

# Managing non-financial risk in banking: Paradigm shifts in the making



**Authored by:**

Timo Beck  
Helmut Heidegger  
Daniel Mikkelsen  
Anke Raufuss  
Oren Salomon  
Outi Simula



# Summary

The management of non-financial risk (NFR) has become increasingly critical for banks because of losses incurred and increased stakeholder expectations that banks will manage future incidents better. While banks take on financial risk as part of their business model to generate profit, they would prefer not to incur NFR, which has only downside and no upside. We use the term NFR management deliberately (and contrast it with the better understood areas of credit and market-risk management), as the commonly used terms compliance risk, conduct risk, and operational risk are often ill-defined, potentially too narrow, and partly overlapping. We postulate that the prevailing approach of making mainly incremental improvements to NFR management falls short of customer, regulator, and shareholder expectations, especially given the hundreds of billions of dollars of NFR that have already materialized as losses or fines in the financial-services industry in the last decade. This view is supported by our extensive project work in this field with many financial institutions globally and a recent McKinsey survey conducted with more than 15 leading global and regional banks.

NFR management requires paradigm shifts in nine areas within the categories of roles and responsibilities, enablers, and business:

## Overall roles and responsibilities

- Invigorate the first line of defense with real end-to-end NFR accountability.
- Align second-line-of-defense responsibilities to increase effectiveness and efficiency.
- Better engage the board on NFR appetite, top-risk assessment, execution, and remediation.

## Classic risk-management enablers

- Make integrated NFR risk taxonomy the norm.
- Set up an effective, structured control framework focused on prevention.
- Deliver management-level, forward-looking risk assessment.
- Enter the domain of quantitative NFR assessment.

## Business transformation

- Organize the process around structural and strategic remediation.
- Transform the culture in both first and second lines.

The McKinsey survey confirmed the importance of the nine paradigm shifts across all banks and showed that banks still feel significant effort is required to advance in all nine paradigm shifts. While some of these shifts are starting to be adopted by industry leaders, but very few have been adopted more widely. Others are truly in their infancy, with few good working examples. Shifting the paradigm and reaching the level of robustness stakeholders expect from banks today will require a major transformation of both the capabilities and the approaches used in managing NFR across the industry.

Exactly how a particular institution should prioritize and deliver paradigm shifts, however, depends on its business mix, its complexity, and its starting point. We expect to see success achieved both through a series of highly targeted interventions and through holistic transformations. We strongly believe that these nine paradigm shifts will make banks more successful in managing NFR and in reducing risk.

In this paper, we will review the critical importance of NFR, explore current mainstream approaches to enhancing NFR, outline our perspectives on the nine areas where a paradigm shift is required, and reflect on potential implementation approaches.

### Managing NFR is increasingly important and requires a new, integrated approach

In the years since the crisis, we have seen an increasing occurrence of major operational risk, compliance, and control incidents, resulting in large financial impacts in many banks.










Financial institutions have suffered enormous losses in this space. In just five years (2008-2012), the top 10 banks have among them lost close to \$200 billion through NFR-related incidents.<sup>1</sup> The press has reported over the years that there have been at least 17 single incidents with losses totalling above \$1 billion and over 65 incidents with losses above \$100 million, and large losses continue to be incurred.

Quantifying the full extent of NFR losses remains a challenge. Fines and settlements reached 4.8 percent of revenue in 2014 for the top 40 banks globally. Regarding capital requirements, operational-risk capital already accounts for on average 7 percent of total capital among the top 100 banks (of those that report separate numbers). Regulation will only increase the cost of NFR incidents going forward. For example, the Basel Committee on Banking Supervision is proposing to abolish the advanced measurement approach (AMA) and is also proposing to roughly double standardized-approach capital charges, reflecting the perception of under-management and undercapitalization of NFR pre-crisis.

The distribution of incidents, losses, and costs is obviously slanted toward large global banks, especially in the United States, but Western European and regional banks are also increasingly affected. (Exhibit 1)

## Exhibit 1 The financial industry is facing significant challenges around non-financial risks and controls.

\$ Billion

Examples of control-related failures in the industry			Fines	Losses
	Mortgage misselling	96.5 <sup>1</sup>	n/a	
	Payment protection insurance	36.2 <sup>2</sup>		
	Rogue trader	0.1	7.2	
	London Whale	0.9	6.0	
	LIBOR manipulation	5.9	n/a	
	Rogue trader	0.1	2.3	
	AML <sup>3</sup> failure in Mexico	1.9	n/a	
	Tax evasion	0.8	n/a	
	Embargo violation	9.6	n/a	

**Significant increase in regulatory scrutiny**

- Number, intensity of regulatory reviews and investigations increasing
- New, more complex regulation issued on a continued basis including further localization

**Addressing the control environment one of, if not the biggest, industry challenges**

- A question of survival vis-à-vis regulators and public perception
- A competitive advantage in the ability to capture new opportunities and work with clients

<sup>1</sup> Fines and settlements connected to mortgage misselling, not including protection insurance or other related cases.  
<sup>2</sup> £22 billion set aside for claims.  
<sup>3</sup> Anti money laundering.

