Baking in Non-Financial Risks in Business of Finance[1]

The risk of an ever-expanding risk taxonomy, at times, need to be reckoned with. I realized this when one of director of a bank, in a candid conversation, asked if a bank is managing its financial risks so well, why it should worry about non-financial risks? I am not sure if the term Non-Financial Risk (NFR) tends to soothe many non-risk managers and senior management to believe that core bankers need to be worried only about financial risks and non-financial risks are rather buzz talks. This is probably based on the misunderstanding that financial risks end up in financial loss and non-financial risks end up in non-financial loss. The audience in the room knows better. When risk is a second name in any taxonomy, it is always ends up with real financial consequences, regardless of its first name or the source; no matter how many cascades before it hits. Non-Financial Risk (NFR) is one of the camouflaged drivers of overall risk within any bank and have increasingly become the root cause of significant losses in recent times. The specific reasons for a bank's failure can be complex and multifaceted, often involving a combination of financial and non-financial factors. However, many of the storied cases of bank busts ran a common thread of primarily NFR's doing them in. The list ranges from Barings Bank, UK and Daiwa Bank of Japan in 1995, Northern Rock Wachovia Corporation, Lehman Brothers, Washington Mutual Fund in USA and RBS in 2008, the Franco-Belgian bank Dexia SA in 2011, Spanish Bank Bankia in 2012, Cyprus Popular Bank (Laiki Bank) in 2013, to Silicon Valley Bank of USA in 2023. The resolution of Global Trust Bank in 2004 too had all the characteristics of NFR precipitation. Earnest Hemmingway in 1926 wrote the dialogue: "How do you go bankrupt?" – Two ways; Gradually and then suddenly".

2. Reflecting the complexity of today's market and banking environment, there is a "fat tail" of diverse NFRs which can arise from unforeseeable circumstances and time points with an inevitable 'butterfly effect'. The non-linear or second order effects of NFR can lead to financial volatility affecting individual banks or the banking sector as a whole, mainly through trust corroding factors among stakeholders. Unlike traditional risks, NFR losses are hard to estimate and the procyclical nature of its probabilities can compound the impact of a crisis. While operational risk can be broken down into

[1] Keynote address by Jayant Kumar Dash at CAFRAL Conference of Chief Risk Officers and Heads of Risk Management on December 20, 2023 at Mumbai.

more specific concepts i.e operational risk taxonomies, the challenges arise from ever-changing nature of such concepts and categories riddled with further sub-categories. Banking is a heavily regulated industry, nearly the only industry, for example, with a regulatory obligation to include a chief risk officer (CRO) in its C-suite ranks. As a consequence, it has developed a highly centralized approach to risk management over time, not always close to where the butterfly flaps its wings.

Understanding and labelling NFR

3. Jargonized around 2019, NFR is essentially an umbrella badge for a host of risks that have been identified or dealt with in the past but without a collective identity and a few more neoteric risks added. Reference can be drawn to the concept of Residual Risk[i] under Pillar 2 of Basel II guidelines issued in 2004 to relate it to past. NFR typically enjoys an exclusionary definition, that is, any risks other than the traditional risks of credit, market, and liquidity. NFRs are generally not considered core or directly associated to the primary business and revenue-generating activities of banks involving financial decisions getting reflected in their financial statements. Hence, they are characterized only as 'downsides' with substantial negative strategic, business, economic, and/or reputational implications. These risks could arise on account of management failures, competition, non-availability of suitable products/services, external factors etc. NFR includes not only operational risks as defined in the seven Basel operational risk event types[ii], but also other important risks such as cyber, IT, conduct, model, compliance/legal, strategic, and third-party risk with numerous sub-categories. The oft-used term reputation risk has an entirely different meaning if it compounds with the 'social amplification of risk' (SARF) framework[iii]. There are multiple sub-components of NFRs include settlement risk, model risk, tail risk, solvency risks etc. It will be interesting to note that while climate risk has been categorized as a financial risk, ESG continues to be a non-financial risk.

4. Identifying NFRs poses significant challenges in large part, because banks lack an agreed definition and risk taxonomy across assurance functions. Banks need to begin with a comprehensive and hierarchical NFR Taxonomy (e.g risk categories, risk sub-categories and risk types), with tailored customization to prevent any NFR from being glossed over. This will also create a consistent language for all the three lines to apply

across the bank, understand their correlations and interactions and build a foundation for an integrated approach for NFR management. Although NFRs are global, interconnected, and multi-tiered, designating primary ownership for each risk type will bring better focus on its identification and management and lend it uniform risk governance processes. Interactions between risks – both financial and non-financial – usually become more marked during market stress and the compounded impact may exacerbate one another to dial up the total risk at bank or system level.

