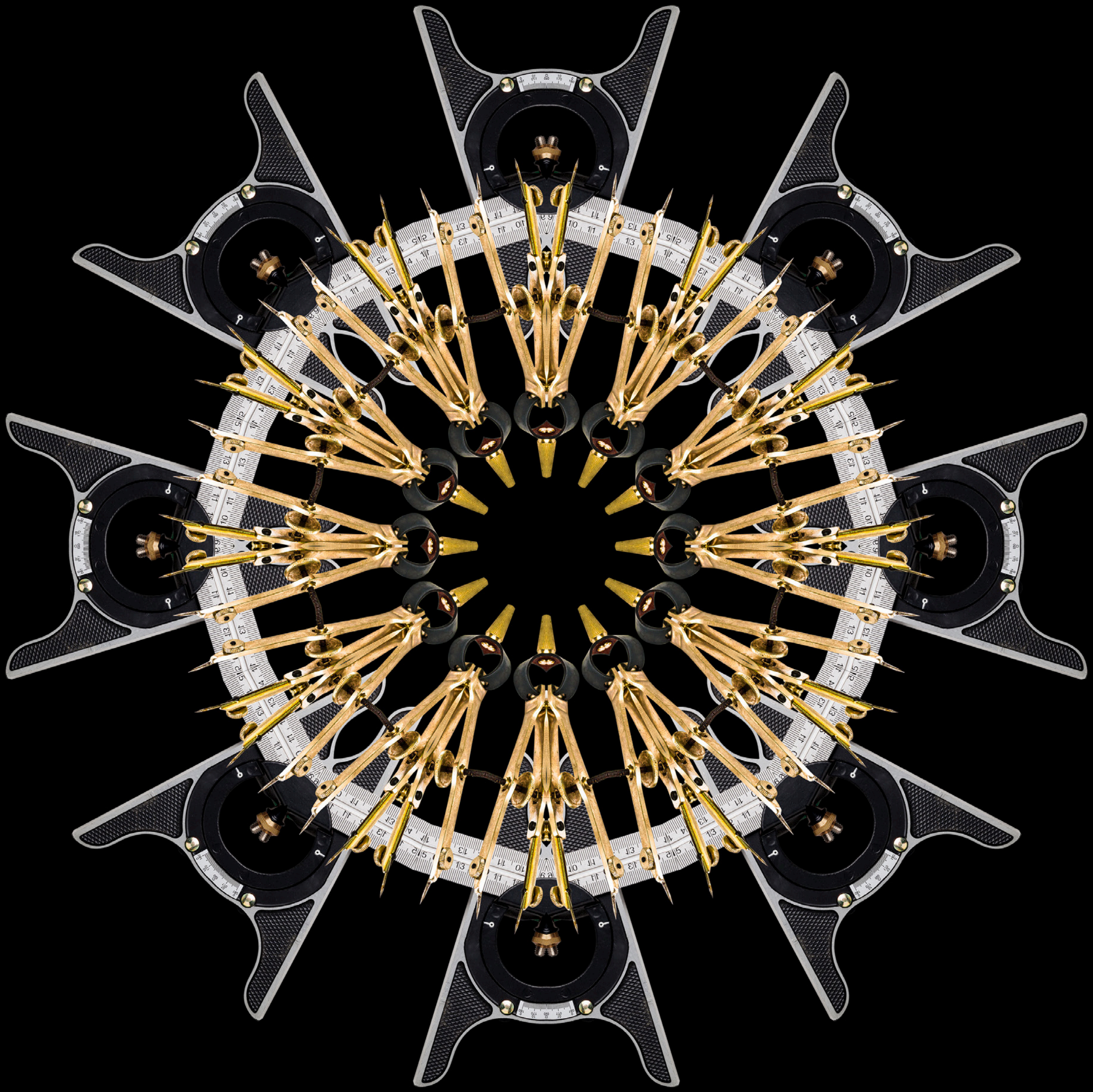
Deloitte.

