KRM22

Best Practices Guide to Operational Risk

Four step process for embedding Operational Risk Management

INTRODUCTION

Over the last 20 years or so, Operational Risk Management has emerged as a separate and specialised risk management discipline, one which has become increasingly vital for firms as they have rapidly evolved their technology landscapes, adopted new ways of working and faced new workforce challenges such as hybrid working.

In this article, we will start by outlining what is Operational Risk before moving on to Operational Risk Management and why is it important before outlining a four-step process to help you manage operational risks more effectively in your firm. Finally, we will conclude with an overview of an accountability framework which is the glue that makes the process work.

What is Operational Risk?

Operational risk is a category of risk that refers to risks arising from the day-to-day operations of firms. It is somewhat of a catch-all phrase, often taken to mean all risks that are not related to market or credit risk.

> *Operational Risk - The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. – The Basel Committee*

The category of operational risk is broad, covering everything from supply chain risk to people risk to cyber risk. It is also a category of risk which has tended to be seen as a lesser risk than credit and market risk, however, operational risk failures are often the root cause or a major contributory factor in many credit risk or market risk losses.

The Basel II accord defines seven event type categories:

- Internal Fraud – misappropriation of assets, tax evasion, intentional mismarking of positions, bribery
- External Fraud – theft of information, hacking damage, third-party theft and forgery
- Employment Practices and Workplace Safety – discrimination, workers compensation, employee health and safety
- Clients, Products, and Business Practice – market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning
- Damage to Physical Assets – natural disasters, terrorism, vandalism
- Business Disruption and Systems Failures – utility disruptions, software failures, hardware failures
- Execution, Delivery, and Process Management – data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

WHAT IS OPERATIONAL RISK MANAGEMENT & IS IT IMPORTANT?

Operational Risk Management is a management discipline which takes a structured approach to managing operational risks across the firm with the ultimate aim of managing operational risk within clear risk appetite boundaries while improving the operational effectiveness and efficiency of the firm.

In capital markets, operational risk can have huge implications on firms and their investors. Operational risk events can trigger defaults in collateralized transactions, trigger margin calls, or even lead to operational failures such as major IT systems failures, loss of key people or data breaches. Therefore, effectively managing operational risk can have a significant impact on the firm's value, reputation and standing with counterparties, customers, regulators, and other stakeholders.

As shown in figure 1 below, the level of operational risk losses increased significantly in the 10 years post the 2008 financial crisis and remains high.

Operational-risk losses increased rapidly after the 2008–9 financial crisis and have remained elevated since.

Banking litigation: costs, fines, and operational losses, $ billion

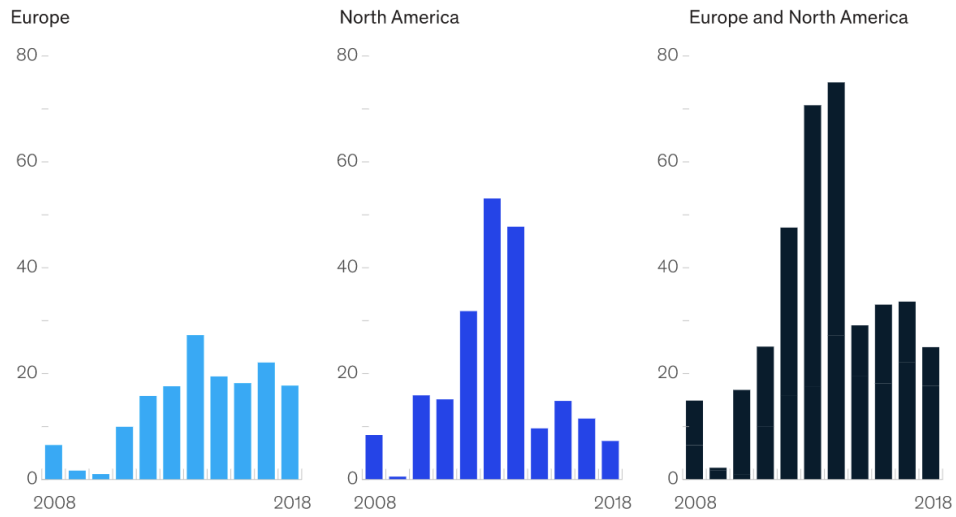

Figure 1 - Operational Risk Loss trends

As we fully emerge from the COVID-19 crisis and navigate the new world of digital transformation and hybrid working, strong Operational Risk Management will have an important part to play in creating and sustaining resilient firms. Key benefits of good Operational Risk Management include;