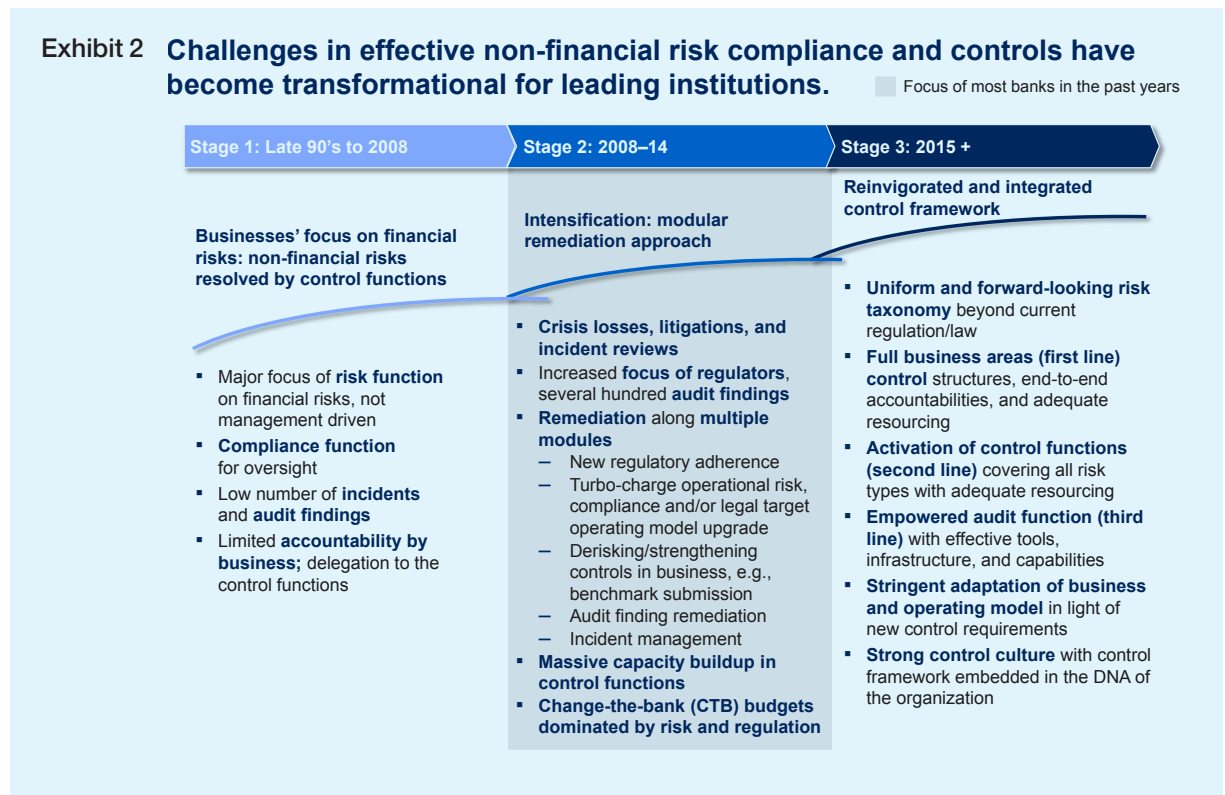
Looking forward, regulation and stakeholder expectations for NFR management will only continue to tighten: conduct risk rules, UK Senior Managers' Regime, the spread of rules requiring compliance functions (such as MaRisk and MaComp in Germany), and the heightened expectations of the US Office of the Comptroller of the Currency (OCC) are just some examples. Moreover, the trend is intensified by the increasing convergence of compliance standards (for example, via the European Central Bank in Europe).

The high and increasing cost of NFR, as well as the heightened expectations around banks' capabilities to manage and mitigate such risks, is creating a clear imperative for banks to do better. A recent McKinsey survey on the topic showed that banks are fully aware of these heightened expectations and the effort that is still required over the coming years.

Prevailing approaches to strengthening NFR capabilities risk stifling the front line with bureaucracy without fully addressing the need

In response to the increased importance of NFR management, many banks have already significantly boosted their head count and investments in operational risk, compliance, and conduct (for example, HSBC and JPMorgan Chase have both added thousands of compliance-related fulltime-employees in recent years. Many banks have created new committees and governance structures explicitly to deal with NFR (such as HSBC's Financial System Vulnerabilities Committee, and elevated reporting lines of chief risk officers and chief compliance officers). Specifically, there has been a great deal of investment in operational risk, compliance, conduct, and control frameworks (for example, head count, systems, frameworks, tools, and approaches). Despite these investments over the last years, the McKinsey survey shows that this trend is continuing with most banks still increasing their budgets and hiring further resources.

While most banks have pursued a modular fire-fighting mode on NFR in the past few years, there is a step change in larger institutions to implement a reinvigorated and integrated control framework (Exhibit 2).



The integrated approach has been key for those who have adopted it, helping to guard against duplicative investment. But it has not been universal, and some duplicative investment persists. For example, there are often parallel approaches to risk identification and assessment, parallel reporting structures, and parallel IT systems (instead of one integrated governance, risk, and compliance solution). Better integration and coordination in these areas could yield significant benefits in terms of both effectiveness (for example, better line of sight into risks, and better control outcomes) and efficiency (for example, less duplication and lower costs, and less burden on the front line).

Similarly, for attempts to mitigate and manage incidents, fines, and losses, it is often hard for banks to delineate operational risk, compliance, and conduct risk. It is increasingly difficult to manage the complex discipline of NFR without an integrated approach across operational risk, conduct, and compliance.

However, in most institutions, the NFR functions (operational risk, compliance, internal control, and so on) remain siloed and their approaches insufficiently coordinated. Simply adding head count or targeted capability improvements has not addressed the underlying need for more cohesion within the complex discipline of NFR. Instead, these incremental and additive approaches risk generating layers of bureaucracy that can have a stifling effect on the business while still leaving major gaps in capability. Here is why:

- NFR is much more complex organizationally than financial risk. The boundaries of different NFR functions (operational risk, compliance, internal control, HR, finance, operations, and others) are often not well defined, with significant risk of overlap. The debate on mitigation and control priorities is additionally complicated by the fact that risk quantification is more difficult.
- Adding people into an organizational setup that is not supported by an integrated risk framework can create complex bureaucracy for the front line to

navigate. Many banks now feel they are drowning in parallel risk-identification and assessment processes (e.g., operational risk-and-control self-assessments, operational risk scenario analysis, conduct risk assessments, compliance risk assessments, IT risk assessments, emerging risk assessments, and ERM assessments). To add to the workload, these parallel processes often use different taxonomies, methodologies, templates, and IT platforms. And they result in the same key individuals being approached over and over again to assess the same risks, which are then aggregated in different ways and reported differently. Many boards, businesses, and senior management teams, as well as front-line personnel, complain about this—and rightly so.

- A lack of clarity often remains on final accountability or decision rights across operational risk, compliance, conduct risk, and internal control, resulting in ambiguity, confusion, delays, gaps, and overlaps.

As a result, for many banks, NFR management is still unduly fragmented, involving lots of functions, methodologies, systems, reporting, and people.

A more integrated approach could improve efficiency and effectiveness. We see a strong need for much better coordination, reduction of duplication, and clarification of roles and responsibilities across all the functions involved in this space. This view is shared almost unanimously by the banks that participated in the recent McKinsey survey, the majority of whom report a need for a holistic transformation or at least a broader change program across second-line functions.