BU CF Deloitte Banking Union Centre in Frankfurt

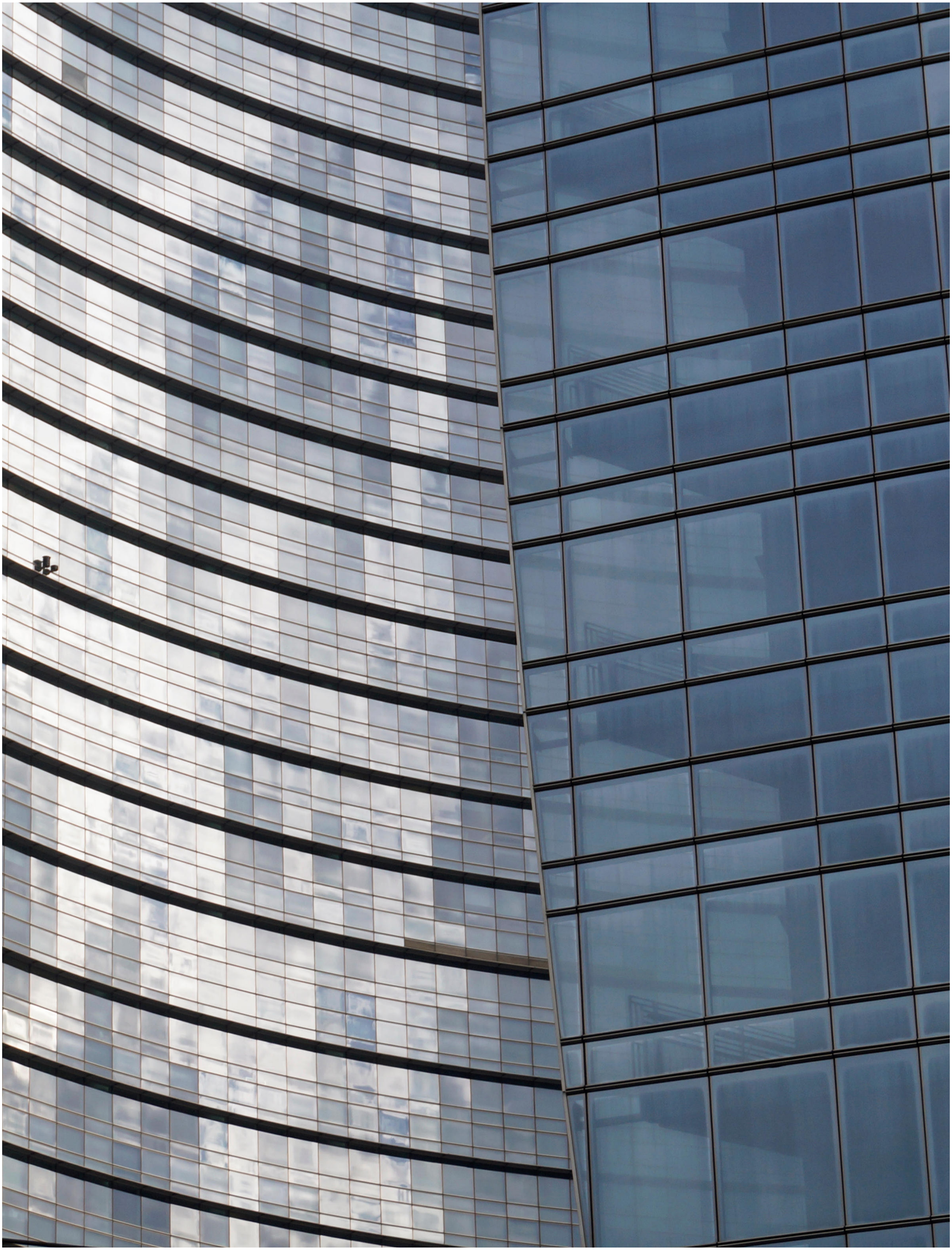


The future of Non-Financial Risk in financial services:

Building an effective Non-Financial Risk management program

The future of risk series

Risk Advisory



Executive summary

In the years since the global financial crisis, financial institutions have made substantial investments to upgrade their risk management programs and comply with ever more stringent regulatory requirements. While most institutions now have well-developed risk management frameworks to manage market, credit, and liquidity risk, there is a growing recognition of the need to enhance management of Non-Financial Risk (NFR). Many of the largest risk events in recent years have stemmed from NFRs such as conduct and cyber risk, rather than from traditional financial risks.