Global Regulatory Trends for NFR

5. The Bank for International Settlements (BIS) identified the management of NFR as a relative weakness of financial institutions in 2009 and it has been 15 years since the Basel II capital accord prescribed a capital charge for operational risk. Apart from fraud losses, operational risk losses in most part consist of regulatory enforcement fines, penalties, and litigation costs for banks. According to an old industry estimate, the CET-1 ratios of EU G-SIBs would be around two percent higher without the fines that have been levied on them for conduct risks. Increasing regulatory stress on the effectiveness of governance, conduct and culture, misaligned compensation/ incentives and lack of accountability is common across global jurisdictions. Therefore, NFR management has been assuming predominance equally for banks as well as bank supervisors. Regulators have increasingly recognised the need for expansion of regulatory requirements, going by the incompetent risk monitoring in the past leading to large losses. For example, the EBA Internal Governance Guidelines, which were revised in 2017, reflect the supervisory expectation for transparency of non-financial risks by enumerating the main NFRs. In addition to financial risks, non-financial risks, including ”operational, IT, reputational, legal, conduct, compliance and strategic risks” must be adequately addressed in the risk management framework. Looking at the 2020 priorities, released by supervisors worldwide, it was clear that non-financial risks are globally climbing up the chart.

6. The Financial Stability Report 2023 of Federal Reserve Board of Governors carried a survey in which NFR comprised 2 of the top 5 salient risks to the US financial system. As per the annual risk outlook report 2023 of Office of the Superintendent of Financial Institutions (OSFI), out of 9 most significant risks facing Canada in the upcoming year,

4 were NFRs. This increased importance is also reflected in the current amendment to MaRisk (Minimum Requirement for Risk Management) by BaFin in June 2023, which arrayed a set of current 'priority areas' including ESG, remote working, real estate market trends and business viability. It also requires operational risks to be integrated e.g. with compliance, information security, the adjustment processes, and the internal control system. In October 2023, OSFI published two new draft rules on NFR aimed at stemming foreign interference affecting integrity / security and other non-financial risks such as hacking, fraud, money laundering and terrorism financing to the country's banking system. The draft rules, also address issues including the character of board members and management, governance, and controls around physical premises, data and technology systems.

7. As for India, while the term NFR may not easily be explicitly found in regulatory communications, it will be hard to miss regulatory guidelines and supervisory expectations on most key components of NFR. In recent times, you must have heard about RBI Governor's emphasis on business models, strategy and a range of conduct issues for banks which is finding more traction in supervisory processes and interventions.

Quantifying and Measuring NFR

8. Quantification of risk i.e measurability of its impact in financial terms, is equivalent of a 'made real' of an abstract concept for the board, senior management, and other stakeholders. As NFR arises from unexpected, even unique and sometimes mutated sources, the impediments to finance functions in engaging more effectively on NFR metrics can be challenging. Statements such as "financial institutions are bad at managing non-financial risk" or defining non-financial risks as "those for which CFO is not worried" are reflective of the perception about its quantification, unlike financial risks. The complexity in incorporating NFRs into the existing risk appetite and risk management frameworks arise from such perceptions. However, certain quantified manifestation of NFR already appearing in the financial statements of banks are often ignored. For example, litigation risk requires provisioning, cyber risk management and mitigation requires capital investments and significant operating budget. Quantification of third-party risks are set against operating margin and efficiency ratio. Like traditional

financial risks, these vital numbers belong to the financial function domain. Hence, both operational risk management (ORM) and finance need to be part of quantifying and managing NFR. Quantification enables comparison and prioritization of risks based on exposure and enables CRO to run more insightful analyses. The short history and developing nature of NFRs make them hard to quantify. Banks are challenged by how to adopt traditional tools, e.g risk ratings, on the face of insufficient data to develop different assessments of the probability of default—or of loss given default—despite having a possible opinion on the extent of the risk. Of NFRs, quantification is the key difficulty driving host of other difficulties.

9. In the absence of robust risk quantification capabilities of NFR, certain proxy methods are used to incorporate it into overall risk management frameworks. One approach is to create an integrated qualitative-quantitative approaches for managing risk (as opposed to purely quantitative) by testing each NFR individually and manage the exposures accordingly. The other approach is by matrixing of various NFR factors for gaining insights for managing overall risk. Some of the banks use the US' FFIEC Cybersecurity Assessment Tool (CAT) to measure our cyber posture and the Factor Analysis of Information Risk (FAIR) risk management framework for understanding probabilities / impacts and to quantifying the risks. Ideallt, NFR measurement methodology must combine quantitative and qualitative approaches to reach a risk score in alignment with the bank's set risk framework. Quantitative assessment could consider appropriate Key Risk Indicators (KRIs) for each eligible risk category and sub-category while subduing subjectivity through a frequency and impact quantification. Qualitative assessment should also combine results from the processes and control gap quantification. Stress-testing models are gaining acceptability in banks for scenario analyses to apprise management of potential NFR exposures and provide insight into appropriate risk mitigation. As opposed to dependence on past loss databases, advanced analytics, supplemented by the analysis of a broader range of relatable external data hold promises for improved NFR quantification. Such methods have been successfully used in some cases to detect deviant behavior in trading and client/internal transactions, reduce employee turnover, improve hiring decisions, warn fraud attempts, and minimize both Type I and Type II errors in their money-laundering transaction monitoring processes.

