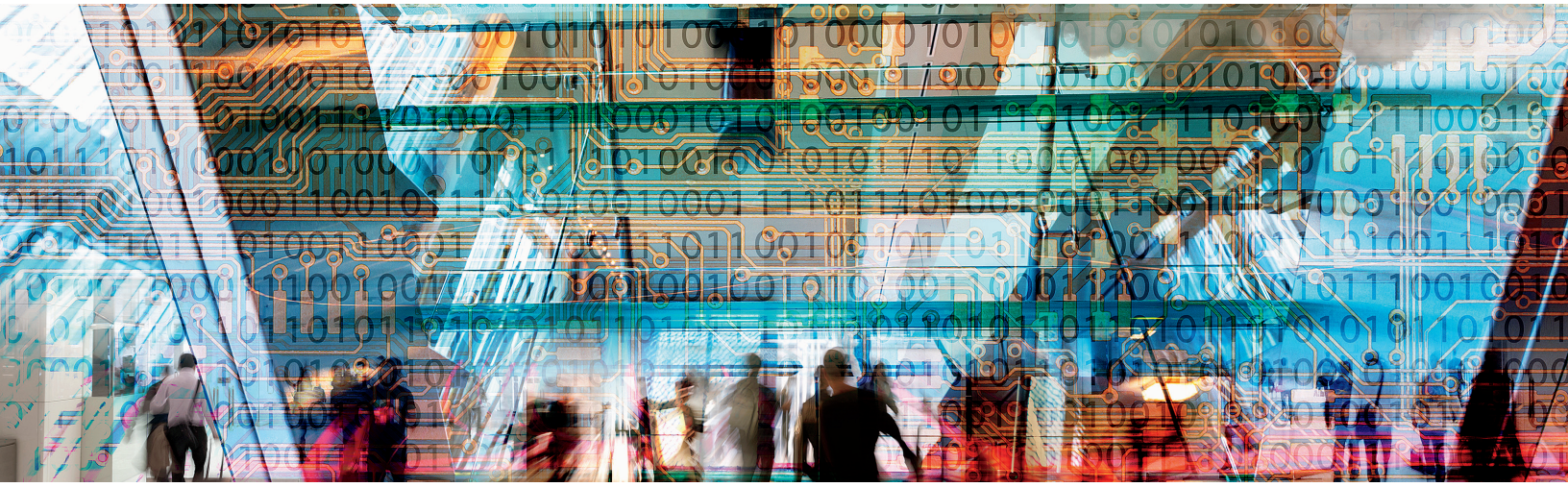
JULY 2016



RISK

Nonfinancial risk: A growing challenge for the bank

With credit and market risks now under better control, the focus is shifting to nonfinancial risks. Managing these well will require big shifts in banks' practices.

Piotr Kaminski, Daniel Mikkelsen, Thomas Poppensieker, and Anke Raufuß

Banks are accustomed to taking on financial risk and generating profit from it. It is the premise of their business models. But nonfinancial risk (NFR), whether related to compliance failures, misconduct, technology, or operational challenges, has only a downside. And the downside is large.

Foremost are the financial consequences. Between 2008 and 2012, the top ten banks globally lost close to $200 billion through litigation, compensation claims, and operational mishaps.[1] At least 17 incidents racked up losses of more than $1 billion each; another 65 incidents each resulted in losses above $100 million.

Yet the direct financial consequences of NFR are not the only concern. The reputational damage wrought can hit a bank hard at a time when customers, shareholders, and public stakeholders are questioning banks' business models. And there are also the personal consequences for senior managers, whom regulators increasingly hold accountable for misconduct or failure to comply with laws and regulations.[2] All of this, and the prospect of still tighter regulation, puts considerable pressure on banks to manage NFR better.[3]

Many have already invested heavily to do so, boosting head counts, creating new governance structures, and making operational improvements to control risks related to compliance, fraud, and IT. Yet the mitigation of NFR remains elusive. Much time is spent firefighting and remediating audit findings, yet too often there is no warning of when or where the next risk might materialize.

An important factor underlying this is a fuzzy definition of the responsibilities between the first line of defense, in the businesses, and the second-line control functions. In addition, control functions are siloed, each having its own risk-identification processes, reporting structures, and IT systems.

The result is duplicated work as well as costs. Banks feel they are drowning in parallel efforts aimed at identifying, assessing, and remediating risks, with the same individuals being approached over and over again, and diluting scarce resources and attention from running the business. Inevitably, the chief risk officer and his or her operational-risk unit struggle to provide the board and regulators with a thorough view of risks faced and controls required.[4]

Against this backdrop, many institutions seek a more integrated NFR-management approach in order to reduce the risk of further failures, meet stakeholders' requirements and expectations, and limit costs. This article describes the three key components of such an integrated approach: an enhanced governance framework, a set of enablers, and changes in the front office's approach and mind-set. It is based on our work with many financial institutions globally and an informal survey of 15 global and regional banks. Some of the structures and ideas we outline here are familiar to banks from their work on financial risk; many are newly conceived for the management of nonfinancial risk. Taken together, a full implementation of these concepts represents a paradigm shift in the NFR-management practices of many banks today.