The growing importance of NFR management comes at a time of particular uncertainty and volatility in the business environment due to uneven economic growth, increased political and regulatory uncertainty, and varied revenue opportunities and returns on equity for many firms. Given these turbulent developments, institutions need to rethink their approach to risk management in general in order to reduce expenses, while simultaneously improving effectiveness.[1]

Institutions will need to move from the current piecemeal efforts to instead adopt a holistic approach to NFR. The foundation of an effective program to manage NFR, and a step that presents a challenge for many institutions, is to implement a comprehensive process to identify all the NFRs facing the organization. In this effort and as a first step, institutions should employ a comprehensive Risk Taxonomy and a comprehensive Risk Identification process.

As financial institutions develop their overall approach to managing NFR, they should consider carefully the following four key levers to achieve success in today's risk management environment.

- **Strategy.** Institutions require a clear process and explicit ownership to incorporate all material NFRs into their business strategies and risk appetite, while having in place appropriate metrics and risk limits.
- **Three lines of defense.** The three lines of defense risk governance model should be reassessed to clarify the responsibilities of each line of defense in managing NFR.
- **People and culture.** Many institutions will discover they need to hire or develop additional skills among their employees to address NFRs, such as in cyber risk, and also to build a culture, led by senior management, where employees throughout the organization recognize the importance of managing NFR.
- **Emerging technologies.** New technologies—such as big data, natural language processing, robotic process automation, and predictive analytics—should be leveraged to automatically scan a wider set of data sources to provide early warning signals of potential risk events while at the same time reducing compliance costs through automation.

Institutions that take these and the other steps discussed below will be better positioned to manage NFR and meet increasing regulatory expectations in today's fast-changing risk management environment.

The challenge of managing Non-Financial Risk

NFR is a broad term that is usually defined by exclusion, that is, any risks other than the traditional financial risks of market, credit, and liquidity. NFRs are generally not considered core or directly associated to the primary business and revenue-generating activities reflected in the P&L statement and the balance sheet. They can nevertheless have substantial negative strategic, business, economic, and/or reputational implications.[2] NFR includes operational risks as defined in the seven Basel operational risk event types, but also other important risks such as cyber, conduct, model, compliance, strategic, and third-party risk.

A 2018 survey of consumers found that financial services is the least trusted sector globally and has had this dubious distinction for the last five years.[3] A negative perception of the industry as a whole represents unstable ground for individual firms' efforts to manage reputational risks; NFRs can damage an institution's reputation and brand in addition to having financial impact.

NFR is not a new topic. The Bank for International Settlements (BIS) identified the management of NFR as a relative weakness of financial institutions already in 2009,[4] but only limited progress has been made since then. The greatest attention has been paid in recent years to operational risk. Illustrating the magnitude of operational risk, the ORX financial services operational risk loss database has now grown to include over €400 billion in operational risk losses at its contributing institutions.[5] Regulatory enforcement fines, penalties, and litigation now comprise the bulk of the operational risk losses at most major banks.

The Basel Committee on Banking Supervision (BCBS) as part of its reforms recently finalized the Basel III framework, which will fundamentally alter how operational risk capital (ORC) is calculated at many institutions. In the past, many internationally-active banks used a model-based approach for calculating ORC that included a number of variables. Under the new standard, the model-based advanced measurement approach (AMA) is being replaced by the Standardized Measurement Approach (SMA). The SMA is based on three variables, the Business Indicator Component (BIC), which is in turn based on selected financial data intended to be representative of the bank's business volume in different aspects, and the Internal Loss Multiplier (ILM), which is in turn based on the bank's actual operational risk loss history.[6]

The implications will be far reaching. Banks will need to ensure that they have comprehensive and accurate internal loss data to support and substantiate their calculated ILM. The change is likely to alter the attitude that banks take to operational risk in particular and NFR in general. Now banks will have a stronger incentive to take proactive steps to minimize operational risk losses in order to lower their ILM and resulting regulatory capital requirement.

