O.R.X

Understanding conduct risk practices

Summary report
October 2017

About this study

In 2017 we surveyed 36 banks and insurers to see how they address conduct risk. We asked them:

- How they have defined conduct risk within their organisation
- How conduct is governed within their risk management framework
- How conduct is identified, assessed and monitored
- How they have sought to mitigate misconduct

This summary report discusses the results of the survey and secondary research we conducted, as well as discussions from the ORX Scenario Forum and Analytics Meeting held in May 2017.

Participants

- ABN AMRO
- Aegon Group
- AIG
- Allianz SE
- ANZ
- Assicurazioni Generali S.p.A
- AXA Group
- Banco Popular
- Bank VTB 24 (PJSC)
- Barclays Bank
- CBA
- CIBC
- Crédit Agricole SA
- Credit Suisse
- DBS Bank Limited
- Deutsche Bank AG
- Discover Financial Services
- Erste Group Bank AG
- FirstRand
- Grupo Santander
- Lloyds Banking Group
- Macquarie Group
- Millennium BCP
- National Australia Bank
- Nedbank Group
- OTP Bank
- Prudential Financial
- RBC Financial Group
- SEB
- Société Générale
- Standard Bank Group
- Swedbank AB (publ)
- TIAA
- UniCredit S.p.A
- Wells Fargo & Company
- Westpac Banking Corporation

Executive summary

Conduct risk is a top boardroom priority and regulatory expectations are fast-evolving

Recent years have seen conduct risk rising to the top of boardroom agendas at banks and insurers. Globally, regulators are serious about tackling conduct in financial services, demonstrated by the significant penalties levied for a range of conduct-related events.

As early as 1997, Australia introduced the so-called twin-peaks regulatory model, which separates macro-prudential regulation from conduct supervision. Following the global financial crisis, we have seen the popularity of this regulatory model spread to the Netherlands in 2002, and from there to Canada, the UK, and, more recently, South Africa.

This structural reform has elevated supervisory scrutiny of financial misconduct – a trend that is unlikely to change in the near future.

No universal understanding of conduct, though common themes emerge

Despite the regulatory pressure and its priority status, there is no universal definition of conduct risk. Definitions are typically broad, principles-based and encompass a range of existing operational risks. The idiosyncratic nature of institutional cultures and business models will necessarily mean there is some diversity in the understanding of conduct risk. This is particularly clear when looking at how firms have mapped conduct risk to their operational risk taxonomies.

That said, there are some common characteristics. Unlike many existing operational risk categories, conduct risk definitions often focus more on the customer or market outcome, rather than solely on the behaviour or activity.

Progress being made on addressing conduct risk

In response to the supervisory challenge institutions have been doing considerable work to address conduct risk within their organisations. While some firms have begun to create separate structures to oversee the measurement and management of conduct risk, most are retaining conduct risk under the operational risk function.

Fixing culture to improve conduct

Globally, regulators are focusing on the role organisational culture plays in driving behaviour and conduct – in 2015, the Group of Thirty outlined supporting and monitoring cultural change in financial services as a top regulatory priority (2015). Of all the initiatives to tackle conduct risk, respondents report that culture is one of the most critical.

While regulators are taking an increasing interest, to make cultural reform sustainable it needs to be driven from within the institutions themselves. Respondents are making significant progress in addressing this challenge and report a range of initiatives and programmes which have been implemented to drive positive cultural change. Embedding this change across an organisation is not an easy task, however, and it is expected to take time.

Defining conduct risk

As part of this study, firms were asked to submit their definition of conduct risk. This showed that they often use considerably different concepts. These can be approached from two different perspectives: in terms of actions versus outcomes, or in terms of where the accountability of the misconduct lies, for example with the firm, the individual employee, or both.

Actions versus outcomes

One perspective is to think about conduct risk in terms of the actions that trigger the event versus the outcome itself. Almost half of the surveyed institutions think of conduct risk in terms of the actions, i.e. the misconduct, that led to it (Figure 1).

Not quite as many (36%) focus on the effective outcomes, often in terms of detriment to their customers. A small group of firms (15%) reconcile both aspects in their definitions.

A question of accountability

Another central aspect of establishing a definition of conduct risk is the question of accountability. Does accountability lie with the individual employee or with the firm as a whole? To ask this question means asking questions about the role of company culture and, as some regulators emphasise, of senior management accountability.

Our results suggest that about half of the surveyed firms think accountability lies both with the firm and the individual (Figure 2). Another large group (39%) consider it to be a matter of firm-wide business practices and company culture. Only a small number of firms (13%) consider misconduct to be due to the individual decisions made by an employee.

Mapping conduct risk

A large fraction of survey respondents said they map conduct risk to Basel event types (47%). Out of these respondents, the majority map the risk type either to Clients, Products & Business Practices (EL04) alone, or to Internal Fraud (EL01) and EL04 (19% respectively). Of those firms that use the latter approach, five institutions are supervised by the EBA.

