



Preventing Disaster: How Banks Can Manage Operational Risk

Operational risk events can trigger huge losses. Banks can use new techniques to anticipate and fix problems.

By Sebastian Fritz-Morgenthal, Jan-Alexander Huber and Daniele Funaro

Sebastian Fritz-Morgenthal is an expert principal with Bain's Financial Services practice and is based in Frankfurt. Jan-Alexander Huber and Daniele Funaro are partners with the Financial Services practice and are based, respectively, in Berlin and Milan.

Executive Summary

- ▶ Banks have struggled to control operational risk, which is the risk of loss due to errors, breaches, interruptions or damages.
- ▶ Major banks have suffered nearly \$210 billion in operational risk losses since 2011.
- ▶ The key to effective operational risk management is training people to anticipate what could go wrong, especially when a business unit is about to do something new.

In the decade since the global financial crisis, banks—and their regulators—have become increasingly mindful of the need to manage risk. However, while banks have developed sophisticated systems for controlling financial risk, they have struggled to deal effectively with operational risk.

Financial risk includes credit risk (the likelihood that borrowers will pay back their loans), market risk (the likelihood that a security will fluctuate in value) and liquidity risk (the ability of a bank to meet its obligations to its depositors and counterparties). Operational risk (OR) is the risk of loss due to errors, breaches, interruptions or damages—either intentional or accidental—caused by people, internal processes, systems or external events.

In the decade since the global financial crisis, banks—and their regulators—have become increasingly mindful of the need to manage risk.

Losses from these operational risk episodes can be catastrophic, not just in a strictly monetary sense, but in terms of the impact on the bank's overall business and reputation, sometimes threatening its very existence. In recent years, banks around the world have been caught up in headline-generating scandals triggered by failures to contain operational risk. From 2011 to 2016, major banks suffered nearly \$210 billion in losses from operational risk (see Figure 1). Most of these losses stemmed from preventable mistakes made when employees and systems interacted with clients, flaws in the way transactions were processed or outright fraud.

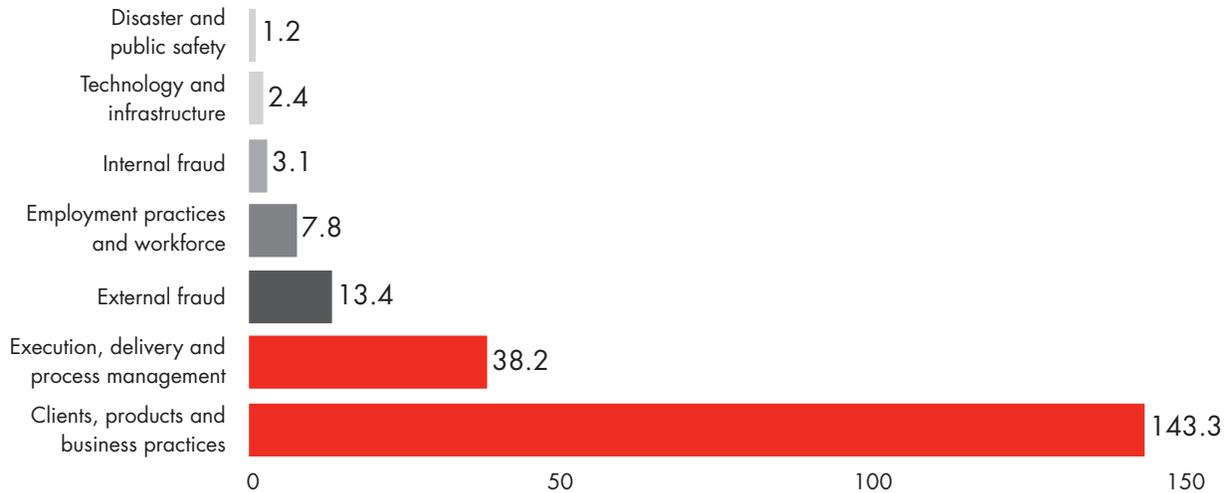
Regulators regularly review a bank's vulnerability to operational risk. As they do with financial risk, the regulators require banks to maintain capital buffers to help them manage an OR episode, should it occur. The regulator's assessment of a bank's ability to control OR can thus directly affect how much capital the bank has available to conduct normal banking activities. When an operational risk event does occur, it can have profound, long-lasting spillover effects. For example, an error or fraud in a bank's credit-underwriting process can cause the bank's credit costs to rise.

