



The pressing case to design and implement a Non-Financial Risk Management Framework

Senior executives are increasingly being tasked with addressing Non-Financial Risks (“NFRs”) holistically. Success will depend on their ability to rapidly create and implement their own risk frameworks and methodologies.

After the 2008 financial crisis, most banks invested considerable time and resources in enhancing existing risk management capabilities. Some also re-examined and strengthened their risk management frameworks, such as the three lines of defence model. Most efforts were largely limited to risks already identified by the Basel Committee on Banking Supervision

(BCBS) and, while they included operational risk within their reviews, they often paid less attention to non-traditional or emerging risks, including specific types of conduct and model risks. They also failed to consistently improve critical policies, processes, controls or systems and embed them into the businesses. ➤

“... as with commercial banks, risk management at central banks is more advanced with respect to financial than to non-financial risks ...”¹

BIS – 2009

¹ Issues in the Governance of Central Banks, p. 151; www.bis.org/publ/othp04.pdf.

So despite the BIS having identified NFR risk management as a relative weakness as long ago as 2009, the industry to date has made limited progress in this critical area. Recent losses and market events provide the evidence to bear this out: many of them did not emanate from traditional market, credit or operational risks in financial institutions' (FIs') portfolios, but instead from NFRs. These include, but are not limited to, conduct, cyber, compliance, model and IT risks. Despite significant investment, especially related to operational risk regulatory capital analytics and data management, current approaches to managing operational risk are not always effective: over \$500billion² of losses have occurred in the last ten years.

Although the definition and understanding of operational risk has undoubtedly evolved significantly from the initial generic "catch-all" approach, in large part because of the post-crisis investments to improve capabilities, more work is needed. This paper advocates a new approach to NFR risk management and proposes to accelerate progress in this emerging discipline by introducing the key components of an integrated framework for identifying, measuring and monitoring NFRs.

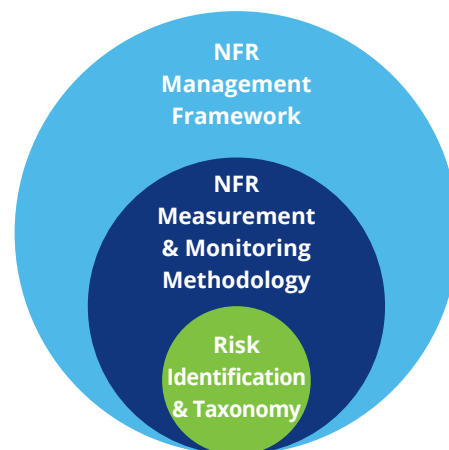
Our proposed methodology introduces and leverages an improved and comprehensive taxonomy that distinguishes between operational risk and other NFRs, and is designed specifically for FIs. The combination of an NFR taxonomy and methodology introduce the common risk language necessary to build NFR into banks' risk appetite frameworks. It's this common firm-wide language that will enable banks to articulate their NFR culture and risk appetite statement, to determine related limits, thresholds and triggers and to clearly assign roles and responsibilities across its three lines of defence.

High-severity losses derived from isolated and sometimes interconnected NFRs will likely continue. Largely because of that realization, NFRs have become a growing concern to FIs' CROs, CCOs, CEOs, boards and regulators.

There is also a very important regulatory dimension. Regulatory enforcement fines, penalties and litigation now dominate most large bank operational risk losses. Regulators, in addition to FIs' boards and executive teams, want to avoid events that could have systemic repercussions or could raise further questions about the industry's ability to learn from the mistakes of the past. Regulators too are expecting to see FIs adopt a common definition and understanding of NFRs to help distinguish risks traditionally - and perhaps simplistically - included under operational risk.

