and IT.

Such an umbrella operational risk function would also help bring together, simplify and streamline the proliferation of specialist control functions and approaches that often exist today – each with its own frameworks, reporting requirements and metrics – leading to a costly duplication of effort. Improving efficiency lets companies free up resources to reinvest based on their prioritisation of risks across the business.

Five building blocks to support a reinvented operational risk management

An operational risk management function that wants to step forward and step up needs to build on its strengths but, more importantly, overcome its weaknesses. There was a high degree of consistency from the CROs on what these typically were (Table 1).

Table 1: Frequently cited strengths and weaknesses in operational risk management

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk-neutral framework</td>
<td>Sub-optimal management information</td>
</tr>
<tr>
<td>Well-developed set of standard and mature tools</td>
<td>Minimal integration of advanced analytics</td>
</tr>
<tr>
<td>Good visibility of major risks</td>
<td>Ineffective and inefficient controls</td>
</tr>
<tr>
<td>Strong senior management mandate</td>
<td>Risk culture not sufficiently embedded</td>
</tr>
<tr>
<td></td>
<td>Lack of business and specialist skills</td>
</tr>
</tbody>
</table>

More than a third of CROs reported the overall framework as a strength, while a quarter identified risk culture as a positive force in their organisations. This translates into five building blocks, and action is needed to strengthen all five if the function is to be reinvented and elevated to a level where it cannot just cope with the challenges ahead but deliver real value to the underlying business. Organisations specifically need better management information, improved analytics, stronger risk controls, a deeply embedded risk culture and upgraded skills. These five areas will be discussed in more detail in the following section.
01 | Improve risk management information

A key role of any risk function is to provide a complete, consistent and comparable view of risk across an organisation. This enables senior management to make better decisions and appropriate trade-offs. Although the majority of CROs we surveyed said that they had good visibility of operational risks, many still described existing operational risk management information as backward looking, shallow, not dynamic and hard to compare across the organisation when what they wanted was information that was regularly available, comprehensive, comparable, action oriented and forward looking. As one succinctly put it, “We don’t have a good way to aggregate risk reports.” Another pointed out that they wanted to understand “vulnerability, not the size of the problem.”

Specifically, management needs information that enables risks and mitigation efforts to be prioritised; this creates a feedback loop on the effectiveness of management action.

For example, the use of different non-financial metrics across different risk types makes it very hard to consistently prioritise risks or to build the business case for investment in mitigation. Rather than reporting measures that are hard for non-specialists to understand or concentrating on myriad indicators rather than directly quantifiable metrics, management information needs to deliver results that are meaningful and comparable for senior management. “We want reporting that changes behaviour”, said one CRO. Specifically, management needs information that enables risks and mitigation efforts to be prioritised; this creates a feedback loop on the effectiveness of management action.

An important demand heard from some CROs was for a consistent core metric (or metrics). This would enable prioritisation and feedback and would be the foundation for strengthening the risk culture, focusing scarce resources on the right priorities and
enabling a portfolio view of operational risk. Developing such metrics would be a critical task for an umbrella operational risk function.

Our view is that such metrics are likely to include a financial estimate of operational risk exposure, which would enable the business to make the case for mitigation, make operational risk transparent to management and provide a way to record success or failure that fits into existing enterprise-risk reporting. Without progress on this front, there will be a limit to what can be achieved.

There were also demands from some CROs for more in-depth information on risks and mitigating actions and more information on emerging risks within organisations and across the industry. Such demand for different data reflects different goals: institution-wide metrics make different risks comparable and help prioritisation and resource allocation, while specific business metrics support active risk management and control.

02 | Embed advanced analytics

CROs identified advanced analytics (beyond capital modelling and stress testing) as a potential game changer for operational risk management and around half earmarked it as a priority for innovation and investment over the next five years. “We need to move from reporting to forward-looking risk management through analytics,” said one CRO. “The trick is to convert data into information.”

Advanced analytics has the potential to reduce losses as well as reduce the number of people required to manage specific operational risks. Today, however, advanced analytics initiatives are often nascent, sub-scale and beset by teething problems. Nevertheless, several CROs told us that they are making good progress in seeking to capture the full value of high-priority use cases such as enhanced internal and external fraud detection, improving the efficiency and effectiveness of financial crime management – for example by reducing the number of false positives in transaction monitoring – as well as in trade surveillance, where analytics can help flag potential rogue traders, to give one proven use case.

03 | Strengthen risk controls

Controls are a weak link in many operational risk frameworks – there is a sharp focus on identification and assessment of risks but less focus on controls, which tend to have proliferated organically with no formal coordination. A robust control management framework will paint a clear picture of the cost/benefit of controls. Several CROs said they were reviewing their control setups, setting up a central control inventory, moving toward a process view of controls and rationalising in order to concentrate on the key controls to ensure they are efficient and effective. They suggested that these efforts will continue and intensify because of cost pressures and continually elevated risk levels.