While banks have made progress in managing some operational risks, typically they have lagged in developing the policies, processes, and controls required to identify and manage other NFRs. A number of developments have raised other types of NFR to greater prominence and the increasing importance of managing NFRs is not limited to banks, but includes insurers, asset managers, and other financial services firms that typically draw selected risk management practices from their banking counterparts

Conduct risk. In recent years, well publicized instances have occurred of inappropriate behavior by employees at major financial institutions, both in retail and wholesale markets. The top 20 global banks are estimated to have lost $348 billion from 2012 – 2016 through conduct related costs.[7] According to one estimate, the Common Equity Tier 1 ratios of EU G-SIBs would be around 2 percent higher without the fines that have been levied for problems stemming from conduct risk.[8] Regulators in many jurisdictions have focused on the importance of conduct and culture, looking at such issues as misaligned compensation incentives and lack of accountability. Locations in which regulators have addressed conduct risk include the European Union, Hong Kong, Australia, the United Kingdom, and the United States. For example, in August 2017, the head of the European Central Bank's (ECB) supervisory board said that it "has identified conduct risk—which includes compliance with anti-money laundering (AML) laws—as one of the key risks for the euro area banking system."[9]

Cyber risk. The losses from cyber-attacks were an estimated $445 billion across all industries in 2016, up 30 percent from three years before, and banks and other financial institutions are prime targets of hackers.[10] The number of cyberattacks against financial institutions is estimated to be four times greater than against companies in other industries.[11] In November 2017, SWIFT warned banks around the world that cyber risk was on the rise, saying that hackers had advanced their capabilities since a hacker stole $81 million from Bangladesh Bank in February 2016.[12] Regulatory initiatives focused on cyber risk can be found in the United States, the United Kingdom, Hong Kong, mainland China, Japan, Singapore, and Australia. The US Treasury Department has named cyberattacks as one of the top risks facing the US financial sector.[13]

Third-party risk. The increasing use of outsourcing by financial institutions in an effort to reduce costs has increased third-party risks such as contractual nonperformance, the potential that vendors will violate laws or engage in unethical behavior, data breaches, loss of intellectual property, and an inability to maintain operations in the instance of a natural disaster or infrastructure breakdown, among others. Regulators have made clear that financial institutions are responsible for managing the risks posed by their third parties; while European regulators have made this a thematic priority for on-site inspections.

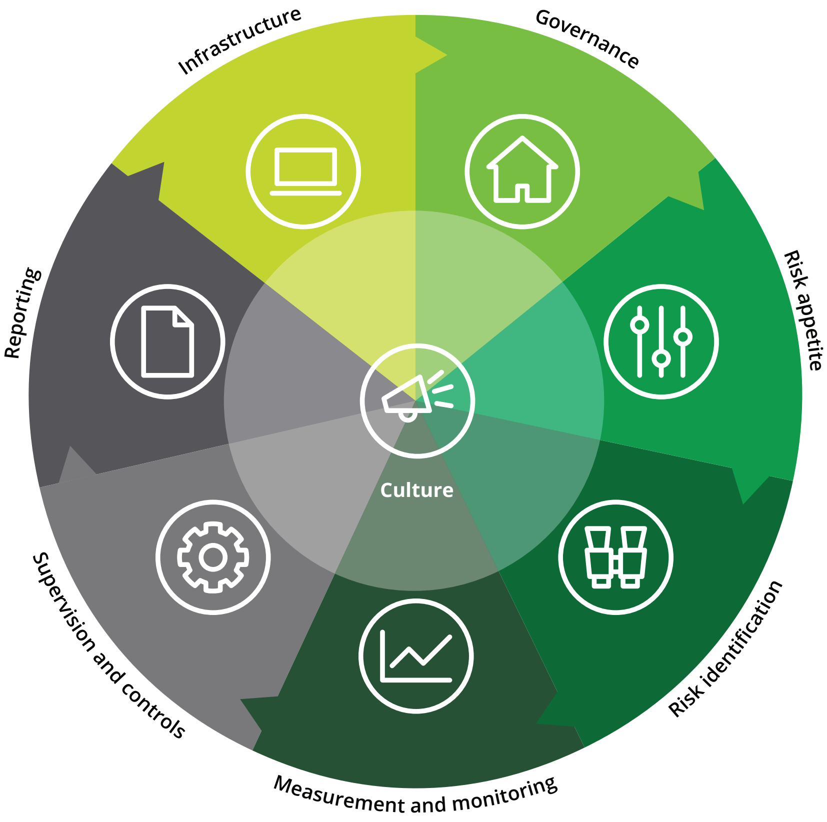
Model risk. Model risk has grown as financial institutions have come to rely more heavily on models in such areas as risk and capital management, product pricing, AML, and financial reporting. These risks can arise from a variety of sources such as inaccurate data, incorrect assumptions, inappropriate methodology, or errors in implementing processes based on models. Managing model risk has received significant attention by regulators and financial institutions over the last several years. In the United States, the Federal Reserve SR 11-7 guidance and OCC 2000-16 guidance specifically addressed model risk management. In other jurisdictions, regulatory expectations are less well-defined but are nevertheless increasing as well.