**Financial institutions need paradigm shifts in their approach to managing NFR to mitigate future losses, account for increasing complexity, and meet heightened stakeholder expectations**

There is broad anecdotal and survey evidence across the industry that suggests current NFR management faces vast challenges, which will require a significant step-up in managerial sophistication and talent injection at many levels.

First, overall roles and responsibilities regarding NFRs are less clear than for financial risks. For example, in contrast to credit risk, the first line does not always feel that NFRs are part of their job; while there are examples of banks that have successfully shifted risk ownership from second-line functions to first-line business, most still fail to do so. Second-line and third-line functions are often not aligned with regard to their responsibilities, creating duplication and gaps; and often the board is not deeply engaged in the way it increasingly needs to be. Many banks would still benefit from a more complete mapping across all risk disciplines of who does what across the three lines of defense. Overall, talent has vastly improved since the crisis. However, jobs in this space still have far less prestige, less clear career tracks, and less recognition than, say, positions in credit risk. Incumbents in these jobs are often still former auditors, accountants, and lawyers, and organizations suffer from limited lateral thinking on hiring colleagues with backgrounds in business, engineering, data analysis, and so on.

Second, risk-management enablers are often unsophisticated. For example, many banks still do not use an integrated risk taxonomy across all of NFR, and most banks are even less equipped to perform an integrated risk assessment across all of NFR. Use of advanced analytics (e.g., machine learning) to identify, assess, monitor, and manage

NFRs has been started only very recently and by only a few leading banks, although it is rapidly gaining wider adoption.

Third, true business transformation (involving single-point leadership, clear setup, aspirations, timelines, milestones, real leadership participation, and so on) is usually postponed due to tight deadlines. Banks often apply tactical fixes and additional layers rather than true strategic remediation. Most banks also still pay insufficient attention to the need to work on a transformation of risk culture, even though incidents often have a cultural root.

We see banks that have started trying to find solutions to all of these challenges and their experiences show that improvement is indeed possible. From our work with these banks, we see a need for nine distinct paradigm shifts in NFR management in three areas: roles and responsibilities, classic risk-management enablers, and a true business transformation of the way NFRs are managed (Exhibit 3). Our recent survey of more than 15 banks confirmed the importance of all nine paradigm shifts, and also showed that banks still feel that a lot of effort is required to advance in these areas.

For all nine paradigm shifts, banks will need to start by defining and owning the problem that remains around NFR. The exact shape of the challenge will vary by bank, depending on business model, operating model, and regulatory environment.

**Exhibit 3 The nine paradigm shifts are divided among three categories.**

**Overall roles and responsibilities**

- 1** Invigorate the first line with real end-to-end NFR accountability
- 2** Align second-line responsibilities to increase effectiveness and efficiency
- 3** Better engage the board on NFR appetite, top-risk assessment, execution, and remediation

**Classic risk-management enablers**

- 4** Make integrated NFR risk taxonomy the norm
- 5** Set up an effective, structured control framework focused on prevention
- 6** Deliver management-level, forward-looking risk assessment
- 7** Enter the domain of quantitative NFR assessment

**Business transformation**

- 8** Organize the process around structural and strategic remediation
- 9** Transform the culture in both first and second lines

# Overall roles and responsibilities

The first three paradigm shifts concern roles and responsibilities.

## 1. Invigorate the first line with real end-to-end NFR accountability

In theory, this paradigm shift should be easily implemented: the first line of defense simply needs to own and control its risks. However, in practice, this transformation means that banks have to invest considerable effort in the following areas:

- **Role definition.** Clearly define who is in the first line of defense and who is in the second line, and specify their associated roles and responsibilities. This is generally easy for the business (which is part of the first line) and functions such as compliance and operational risk (which are in the second line). For other functions such as HR, operations, and IT, the question is not as easily answered and requires a more differentiated assessment. For example, HR is often responsible for payroll services, a first-line activity, but it also often has the second-line control responsibility for HR risks such as compensation or employee-skills risk.
- **Reinforcement of the role of the first line.** Banks must clarify the role of the first line with respect to risk ownership and the responsibility for risk assessment. This often requires strengthening control resources in the first line—for example, creating dedicated divisional control units to replace the scattered divisional operational risk, compliance, and control resources that typically exist today. Giving the front-line NFR objectives through balanced scorecards—including key risk indicators (KRIs) or key control indicators (KCIs) with clear thresholds and clearly specified impact on compensation in case of breaches—can also make NFR priorities more visible.
- **Establishment of full end-to-end accountability.** Business accountability needs to be clear along entire processes. The business

must jointly remediate issues along processes, even if they occur further downstream, outside the business' organizational remit—for instance, in operations or IT. A frequent obstacle preventing the business from taking on such accountability lies in a lack of end-to-end transparency on processes or in the absence of forums or governance mechanisms to deal with these issues.

- **Engagement of frontline senior management.** Managers, especially senior managers, must be required to spend significant time on NFR. Senior managers need to have a clear view on the top NFR risks and on the sufficiency of controls, as well as on factors such as remediation priorities.

## 2. Align second-line responsibilities to increase effectiveness and efficiency

Alignment of second-line responsibilities also sounds fairly easy in theory. However, in order to make the second line of defense more effective and efficient, banks need to put considerable effort into clearly delineating responsibilities for the first line and between all the different second-line functions. Such alignment ensures close coordination among second-line functions for topics relating to more than one of them. The following are necessary:

- **Broad second-line definition.** Leading banks take a broad view on the second line. In other words, besides the “usual suspects” (risk and compliance), functions such as legal, HR, finance, and tax are also considered second-line control functions for the specific risk types they own. This extended view is supported by regulators (for example, the OCC) and facilitates full coverage of the broad range of diverse NFRs without unnecessarily duplicating required expertise. For functions considered in the broad view, it is vital to differentiate between first- and second-line responsibilities within the same function by taking an activity-based view. The HR function, for example, may act as a second-line control function for most employee risks (for example,



compensation and non-performance), but may also have a first-line responsibility for background checks on new employees or for payroll services. Some leading banks have already started to put efforts into further clarifying second-line responsibilities through this activity-based view (for example, JPMorgan Chase has published a paper describing its three-lines-of-defense framework and the roles within it<sup>2</sup>).