An enhanced NFR-governance framework

In line with regulatory expectations, banks are building a governance model with three lines of defense. The first line owns and manages risks, the second line sets control standards and monitors adherence to them, and the third line—audit—checks on the adequacy of the first two.

Whereas all institutions regard the business divisions as the first line of defense, some overlook the role of central-infrastructure areas, such as IT and operations. These central areas do not take on financial risks from the balance sheet, but they are where the risk of most operational failure resides. Hence, many banks have extended the definition of the first line to include them.

In addition, they have broadened their definition of the second line beyond the risk and compliance functions to include areas such as legal, HR, finance, and tax, recognizing their role in managing the institution's control framework in their respective areas of risk expertise. Take legal. Like credit risk, it is often directly involved in business transactions, advising on and approving legal structures. HR, meanwhile, often sets and monitors policies on hiring, promotions, and compensation.

How a bank chooses to delineate first- and second-line activities in these areas might vary—there is no one-size-fits-all approach—but it is essential that the bank defines a consistent set of principles that reflect its governance structure, operational complexity, and specific regulatory requirements. These principles need to be permanent enough to guide future adjustments to the organization and operating model. They should clarify the organizational separation of the first and second lines to ensure independent control by second-line areas, while permitting them to perform activities as adviser or servicer. This is culturally important, so that second-line areas are seen as vital to the bank's business model.

The principles also need to emphasize the importance of first-line areas taking responsibility for NFR management, rather than focusing entirely on revenue or cost management. To be sure, given the complexity of managing controls consistently across the bank while meeting regulatory standards,

the first line may need additional expertise. For example, dedicated control units can help senior management identify and design improvements. Balanced scorecards, which measure control effectiveness and review thresholds and penalties for breaching them, can also help. Ultimately, the principles must promote a change in the organization's thinking so that risk management and controls are at the front of senior management and employees' minds.

Once they are agreed, the risk-governance principles need to be shared across the organization and formalized as part of the risk-policy framework, while the chief risk officer ensures their consistent application.

The role of the board

Despite recent improvements, many bank boards do not routinely consider NFR management, engaging only in some firefighting when risk controls fail. They can increase their engagement in various ways. Quarterly board meetings or a board committee dedicated to risk control are options. The meetings will need to provide auditable proof of appropriate risk-taking and risk-management decisions in line with the board's regulatory and legal accountability. Their quality will depend on input from both first and second lines and, crucially, on action-oriented reports on nonfinancial risk that align to a clear definition of risk appetite.

These meetings and reports are required so that boards can build a forward-looking perspective of the bank's top risks (and challenge the bank's risk profile), to assess the adequacy of the overall control system to keep the bank within its agreed risk-tolerance boundaries, and to ensure that any control gaps are addressed.

To these ends, the reports should consolidate risks by business and type of risk, and aggregate the following information:

1. *A set of quantitative risk indicators* that can be monitored to ensure the bank's tolerance of risk is not breached. These might include the history of operational losses as the basis for capital quantification, as discussed later, but can be more business specific, ranging from employee turnover (if the ability to recruit and retain is regarded as a top risk) to the number of customer complaints (if compliance is regarded as a priority risk).

2. *A record of major incidents and near misses,* and their impact in terms of financial losses or capital implications. The report should analyze the causes of such incidents, state what lessons have been learned, and indicate where similar incidents might occur elsewhere in the organization. This process can be augmented by scenario analysis.

3. *The results of risk and control assessments and internal and external audits,* highlighting control effectiveness and critical control themes.

4. *The status of efforts to reduce risks,* be they better controls or business adjustments—such as exiting certain businesses or improving processes—or an indication of new controls that might be needed as a result of regulatory change. Timelines for implementation should be clear.

Risk-management enablers

Banks have a standard set of tools and processes in place to manage NFR, but they are not always up to the job of managing risk effectively. Good NFR management depends on four elements: an integrated risk taxonomy, a control framework focused on prevention, an integrated risk and control assessment that considers emerging risks, and a quantitative assessment of risk.

An integrated risk taxonomy

If NFR management is to be integrated, all parties must speak the same language. Yet it

is common for second-line functions to use different taxonomies with overlapping types of risk and different definitions of those risks. This creates inconsistencies when applied in different risk assessments and reports or used to assign responsibilities. The number of taxonomies within an institution can easily exceed a dozen and may contain several hundred risk definitions. Consolidation into a single taxonomy can reduce the number of risk types to around 100, which in larger institutions can then be assigned to about a dozen second-line functions.

