Deloitte.

BU CF Deloitte Banking Union Centre in Frankfurt

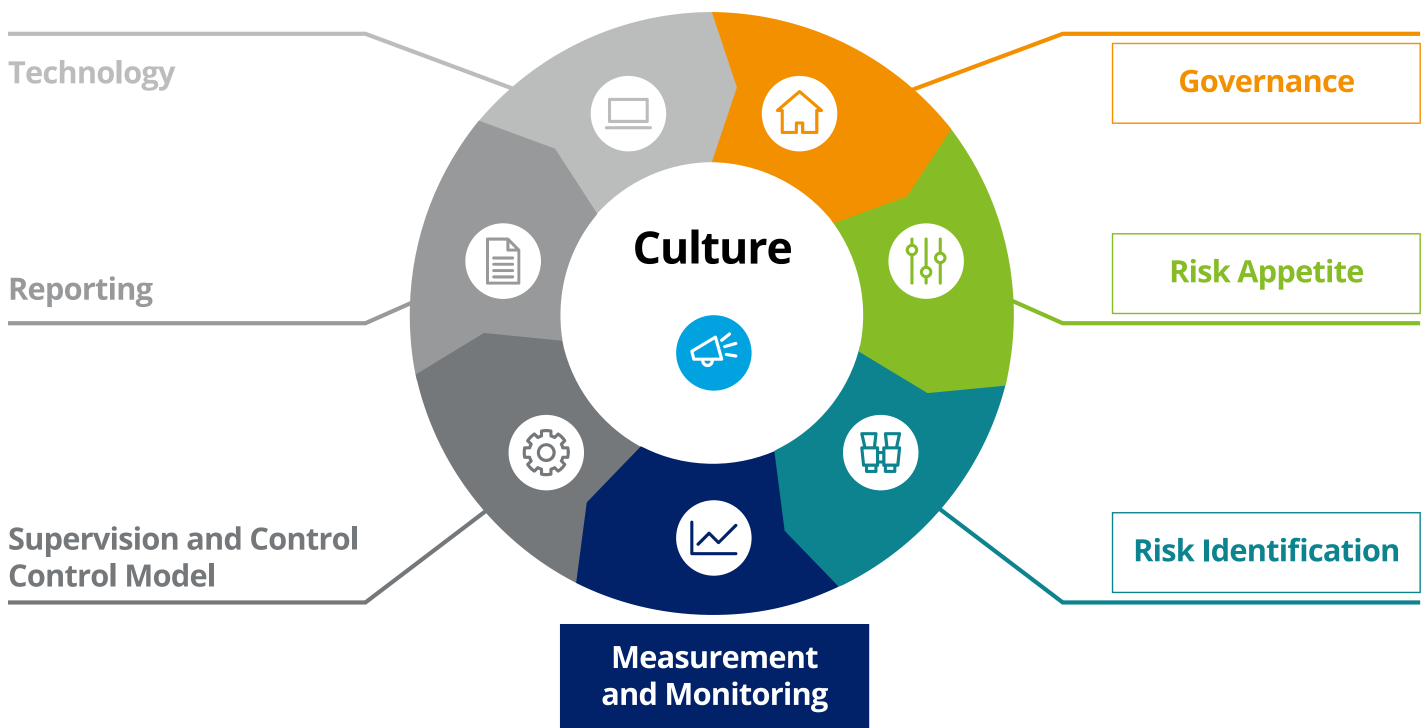
Non-Financial Risk Management Insights Series

Issue #5 – Measurement and monitoring

Measurement and monitoring contribute to an informed evaluation of non-financial risk (NFR). They can also help mitigate NFR and reduce the amount of operational risk capital that financial institutions must hold. In this issue, we examine what makes NFR uniquely challenging to measure and monitor, then explore an integrated model for overcoming these challenges and reducing the impact of NFR on an institution's risk profile.

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

Introduction

Risk measurement helps determine how much capital to allocate to each business line as a cushion against financial losses. Risk monitoring shows how business lines are managing the risks they have. Together, the two principles offer a fairer way to assess the risks each business assumes and strengthen the incentive for business lines to reduce their risk profiles.

But when it comes to non-financial risk, data is a common stumbling block. For one thing, much of the data around NFR may not be readily available. NFR-related data also tends to be heterogenous, making it harder to analyze. Partly due to these challenges, many banks may be tempted to conclude that non-financial losses are beyond their control, accepting them instead as a cost of doing business.

An integrated NFR measurement and monitoring capability can turn this mindset around. In the following sections, we review the regulatory impetus to track NFR and take a closer look at the drawbacks of traditional approaches. After that, we discuss an alternative approach that integrates measurement and monitoring so that lines of business can continually evaluate NFR, positioning them to mitigate risks before they turn into major losses. This in turn can reduce the amount of capital the business must hold, boosting the balance sheet as a result.