- Improved effectiveness, efficiency and reliability of business operations
- Improved operational decision making by taking a risk-based approach supported by real-time data.
- Reduction in Operational Risk related and other losses
- Early identification of unlawful activities
- Lower compliance costs, including reductions in regulatory fines
- Reduction in potential damage from future risks

FOUR STEP PROCESS FOR EMBEDDING OPERATIONAL RISK MANAGEMENT

To help firms embed the monitoring and management of operational risks into their daily, business as usual activities, we recommend a four-step process, which is;

1. Measure
2. Monitor
3. Analyse
4. Optimise

Measure

The first step in the process is to identify and measure the firm's operational risks, looking across the firm's processes, projects, technology, information assets, vendors and other partners and within its workforce and across its people. Historical risk events are also a good source of data to help define the firm's risks. Of course, another common way of defining the firm's operational risks is via a series of risk workshops and one-to-one interviews with staff.

Start by measuring the Inherent level of risk then consider the controls in place and how they are effective they are working. Also, consider any change projects which may influence the level of risk.

Having built up a picture of risk and the various things that influence levels of risk, the initial residual risk should be assessed.

Monitor

Having identified operational risks and measured the level of risk, both the inherent and residual levels, we recommend the implementation of a suite of metrics, balancing predictive and outcome metrics and over time, building the suite of metrics to include Key Performance Indicators (KPIs), Key Risk Indicators (KRIs) and Key Control Indicators (KCIs).

- Key Performance Indicators (KPIs) – use to monitor levels of operational performance, which is the ultimate outcome of good operational risk management.
- Key Risk Indicator (KRIs) – use to monitor levels of risk, and changes to risk levels. indicate the level and changes related to risk severity.
- Key Control Indicator (KCIs) – use to monitor the level of, and changes to control effectiveness.

In addition to implementing a suite of metrics, capturing and monitoring risk events and linking those back to risks provides powerful insights into the firm's risk landscape.

Analyse

The third step in the operational risk management process is to analyse the various risk-related quantitative and qualitative datasets to identify correlations and generate real-time decision-making insights. We recommend using interactive, visual management dashboards to present these risk insights.

Optimise

The fourth and final step in the operational risk management process is to optimise risk taking, including the level of controls within the firm, in line with the operational risk appetite to maximise operational performance across the firm.

This four-step process is not a one-off process, rather it is a continuous process to ensure that new risks are identified as they emerge and that the firm always has an up-to-date view of its operational risk universe.

THE RACI ACCOUNTABILITY FRAMEWORK

When seeking to embed better Operational Risk Management, one of the most important success factors is the establishment of clear accountability for the overall process, and the individual risks, controls etc within the process.

To establish clear accountability within the Operational Risk Management process, we recommend the adoption of the RACI Accountability framework.

This is a technique which was originally designed to be used in a programme/project management environment to clarify the roles of individuals and functions in the delivery of a programme/project. However, since its inception, it has been used within many management disciplines outside of the programme/project management world, and at KRM22 we have embraced this proven approach as an important part of how we do Operational Risk Management (and it is embedded within the Risk Cockpit).

RACI is an acronym that represents the RACI Accountability roles;

Responsible(s) – the individual(s) who are managing operational risk.

Accountable – the individual who is ultimately accountable for the management of the operational risk process or individual operational risks.

Consult - the individual(s) that must be consulted before major decisions are taken about operational risks.

Informed - the individual(s) that must be informed after major decisions are taken about operational risks.

RACI is a governance and decision-making framework that clarifies the role and authorities of an individual within a process or activity where ambiguities and uncertainty exist. When implementing and using RACI, it draws out misunderstandings and differences between individuals regarding their role, level of authority and boundaries, which once surfaced, can be openly discussed and resolved. For firms using RACI, this enables greater decision-making transparency, faster decisions and a systematic streamlining of organisational decision-making processes.

ABOUT THE RISK COCKPIT

The KRM22 Risk Cockpit is an Integrated Risk Management (IRM) application that enables firms to reduce their use of cumbersome spreadsheets and reduce their reliance on manual risk management processes. In doing so, we deliver a real-time, firm-wide, single version of risk truth with drill-down and drill-across capabilities, covering each of the five domains of risk: Enterprise Risk, Market Risk, Compliance Risk, Operational Risk and Technology Risk.

Within the Operational Risk domain, we work with CROs, COOs and CIOs who are tasked with building a robust approach to Operational Risk to deliver better, timelier, and more accurate risk-based management information.

Often, they struggle under the burden of multiple spreadsheets, a vast number of systems to monitor, and critical information being sent (and sometimes missed) via email. They are frustrated by the lack of real-time, event-driven risk information which is required to improve the day-to-day management of their Operational risk whilst also making it easier, faster and less painful to generate operational and executive-level reports which are consistent across the firm.