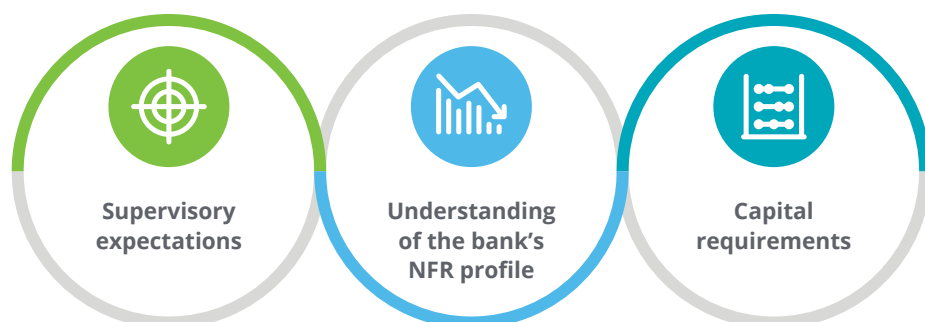
Some regulators are already actively embracing holistic NFR risk management methodologies that transition from a piecemeal and ad-hoc assessment of NFRs to a more integrated approach and allow greater comparability across FIs. Once confirmed as a priority in their supervisory agenda, timelines to comply could be aggressive. Moreover, we anticipate that regulatory expectations will not be limited to cosmetic changes; profound and meaningful improvements will be expected in order to avoid financial penalties and direct personal liability to senior management and boards. Consequently for FIs, a more robust, structured and holistic approach to managing NFRs will become necessary.

Risk management practices continue to evolve, our preliminary considerations on the future of NFR include a framework that will continue to mature, thus allowing FIs to more confidently identify, measure and manage NFRs.



² Source ORX

What will be the performance drivers and metrics for NFR managers?



Executives will need to focus on and address three key interconnected priorities, and will likely be judged or assessed by their ability to:



Meet or even surpass evolving supervisory expectations.

Regulators have traditionally focused on individual risks. As an example in Europe, many NFRs have been included in the Supervisory Review and Evaluation Process ("SREP") and stress testing exercises. As stated earlier, when expectations evolve to include an integrated assessment of NFRs, banks will be required to demonstrate and evidence a holistic approach.



Demonstrate a comprehensive understanding and enhanced control of the bank's NFR profile.

Evidence of that understanding to third parties (including regulators and internal stakeholders) will be based on available NFR metrics and indicators that incorporate qualitative and quantitative approaches.



Translate understanding of NFR and risk management capability improvements into reduced cost of compliance and economic capital.

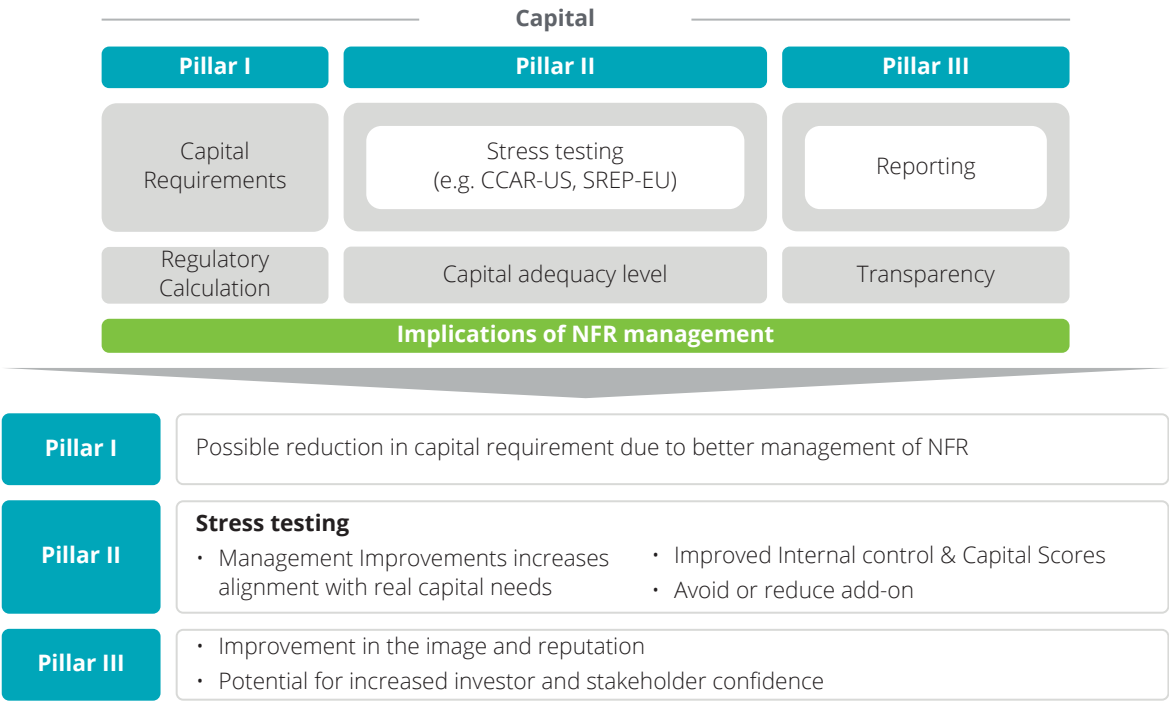
FIs should be able to translate the improved understanding of their NFR profile into a risk mitigation strategy to minimize potential losses, thus reducing Pillar II capital add-ons through ICAAP and SREP requirements.