- **Holistic first- and second-line control framework.** Second lines need to define clear standards for the control framework for each risk type (typically in the form of a policy) and more detailed procedures and guidelines. Policy defines appropriate controls and their intensity through a prioritized, risk-based approach that takes into account the level of risk across both the first and second lines (for example, full portfolio reviews versus sample testing). Standard day-to-day controls are typically performed by the first line of defense, while the second line of defense monitors and assesses the effectiveness of the first line's controls. In some cases, however, the second line is more involved in supporting first-line controls, such as in cases of conflict of interest (such as a compliance-led control room) or, more generally, where there is strong expertise in the second line which it does not make sense to replicate in the first (as in the case of legal contracts). Overall, the bank's combined first- and second-line control framework needs to be effective, identifying the vast majority of issues before a third-line audit does so. Leading banks that have started defining such a holistic and integrated control framework have been able to reduce their control-related costs.

- **Control mind-set in second line and focus on activities rather than entire functions.**

For some control functions, this means a major shift in mind-set, from a supporting or advisory role to a risk-management and control mandate, which in turn implies an obligation to provide proper second-line challenge. (See sidebar on next page for a full list of second-line-of-defense responsibilities). In order to foster the mind-set shift toward a strong second-line control role, some banks are taking a functional or organizational view that is classifying full organizational units as either first- or second-line units, typically at the board level or one below in the hierarchy. While this simplifies the setup of first- and second-line controls in the organization, it falls short of the activity-based view required to properly clarify roles and responsibilities across the first and second lines.

- **Operational risk management as**

**coordinator.** Given the complexity of the more than 100 types of NFR that are often covered by second-line controls, we see a need for one functional area to take the role of coordinator across the various second-line functions. This coordinator (most often the operational risk management function) should ensure that all risk types are assigned to a second-line control function and that responsibilities between the control functions are clearly delineated. Moreover, the coordinator will often facilitate various processes where all second lines are involved (for example, risk-and-control assessments and reporting, and maintenance of a comprehensive risk taxonomy).

---

2 "How We Do Business— The Report." <http://investor.shareholder.com/jpmorganchase/how-we-do-business.cfm>

## *Second-line-of-defense responsibilities*

Although there is no precise regulatory definition of second-line responsibilities, the following are seen at many banks.

- Recommend the specific risk strategy to the board; set standards and policies.
- Ensure adherence to group risk appetite as defined and approved by the board.
- Design a risk-management framework, defining responsibilities for identification, assessment, management, mitigation, monitoring and reporting of risk in the first and second lines of defense.
- Advise the business on control requirements and creation of appropriate, effective, and auditable first-line controls.
- Define own minimum control standards, which are complementary to the control standards set for the first line.
- Independently evaluate first-line control effectiveness, appropriateness, and reporting.
- Conduct risk assessments (including risk modeling and analytics) to inform second-line monitoring and activity plans, and support first lines in assessments, especially where those first lines are less mature.
- Implement and participate in appropriate sign-off and approval processes regarding changes in areas such as business strategy, new products, and transactions.
- Design and implement appropriate, effective and auditable second-line controls.
- Attest to compliance with regulatory and internal requirements, in part based on first-line attestations.
- Report and escalate independently on risk assessment results and control and compliance issues to senior management and board as required.
- Coordinate and align with other second-line functions.

## **3. Better engage the board on NFR appetite, top-risk assessment, execution, and remediation**

Many bank boards are still not appropriately engaged on NFR. And many of those that are spending time on it are focused on fire-fighting specific incidents rather than taking a forward-looking view to identify the major risks and effectively set appetite and controls.

Boards should engage specifically on NFR appetite, which requires better definition in many banks. The NFR appetite should encapsulate a clear, forward-looking perspective on the bank's top risks and required remediation and controls, in keeping with the bank's strategy and operating environment. And it should specify unambiguous, measurable risk indicators to enforce the risk tolerance. This is essential, as the risk appetite serves as the vehicle that links the top-of-the-house view with the broader risk management framework and the implementation of controls. Without it, the board cannot effectively steer the institution in this area of increasing regulatory focus.

In particular, we often see banks getting stuck in the "zero-tolerance trap": while there should be zero tolerance regarding failures to adhere to critical standards, it is often unrealistic to expect zero incidents or losses in practice. Instead, banks should set realistic boundaries for incidents and losses.

Boards should also review their role in risk assessment and remediation, ensuring they have a clear view on the top risks in the bank. This means they should actively challenge the groupwide risk-assessment results. The groupwide risk assessment should form the basis for the board to actively steer the remediation discussion and give clear guidance on the overall remediation portfolio and the prioritization that is required.

Further, boards should demand that the risk appetite to which they agree should be well embedded and operationalized. Banks must ensure that risk

appetite can be monitored on an ongoing basis to track performance against it and that clear enforcement mechanisms are in place in case of risk-appetite breaches. Such operationalization requires that risk-appetite statements link with meaningful KRIs and that clear tolerances are set for them. Further, a pre-established view of what will happen if a tolerance is breached needs to be established. The days of “paper tiger” risk appetite statements should be over. For example, leading banks now use scorecards of KRIs and KCIs on a group level to monitor risk appetite for their top risks on an ongoing basis, including indicators such as high-performing FTE turnover (for employee risks) or number of customer complaints (for compliance risks). Further, leading banks cascade the risk appetite statements and associated risk indicators down to divisions/regions/countries to create transparency and facilitate better and more consistent risk management.

Additionally, boards should push control functions to provide transparency on how the bank’s “control dollars” are spent and the associated “return on investment”. Boards are then better placed to ensure that their control spend is commensurate with their risk appetite and commercial strategy.

We see increasing regulatory pressure on boards, including expansion of the role of nonexecutive directors and a clear focus on individual board-member accountability. Many bank boards therefore need to reset their NFR-management-related processes and decision making to a different level of rigor, especially with regard to issue identification and follow-up. For example, we expect auditable proof of appropriate risk-taking and risk-management decisions to become increasingly common across bank boards. Of course, there will be marked differences between regulatory environments, with UK regulators leading the way with the Senior Managers’ Regime.

