Deloitte.

BU CF Deloitte Banking Union Centre in Frankfurt

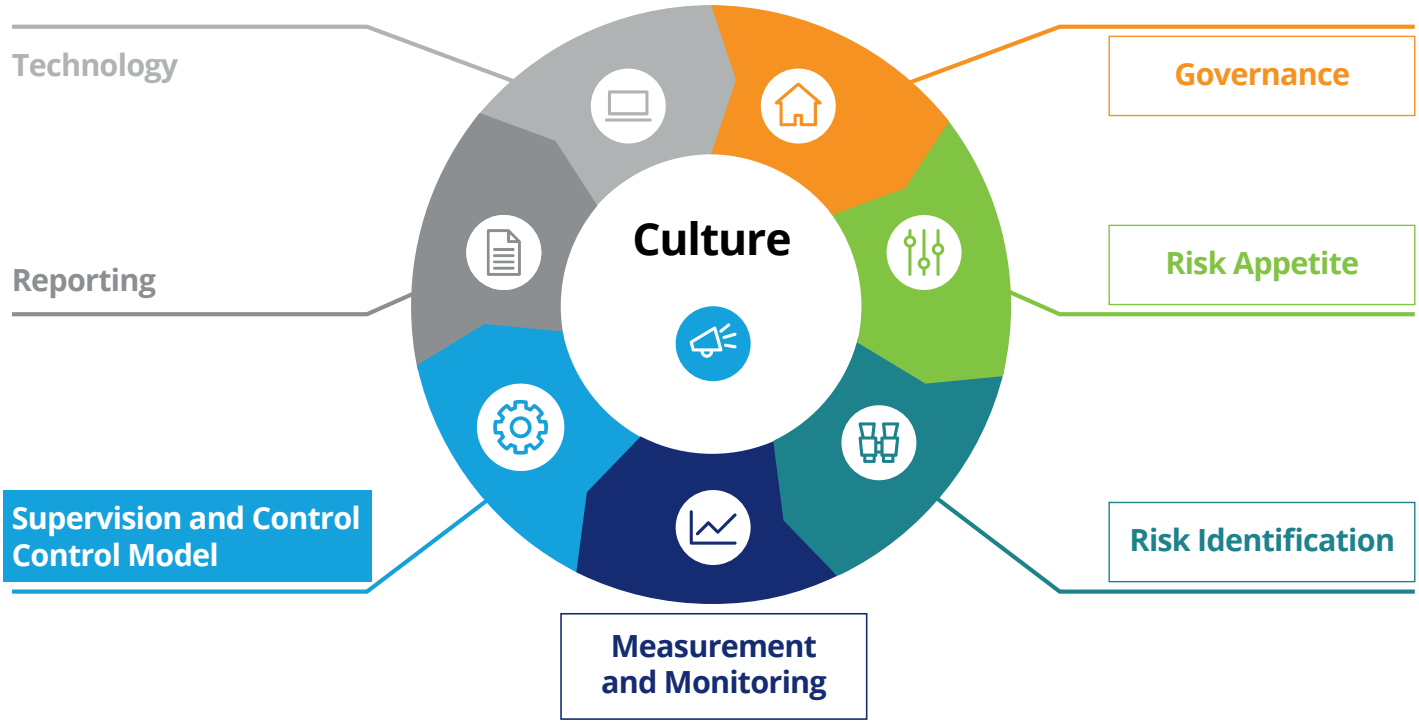
Non-Financial Risk Management Insights Series

Issue #6 – Supervision and Control Model

A supervision and control model for non-financial risk (NFR) identifies and reflects the controls associated with all relevant processes across all businesses and functions. In this issue, we review the challenges that commonly arise in the absence of a top-down control framework. We also look at what it takes to build an effective and efficient NFR control framework so that financial institutions can identify, measure, monitor, and mitigate NFR risks in a comprehensive yet efficient way.

Non-Financial Risk Management

A Deloitte series explores the eight dimensions of managing non-financial risk.



- The pressing case to design and implement a Non-Financial Risk Management Framework
- Issue #1 – Risk taxonomy and risk identification
- Issue #2 – Risk appetite
- Issue #3 – Governance
- Issue #4 – Culture
- Issue #5 – Measurement and monitoring

Introduction

Risk and control failures across the NFR landscape have hit the headlines in recent years, leaving a trail of fines and reputational damage among affected institutions. For example, conduct risk has led to LIBOR manipulation and violation of trading limits. Compliance risk has shown up in the form of money laundering, sanctions violations, and financing of terrorism. And cybersecurity risk has accounted for numerous incidents of data exposure or loss.

As a result, the stakes have gone up. Due to public scrutiny of a range of banking practices, regulators require accountability and attestation from top management.[1] Meanwhile, regulatory and economic uncertainty, due to an unsettled geopolitical landscape and disruptive innovation, have complicated firms' efforts to oversee NFRs and maintain effective controls. Regulatory authorities have taken notice: The Supervisory Review and Evaluation Process (SREP) is but one example of how they are putting internal controls to the test.[2]

All this has pushed NFR supervision and controls high on senior management's agenda, sending financial institutions in search of ways to reimagine the effectiveness and efficiency of their NFR control frameworks.

