Deloitte.

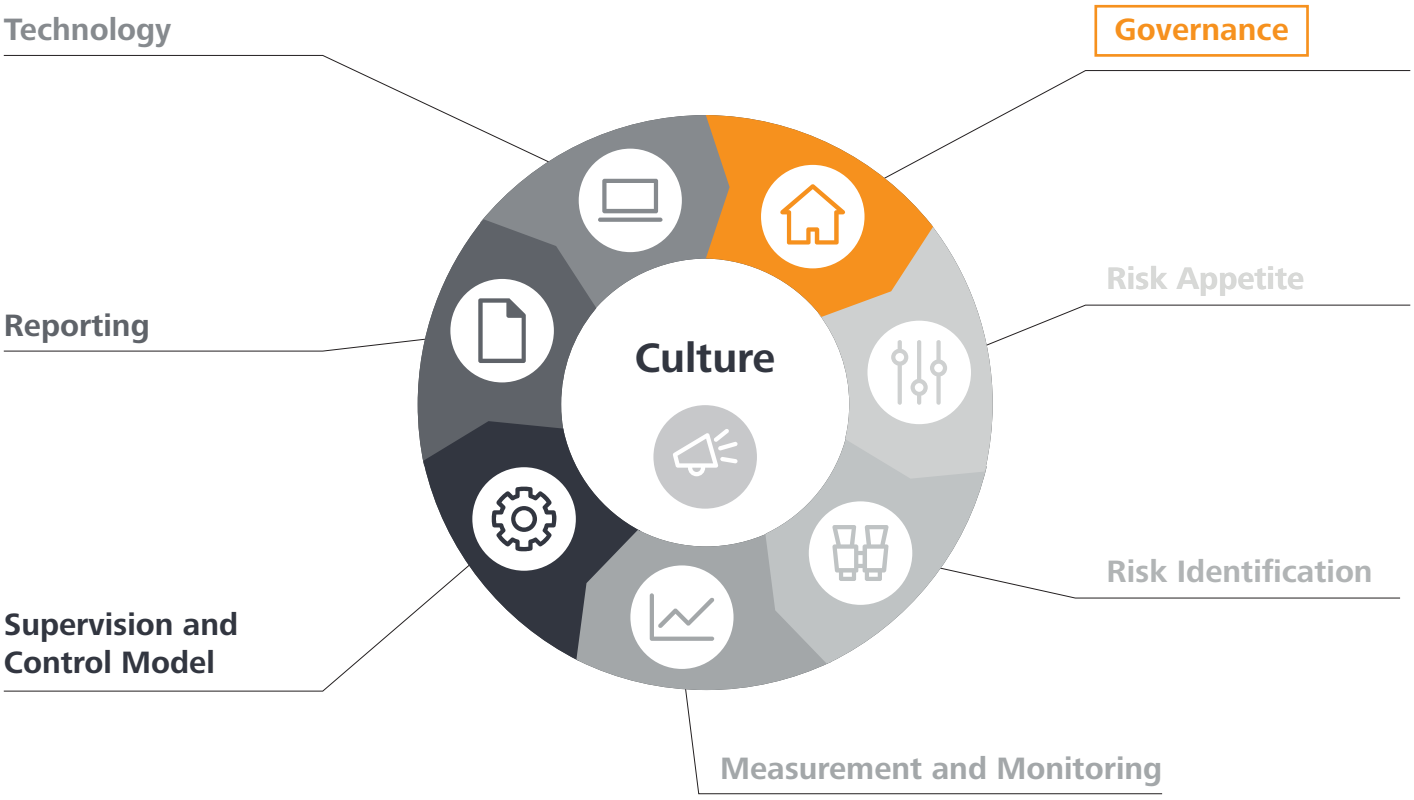
BU CF Deloitte Banking Union Centre in Frankfurt

Non-Financial Risk Management Insights Series

Issue # 3 – Governance

Setting up a governance model with clearly defined roles and responsibilities, a compatible organizational structure and oversight committees is a prerequisite for effective and efficient NFR management. An emerging trend in the industry includes centralizing NFR responsibilities in the second line of defence, often referred to as “umbrella function”.

Our Non-Financial Risk (NFR) Insight series continues with an exploration of the importance and implications of a dedicated NFR Governance model. The series brings into focus each one of the implementation categories first introduced in our original Point of View: The pressing case to design and implement a Non-Financial Risk Management Framework[1]



Introduction

Over the past decade, banks have incurred significant losses due to risk and control failures which emanated from outside traditional market, credit, and operational risks.[2] Going forward, the banking industry's exposure to NFRs is likely to grow, driven by the complexity of the business environment in which banks are operating, including new technologies, volatile markets, and global political uncertainty.

Increased risk of personal liability for executives[3] has contributed to additional focus on NFR governance. In addition, the focus of supervisors has shifted towards NFRs and individual NFR types.[4] Increasing supervisory scrutiny adds pressure on top management to demonstrate proper oversight, management, and control of NFRs.