This strong board engagement can be achieved in many ways, including through dedicated time in regular board meetings or separate sessions on NFR. For example, HSBC’s board has been at the forefront of recognizing the importance of NFR issues, establishing a Financial System Vulnerabilities Committee a few years ago and more recently creating a Conduct and Values Committee. Broader industry action is now required in this direction.

# Classic risk management enablers

Paradigm shifts 4 to 7 concern classic risk management enablers.

## 4. Make integrated NFR risk taxonomy the norm

While an integrated NFR risk taxonomy should be the industry norm, we still see many institutions struggling to align and integrate multiple risk taxonomies into one single taxonomy across all NFRs. Often, different second-line functions use separate risk taxonomies that differ in language, often overlap, and do not necessarily cover all risk types.

Banks that still use various risk taxonomies across NFR should invest in integrating them for the following reasons:

- **Common language.** An integrated taxonomy creates a common language with aligned terminology across the bank and hence greatly facilitates interaction and communication between second lines and especially between second lines and first lines, preventing unnecessary disruption and confusion for the business. Some banks even go as far as to merge second-line functions. However, this is not a requirement for achieving alignment.
- **Assignment of responsibilities.** Integrating taxonomies provides a basis for assigning and clearly delineating responsibilities between second lines. The common challenge with the use of various taxonomies is to ensure that all risks are covered and that first lines are not overburdened by several second lines controlling the same risk types. A single risk taxonomy creates transparency and hence allows banks to identify current gaps and overlaps in second-line responsibilities. Where operational risk and compliance are in separate organizations, a single “framework owner” should be assigned to coordinate activities across all functions.
- **Tree structure for different uses.** Integration serves different purposes through different levels of the taxonomy (or tiered tree structure). For example, one major global bank uses three levels

of taxonomy: level one, with 10–15 categories for assigning second-line responsibilities; level two, with 30–40 categories for high-level reporting purposes; and level three, with 100–150 categories for the definition of the detailed control model that also serve as a basis for an integrated granular risk assessment across all NFRs.

- **Top-down definition.** While a bottom-up approach to integrating risk taxonomies based on already-existing taxonomies within the bank has the advantage of creating stronger buy-in from second-line functions, several banks have had good experiences using a top-down approach for the definition of a single, integrated taxonomy. Often the taxonomies that are currently used differ substantially in structure, language, and so forth, and aligning them takes significant effort. A good starting point for the top-down definition is the Basel II loss-event types that can be amended to reflect the bank’s specific situation (with input from existing taxonomies). A further advantage of using Basel II loss-event types as a starting point is the close link to ORX<sup>3</sup> loss events to ensure proper external loss reporting.
- **Basis for policy framework.** As a last point, an integrated risk taxonomy can also be used as the anchor point for a comprehensive and well-structured policy framework with clear definitions of global standards and accountabilities. A conformance framework along the risk taxonomy can be used to determine how the second lines perform their oversight of the first lines, significantly reducing complexity.

In addition to unified risk taxonomies, leading banks are working on common process taxonomies to ensure better operational alignment across functions.

## 5. Set up an effective, structured control framework focused on prevention

Financial institutions need to move to a more systematic and structured overall control framework. Building such a framework creates more transparency on controls end-to-end to help identify the most

---

<sup>3</sup> Operational Riskdata eXchange Association

important controls along the main processes, thus improving the overall control setup. Banks especially need to work on two shifts:

- **From detective to preventative controls.** A shift is needed from reactive to preventative controls—that is, from cleaning up to preventing risks at the root cause. This shift includes, for example, moving controls further upstream in the process, such as by ensuring error-free data capture and hence reducing the need to rely on reconciliations further downstream. Clear early-warning signals or behavioral indicators should be further used to identify risks as they materialize. Because this shift requires proximity to the process, often the first line is better placed to deploy preventative controls and mitigate risks early, especially when clear process owners are assigned (for example, system-enforced checks of trader mandates in front-office systems, preventing the generation of trades if the product or asset class is not approved for a specific trader or desk, rather than sample testing of trades by the back office).
- **Controls along end-to-end processes.** Leading banks are gradually moving toward greater end-to-end process transparency and a better understanding of the underlying risks and appropriate controls via process-risk-control (PRC) mapping. This shift enables them to focus their efforts on key processes and controls, such as by taking a prioritized, risk-based approach and not “boiling the ocean.” Such banks clearly define what constitutes a control and create a structured view, underpinned by a standardized “control catalog” and systems that support integrated tracking. This development is also driven by regulators asking more and more about a central view on key controls for a specific business or process.

The structured end-to-end process view further enables systematic testing and tracking of both control design and control effectiveness. It also provides the basis for a systematic evaluation of the cost of control (for example, through a clear view

on which controls are in place along each process, identification of key controls, and end-to-end improvement of control processes).

## 6. Deliver management-level, forward-looking risk assessment

The following five main shifts are required in risk assessment and reporting for NFRs:

- **Clear first-line accountability for risk assessment.** Leading banks structure their risk-and-control assessments along end-to-end processes. They divide their organizations into manageable units—parts of the organization with a meaningful cut (that is, those aligned with management accountabilities) and a manageable risk-and-control scope. Such alignment makes the business the clear owner of the assessment and helps ensure meaningful sign-off of the risk-and-control assessment. Senior managers have to “sign in blood” as to the accuracy of the risk assessment for their now well-scoped part of the organization. The challenge many banks still face is to find a meaningful level and not to boil the ocean. Some granularity is certainly required, but it should be kept to a level that is still manageable. Manageable units can differ in size according to, for example, risk and complexity aspects: for instance, from front-office structuring units of about 50 FTE to back-office settlement units of more than 300 FTE. Unfortunately, we still see banks that perform their risk assessments on a relatively granular level but do not use this level of detail to align them with clear senior accountabilities.
- **Second-line challenge of risk self-assessments.** In addition to clearer first-line accountability, we also see a shift to more closely involving the second lines in the risk-and-control self-assessments. Often, risk assessments are still performed only by the businesses and not sufficiently challenged by second lines. In an upgraded risk-and-control self-assessment (RCSA), second lines should be playing a more active challenger role throughout the entire process for their respective risk types. However,

banks should be careful to avoid first lines “outsourcing” their risk assessments to the second line and surrendering ownership of risks. Second lines should also assess and challenge the risks they themselves give rise to.