Out of the remaining firms that map conduct risk to Basel event types, one firm maps conduct risk to EL01 and Employee Practices & Workplace Safety (EL03), a second firm maps it to EL01, EL03, and EL04, and a third firm maps conduct risk only to EL01.

Just under a third of respondents (31%) stated that they map conduct risk to their internal risk taxonomy, and 22% said they do not map conduct risk.

Figure 1. Study participants' definitions categorised by actions and outcomes

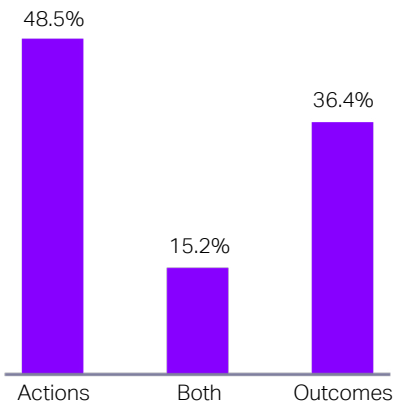
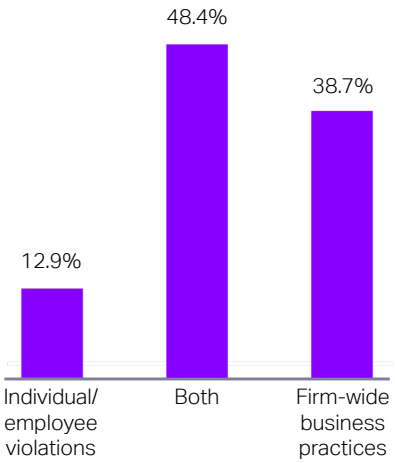


Figure 2. Study participants' definitions categorised by assigned accountability



Conduct risk governance

Over recent years, some firms have created risk-specific silos to manage certain risk types, which formerly fell under operational risk. Sometimes in response to regulatory pressures, a number of banks have now established separate conduct risk functions. This has at times led to situations where firms have several frameworks in place that duplicate risk governance efforts and lead to overlap and inefficiencies.

The creation of these silos can lead to the "Balkanisation" of operational risk. This geopolitical term, originally used to describe the historical break-up of the Balkan states, serves in this context to convey the potentially considerable drawbacks of a fragmented operational risk discipline with several, smaller risk silos. These silos run the danger of working in isolation from one another and creating considerable management overlap, sometimes unilaterally claiming areas of responsibility.

This "Balkanisation" may also make it more difficult for Chief Risk Officers (CRO) to effectively monitor and challenge the various risk functions when their time is being divided between a multitude of risk silos. As a result, some banks have started to bring operational risk governance back together under an umbrella risk function, responsible for all operational risk types including those overseen by specialist teams outside the operational risk function.

Discussions at the 2017 ORX Heads of Operational Risk Forum showed that there is a notable effort across the industry to reduce the number of risk silos. The majority of attendees are currently operating an umbrella risk function or are moving towards this model (ORX, 2017a).

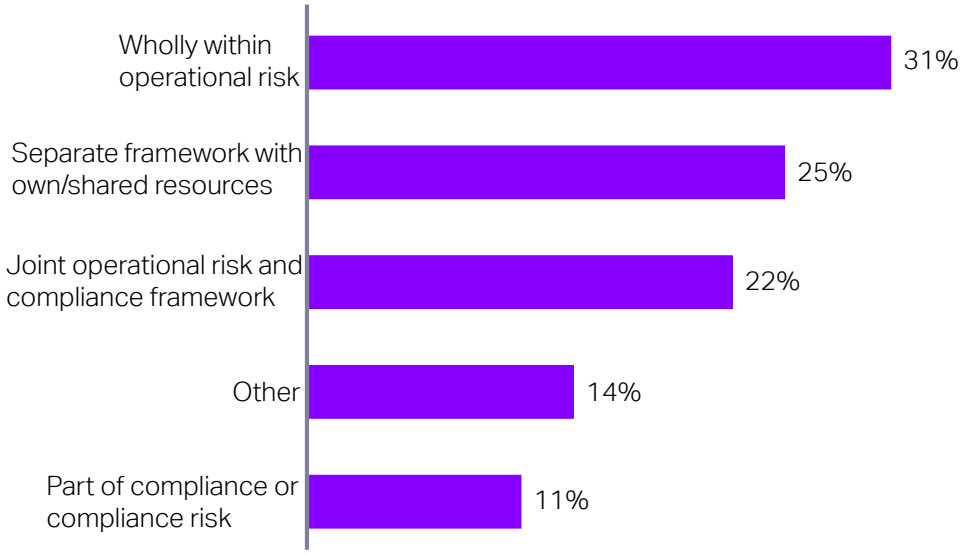
Under the umbrella

The majority of institutions surveyed for this report told us that they manage conduct risk as part of their operational risk framework (Figure 3). More than 30% said that conduct risk is managed wholly within operational risk and just over 20% manage it across the operational risk and compliance frameworks. A quarter of survey participants manage operational risk in a separate conduct risk framework.