Preventing Disaster: How Banks Can Manage Operational Risk

Figure 1

Major banks lost nearly \$210 billion from operational risk events from 2011 to 2016, mostly from client interactions and process management

Operational loss by type, \$ billions



Note: Data from 96 banks includes all events of more than €20,000, January 2011 to December 2016
Sources: ORX; Bain & Company

Banks, in short, have every incentive to contain OR. Yet, they often find it hard to do. Compared with financial risk, operational risk is more complex and more challenging to monitor, control and manage. Even though OR can have a broad economic impact on a bank, banks have struggled to integrate operational risk management (ORM) in their overall framework of enterprise risk management (ERM).

Many banks have a tough time understanding, measuring and managing the interconnected factors that contribute to operational risk, including human behavior, organizational processes and IT systems. They find it challenging to create cultural, governance and management structures that can systematically control these risks. Instead of taking a deeply integrated, proactive and long-term approach to ORM, they end up managing operational risk with reactive, short-term measures.

Banks *are* making progress with ORM. As banking becomes more customer-centric and customers increasingly use digital channels, banks can gain greater visibility into what their customers, employees and IT systems are doing and better insights into what could go wrong. With digitalization and straight-through processing, banks can reduce or eliminate human intervention in many transactions, thus containing the risks of employee error and fraud. And, thanks to leaner and less bureaucratic organizations and Agile ways of working, managers can recognize and respond quickly to threats.

However, customer focus, digitalization and Agile methods aren't panaceas. In some ways, these measures can increase operational risks, or even create new ones. With decentralization, banks can end up with less control

Preventing Disaster: How Banks Can Manage Operational Risk

vested in their central ORM function and more of it devolved to business units. Executives may discover that they have less, not more, transparency into business decisions made at lower levels; they may find themselves playing catch-up with a front line that is innovating rapidly.

While automating processes once done by hand can reduce human operational risk, it can, if not monitored properly, magnify cybersecurity risk. In addition, banks can take their zeal for cost cutting and efficiency too far, to the point where it actually undermines the quality of ORM efforts.

When it comes to ORM, banks still have much room for improvement. The potential rewards are significant. In recent years, losses from operational risks at major banks worldwide have fallen sharply, from a peak of 6.2% of gross income in 2011 to 1.6% in 2016, according to ORX, an organization that tracks operational risk (see Figure 2). By taking steps to reduce those losses further, banks can have a direct and measurable impact on their bottom lines. Improving the 2016 loss ratio by 20%, for example, would be equivalent to a 32-basis-point increase in net profit margins. However, the real power in better management of operational risks is preventing the kinds of catastrophic events that have hit major banks in recent years.

Managing operational risk: Four areas to watch

Banks that take a comprehensive approach to ORM recognize four broad areas that need attention. The first is people. Even in a digital age, employees (and the customers with whom they interact) can cause substantial

Figure 2

Improved operational risk management has helped major banks cut their losses in recent years

Operational risk losses as a percentage of gross income



Note: Data includes all events of more than €20,000
Sources: ORX; Bain & Company

Preventing Disaster: How Banks Can Manage Operational Risk

damage when they do things wrong, either by accident or on purpose. Problems can arise from a combination of factors, including intentional and illegal breaches of policies and rules, sloppy execution, lack of knowledge and training, and unclear and sometimes contradictory procedures. Unauthorized trading, for example, can cause billions in direct losses and multimillions more in regulatory, legal and restructuring costs.