Need for holistic Risk Identification

In addition to initiatives that focus on specific types of NFR, supervisors are also stressing the importance of effectively managing NFR as part of the risk management control framework of individual institutions and the functioning of the financial system as a whole. They are encouraging institutions to adopt an integrated NFR management framework rather than the ad-hoc and often reactionary assessments of specific risks in place at many organizations. An integrated approach to NFR would link to the institution's risk appetite framework, employ a comprehensive inventory of risks and relevant controls, use a consistent assessment approach, and offer the ability to provide feedback and enhance the process on an ongoing basis.

Figure 1

NFR Management Framework[16]



Financial institutions will need to meet, or even exceed, these evolving supervisory expectations. An NFR Management Framework provides a comprehensive approach to managing NFR including alignment with the organization's risk appetite statement, the role of each line of defense, measurement and monitoring while considering any interconnections and correlations among NFRs, controls, reporting, and relevant technology tools (Figure 1). The end result is a risk mitigation program that effectively integrates all efforts and capabilities designed to minimize potential losses from NFR.

A critical first step is to have an effective risk identification process that captures all relevant NFRs, which is a regulatory expectation. In Europe, risk identification is a key component of the Internal Capital Adequacy Assessment Process (ICAAP) and the Internal Liquidity Adequacy Assessment Process (ILAAP). The Supervisory Board of the ECB has published specific expectations that institutions implement a process to comprehensively identify all material risks at least annually, define an internal risk taxonomy and maintain a complete risk inventory that incorporates an inherent risk assessment.[14] In the United States, risk identification is a key component of the Comprehensive Capital Analysis and Review (CCAR) stress-testing programs, and the Federal Reserve has published similar expectations.[15]

Identifying NFRs is a significant challenge in large part because financial institutions lack an agreed definition and taxonomy of these risks. Since NFR is often defined by exclusion as being risks other than market, credit, or liquidity risk, institutions may find it difficult to identify all their NFRs and establish a robust risk control framework for each of them.

Institutions need to begin with a comprehensive NFR Taxonomy, which they can then customize as needed. 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 of them 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 to be part of NFR. Undoubtedly new risks will emerge or become more prominent in the years ahead.

A risk taxonomy helps prevent some NFRs from being overlooked, provides a standardized language for all three lines of defense to employ across the institution, and establishes a foundation on which an institution can build an integrated approach to managing all the NFRs it faces, including their correlations and interactions. For this reason, all three lines of defense along with senior management should be actively involved in developing the Risk Taxonomy to provide an effective review and to raise awareness of NFR across the organization. Once developed, the Risk Taxonomy needs to be built into the institution's risk appetite framework. A primary owner for each risk type should be specified who is responsible for identifying and managing risk events within the risk type.

Many institutions will have to address a lack of accurate and comprehensive data that can make it difficult to identify and manage NFRs. Institutions need to record events across the organization for all the risk types in the Taxonomy. This event database will yield a comprehensive view of the organization's experience with all types of NFRs, including hard-to-quantify risks. The risk identification process should be linked to an organization-wide risk assessment, employing both quantitative (e.g., P&L impact) and forward-looking qualitative factors, and also an assessment of the effectiveness of related controls.

Figure 2

Risk taxonomy–Highest level of aggregation into risk classes, including NFR

Risk class	Category	Subcategory**	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 July 2018, 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

Four key levers to enhance management of NFR

Effectively managing NFR in the current unpredictable environment will require institutions to develop new capabilities and rethink traditional approaches. Specifically, Deloitte has identified four key levers that can be used to drive change and respond to the evolving risk management environment:[17]

- Infuse NFR management into strategy;
- Rethink the three lines of defense;
- Focus on people and culture; and
- Leverage emerging technologies.