Additionally, in Pillar III, FIs should be able to increase transparency with stakeholders, including a detailed description of their holistic NFR risk management.

"The real difficulty lies in the measurement of those risks. We would love to speak the same language as the rest of the risk managers of the organization"

NFR officer, large financial services company

Fig. 1 – Summary of potential economic capital implications derived from improved NFR management



There are other, perhaps less obvious but still important benefits derived from a holistic approach to NFRs. With the term “holistic” we envision an end-to-end and common approach to managing risk, starting with a link to the risk appetite framework, an inventory of risks and relevant controls, a consistent quantitative and qualitative assessment approach, and concluding with the ability to provide feedback and enhance the process.

A holistic approach to NFRs can be used to understand and optimize the NFR profile and rationalize the controls required to manage a specific portfolio of identified risks. FIs should then be able to map these risks to business activities and the associated revenue.

Some large FIs headquartered in Europe have already decided to give the responsibility of managing NFR to senior executives outside the traditional CRO governance model. These executives with specific NFR responsibilities will benefit the most from a clear understanding of expectations and how they can demonstrate their value.

The three priorities discussed above should serve as useful guidance to focus initiatives and obtain results.

It is difficult to manage what you can't explain

It is a widely accepted premise that you cannot manage what you cannot control, you cannot control what you cannot measure, and you cannot measure what you cannot define.

In early stages of implementation of an NFR framework, FIs can perceive NFRs as an evolving list of uncontrollable variables. A common industry understanding and nomenclature are yet to be agreed. NFRs are also sometimes referred to as non-portfolio or non-traditional risks.

As implied by these alternative names, NFRs can be difficult to isolate and can be better defined by exclusion. For the purposes of this paper, we understand NFRs as those risks that are not core or directly associated to the primary business and revenue generating activities reflected in the balance sheet, but can nevertheless have negative strategic, business, economic and/or reputational implications.

A detailed taxonomy with different levels of aggregation or hierarchies and clearly defined terms becomes a crucial early step. The Basel accord provides a definition of operational risk, including seven associated event types. As shown in Figure 2, our proposed taxonomy includes operational risk as one of the key NFRs, but also extends to other emerging and important risks that are now widely included in the NFR agenda.

NFR can in turn be divided into Risk Sub-Categories and Risk Types. An extract is shown below as an illustration. (Fig. 3) Deloitte's detailed proprietary taxonomy includes close to thirty Sub-Categories and more than one-hundred fully differentiated Risk Types and corresponding definitions that can be used as a starting point to create a customized bank-wide taxonomy. Our taxonomy is not designed to be static, it continues to evolve and represents the latest thinking, based on project and research results. For example, categorization of reputational risk continues to be a source debate, as some FIs consider it part of NFR.