A total of 11% manage conduct risk solely within the compliance framework. One insurance company stated that conduct risk is exclusively managed in the first line, sharing compliance and operational risk resources.

Conduct risk is also usually included in operational risk reporting – 74% of surveyed firms said they include reporting on conduct risk. Moreover, 46% say that conduct risk events are flagged in their operational risk databases.

Figure 3. Frameworks used to manage conduct risk



Managing conduct and culture

Perhaps for more than any other risk type, establishing and embedding a strong organisational culture is fundamental to effective conduct risk management. According to a CRO interviewed for the Future of operational risk study, "[r]isk culture is the single most important element of risk management."

We have also seen increasing regulatory interest in the topic in the past few years. In the Netherlands, for example, the central bank has formed a 'Governance, Behaviour and Culture' unit, counting social and organisational psychologists among its staff. The team assesses culture through periodic interviews with members of the executive and supervisory boards and other management tiers (Vox EU, 2015).

Looking ahead, demonstrating to supervisors that a positive culture is embedded across the institution appears to be an increasing priority for many Members. Responses from our survey suggest that Members are embedding a range of initiatives to address institutional culture and risk culture more specifically.

We have identified four key cultural themes used to incentivise good conduct and mitigate potential risks: communication and tone from the top; risk awareness and training; remuneration and staff appraisal; and understanding employee engagement.

Strengthening processes and controls

Alongside cultural initiatives, other more traditional improvements to the control environment were cited as important to conduct risk management.

A recent ORX study benchmarking Members' control frameworks indicates that Members rank their conduct risk controls as less developed than other types of operational risk controls (ORX, 2017b).

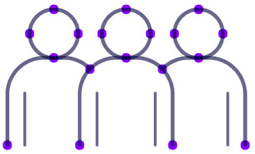
Our survey shows that several firms have established new frameworks for managing conflicts of interest, whistleblowing policies and other initiatives to drive risk ownership in the first line of defence.

Updating the new product approval process was cited by several Members as an important way to avoid customer detriment. This is in line with an understanding that conduct risk is a firm-wide responsibility and not the result of individual misconduct.

Initiatives to inform good conduct

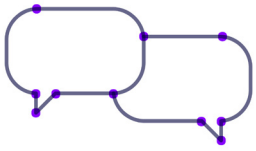
Risk awareness and training

A range of initiatives across the organisation including at senior management targeting client centricity, integrity, etc.



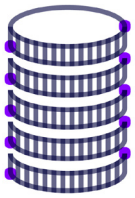
Understanding employee engagement

Employees survey assessing whether the bank is delivering good customer outcomes, independent culture risk awareness surveys, exit interviews.



Communication and tone from the top

Senior management and leadership championing conduct risk.



Remuneration and appraisal

Majority of firms now have direct conduct risk link to staff appraisals – behaviour objectives in performance appraisal, bonus driven by customer outcomes.

Bibliography

Group of Thirty. (2015). *BANKING CONDUCT and CULTURE A Call for Sustained and Comprehensive Reform*. Retrieved from http://group30.org/images/uploads/publications/G30_BankingConductandCulture.pdf

Mckinsey. & ORX. (2017). *The future of operational risk*. Retrieved from https://managingrisktogether.orx.org/research/future-operational-risk

ORX. (2017 a). *My five top takeaways from HORF 2017*. Retrieved from https://members.orx.org/news-and-blogs/my-five-top-takeaways-horf-2017

ORX. (2017 b). *Understanding control management practices*. Available from https://managingrisktogether.orx.org/research/understanding-control-management-practices

Vox EU. (2015). *Supervising culture and behaviour at financial institutions: The experience of De Nederlandsche Bank*. Retrieved from http://voxeu.org/article/supervising-bank-culture

O.R.X

www.orx.org
+44 (0)1225 904 397

Managing risk together

ORX believes many heads are better than one. We're here to bring the best minds of the international operational risk community together. By pooling our resources, sharing ideas, information and experiences, we can learn how best to manage, understand and measure operational risk and become less vulnerable to losses.

We work closely with over 90 Member firms to develop a deeper understanding of the discipline and practical tools. We set the agenda, maintain industry standards, and garner fresh insights.

ORX is owned and controlled on an equal basis by its Members.

For more information about ORX, visit our website at **www.orx.org**

Contacts

John Mears
Research Manager, ORX
john.mears@orx.org

Annika Westphal
Research Analyst, ORX
annika.westphal@orx.org