- **Integrated risk assessment across second lines.** The risk-and-control assessment process itself and the associated reporting should move toward a fully integrated approach across all second-line functions and risk types to enable a holistic view. Today, many banks still perform a panoply of risk assessments—for example, for operational risk, compliance, and conduct risk—that often overlap, provide fragmented results, and lead to inconsistencies and different versions of the truth. Thankfully, however, the use of standardized risk-and-control taxonomies and integrated assessment processes to ensure a coherent picture is becoming more common. An integrated assessment further allows leading banks to consolidate system platforms and hence move toward a more cost-efficient assessment process. It also enables a clear link with other sources of information such as audit or loss databases that can be used as key inputs for the assessment. All of these moves help senior management obtain greater transparency on the overall risk profile.
- **Forward-looking risk-and-control assessment.** A challenge in NFR assessment is to generate forward-looking insights. Traditional risk assessments are often built on a backward-looking perspective that focuses on past losses. While the top risks of a bank, on an aggregate basis, are unlikely to change dramatically from quarter to quarter, there are notable examples of risks that were not on the radar of banks and turned out to be very critical. A good example is LIBOR, which was often not perceived as a risk-bearing activity, as it was not profit-generating or directly client-facing. Also, even though broad risk categories might be well known on an aggregate basis, often the content within them keeps changing. Cyber risk, for example, has been on most banks’ agendas for more than ten years,

but with regular changes of focus topics and new developments. Hence, banks need to apply a more forward-looking view: risk assessment needs to look at processes where risks could occur, not only where they have occurred. And banks need to reframe the questions about how risky an activity is to include reputational risk. (This could, for example, have made the difference in the LIBOR example above.) Early-warning indicators need to be developed and monitored to identify potential new risks for the bank. Potential approaches to achieve a more forward-looking risk assessment include stress-testing and scenario tools, and a horizon-scanning capability to identify new emerging risks (for example, looking at other financial institutions and across other industries). Examples of leading practices in this area include taking a medium-term (not a one-year) view, convening senior management “think tanks” (e.g., on a quarterly basis), creating an ongoing “all-employees-raise-risks” mechanism, and drawing systematically on external insights.

- **Actionable risk reporting.** Current reporting of NFRs is often fragmented across different reports, such as operational-risk reports, legal-risk reports, conduct-risk reports, and other compliance reports. Too often, management is presented with hundreds of pages of risk data and a sea of red-amber-greens lacking meaningful prioritization, synthesis, root-cause analysis, and clarity on recommended actions. In many banks, the data are presented in siloes, making it more difficult for senior managers to apply pattern recognition over time, across units, and across risk types to spot issues and ask the right follow-up questions. However, leading banks are implementing best-practice risk reporting that is focused on facilitating senior-management action. Such reporting also reflects the risk data aggregation and reporting requirements of BCBS 239. Granular and integrated risk-and-control assessment forms the backbone of such new reporting. In particular, integrated assessment allows for one single comprehensive report across all second-line control functions. Granularity

further allows different aggregation and reporting capabilities along various dimensions such as business, risk type, and legal entities. This allows for pattern recognition and follow-up questions, and it supports the identification of remediation needs and immediate reporting on impact along the same standard process.

## 7. Enter the domain of quantitative NFR assessment

Contrary to credit or market risk, where exposure is relatively easy to quantify at both aggregate and specific levels, NFR measurement is a more recent and complicated phenomenon. This is the case for the assessment of exactly where the risk occurs within a process (through KRIs along process points), for a specific process exposure, for the overall exposure, and for consequent capital requirements. Most banks still very much rely on a systematic red-amber-green (RAG) assessment, which represents a good practice starting point. However, very few banks have started to approach the topic of quantitative assessment sufficiently. More rigorous quantification still tends to be top-down and not at the process level, based on historical losses and their

distribution, while current bottom-up approaches typically still build on a qualitative RAG status logic.

We see three waves of development: with risk markers, bottom-up “exposure-based” modeling, and advanced analytics (including use of big data). Only a few institutions have engaged on the cutting edge of exposure-based modeling and advanced analytics, to methodically measure risks within processes, and to use the information derived to drive process improvements and risk reduction.

- **Risk markers.** Understanding and measuring the relevant indicators for key risks is crucial. Not every risk in every part of every process is quantifiable, and not every process or risk is important enough to warrant specific quantification. However, the key risks and key processes do warrant such efforts, and some banks today are undertaking efforts to identify risk markers in a methodical way that will allow early identification and mitigation of NFRs. For example, a leading North American player systematically uses risk markers where quantitative KRIs are not identifiable (see sidebar “Case example: North American bank”).

### *Case example: North American bank*

For unfair, deceptive, abusive acts and practices (UDAAP), a North American bank developed clear and detailed risk markers to help indicate issues. For example, for product design suitability and usage, looking at markers such as cross-subsidies, concentrated profitability, penalty fees, ability to repay and sources of funds, lack of prescriptive tools to assess suitability for target segment, and incidents of unanticipated usage has helped the bank identify issues such as business models or products designed with excessive profit from a few segments and above-normal churn and sales processes with poor suitability assessment. The bank then addressed these problems early, before they could blow up.

In areas where quantification was possible such as compliance with the Bank Secrecy Act (BSA), anti money laundering (AML), and the Office of Foreign Assets Control (OFAC), the bank identified specific, quantifiable KRIs that were statistically tested to indicate risk. For example, in order to assess report filing and the risk of making incorrect filings, the bank selected and monitored KRIs such as percent of customer transaction reports (CTRs) that were not filed accurately or in a timely manner, percent of monetary instrument logs (MILs) that were not filed accurately or in a timely manner, and percent of suspicious-activity reports that were not filed accurately or in a timely manner. Monitoring these KRIs allowed the bank to understand whether it was adhering to critical customer due diligence questions such as whether the customers were correctly risk rated and whether the assessment of money laundering was completed on time.

The bank used this approach comprehensively across multiple processes.