Fig. 2 – Risk Taxonomy - Highest Level of Aggregation into Risk Classes, including NFR

Risk Class	Category
Financial Risk	Credit Risk
	Market Risk
	Interest rate Risk in the Banking Book
	Liquidity Risk
Non-Financial Risk	Operational Risk
	Compliance Risk
	Conduct Risk
	IT Risk
	Cyber Risk
	Model Risk
External Market Risk	Third-party Risk
	Strategic Risk
	Systemic Risk
	Reputational Risk

Source: Deloitte Banking Risk Intelligence Map@-extract; Draft as of July 2017, subject to change.

A robust NFR taxonomy allows for reduction in complexity, provides a bank-wide standardised language, allows responsibilities to be assigned across the

three lines of defence and is necessary in order to implement a monitoring and measurement methodology.

Fig. 3 – Deloitte's Non-Financial Risk Taxonomy (extract)

The complete taxonomy includes close to thirty Sub-Categories and more than one-hundred fully differentiated Risk Types and corresponding definitions

Risk Class			
Non-Financial Risk			
Category	Category	Category	Category
Operational Risk	Compliance Risk	Conduct Risk	IT Risk
Sub-Category	Sub-Category	Sub-Category	Sub-Category
<ul style="list-style-type: none"> Internal Fraud External Fraud Employment Practices and Workplace Safety Clients, Products & Business Practices Damage to Physical Assets Business Disruption & System Failures Execution, Delivery & Process Management 	<ul style="list-style-type: none"> Compliance Risk 	<ul style="list-style-type: none"> Inappropriate Product Risk Improper Business or Market Practices Risk After-Sales and Recovery inadequate management 	<ul style="list-style-type: none"> IT Risk
Risk type	Risk type	Risk type	Risk type
<ul style="list-style-type: none"> Unauthorized Activity Theft & Fraud Systems Security Risk Employee Relations Risk Safe Environment Risk Diversity & Discrimination Risk Suitability, Disclosure & Fiduciary Risk Product Flaws Risk Selection, Sponsorship & Exposure Risk Advisory Activities Risk Disasters & Other Events Business Disruption Systems Risk 	<ul style="list-style-type: none"> Consumer Protection BSA/AML/Sanctions/ Bribery&Corruption Conflicts of Interest Information Security/ Privacy Safety and Soundness & Prudential Regulation Tax Risk Market Integrity Accounting Legislation [...] 	<ul style="list-style-type: none"> Abusive Pricing Product and Marketing Risk Selling/Misselling sales Risk Breach of contract conditions Sales and client Information absence/deficiency Inadequate resolution of claims and complaints Disclosure of client confidential data Intolerance in collection and recovery procedures [...] 	<ul style="list-style-type: none"> Improper IT architecture design Inappropriate User profiling/ Access Weakness Inappropriate Software/ Hardware maintenance [...]
Category			
Cyber Risk			
Sub-Category			
<ul style="list-style-type: none"> Cyber Risk 			
Risk type			
<ul style="list-style-type: none"> Privacy and data protection Risk Cyber attacks Risk [...] 			
Category			
Model Risk			
Sub-Category			
<ul style="list-style-type: none"> Model Risk 			
Risk type			
<ul style="list-style-type: none"> Deficiencies in the data Estimation uncertainty Risk Inappropriate use of the model 			
Category			
Third Party Risk			
Sub-Category			
<ul style="list-style-type: none"> Third Party Risk 			
Risk type			
<ul style="list-style-type: none"> Concentration SLA compliance Contract breaches [...] 			

Measuring and Monitoring, from theory to benefits



Our proposed NFR Measuring and Monitoring Methodology combines quantitative and qualitative approaches to reach a score. The methodology provides alignment with the Board-approved risk framework and allows for consistent communication within and outside the organization.