Regulatory expectations

Lack of NFR measurement and monitoring has led NFRs to be "insufficiently covered or even completely left out" of an organization's risk appetite framework (RAF), then-ECB supervisory board chairperson Danièle Nouy noted in 2018. "And this leads to a long list topped by risks such as compliance and reputational risks, IT risks, legal risks, and conduct risks."[1]

As part of the new Basel III framework, banks must use the Standardized Measurement Approach (SMA) to determine how much capital to set aside for operational risk. The SMA is based on a formula intended to restore credibility in the calculation of risk weighted assets and to improve the comparability of banks' capital ratios. The only part of the formula that a financial institution can manage in terms of risk is the internal loss multiplier (ILM), which shows the entity's performance relative to operational risk management.

The upshot is that financial institutions have to reduce their ILM if they want to reduce the amount of operational risk capital they are required to hold. This means financial institutions need to improve their processes for collecting, managing, and analyzing internal loss data. Basel has weighed in with criteria for data quality and raised the stakes by specifying that failure to meet the minimum loss data standards could be subject to heavy penalties.[2]

Challenges

The SMA replaces an older, model-based standard called the Advanced Measurement Approach (AMA). The AMA uses advanced modeling given a number of variables that determined the level of operational risk capital. This gives financial institutions considerable flexibility in the way they use and weight their operational risk measures.

However, the AMA relies on loss data and scenario analysis at the expense of business environment and internal control factors such as guiding principles and corporate culture. In other words, although the AMA is more sensitive to risk, the risk is also less transparent because the leeway financial institutions have to create their own models under the AMA makes it hard to compare risk from one firm to another.

Today's formula-based SMA addresses the comparability issue but introduces another one: It looks backward rather than forward, reflecting losses from as long as 10 years ago while ignoring threats that may lurk on the horizon.[3] The EU's General Data Protection Regulation is a case in point. Relatively few organizations have a history of incurring fines under this 2018 regulation, but that does not mean financial institutions have little exposure to such fines going forward.

Capital allocation methods aside, financial firms may run into difficulties with gathering historical loss data, determining qualitative risk drivers with NFR management, and staying abreast of where NFR begins and ends. There is also the tendency to focus on financial risk because it is better understood, leaving NFR off the radar of management-level accountability.

Our approach

A systematic NFR measurement and monitoring capability can address these challenges by evaluating risks and integrating them into capital calculation.

A capability like this involves looking across the different categories of NFR (see sidebar) and assessing each one by sub-category. For example, IT risk as a category can be assessed by sub-categories like architecture design, user identity management, and software and hardware maintenance. The idea is to find out where issues with the process can give rise to risk.

[1] Danièle Nouy, "Risk appetite frameworks: good progress but still room for improvement," presented at the International Conference on Banks' Risk Appetite Frameworks, Ljubljana, Slovenia, 10 April 2018, https://www.bankingsupervision.europa.eu/press/speeches/date/2018/html/ssm.sp180410.en.html.

[2] Deloitte, The future of operational risk in financial services: A new approach to operational risk capital management, p. 5, 2018, https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/financial-services/CY_FS_The-future-of-operational-risk-in-financial-services_Noexp.pdf.

[3] Banks are expected to base their ORC calculations on 10 years of good-quality loss data. In the transition period leading up to January 1, 2022, however, banks that do not have 10 years of data can use a minimum of five years of good-quality data.

Categories of NFR

Deloitte's proprietary Risk Taxonomy has three levels of risk hierarchy including major risk categories, risk subcategories, and then risk types. Of the major risk categories, two-thirds are non-financial risk types (Figure 2). Deloitte member firms use this taxonomy in their client engagements, as a starting point to create a customized taxonomy for each individual institution.

This taxonomy is not static, but instead continues to evolve based on new insights and information gathered from projects, risk events, and research. For example, how best to categorize reputational risk remains a source of debate, with some financial institutions considering it part of NFR. Undoubtedly new risks will emerge or become more prominent in the years ahead.