A control framework focused on prevention

It is important to be deal with risk efficiently when it arises. More important still is to prevent it materializing in the first place. There are two main ways banks can improve their control frameworks to achieve this. First, wherever possible, they should move controls upstream. Rather than relying heavily on reconciling data downstream between finance and risk, for example, they should ensure error-free data capture in their front-office systems from the outset. And rather than having the back office sample-test trades, front-office systems should automatically check trader mandates to prevent a trade being generated if a product or asset class is not approved for a specific trader or desk.

Second, banks should map risks along entire value chains and processes in order to understand where they might lie and their interdependencies. For example, the front office needs to be aware of all risks that can result from trading complex products because of the manual work-arounds that may be necessary to process them in downstream systems.

This end-to-end business view should also enable banks to review their business complexity in the light of control requirements. Controls might be unnecessary if underlying processes and systems or product complexities are addressed in ways that improve the robustness of the business model—which would also reduce the cost of control.

An integrated and forward-looking risk and control assessment

The evidence of audit findings and risk incidents calls into question the comprehensiveness and effectiveness of internal control frameworks. A rigorous assessment of the adequacy of controls will examine the following elements:

1. *A clear breakdown of the organization and its activities into assessment units*. These units should reflect the management structure and provide an end-to-end view of value chains within the bank's operating model.

2. *Common components*. These should include risk and control taxonomies, definitions of risk materiality, and a common aggregation logic. These should be defined for each risk type by the responsible second line.

3. *A common set of control attributes*. These serve as evidence for the design and implementation effectiveness of controls and can include characteristics such as the frequency of controls, the level of automation, and whether they aim to prevent or detect risk events.

4. *A clear governance structure across first and second lines*. Responsibility for identifying, assessing, validating, and reporting on risks and controls should be assigned clearly.

5. *An integrated management information system for first and second lines*. This houses assessments and provides a consistent reporting base by division and risk type.

Assessments also need to consider emerging risks. Traditional risk assessment (especially of

operational risk) often looks at avoiding risks that have led to losses in the past. But it is a reasonably safe bet that many of the risks that will trip up banks in the future are not yet on their radar. Some incidents, such as benchmark manipulation, were not identified because the assessments carried out at the time did not consider these activities specifically. To identify similar risks, systematic business reviews—not just once-a-year, group-wide assessments—are necessary. Leading banks monitor developments in other companies and even other industries for clues as to where new risks might arise, while deploying quarterly senior-management think tanks and mechanisms that encourage employees to flag risks.

These frameworks can help banks move away from the current fragmentation that sees different reports for operational risk, legal risk, conduct risk, and so on. Too often, top management is presented with hefty documents full of risk data from the various functions and a sea of red-amber-green assessments denoting the level of risk in what might be 100 different risk categories, in 50 business lines, and across 2,000 processes. This makes it hard to prioritize. Is a red flag for market manipulation in foreign-exchange trading more important than one for potential money laundering in wealth management, for example? It is also difficult for senior management to recognize patterns across units or types of risk, or to conduct root-cause analysis.

Transparent, aggregated reporting and active management involvement remain key challenges. Regulators tend to spot inconsistencies when reporting is fragmented; more important, they question whether senior management has an aligned view of its major risks and has lined up the appropriate remediation efforts and investments.

A quantification of nonfinancial risk

What gets measured gets managed. Hence, high-quality quantification of NFR is a great enabler of better risk management—at lower cost.

Unlike credit or market risk, where exposure is relatively easy to quantify at the level of each transaction and on aggregate, measuring NFR is hard, and few banks have tackled it sufficiently. Those red-amber-green assessments that banks use are often too imprecise for management purposes, even when combined with complex internal models for calculating capital requirements.

Several approaches to improving the quantification of NFR are gaining ground. A foundational element is to identify quantifiable risk indicators, such as error rates, linked to the top risks a bank faces. If selected appropriately, these indicators capture the true drivers of NFR exposure and the quality of controls, in turn providing a more robust foundation for risk assessments, scenario analysis, risk-appetite definition, and capital calculations.

Accurate capital quantification is also important, especially given the growing levels of risk-weighted assets banks are obliged to hold to cover operational risk. However, the advanced internal models

many banks currently use to calculate regulatory capital requirements have a mixed record. While arguably better than approaches based on income and balance-sheet metrics, they are complex and volatile, and at times unable to capture risks (or their drivers) at a sufficient level of detail. There are ways to ameliorate these issues by, for example, modeling at lower confidence intervals and tying the approach to quantifiable risk indicators. However, institutions need to consider the costs and benefits of making such improvements, not just today but also in light of regulatory developments (such as the Basel Committee's proposal to abolish the use of advanced internal models for calculation of Pillar 1 capital requirements for operational risk).