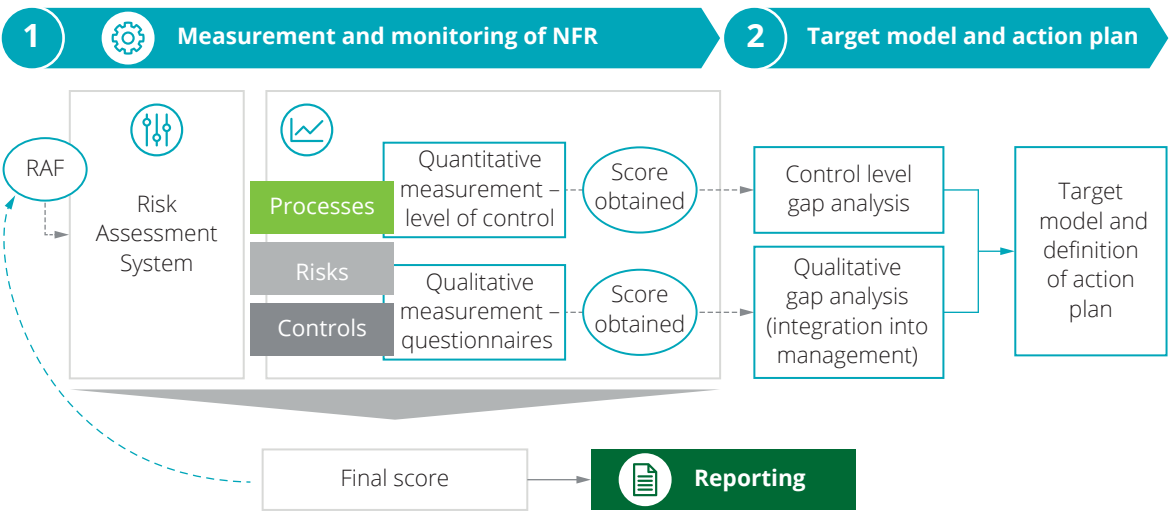
We recommend a risk assessment with the following components as a starting point:

Quantitative assessment: considers different Key Risk Indicators for each eligible Risk Category and Sub-Category. It aims to avoid subjectivity through a frequency and impact quantification

Qualitative assessment: combines results from the processes and control map quantification with management questionnaires

The results can be used as inputs for capital calculations, with potential substantial benefits. Deloitte has already developed an NFR capital model in connection with its Measuring and Monitoring Methodology, which is being implemented by several large FIs.

Fig. 4 – NFR Measuring and Monitoring Methodology* (extract)



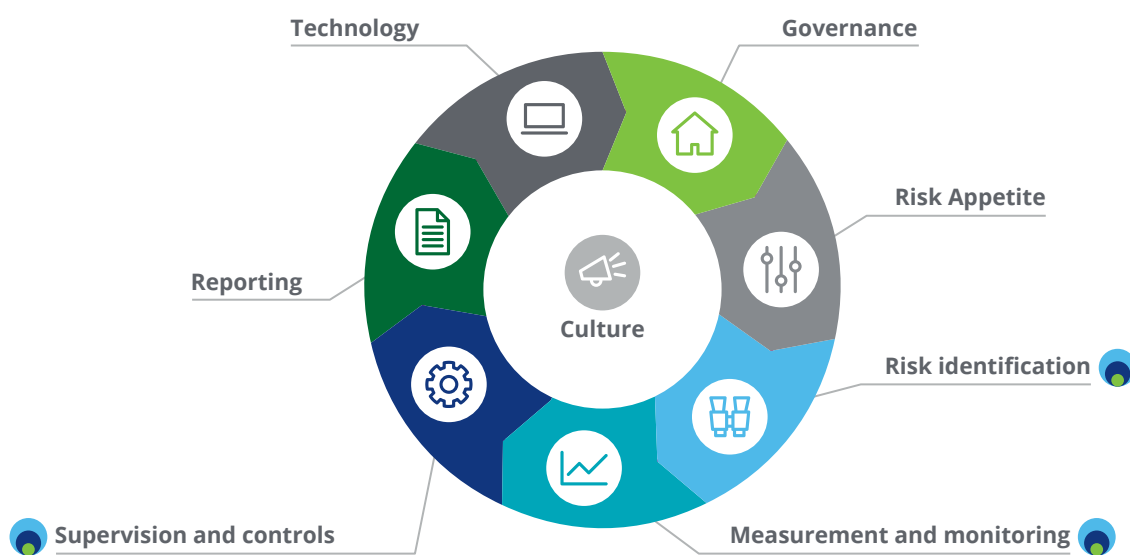
(*) The Three Lines of Defense have an integrated role in the framework