These levers do not stand alone but instead interact. For example, the business strategy an institution adopts will have important implications for the NFRs it faces and the risk management skills required by its business units.

Institutions should consider how they can take advantage of each of these four key levers to enhance their identification and management of NFRs.

Infuse risk management into strategy

Effectively managing NFR will require the risk management function to work in close collaboration with the businesses and senior management to make sure that the NFR risk profile is considered when setting the institution's business objectives and developing its strategic plan. Many strategic risks fall into the category of NFRs, which are inherently difficult to assess. For this reason, these key elements of strategy often do not receive sufficient attention and analysis. As the organization sets its strategic plan, it is important to assess the impact of new products and markets on the institution's risk profile, including the NFRs it faces.

As each business evolves and adopts new strategic objectives, the institution's NFR Risk Taxonomy and resulting risk profile will need to continually be upgraded in tandem. As part of this process, institutions will require a formalized process to continually assess the strategic risks to the business model stemming from new technology and other changes in the external environment.

Rethink the three lines of defense

An NFR Management Framework will require an institution to re-examine the design of its three lines of defense risk governance models, clearly defining the responsibilities of each line of defense and streamlining the structure by eliminating overlapping areas of responsibility. Rather than simply adding individual risk types to the existing structure, an institution should use its NFR Management Framework to re-assess the existing governance model and adapt it as necessary to address this broader set of risks. One of the decision points in implementing its risk governance model is deciding whether an institution should have one individual responsible for oversight of a risk type across the organization, have the responsibility decentralized, or use a combination of these approaches.

A robust NFR taxonomy provides a standardized language for risk across the institution and helps clarify the responsibilities to be assigned across the three lines of defense. It also reduces complexity by bringing order to the many different types of NFRs.

It is important that Risk Identification is conducted in collaboration between the risk management function and individual businesses, which are closest to the institution's products and clients, to make sure that all relevant scenarios are considered. Getting buy-in from business units can be difficult since they are measured and rewarded on revenue generated, rather than specifically on risk management activities. Adding a new set of NFRs to their responsibilities will raise the bar even higher.

Although there are many challenges to assessing the likelihood and impact of NFRs on business issues and incidents, the lack of a sufficiently detailed understanding of the relevant business processes among the risk professionals in the first line of defense poses a significant obstacle at some institutions. Filling this skills gap will require institutions to invest in hiring new talent and upgrading the skills of existing employees. (See *Focus on people and culture* below.)

Focus on people and culture

The rapidly evolving risk management environment requires institutions to ensure they have a sufficient number of specialists with subject matter expertise in high-risk activities, and this will be especially important in the area of NFR. Management of NFR requires different skills than those needed to manage traditional financial risks. Further, NFR requires a far more diverse set of skills since this category includes risks of very different types ranging from conduct and third-party risks to cyber and compliance risks. Based on the results of their Risk Identification process, institutions will need to identify and prioritize the different types of skills and experiences they will need to effectively manage the risks identified. Many institutions may find that they lack sufficient skills and will need to either hire new employees or upgrade the skills of their current workforce with respect to NFR.

Each institution will also have to consider its culture—the habits and behaviors of its organization—and the tone set at the top by senior management to make sure that the importance of NFR and the responsibility of employees throughout the organization to identify and manage NFRs is clearly understood. The importance of NFR should be regularly and consistently communicated by top management, and all relevant employees should be familiar with NFR terminology and risk management processes.

To be taken seriously, however, NFR management needs to have real world consequences. For a start, capabilities for managing NFR could be considered when establishing the operating budgets and available investments for a business unit. Beyond these business-wide impacts, managing NFR should be included among the job responsibilities of relevant employees as well as considered in performance objectives and compensation decisions.

Leverage emerging technologies

The latest technologies are transforming risk management including the management of NFR. Traditionally, banks and other financial institutions have relied on human judgment to examine historical data on losses and attempt to identify correlations and patterns. Today, new technology tools are being applied to many of these manual processes and can complement advances and changes in the use of traditional Governance, Risk and Compliance (GRC) systems that aim to link processes, risks, and controls around NFR.