Some of the CROs mentioned that, as part of a broader shift in operational risk management from being reactive to being proactive, they increasingly expected a focus on preventative controls rather than detective or corrective controls. An example would be to put in place better data governance and upstream data quality controls, which would allow an institution to reduce its reliance on cleaning, fixing and reconciling data downstream.
The future of operational risk

One CRO captured the mood when suggesting that the improvements needed in risk controls in financial services were similar to the changes in quality control in the automotive industry in the 1980s. Resources need to be focused where they will have the greatest impact and duplicative controls should be removed. For instance, quality control is vital in production processes, but not all processes are equally important; therefore, it is important to invest in controls where both the likelihood of a risk event and the resulting impact are highest.

04 | Foster a strong risk culture

Most CROs said senior management was well aware of the importance of operational risk management and was spending a lot of time on it. But while the battle to convince the board may have been won, the challenge has shifted down a level – for some CROs we interviewed, instilling a broader risk culture was high on their agenda. One participant argued that “Risk culture is the single most important element of risk management.” Only a quarter of respondents said risk culture was already a strength in their organisations.

“Operational risk is just accepted as the cost of doing business,” explained one CRO. “That can imply it is not worth managing. The struggle we face is to make a difference each day when many other pressures exist in the business. For instance, changing the retail distribution network incentives from ‘sales’ to ‘responsible and fair sales’ is a substantial challenge.” None of the CROs were relaxed about progress here, and many noted the need for constant effort and reinforcement through a mix of setting the right tone from the top, senior management role modelling, education and training, sanctions and incentives (including financial rewards).

05 | Bolster people and skills

Most of the CROs we interviewed stressed the need for better operational risk managers in both the first and second lines of defence and a third explicitly mentioned skill building as a key investment area. “We have operational risk managers who don’t manage risk,” said one CRO. “We need people who can get stuff done in a complex environment.” Specifically, CROs said they wanted experienced business managers and specialists who can credibly challenge and assist first-line businesses and functions; people with analytical, cyber and IT skills are also in high demand. Unfortunately, progress is difficult because, as one CRO put it, “these are the same people that everyone else wants” – both internally and externally. To move forward, CROs are recruiting in line with their immediate priorities and creating centralised teams of experts who have new skills and on whom business-focused operational risk managers can call.
Conclusion

Our objective was to create an agenda for the future of operational risk management based on conversations with CROs from leading financial services firms. The results of our survey clearly showed that operational risk is expected to increase and it is the operational risk profile that will change the most over the next decade given the scale and complexity of emerging operational risks like cyber and outsourcing. Furthermore, our survey reinforced the idea that managing operational risk is difficult.

The discipline has undoubtedly made great progress over the past 20 years, and CROs expressed satisfaction with the work that has been done in the last few years, specifically on the “core” frameworks (e.g. risk identification and assessment, capital modelling). However, there is also clear frustration that these frameworks alone are not enough to allow their companies to tackle the risk management challenges that lie ahead.

Operational risk management needs to step forward and step up by engaging with the business and ensuring better coordination between different functions, such as operational risk, compliance and IT. The survey highlights five specific building blocks that must be strengthened: risk management information, advanced analytics, risk controls, risk culture and the skills that will be necessary to deliver effective and efficient operational risk management in the future.

Just reinforcing one or two of these five building blocks will not be enough. Action is needed on all five to ensure that firms can reinvent operational risk management when they need it most.

* * * *

The authors would like to thank chief risk officers from the following institutions for participating in the study: Allianz, AXA, Danske Bank, Deutsche Bank, DBS, FirstRand, Goldman Sachs, HSBC, Intesa SanPaolo, Macquarie, Morgan Stanley, RBC, Santander, Swiss Re, U.S. Bancorp.
## Contacts

<table>
<thead>
<tr>
<th>Daniel Mikkelsen</th>
<th>Simon Wills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Partner</td>
<td>Executive Director</td>
</tr>
<tr>
<td>McKinsey &amp; Company</td>
<td>ORX</td>
</tr>
<tr>
<td>Tel: +44 20 7961 6359</td>
<td>Tel: +44 1225 904397</td>
</tr>
<tr>
<td><a href="mailto:daniel_mikkelsen@mckinsey.com">daniel_mikkelsen@mckinsey.com</a></td>
<td><a href="mailto:simon.wills@orx.org">simon.wills@orx.org</a></td>
</tr>
</tbody>
</table>