- **Exposure-based modeling.** Exposure-based modeling is a real paradigm shift in NFR modeling, addressing what banks today are not good at: bottom-up risk quantification, process by process, risk by risk, and unit by unit. The challenge with NFR—unlike credit or market risk—is to determine what the exposure is. Traditional operational risk models use historical loss data (and other inputs) to determine the distribution of potential losses, often for relatively large “units of measure”. Leading banks, however, have started to model NFR exposures bottom-up—that is, they break risks down to their drivers, such as daily trading volumes, to quantify the exposure and then apply risk indicators/markers, such as error rates, to quantify the risk. This approach enables a granular view—for example, a product-by-product view of misselling risk by looking at the number of sold products, the opaqueness of the product, the propensity of individuals to complain or sue the bank, and the regulatory fine distribution— to estimate the exposure and the quantified risk for a specific product, which can then be used as a basis for deciding to continue or stop selling specific products to specific customers.

Challenges clearly remain as these approaches involve many assumptions. However, the benefits are obvious, especially for large risk exposures, and such approaches give a very

different perspective to quantification that helps avoid some of the challenges of many current methods, which tend to be backward-looking and insufficiently granular.

Exposure-based modeling explicitly ties exposure metrics and risk indicators/markers to capital and therefore has the huge advantage of being sensitive to measurable changes in risk drivers.

- **Advanced analytics (including big data)**

Leading operational risk management and compliance functions are also increasingly using advanced analytics capabilities, such as machine learning, to trawl through large data sets to detect patterns that would either not have been found or would have been hard to detect using traditional methods. For example, one leading bank has been using such methods to analyze large, unstructured data sets of transaction information, emails, chats, and similar sources to identify errant behavior, leading to the disciplining of multiple individuals who had not been identified by traditional means. Similarly, leading banks are applying these techniques in the space of anti money laundering and terrorist financing to increase the predictive power of their transaction alert models, thereby significantly reducing the number of false positives and the amount of manual processing required by hundreds of FTEs.



# Business transformation

The last two paradigm shifts concern business transformation.

## 8. Organize the process around structural and strategic remediation

Banks today usually have huge portfolios of initiatives (typically hundreds of initiatives and large budgets running into the hundreds of millions). Often, these initiatives are silo-oriented, with a limited end-to-end view and duplicative work. They focus predominantly on fire-fighting and immediate remediation needs instead of forward-looking structural and strategic remediation to enable significant business benefits.

We see a clear need for banks to review their remediation portfolios and to move toward a more structural and strategic approach to remediation involving mainly the following three levers:

- **End-to-end approach to remediation.** Banks require a more integrated approach to remediation, with an end-to-end view on critical issues and focus on upstream remediations, in order to reduce downstream costs of control. Initiatives need to move from addressing symptoms of the issue to eliminating root causes; an example of such an initiative would be to implement a robust data warehouse, allowing for an increase in straight-through processing and hence avoiding manual data entry along the process. End-to-end accountability in the business will open up a real opportunity to move in this direction; however, it requires downstream transparency on the control environment for the business.
- **Simplification and integration of remediation.** The NFR management approach should be less focused on listing controls and remediating them one by one. Instead, banks need to identify common themes of issues that appear across the organization. The goal should be a true simplification of the operating model across the bank through integrated change initiatives and the consistent application of best

practices. This approach will also help banks prioritize according to the estimated size of the risk, in contrast to traditional approaches that broadly treat all control gaps as very or equally important.

- **Customer/product strategic adjustment.** Banks also need to take a much more strategic approach to remediation. Larger entities are increasingly described as “too complex to manage.” Remediation efforts should include fundamental business decisions, including radical simplifications across products and processes and even exiting entire businesses or countries. The ongoing digital transformation in banking and in the broader financial-services industry can also be a key source of simplification, simultaneously enabling better responses to NFR issues and significant business benefits.

## 9. Transform the culture in both first and second lines

Cultural attention to NFR differs greatly across banks today. In some cases, risk culture is seen as a burden, potentially the flipside of a strong performance culture. Numerous leading banks have concluded that cultural transformation is required in both the first and the second lines of defense. For the first line, the transformation of risk culture is mainly supported by strong top management communication and role modeling, as well as clearer incentives for compliant performance. For the second line, the focus should be on control challenge and on mind-set transformation aimed at driving business value, not just extra layers of policy.

The first-line transformation needs to be led by the front office, and it needs to result in real cultural change: the first line needs to operate in the “spirit of policies” and move away from box-ticking exercises operating by the “letter of the law.” Where good practices are adopted, we expect to see the first line more proactively consulting second lines, flagging issues, and adopting strong whistle-blowing

practices. To achieve this kind of cultural shift, banks need to focus particularly on three key areas:

- **Clear and consistent top management communication and role-modeling.** This is a key driver of risk culture transformation. We are seeing leading banks more visibly communicate on NFR and adopt a zero-tolerance approach to serious breaches of NFR appetite. Often, however, more consistent and pervasive interventions are required. This tends to be hard. The changes need to imply immediate behavior changes and be enforced by visible, strong signals. For example, several banks have radically reviewed traders' ability to communicate on their views and positions, reacting to benchmark manipulation reviews and fines, and issuing clear guidelines on approved conduct. The first line will need to define similar clear boundaries in other high-risk areas.
- **Systematic capability and awareness building integrated into daily work.** NFR identification and mitigation needs to become routine in every first-line organization. And to get there, banks must go significantly beyond rewriting role descriptions and redesigning processes. Some banks have effectively introduced NFR management, especially for operational risk, into their working culture by using daily check-ins dedicated specifically to identifying and mitigating NFR. Similarly, group- or business unit-wide simulations of a risk event with significant senior-management participation have been effective in making the new set of behaviors come to life and in helping highlight remaining gaps and weaknesses. One of the recurring findings from such simulations is a need for a cross-unit task force to lead the response and provide advice based on experience from other similar events.

- **Clear incentives.** Incentives must become clearer, and serious transgressions must consistently lead to immediate and real consequences. Getting this right is critical in aligning business practices with risk appetite and in improving the effectiveness of controls and remediation. For example, several leading banks have already adopted red-flag systems where noncompliant behavior is captured and reported rapidly, and has real impact on compensation. And many UK retail banks have transformed branch staff pay to align behavior with target conduct outcomes (for example, by replacing fixed sales targets with measures on meeting customer needs).