Stress-testing models are growing in importance and can provide valuable additional perspectives, especially as they take into account macroeconomic conditions, and can incorporate forward-looking scenario analysis.

Finally, advanced analytics, such as machine learning, combined with the analysis of a broader range of data than traditional loss databases (including country-specific legal-loss and fraud statistics, as well as voice, chat, and social-media data) hold great promise for better NFR management (and potentially capital calculation). Leading banks are using these methods to catch unauthorized behavior on trading floors and in branches, reduce employee turnover, improve hiring decisions, reduce fraud rates, and reduce both "false negatives" and "false positives" in their money-laundering screening processes. That means better detection of suspicious transactions with far fewer resources.

NFR in the business

Even as banks change their approach to risk management to account for NFR, so they must also make a couple of changes in the business. One is a more structured and strategic approach to the remediation of risk. The other entails cultural change.

Remediation

Almost every bank has been asked by regulators to fix problems and close gaps in their approach to NFR. In many cases, these remediation efforts are so numerous and so extensive that they take on a life of their own and seem to occupy nearly as much management attention as the core business. To avoid more remediations, banks should take three steps. For a start, they must actively engage the businesses, to identify areas where business complexity or footprint leads to unnecessarily high risks that should be addressed at the source, rather than adding costly controls.

Second, control remediation efforts have many interdependencies and often implicate several change projects. Banks need effective governance structures led by senior business managers to provide direction to remediation efforts and align them with the second line. Finally, banks should also strive for a good balance between cost reduction and control enhancements.

All of this requires a lot more participation by business leaders than in the past. These leaders may need additional expertise from control groups in the first line, to work with the second line to establish control environments, translate these into the business context, assess and monitor risk in the front office, and define and prioritize control enhancements.

The chief risk officer too has a role to play, in developing a groupwide understanding of the remediation efforts and establishing credibility (to senior managers, shareholders, analysts, and regulators) on the health of the control system and the adequacy of the risk profile.

Culture

However strong the risk framework might be, NFR management will fall short unless it is supported by a culture that acknowledges its importance, as not all risks can be controlled. Recognizing this, regulators pay specific attention to risk culture.[5]

Company values and norms therefore have to be communicated, and backed up by measures such as awareness training, incentive systems, and sanctions. Performance assessments also need to take it into account.

Senior-management involvement and role modeling will be especially important. Experience shows that in organizations where senior managers take the lead in NFR management, a strong risk culture emerges. If it is delegated down the ranks and senior managers focus instead on revenue generation or cost control, the message received is that what matters most is short-term performance.

The second line has a role to play in cultural change. Senior employees in compliance and operational risk often come from a quantitative, legal, or audit background, and can be seen by business managers as a hindrance rather than as adding value. This perception can be changed if they improve their understanding of the business by, say, spending more time on the "shop floor." Rotation of people with a business background into second-line functions is another way to bring about cultural change. Some banks require senior managers to rotate in this way before being promoted further.

■ ■ ■

The management of nonfinancial risk is complex and evolving, and banks around the globe are at different starting points. The size and complexity of an organization will influence its approach. Some might begin by building capabilities: training senior managers on the front line, for example. Others might overhaul those processes where they detect the highest risks. Or they might decide to embark on a major organizational realignment. Regulatory requirements will no doubt influence the approach as well as the speed of implementation. But whatever the approach, the prize of an integrated NFR-management framework is not only regulatory compliance but also significant business benefits in the form of lower risk and lower costs, as well as the protection of senior management with respect to their personal liabilities. A prize indeed. ■

---

[1] The Conduct Costs Project, CCP Research Foundation, ccpresearchfoundation.com.

[2] See, for example, the Bank of England Prudential Regulation Authority's Senior Managers Regime, bankofengland.co.uk.

[3] As an example of possible tighter regulation, the Basel Committee on Banking Supervision proposes to remove the advanced measurement approach and replace it with a standardized measurement approach. By our estimate, the impact would be to increase European banks' capital requirements by 70 to 80 percent, while US banks would see a much smaller increase because, on average, they already hold more capital for operational risk.

[4] See, for example, *Corporate governance principles for banks*, Basel Committee on Banking Supervision, July 2015, bis.org; *OCC guidelines establishing heightened standards for certain large insured national banks, insured federal savings associations, and insured federal branches; integration of regulations*, US Office of the Comptroller of the Currency, September 2014, occ.treas.gov; and *EBA guidelines on internal governance (GL 44)*, European Banking Authority, September 2011, eba.europa.eu.

[5] See Eric Lamarre, Cindy Levy, and James Twining, "Taking control of organizational risk culture," February 2010, McKinsey.com.

Piotr Kaminski is a senior partner in McKinsey's New York office; **Daniel Mikkelsen** is a senior partner in the London office, where **Anke Raufuß** is a partner; **Thomas Poppensieker** is a senior partner in the Munich office.