The second area is IT. Systems can be hacked and breached; data can be corrupted or stolen. The risks banks face extend to the third-party IT providers that so many banks now rely on for cloud-based storage and other services. Systems can slow down or crash, leaving customers unable to access ATMs or mobile apps. Even the speed of technological change presents an operational risk. With the cyber landscape evolving so rapidly, banks can have trouble keeping up with new threats.

The third area is less tangible than the first two, but no less important: organizational structure. By setting aggressive sales targets and rewarding employees for how well they meet them, bank management can encourage, and, in some cases, explicitly condone inappropriate risk taking. Such activity, when exposed, can lead to management changes, shareholder losses and regulatory fines.

The fourth area that vexes ORM planners is regulation. Since the global financial crisis, regulators have increased the number and complexity of rules that banks must follow. Banks that operate in multiple jurisdictions can face overlapping, inconsistent and conflicting regulatory regimes. Lapses can be expensive and embarrassing, triggering regulatory sanctions and customer defections. As is the case with technology, the speed and magnitude of regulatory change can be daunting. Even as banks are trying to contain costs, they must invest in the people, systems and processes that foster compliance.

Taking a comprehensive approach to ORM

Banks that understand the critical areas that drive operational risk can build an ORM framework buttressed by four guiding principles:

Since the global financial crisis, regulators have increased the number and complexity of rules that banks must follow.

Preventing Disaster: How Banks Can Manage Operational Risk

- They fully implement ORM across all business areas and integrate it into the bank's overall ERM structure.
- They clearly define ORM roles throughout the bank and fill them with the right talent.
- They embed feedback loops in the ORM organization to ensure continuous learning, from both success and failure.
- They regularly validate their approach and recalibrate metrics and incentives when necessary.

The first step to building an effective ORM capability is to fully assess the bank's existing risk profile and then construct a database and a map of all internal and external OR risk events. The bank then develops key risk indicators (KRI) that serve as early warning signs of potential problems. Management publishes some of these KRIs within the organization, and it uses others as part of its ongoing ORM surveillance. Once the bank identifies and categorizes each risk, it can decide on mitigation options.

Next, the bank clearly articulates its overall appetite for risk. This is partly an exercise in setting goals for financial measures, such as the amount of capital the bank is willing—and allowed by regulators—to have at risk, but it is equally a matter of establishing the bank's cultural and governance priorities. Management sets the tone with its behavior, decisions and actions.

The key to effective ORM is training people to *anticipate* what could go wrong, especially when a business unit is about to do something new, such as introduce a product, change a customer interface, alter the way employees are compensated, or outsource part or all of a core business process.

As banks increasingly use Agile teams to innovate, they can make sure that ORM experts are part of the effort. One major European bank, for example, has ORM staffers as integral members of the Agile teams on its innovation campus, where the bank develops and tests new business practices and offerings. Another European bank has built up a dedicated cyber-risk team that simulates realistic cyberattack scenarios and takes action to prevent them from happening.

The key to effective ORM is training people to anticipate what could go wrong, especially when a business unit is about to do something new.

Preventing Disaster: How Banks Can Manage Operational Risk

Anticipating and proactively deterring operational risk events becomes especially critical as banks reorient themselves around the customer experience. Any change to the way a bank onboards customers, creates and launches new products, or targets new customer segments has the potential to create new operational risks or mitigate existing ones. Having ORM experts embedded on Agile teams helps ensure that these potential risk triggers are detected and dealt with early.

However, identifying and mitigating operational risk is too large and important a task to be left only to the ORM experts. Frontline managers can act as the bank's eyes and ears on ORM by reviewing a short checklist of questions, starting with whether their business unit is involved in changes that could materially affect the way it operates.

The questions include:

- How well does your team understand the operational risk appetite guidelines, thresholds and regulatory requirements for your business area?
- Have you mapped the bank's systems that would be affected by your proposed changes?
- Are you aware of the risk/compliance breach events that have occurred in your business in recent years?
- How would your proposed changes affect the KRIs the bank regularly tracks in your area?