In general, institutions are increasingly focusing on customizing their NFR governance model to better reflect their individual business models and NFR exposure.

[1] Cf.: https://www2.deloitte.com/de/de/pages/financial-services/articles/the-state-of-non-financial-risks.html
[2] Cf.: BUCF 2017, The pressing case to design and implement a Non-Financial Risk Management Framework.
[3] Cf.: Bank of England PRA Senior Managers Regime for the financial industry.
[4] Cf.: EBA Consultation Paper 2018/11 on outsourcing arrangements.

Scope and priorities

The key elements necessary to implement an NFR governance model include:

Roles and responsibilities

Roles and responsibilities across the three lines of defense (3LoD) and including all NFRs must be clearly defined and communicated across the organization. A comprehensive end-to-end perspective and collaboration across all 3LoD foster effective NFR and control management.

Organizational structures

NFR responsibilities at some financial institutions are assigned to a centralized group in the second LoD, often referred to as the "umbrella function". This group typically has a coordination role across the institution, effectively setting minimum standards across the risk and controls cycle (i.e., risk identification, assessment, mitigation, monitoring, and reporting). NFR management requires awareness and strong strategic prioritization at Board level.

Oversight committee structures

The increased importance of NFR is appropriately reflected and a senior NFR committee is established at the Board level and composed of first and second LoD representatives.

Challenges

Despite the progress made, major obstacles still remain, these include:

Smart 3LoD design

In most banks, clear mandates and responsibilities for the first and second line roles have not been implemented across all NFRs; room for improvement also exists regarding the centralization and coordination in the second line. Moreover, in the light of high cost pressure, implementing smart 3LoD designs (i.e., avoiding over-engineered models that overburden the frontline with risk and control activities and lead to building unnecessary LoD overhead) continues to pose a challenge with respect to the relative sizing of the first and second LoD.

Integration into the risk governance framework

It is important, but complex to identify and include all relevant NFR types, and harmonize relevant methods, processes, and systems in order to drive cost efficiencies at an enterprise level.

Management reporting

While many banks already exhibit a certain degree of integration of NFR reporting across all levels of the governance framework, progress has generally been slow. Data harmonization, aggregation, and projections remain incomplete. This is largely due to a lack of robust and forward-looking risk indicators and accepted measurement standards.

Evolving models

Prevailing NFR governance models are often fragmented, with differing responsibilities across NFR types (e.g., separate structures for compliance, IT/ cyber, third party/ outsourcing). However, a trend towards centralization of NFR responsibilities and an umbrella function in the second LoD can be observed. Three key models are gaining momentum:

CRO-Model

found at larger banks with a business model focusing on retail and wholesale clients. This model aims to centralize the management of all risks under the responsibility of the Chief Risk Officer (CRO) and fosters a consistent management across all risk types, utilizing common reporting and monitoring platforms as well as enabling a common risk culture and processes between risk control functions and business lines.

CCO-Model

found at larger banks, but tilted towards universal and investment banks. This model places some NFR categories (e.g., compliance and conduct) with the Chief Compliance Officer (CCO) at the Board level. The rationale behind such a set-up is based on the need for a differentiated set of skills and specialization for managing these types of NFR. Nevertheless, the harmonization of processes, systems, methodologies, and reporting structures in this model needs to be actively addressed in order to improve the cost base for such an institution's control functions.

COO-Model

applicable to smaller banks. This model adopts the separation of NFR from financial risks at the Board level by placing the NFR oversight with the Chief Operating Officer (COO), who focuses on process efficiency in managing risks.

Other appropriate governance models exist, including the allocation of NFR management to the Chief Financial Officer (CFO) or the Chief Regulatory Officer (CRegO).

Conclusion

The emergence of NFR adds new requirements and challenges to the risk governance frameworks of financial institutions. Large banks need to find the organizational and governance structures that best fit their business model and risk profile. However, a trend towards centralization of NFR responsibilities into one group in the second LoD, often referred to as an "umbrella function", in order to harmonize processes, systems, and methodologies is observed.

Contact persons

Dr. Michael Pieper
Director | Risk Advisory & NFR Co-Lead
mipieper@deloitte.de

Francisco Porta
Partner | Risk Advisory & NFR Co-Lead
fporta@deloitte.es

Gerhard Schröck
Partner | Risk Advisory & Leader BUCF
gschroeck@deloitte.de

For more information please visit our website: www.deloitte.com/de/nfr

Deloitte.

Deloitte GmbH Wirtschaftsprüfungsgesellschaft ("Deloitte") as the responsible entity with respect to the German Data Protection Act and, to the extent legally permitted, its affiliated companies and its legal practice (Deloitte Legal Rechtsanwaltsgesellschaft mbH) use your data for individual contractual relationships as well as for own marketing purposes. You may object to the use of your data for marketing purposes at any time by sending a notice to Deloitte, Business Development, Kurfürstendamm 23, 10719 Berlin or kontakt@deloitte.de. This will incur no additional costs beyond the usual tariffs.

This communication contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 286,000 professionals are committed to making an impact that matters.