Recent developments in big data, predictive analytics, artificial intelligence, and machine learning are not only driving down costs by automating manual tasks, even more importantly they are providing institutions with the ability to identify and address potential threats, often before they have been recognized by the organization's risk practitioners.

Using natural language processing and optical character recognition, these tools can analyze a much broader range of data such as unstructured data from customer complaints and social media posts. Patterns and correlations can be identified that would have gone unrecognized if relying solely on review by human professionals, as well as flag the potential existence of tail events that were previously difficult to identify. Automatically scanning relevant data sources can provide early warning signals for potential risk events that may exceed the institution's risk appetite, provide decision support, prioritize areas for testing and monitoring, and deploy automated monitoring of limits. Several leading institutions are employing big data coupled with advanced analytics in a variety of areas including anti-money laundering, fraud prevention, third-party risk management, and regulatory reporting.

As an example for conduct risk, a bank would assess its current conduct risk environment and culture, identify relevant structured and unstructured data sources and apply risk analytics to identify trends and correlations that predict potential conduct risk exposures and events.[18] For example, sensing analytics could be deployed to analyze behavior patterns among front-office personnel by monitoring a range of data sources such as email, chat, phone call, voicemail, customer complaints, compliance issues, and employee training, among others. RPA "bots" can be programmed to continuously scan and gather data from specified data sources; when coupled with cognitive technology, optical character recognition, and natural language processing technologies, the result can be streamlined monitoring of key risk indicators in real time—at lower cost and with much higher accuracy than has traditionally been possible by collecting ex-post loss information.

The final step is for the risk professionals to use these analyses to better understand the root causes of conduct risk in the institution such as weak controls, a lack of accountability, or disparate subcultures. Employing predictive risk tools in this situation would provide better understanding of the behavioral patterns in the organization, an increased ability to evaluate how the business model and growth objectives affect the organization's desired cultural values, and improved techniques for managing the organization's human resources and providing incentives.

While the benefits are substantial, to reap them institutions will need to address and overcome several challenges. First, these tools require access to reliable and comprehensive risk and performance data, which will be a challenge for many institutions. Many institutions will need to expand the types of data they source to include additional sources (if allowed in their relevant jurisdictions), such as internal voice mail and chat and external sources such as social media. Second, these technology applications will put a premium on having a robust data governance and integrity process. Finally, the use of predictive analytics will be subject to the potential for modeling errors, so that assessing and managing model risk will be important in this area.

Conclusion

Risk management is today at an inflection point, requiring that financial institutions take their programs to an entirely new level if they are to remain effective in today's more unpredictable economic environment. Financial institutions will need to keep these broader risk management trends firmly in mind to ensure they design and implement a program to manage NFRs that can meet the continually escalating requirements of today's risk management environment.

NFR comprises a diverse and complex set of risks with the potential to inflict substantial financial and reputational damage on financial institutions. Supervisory authorities around the world are increasingly focused on the importance of effective management of specific categories of NFR, such as conduct risk and cyber risk, as well as on NFR Management as a whole.

To meet these increasing supervisory expectations, financial institutions need to implement an integrated framework for managing NFR. A key first step is to adopt a taxonomy of all the types of NFR and then identify the specific NFRs facing the organization.

Financial institutions are undertaking these initiatives to enhance NFR management at a time of exceptional volatility and uncertainty in the business and risk management environment. They need to align their NFR Management Framework, including their Risk Identification process with the fundamental trends that are today transforming risk management as a whole.

Contacts

Edward Hida
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
ehida@deloitte.com

Francisco Porta
Partner | Risk Advisory
Deloitte Advisory, S.L.
fporta@deloitte.es

Michael Pieper
Director | Risk Advisory
Deloitte GmbH Wirtschaftsprüfungsgesellschaft
mipieper@deloitte.de

Ricardo Martinez
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
rimartinez@deloitte.com

Dr. Gerhard Schroeck
Partner | Risk Advisory
Deloitte GmbH Wirtschaftsprüfungsgesellschaft
gschroeck@deloitte.de

Endnotes

[1] For a discussion of the new environment for risk management, please see Deloitte's report, *The future of risk in financial services*, https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-future-risk-in-financial-services.html