A framework is only helpful if it can be implemented


Methodologies and taxonomies are only useful once they have been implemented. Organizations will need to assess their current capabilities in order to create an implementation plan. In our view, moving from theory to reality can be achieved by considering the following work dimensions, all surrounding an improved culture of risk.







None of these implementation dimensions are new to FIs. NFR risk management will require adaptations or customized strategies for implementation. The table below includes a brief overall description, as well as early NFR-specific considerations to improve the likelihood of a successful implementation.



An integrated framework will lead to a higher understanding of how risks are identified, monitored and mitigated.



Supported and enhanced by Deloitte's Non-Financial Risk Management Framework

Dimension	General Concept	NFR Implementation Recommendations and Considerations
Culture 	<p>The habits and behaviours of the entire organization. Management is in charge of setting and maintaining the “tone at the top”</p>	<p>NFR references and terminology should be regularly and consistently included in communications from top management; consistent and repeated use will raise its profile as a legitimate area that deserves attention and focus</p>
Governance 	<p>Defines the applicable policies and establishes the role and responsibilities of the different lines of defence (e.g., committee structures, definition of functions and roles of 1st, 2nd and 3rd lines). A robust governance structure must facilitate the decision-making process by helping management to better understand the entity's NFR profile and strategy</p>	<p>Responsibilities to manage NFRs should be clear and explicit; implementing an NFR Framework makes it possible to revisit and re-assess the existing governance model. It is not about adding NFR to the model, but adapting the governance to include NFRs</p>
Risk Appetite 	<p>The amount and type of risk that an organization is willing to assume within its risk capacity in order to meet its strategic objectives and business plan</p>	<p>It can be beneficial to think about that portfolio of NFR as something that can be influenced and mitigated, and not as an unavoidable consequence of conducting business; the entity should identify its potential NFRs based on a bank-wide vision and structure based on an agreed taxonomy, and decide how much it is capable and willing to assume</p>

Dimension	General Concept	NFR Implementation Recommendations and Considerations
Risk Identification 	<p>Risk identification is the starting point of the risk process, enabling awareness of these risks to be raised in the organization</p>	<p>The experience with operational risk is that banks' data capabilities can inhibit timely identification and mitigation of new and emerging risk types; this could be an early challenge for NFR Managers when they want to demonstrate value early in their programs</p> <p></p> <p>Deloitte's Non-Financial Risk Management Framework provides a customizable taxonomy to serve as a starting point for identification</p>
Risk Measurement and Monitoring 	<p>Includes specific activities, models and processes to monitor risks and provide the information to assess if they exceed the defined appetite, both quantitatively and a qualitatively</p>	<p>A qualitative and quantitative methodology is necessary in order to measure and monitor NFRs; as an emerging discipline, NFR Managers may be obliged to create and implement a methodology relatively quickly</p> <p></p> <p>Deloitte's Non-Financial Risk Management Framework provides a customizable methodology to accelerate implementation</p>
Supervision and Controls 	<p>A model that identifies and reflects the controls associated to all relevant processes and under all lines of defence</p>	<p>The ability to leverage a rationalized inventory of controls across a wider spectrum of risks and processes is likely to result in cost and efficiency benefits that can support the business case and result in early buy-in</p> <p></p> <p>Deloitte's Non-Financial Risk Management Framework accelerates the identification of processes and controls, and helps identify gaps</p>