[1] For example, the UK's Senior Managers and Certification Regime (SMCR) holds financial services executives to account for misconduct that occurs under their authority. See: Jennifer Thompson, "Are asset managers ready to take responsibility?" *Financial Times*, 21 September 2019, https://www.ft.com/content/d783323b-af13-3109-b55e-80d417d8f882

[2] Deloitte, *The pressing case to design and implement a Non-Financial Risk Management Framework*, July 2017, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Deloitte_Non-Financial-Risk-Management-Framework-July2017.pdf

Challenges

A key challenge of NFR supervision and control is that risk mitigation and control measures can be highly specific to the risk type and business activity. To be effective, risk and control owners must be familiar with the business decisions and day-to-day activities that can trigger NFR. Without a top-down control framework, however, control functions may operate in silos, potentially leading to:

- Duplication of controls
- Multiple control inventories across the organization
- Gaps in oversight where process handoffs take place
- Redundancy between risk and control self-assessment (RCSA) and other risk assessment exercises

Objectivity can be an issue as well. A lack of independence between the second and first lines of defense can undermine the quality of monitoring and testing processes. On the flip side, it is also possible for risk and control owners to be too remote from the business activities, limiting the effectiveness of NFR control models.

These tensions can engender costly control frameworks and complexity at the point of interaction. The front office, for example, can find themselves responding to multiple internal control functions, all asking many of the same questions and with little understanding of the underlying business process—a scenario that is particularly relevant for financial institutions with a global footprint.

In addition, in many organizations the majority of controls are manual. Compared with automated controls, manual ones are less consistent and more prone to error. It also takes significant time and effort to execute and test manual controls, which runs contrary to the internal control function's ongoing efforts to reduce costs and identify emerging risks in a timely manner.

Our approach

An effective supervision and control model for NFR will look different from a model designed for financial risk. It assumes that risk management is embedded in the business routine, close to the everyday business decisions that can give rise to risk. For example, risk assessments can become part of the approval process for new products or large-scale IT projects, bringing a more proactive, dynamic approach to reducing NFRs and their associated costs.

This model requires active management of every part of the Non-Financial Risk Management Framework.[3] Components of particular importance include:

- A comprehensive risk inventory developed through a consistent, dynamic, and well-governed Risk Identification process [4]
- A governance model with clearly defined roles and responsibilities, a compatible organizational structure, and oversight committees [5]
- A culture in which everyone understands the organization's approach to risk management and compliance, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example [6]

[3] Deloitte, *The pressing case to design and implement a Non-Financial Risk Management Framework, July 2017,* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Deloitte_Non-Financial-Risk-Management-Framework-July2017.pdf

[4] Deloitte, *Non-Financial Risk Management Insight Series: Issue #1 – Risk Taxonomy and Risk Identification*, March 2018, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Deloitte_NFRI_Nr_1_2018.pdf

[5] Deloitte, *Non-Financial Risk Management Insight Series: Issue #3* – Governance, January 2019, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/NFRI_Nr_3_2019_web_safe.pdf

[6] Deloitte, *Non-Financial Risk Management Insight Series: Issue #4* – A Risk Culture Built to Last, April 2020, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-non-financial-risk-management-issue-4-culture.pdf

Bringing clarity to supervision and control team roles

Financial institutions can reduce complexity and improve compliance with supervisory expectations by making it clear who is responsible for each aspect of NFR control.

For instance, the first line of defense is responsible for identifying and assessing risk as well as identifying, carrying out, and testing controls. Ordinarily the business owns the first line of defense, although a business risk advisor can provide a second layer of accountability in carrying out operational risk and control management activities.

The second line of defense manages the NFR risk and control framework. This includes (for instance) setting standards for risk identification and assessment, maintaining a single control inventory, and independently testing the effectiveness of controls. A group of specialists in specific risks (such as fraud, third-party risk management, or cybersecurity) may contribute to the second line of defense, reporting to the financial institution's risk officer.

With this foundation, financial institutions can build a robust control model to identify, measure, and monitor NFR risks via:

Comprehensive risk and controls linkage. This step involves the comprehensive identification of NFRs across the whole risk taxonomy, classifying each one by risk type and source (including business units and legal entities). From there, controls are linked to each relevant risk. Different linkage models exist, e.g., some institutions choose a risk-driven approach while others opt for a processes-driven approach. The result is a standard inventory of NFR controls that institutions can use to boost comparability, avoid repetition, and optimize the NFR governance structure.

Prioritization. Top-down prioritization aims to identify key risks so that all processes covered by the control model are relevant and complete for all businesses and functions. A practical approach is to identify all key processes, determine their primary risks, then evaluate controls by order of impact. This produces a control model that the appropriate lines of defense can measure and manage (and keeps a less effective model from taking hold).

Digitalization. By automating the controls environment, firms can test controls more frequently and on a larger scale. Control digitalization also eliminates the need for sampling, making tests more accurate. On top of that, an automated, real-time dashboard of key risk and control indicators can help financial institutions monitor the NFR control function in an objective, systematic fashion. Finally, modern analytical tools and cognitive intelligence can tap into the data collected in the system to extract insights that inform business and risk management decisions in a timely, cost-effective manner.

Conclusion

Recent headlines have put NFR banking practices in the spotlight, prompting financial institutions to revisit their NFR control frameworks. What they often find are organizational challenges that require a focus on culture, governance, and risk identification processes to address. A comprehensive inventory of risks and associated controls lays the foundation for an efficient and effective NFR supervision and control model. Next is prioritization, followed by digitalization to extend insight and control across the appropriate lines of defense.

Contacts

Dr. Michael Pieper
Co-Lead Non-Financial Risk BUCF
Germany
mipieper@deloitte.de

Francisco Porta
Co-Lead Non-Financial Risk BUCF
Spain
fporta@deloitte.es

Encarnación Jurado Cano
Spain
enjurado@deloitte.es

Deloitte.

Issued 7/2020