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

[3] For additional details on the survey, refer the *2018 Edelman Trust Barometer: Global Report*, https://http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

[4] Issues in the Governance of Central Banks, p. 151, http://www.bis.org/publ/othp04.pdf

[5] ORX Annual Banking Loss Report - Operational risk loss data for banks submitted between 2012 and 2017, June 2018, https://managingrisktogether.orx.org/orx-loss-data/annual-banking-loss-report

[6] For a discussion of operational risk issues, please see Deloitte's report, *The future of operational risk in financial services*, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-the-future-of-operational-risk-in-financial-services.pdf

[7] CCP Research Foundation, Conduct Costs Project Report 2017, Press Release, http://foreigners.textovirtual.com/ccp-research-foundation/271/221503/conduct-costs-project-report-pr-no-1-aug-2017.pdf

[8] For a discussion of conduct risk, please see Deloitte's report, *Managing conduct risk*, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-managing-conduct-risk.pdf

[9] Danièle Nouy, Chair of the Supervisory Board, European Central Bank, Letter to Mr. Sven Gould, Member of the European Parliament, August 18, 2017, https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.mepletter170818_Giegold.en.pdf?bda3955c6b1e32eba44c53afdb430dd6

[10] *Economic Impact of Cybercrime—No Slowing Down*, McAfee, February 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf; Stacy Cowley, "Banks Adopt Military-Style Tactics to Fight Cybercrime," The New York Times, May 20, 2018, https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html

[11] Warwick Ashford, "Financial institutions on high alert for major cyber attack," ComputerWeekly.com, February 11, 2016, https://www.computerweekly.com/news/4500272926/Financial-institutions-on-high-alert-for-major-cyber-attack

[12] Jim Finkle, "SWIFT warns banks on cyber heists as hack sophistication grows," Reuters.com, November 28, 2017, https://www.reuters.com/article/us-cyber-heist-warning/swift-warns-banks-on-cyber-heists-as-hack-sophistication-grows-idUSKBN1DT012

[13] *2017 Annual Report to Congress*, Office of Financial Research, US Department of the Treasury, December 5, 2017, https://www.financialresearch.gov/annual-reports/2017-annual-report/

[14] ECB Supervisory Board, *Multi-year plan on SSM Guides on ICAAP and ILAAP*, February 20, 2017, https://www.bankingsupervision.europa.eu/ecb/pub/pdf/170220letter_nouy.en.pdf

[15] FED SR Letter 15-18, https://www.federalreserve.gov/supervisionreg/srletters/sr1518_PW.pdf and FED Docket No. OP 1594, https://www.gpo.gov/fdsys/pkg/FR-2018-01-11/pdf/2018-00294.pdf

[16] For a discussion of a NFR Framework, please see Deloitte's report, *The pressing case to design and implement a Non-Financial Risk Management Framework*, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Deloitte_Non-Financial-Risk-Management-Framework-July2017.pdf

[17] For a discussion of the four levers to drive change in risk management, please see Deloitte's report, *The future of risk in financial services*, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-global-RA-Future-of-Risk-POV.pdf

[18] For a discussion of these issues, please see Deloitte's reports, *The future of operational risk in financial services*, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-the-future-of-operational-risk-in-financial-services.pdf and Managing conduct risk, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-managing-conduct-risk.pdf

Deloitte.

The Banking Union Centre Frankfurt
The introduction of the Single Supervisory Mechanism (SSM) in the Banking Union by the European Central Bank (ECB) represents a fundamental innovation in supervision of financial services with significant consequences for the structure of the banking sector in the Eurozone and beyond, affecting business models and strategies. The Banking Union Centre Frankfurt (BUCF) is Deloitte`s response to the European Supervision and brings together a multidisciplinary team of senior and experienced professionals from its Financial Services practices in Deloitte member firms across Europe. Our aim is to anticipate needs and requirements of financial institutions and supervisors with regard to regulation and supervision, and to accompany both in this process. Based on very close team collaboration and the bundling of experiences and expertise, Deloitte is a very important advisory partner for the supervisors and the financial institutions in the Eurozone.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. 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 network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 264,000 people make an impact that matters at www.deloitte.com.

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.