The second line, on the other hand, often needs to transition from being a business obstacle to being a "business value-add"—without compromising its independence and challenge role. This means banks need to change the way second lines engage with the business, ensuring that leaders, particularly the heads of the functions, spend real time on the shop floor. Today there are still too many banks that have more than 1,000 effective policies and lack an effective and integrated policy framework. The second-line approach needs to go from pushing out policies to using business language and building motivation to support real behavior change around the most critical risks. The following are key elements include:

- **Training and job rotation.** This is required for the second line to deepen its understanding of the business: too much of today's compliance and operational risk workforce has a legalistic rather than a business background. Similarly, more rotation of people with a business background into second-line functions should also be instituted. Some leading banks already encourage significant job rotation of this kind or even make them a prerequisite for promotions into management positions.

- **Second line as a thought partner.** The second line can help the business with control-and-remediation questions as decisions are being made, adopting an expert advisory role. For example, second-line representatives should participate in the main first-line governance meetings more often, which would provide a forum for the second line to give guidance on potential actions to take. However, the second line should of course be careful not to get too involved in first-line processes to avoid creating conflicts of interest.
- **Integrated approach to second-line culture transformation.** The various functions need to integrate their culture-transformation efforts, as experience in multiple banks suggests standalone efforts in individual functions do not work. For example, collaboration is often required to integrate parallel risk-assessment and culture frameworks across operational risk, compliance, and other NFR disciplines.

# The journey ahead

The nine paradigm shifts are relevant to the vast majority of banks, as very few are at the leading edge across all of them. Significant transformations are required to ensure the NFR approach and capabilities are well coordinated and meet external and internal stakeholder expectations.

However, there is no one-size-fits-all solution. The implementation of this integrated framework will look very different depending on the size and complexity of the organization. As a result, both the starting point and immediate priorities will differ greatly across banks.

## Global banks

Many global banks, which have already been hit by a series of NFR events, have started work on several of the paradigm shifts, either through a series of targeted interventions or through large multiyear programs. However, according to our recent survey of more than 15 large banks, most still feel very constrained by work on major legacy remediation portfolios, with notable areas of capability improvement yet to be initiated.

## Regional banks

Most regional banks are not yet as advanced in their NFR capabilities as the global banks, but they are also not as complex. Still, many regional banks have been operating with siloed leadership structures, with piecemeal approaches to NFR management. As regulatory attention is increasingly focused on the regional banks, they will need to scale up their efforts. They will increasingly need to define a consistent NFR framework and common “gold standards” across the group. Some regional banks are already leading the way, taking a more focused approach centred on the largest risk exposures. For example, IT risk and cyber risk have recently been a stepping-stone for regional banks to rethink and rapidly transform their NFR capabilities.

## National banks

Most domestically focused banks have tended to concentrate on financial risks and often have underdeveloped approaches to NFR. Relatively immature control systems and unsystematic approaches to identifying, assessing and measuring NFR are common. Some notable exceptions exist, mainly driven by two differentiators: how stringent the home regulator is and whether the bank has incurred sizeable NFR losses. A handful of domestically focused banks have led the way and have already built solid capabilities. Some banks in this category are at the inflection point of rapidly building up their capabilities, but many are still advancing their NFR capabilities gradually through evolutionary approaches. Going forward, most domestically focused banks will need to significantly upgrade their NFR capabilities. A typical first step will be the development of a structured and comprehensive risk taxonomy with clearly assigned responsibilities per risk type and an integrated risk-and-control self-assessment approach.

Because their starting positions differ, banks will need to adopt approaches that range from overarching programs to targeted interventions. We expect three different types of approaches: focused improvement of core NFR capabilities; deep-dives into businesses and processes driving the bulk of NFR; and major organizational realignments. We see a number of banks already undertaking such programs (see box on next page for examples).

The scope and speed at which banks will drive such transformations will differ, depending on their starting position and the specific circumstances they are in, such as recent incidents and regulatory feedback. Regardless of the approach taken, we expect the most successful banks to embark on multiyear journeys to generate tangible business benefits and meet regulatory requirements.

### **Focused Improvement of Core Capabilities**

One global bank launched a multiyear program aimed at capability creation for the management of NFR in the first line of defense. The key challenge had been to create a meaningful business case for the businesses to actively engage in NFR identification and management, beyond regulatory requirements. A “driver’s license” approach with training courses, exams and independently certified NFR management capabilities was introduced to recognize and promote greater empowerment of the first line. The multiyear program covered dedicated interventions on culture, processes, and tools affecting more than 10,000 employees.

### **Deep-Dives into High-Risk Businesses and Processes**

One regional bank initiated a focused review and overhaul of its compliance-related customer-facing processes in one of its business lines, most notably the client profiling (KYC – “know your customer”) and client review processes. Given regulatory findings by the bank’s home regulator on practices in some countries, the objective was to strengthen global standards that would be rigorously enforced in all jurisdictions. The bank views this as means to ensure sustainable performance and growth within the boundaries of its risk appetite.

### **Major Organizational Realignment**

One bank created a large, overarching board-mandated program for a holistic transformation spanning all of the bank’s divisions and functions. The program contained three central modules that overhauled the governance, operating model, and risk management processes of the bank, resulting in radical, groupwide changes. Additionally, more than 15 modules were initiated to ensure implementation of all defined changes in each individual division and function.

## Our vision

At the end of a successful multiyear journey, the control framework will not only be more effective, but also more efficient and smarter. An efficient control framework typically reduces the operating cost of conducting controls in the first, second, and third lines due to standardization of the control framework, an overhaul of end-to-end control processes, and a clear governance structure. In addition, an enhanced control framework will increase customer satisfaction as customer requests can be met faster, front-line time will be released for interaction with customers, and significantly fewer cases of misselling will occur.

# Contact

For more information about this report, please contact:

**Helmut Heidegger**

Director

Vienna, Austria

helmut\_heidegger@mckinsey.com

**Daniel Mikkelsen**

Director

London, UK

daniel\_mikkelsen@mckinsey.com

**Anke Raufuss**

Principal

London, UK

anke\_raufuss@mckinsey.com

**Timo Beck**

Engagement Manager

Stuttgart, Germany

timo\_beck@mckinsey.com