Maturity Curve of NFR Management and Challenges

10. The complexity and challenges in managing NFR does not arise only from the size of the canvass. Decentralized responsibility required for NFR management, lack of clear and unambiguous definition of roles and responsibilities for NFR management, heterogeneity in risk assessment methodologies and still back-ward looking nature of NFR management add to the challenges. Two broad characteristics of the current approaches in India are (i) reactive approach involving establishment of functions only in response to risk events and / or regulatory actions, often through an 'at any cost' approach and (ii) uncoordinated design creation involving additional risk management frameworks without consideration of existing processes, functions and more efficient set ups. This silo approach limits its enterprise effectiveness with inconsistent understanding of risk resulting in failure to identify all risks and potential impact; inefficient handling of overlapping risks; coming in the way of synergistic cooperation across expert teams; inefficient resource allocation; fragmented systems and processes risk; multiple overlapping communication resulting in inconsistent messages and avoidable burden. An important challenge in transforming to an integrative assurance function remains to be a fuzzy definition of the responsibilities between the lines, in the businesses, and the second-line control functions. In addition, control functions are siloed, each having its own risk-identification processes, reporting structures, IT systems. The result is duplicated work as well as costs. Banks feel they are drowning in parallel efforts aimed at identifying, assessing, and remediating risks, with the same individuals being approached over and over again, and diluting scarce resources, and attention from running the business by creating fatigue. In addition, the relevance of a clear definition and allocation of NFRs to specific business areas as well as an evaluation of their potential business impact is yet to be appreciated. Inevitably, the chief risk officer and his or her operational-risk unit struggle to provide the board and regulators with a thorough view of risks faced and controls required.

11. Globally, the NFR management, proxied by compliance and controls, has evolved through three operating stages. In initial stage, bank's focus on NFR is addressed by oversight of compliance functions, characterised by low number of incidents and audit findings with limited accountability. In the second or intensification stage, a modular remediation approach has been adopted with increased focus of regulators. Finally,

an integrated / combined assurance framework emerged with uniform and forward-looking risk taxonomy, second line covering all risk types with right resourcing, empowered audit functions, stringent adoption of business and operating model, accountability across all lines, and developing strong control culture. A significant readiness gap between banks' current and targeted NFR management capabilities is a serious issue globally.

12. In the past, operational risk management focused on modeling and managing the data basis, such as loss events and risk assessments, keeping an eye on compliance with regulatory requirements without any active NFR management focus. As the banks' NFR profile is undergoing constant churn, the need for appropriate and comprehensive NFR management is also increasing. At present, this is mainly achievable through digitalization and automation of processes. This may result in fewer manual processing errors but will increase the risks posed by cyber-attacks or data breaches. The operational risk and resilience maturity, a key component of NFR, involves designing and enhancing risk governance and oversight models across the three lines; assessing their operational resilience capabilities including governance and controls in order to identify gaps and remediation plans (e.g operational resilience self-assessment); preparing to face and recover from emerging threats (e.g orchestrating a crisis management exercise); and finally embedding an operational resilience culture across the bank.

An Effective NFR Management Program

13. Effective risk management is at the heart of every successful bank. The interlocking relationship between Non-Financial Risk (NFR) and Financial Risk (FR) creates a demanding landscape of scrupulous attention and strategic acumen. Often said in the context of NFR management, it is not so much about what banks should do, but how they should do it. That has become growingly more challenging due to the snowballing complexity from rapid shifts in technology with accompanying hypes, process automation trends, and migration to systems from people. The mitigation of NFR is intrinsically linked to the quality of internal processes and procedures, technology systems, specialized governance framework or compliance characteristics of a bank. The impact of changes in internal and external environment on a bank's risk

situation requires an adaptation of its structure used for risk management. A more integrated NFR-management approach limits costs by helping reduce the risk of further failures. The key pillars of such an approach is an enhanced governance framework with right set of enablers and changes in the approach of the external interfacing units. This needs to be implemented across four primary areas viz. process, risk, controls and incident management with continuous evaluation.