Risk Taxonomy—Highest Level of Aggregation into Risk Classes, including NFR

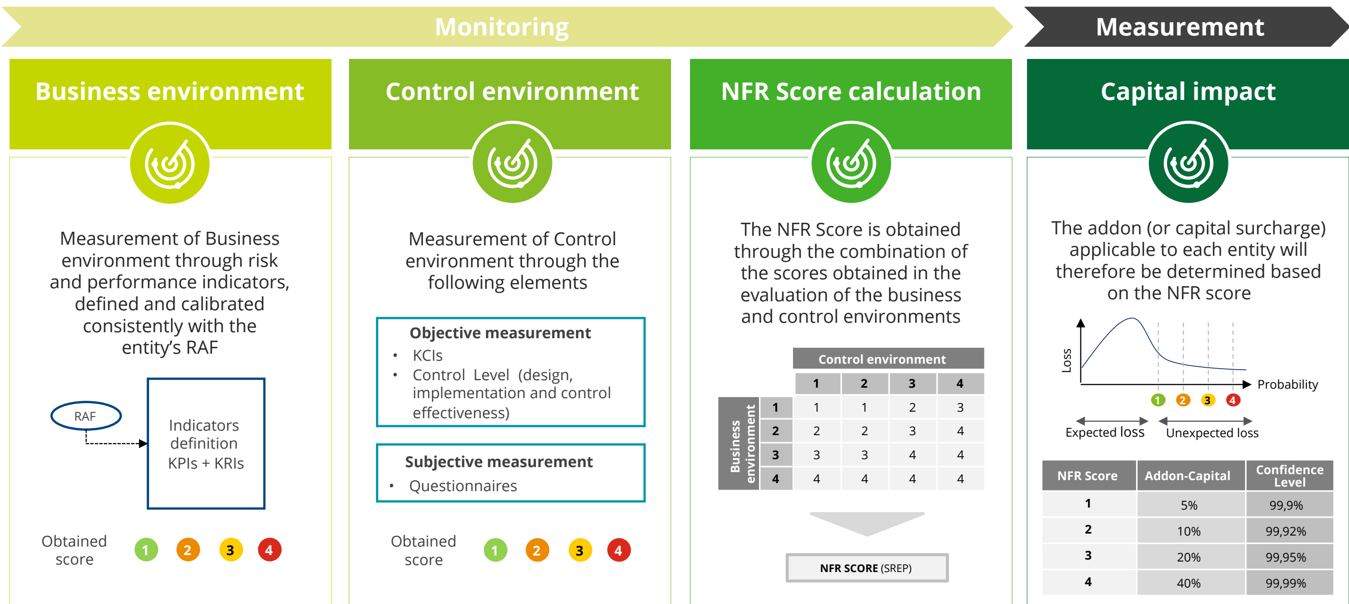
Risk Class	Category	Sub - category**	Type**
Financial Risk	Credit Risk	~ 10	~ 50
	Market Risk		
	Interest Rate Risk on Banking Book		
	Liquidity Risk		
Non - Financial Risk	Operational Risk*	~ 20	~ 70
	Compliance Risk		
	IT Risk		
	Cybersecurity Risk		
	Conduct Risk		
	Legal Risk		
	Model Risk		
	Third–Party Risk		
	Strategic Risk		
	Reputational Risk		

Source: Deloitte Banking Risk Intelligence Map – Extract
Draft as of June 2020, subject to change

* Operational Risk Event Types under Basel II include risk components that some banks may decide to address separately as an independent Risk Category

** Numbers represent an approximate number of Sub-categories and Risk Types currently represented in the taxonomy

Deloitte NFR measurement and monitoring approach



NFR may be assessed against numeric (quantitative) or descriptive (qualitative) measures. A quantitative assessment aims to take subjectivity out of the equation by revealing the organization's risk profile against a set of key risk indicators. For instance, a key indicator of IT risk might be the number of user identities belonging to inactive users. Meanwhile, a qualitative assessment aims to capture management observations, like seeing users share the same set of login credentials.

Deloitte's approach makes use of both kinds of measures. At a high level, the process unfolds this way:

1. Monitor key performance indicators (KPIs) and key risk indicators (KRIs) for risk in the business environment. Each indicator is calibrated against the business line's non-financial risk appetite framework to arrive at an objective measure of inherent risk.
2. Monitor risk in the control environment via objective and subjective measures. Objective measures include key control indicators (KCIs) and control levels (e.g., do controls exist for each risk? How effective are they?). Subjective measures focus mainly on governance issues (e.g., are policies and procedures up to date? Do certain committees exist?).
3. Adjust each inherent risk measure from the business environment to reflect the extent the control environment mitigates it. The result is the business line's residual risk, expressed as an NFR score.
4. Use the NFR score to measure the capital add-on, or surcharge, for each business line.

Because our approach generally relies on AMA models, it can support a range of capital management exercises. The NFR score can lead to an adjustment in the risk model by:

- Increasing the confidence level
- Incorporating more severe loss scenarios
- Stressing the loss data parameters
- Stressing the calculated capital

The final adjusted score can inform decisions about capital allocation while allowing for consistent communication within and outside the organization.

With this kind of integrated approach, financial institutions can get a more granular, comprehensive view of NFRs within different business lines. They can also customize economic capital according to each business line's real risk exposure and control environment, then determine appropriate incentives via a bonus-malus system. The result is an incentive-based measurement and management system that can close gaps in data availability, allocate capital more effectively, and highlight specific actions management can take to tighten preventive controls in ways that lead to reduced capital requirements.

Conclusion

Non-financial risk is heterogeneous and complex. A robust measurement and monitoring system can help financial institutions understand the NFR in their organization while staying on top of them in a consistent manner. By integrating measurement and monitoring in a single approach, firms can create appropriate incentives, develop effective strategies for mitigating risk and reducing losses, and carry out risk-sensitive capital allocations that can grow smaller over time.

Contacts

Dr. Thomas Moosbrucker
Partner | Risk Advisory
Deloitte DCE
tmoosbrucker@deloitte.de

Francisco Porta
Partner | BUCF non-financial risks lead
Deloitte Advisory, S.L.
fporta@deloitte.es

Dr. Suren Pakhchanyan
Manager | Risk Advisory
Deloitte DCE
spakhchanyan@deloitte.de

Victor Claudio Osuna
Manager | Risk Advisory
Deloitte Advisory, S.L.
vclaudioosuna@deloitte.es

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.
This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") 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 representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.
© 2020. For information, contact Deloitte Touche Tohmatsu Limited.

Issued 6/2020