Technology-enabled risk surveillance

Banks have traditionally relied on a series of small-sample audits and spot checks to detect operational risk. With audits, banks delve deeply in a focused operational area, with the goal of finding—and fixing—excessive exposure to risk and outright wrongdoing. Such an approach can be effective, but it is, by definition, limited in scope.

Operational risk lurks everywhere—in people, processes and systems. The stakes are high. First, there are the obvious, near-term consequences of an operational risk event: financial loss, legal costs and regulatory fines. Then there are the indirect effects, which can be longer lasting and more pernicious.

Leading banks now use technology to supplement, and sometimes replace, audits. Using advanced analytics and machine learning, they leverage their tremendous trove of data to screen the entire bank's operations continuously and automatically. They use insights from this ongoing surveillance to quickly develop and adapt KRIs.

The automated surveillance runs constantly in the background and flags managers when something looks unusual or suspicious—much the way a credit card company alerts cardholders when there has been out-of-the-ordinary

Preventing Disaster: How Banks Can Manage Operational Risk

activity on their accounts. With automated screening, banks can direct ORM staff to focus on high-value, high-risk areas instead of having them conduct random, narrow, time-intensive—and often fruitless—audits.

Operational risk lurks everywhere—in people, processes and systems. The stakes are high. First, there are the obvious, near-term consequences of an operational risk event: financial loss, legal costs and regulatory fines. Then there are the indirect effects, which can be longer lasting and more pernicious: higher credit costs, mandated increases in risk-weighted asset thresholds, and reputational damage that can indelibly affect how customers, shareholders, regulators and counterparties view the bank.

Operational risk is driven by complex, interconnected factors that can be difficult to disentangle, including human behavior, organizational processes, change agendas and cultural issues. Banks that formulate a winning approach to ORM create a risk culture based on formal rules on governance and capital requirements, as well intangible elements such as training and leading by example. They make use of advanced analytics and machine learning to constantly monitor OR and to continuously learn from experience. Banks that are integrated and proactive about the way they manage organizational risk can realize real financial benefits and, more important, help prevent the kind of catastrophe that can have consequences for years to come. 

Preventing Disaster: How Banks Can Manage Operational Risk

Shared Ambition, True Results

Bain & Company is the management consulting firm that the world's business leaders come to when they want results.

Bain advises clients on strategy, operations, technology, organization, private equity and mergers and acquisitions. We develop practical, customized insights that clients act on and transfer skills that make change stick. Founded in 1973, Bain has 56 offices in 36 countries, and our deep expertise and client roster cross every industry and economic sector. Our clients have outperformed the stock market 4 to 1.

What sets us apart

We believe a consulting firm should be more than an adviser. So we put ourselves in our clients' shoes, selling outcomes, not projects. We align our incentives with our clients' by linking our fees to their results and collaborate to unlock the full potential of their business. Our Results Delivery® process builds our clients' capabilities, and our True North values mean we do the right thing for our clients, people and communities—always.



Key contacts in Bain's Financial Services practice

Americas

Mike Baxter in New York (*mike.baxter@bain.com*)

Joe Fielding in New York (*joe.fielding@bain.com*)

Andre Leme in São Paulo (*andre.leme@bain.com*)

Nicolás Masjuan in Buenos Aires (*nicolas.masjuan@bain.com*)

Marcial Rapela in Santiago (*marcial.rapela@bain.com*)

Asia-Pacific

Mark Judah in Melbourne (*mark.judah@bain.com*)

Thomas Olsen in Singapore (*thomas.olsen@bain.com*)

Europe, Middle East and Africa

Sebastian Fritz-Morgenthal in Frankfurt (*sebastian.fritz-morgenthal@bain.com*)

Daniele Funaro in Milan (*daniele.funaro@bain.com*)

Jan-Alexander Huber in Berlin (*jan-alexander.huber@bain.com*)

For more information, visit www.bain.com