Dimension	General Concept	NFR Implementation Recommendations and Considerations
Technology 	<p>The necessary infrastructure to support measurement and management of risks, while ideally enhancing automation and transparency</p>	<p>For the emerging NFR risk management discipline, firms should also consider using innovative tools and techniques: robotic process automation and cognitive intelligence, cloud computing and other big data analytics approaches are changing underlying business operating models, but can also be used to monitor and control risks</p>
Reporting 	<p>Periodic information to risk management stakeholders across all lines of defence is necessary in order to communicate status of risks, controls and related responses</p>	<p>A common language to identify and measure NFRs based on an agreed taxonomy is only helpful if it can be supported by a common reporting framework, where risks are monitored and communicated consistently across all lines of defence</p>

Conclusions and suggestions to initiate change

We strongly believe in advancing the assessment and implementation of Non-Financial Risk Management and have therefore proposed a supporting framework, introduced only at a high level in this document.

Articulating expected internal and commercial benefits related to a Non-Financial Risk Management framework are helpful in order to initiate change. Avoiding losses and satisfying regulatory expectations are two major drivers, but highlighting the potential benefits in the form of reduced cost of compliance can be just as powerful.

History teaches us that banks that embrace regulatory change and articulate expected benefits early in the process will be most likely to succeed. It may be difficult to initiate change if there is a lack of understanding of the topic and its implications. Raising awareness and initiating change in an organization may require a self-assessment, which can be formal or informal. The initial evaluation can leverage Deloitte's proprietary framework.

FIs that start the transformation early will benefit the most. The executives in charge have a rare chance to influence how they will be judged.

Risk management is episodic, and tends to advance in bursts of activity. As it is natural for an emerging discipline, our NFR risk management framework, including a detailed taxonomy and measurement methodologies, will continue to evolve. We acknowledge that regulatory developments can be event-driven, which means that their direction cannot always be anticipated. The evolution of NFR risk management will need to be monitored; outcomes and learnings will be included in future iterations of our proposed framework and in updates to this publication.

Sample self-assessment questions to initiate change

- Does the entity have an NFR risk inventory?
- Is there an existing Risk Appetite Statement approved by the Board of Directors of the Entity for NFRs?
- Is the board and senior management aware of and involved in management of NFRs?
- Has the entity defined a three lines of defence model for managing NFRs?
- Has the entity differentiated the management structure for financial risk management and NFR?
- Has the entity established a methodology for the measurement and monitoring of NFRs?

Authors

Hans Jürgen Walter

Partner - Financial Services Industry Leader (Germany)
hawalter@deloitte.de

Ricardo Martinez

Managing Director - Risk Advisory (Germany)
ricarmartinez@deloitte.de

Matthias Rode

Partner - Financial Advisory (Germany)
mattrode@deloitte.de

Francisco Porta

Director - Risk Advisory (Spain)
fporta@deloitte.es

Eelco Schnezler

Director - Risk Advisory (Netherlands)
eschnezler@deloitte.nl

Luxembourg Contacts

Laurent Berliner

Partner - EMEA FSI Risk Advisory Leader
lberliner@deloitte.lu
+352 451 452 328

Martin Flaunet

Partner - Banking Audit Leader
mflaunet@deloitte.lu
+352 45145 2334

Vincent Gouverneur

Partner - EMEA Investment Management Leader
vgouverneur@deloitte.lu
+352 45145 2451

Pascal Martino

Partner - Banking and Human Capital Leader
pamartino@deloitte.lu
+352 45145 2119

Jean-Philippe Peters

Partner - Risk Advisory
jppeters@deloitte.lu
+352 45145 2276

Arnaud Duchesne

Director - Risk Advisory
aduchesne@deloitte.lu
+352 45145 4852

Bertrand Parfait

Partner - Risk Advisory
bparfait@deloitte.lu
+352 45145 2940

Thomas Gruenwald

Director - Audit & Assurance
tgruenwald@deloitte.lu
+352 45145 4869



Deloitte is a multidisciplinary service organization which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

This communication contains general information only, and none of 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. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. 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/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on **Facebook**, **LinkedIn**, or **Twitter**.