14. A successful NFR management approach has to bank on certain key levers starting with a proportionate strategy, backed by a risk governance model, aligned people & culture and adoption of emerging technologies. As for strategy, a clear process with explicit ownership incorporating all material NFRs into bank's business strategies and risk appetite (with appropriate metrics and risk limits in place) is the first step in NFR management. Fine-tuning or radical adjustments in business models / structures followed by digitalization and process optimization boost the efficacy of the internal control functions. The enhanced three lines model envisaging a combined assurance function of risk management will be essential in managing NFR. As for the people & culture, acquiring or developing necessary skills among employees to address NFRs, as also to build a culture of recognizing the importance of managing NFR is required. Leveraging new technologies, such as Generative AI, Machine Learning, robotic process automation, and predictive analytics to automatically scan an expanded set of data sources, both within business verticals and external, not only provides early warning signals of potential NFR events but automation also reduces compliance costs. Technology transformation should follow an iceberg model and should not focus on front-end, i.e the user experience alone. It is more important to undertake technological change focusing on the back-end processes.

NFR Governance Enhancement and Role of the Board

15. Board governance always occupies the crown position for any significant change to occur within a bank, in terms of setting out the high principles. A meticulous analysis of full risk profile encompassing business model and strategic direction of the bank is a foundational prerequisite for an effective risk and control management framework. A comprehensive risk taxonomy and a dynamic Risk Identification process sets up the base camp. It goes without saying that the Board must include NFR within the risk

appetite framework (RAF) and articulate a more enhanced Risk Appetite Statement ("RAS"). The involvement of the Board should be visible as part of their regular and driven monitoring rather than as firefighting in reaction to emerging situations from control failures. There is a need for increased engagement of the board to challenge the risk profile and build a forward-thinking perspective of the bank on the top-impact risks. As a corollary, directors should be capable of understanding the nature of NFRs and rank their impact. Against this, the adequacy of the control system and plugging of any gaps to hold the lines firmly to ensure that there is no breach in its set risk-tolerance boundaries assume importance. Objectively assessable target variables in respect of risk strategy and appetite for NFR must be incorporated for performance of all levels of executives. Risk management for risk categories under the current regulatory focus (e.g. conduct risk, model risk) should also be expanded.

16. As mentioned earlier, NFR-governance framework should use the enhanced three lines model with an integrative or combined assurance function. Some adoptions have extended the definition of the first line to incorporate in NFR management. The domain of the second line has been broadened beyond the risk and compliance functions to include areas such as legal, HR, finance, and tax, recognizing their role in managing the institution's control framework in their respective areas of risk expertise. Principles always lead the processes. Delineation of first and second lines may vary across banks but defining a consistent set of principles reflecting the structure of governance, complexity of operations and specific requirements is of paramount importance. The principles need to be enduring enough to guide future alignments to the risk-aware business strategy and operating model of the bank. The functional separation of the first and second lines ensure independent control by second line as the second line is seen as crucial to the bank's business model. The importance of first line's taking responsibility for NFR management, rather than focusing entirely on revenue or cost management, cannot be overemphasized. This can be supplemented by balanced scorecards measuring control effectiveness and review thresholds and penalties for any breach. A change in the organizational culture to keep NFR management and controls at the front of senior management and employees should be the ultimate goal of such principles. The risk-governance principles need to be shared across the verticals of the bank and formalized as part of the risk-policy framework, while the CRO ensuring its consistent application.

17. It is often said, culture isn't only for the good times, it's for all times. Its significance increases for non-financial risk (NFR), as creation of policies and procedures to manage all of them is difficult. Risk culture refers to the norms, attitudes, and behaviors related to risk awareness, risk taking, and risk management in a bank. A misalignment of risk culture often results in shortcomings in conduct, compliance, and other elements of NFR. Of late, regulators in more and more jurisdictions have been setting up individual accountability frameworks. In the context of NFR, a unified governance structure would mean unifying methodologies across all subcategories and assurance functions. Integration of non-financial risks in the area of risk culture is an essential prerequisite for an optimal outcome. Data transformation must be at the forefront to enable long term change within an organisation. Once the data transformation is complete, new technologies such as big data, natural language processing, automation, process mining, and predictive analytics should be leveraged to develop an 'always on' risk management model. This includes technologies that can 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 of reporting, controls and key risk indicator monitoring.

Conclusion

18. Non-financial risks are becoming increasingly consequential in the banks' risk heatmap arising from instances spectacular losses at times. On the other hand, supervisory authorities and standard setters are also increasingly focusing on these risks in the assessment of risk bearing capacity of banks. By now, we know that NFRs can only be reduced or mitigated, but not eliminated. BCBS in 2020 said, while it may not be possible to fully avoid certain non-financial risks, it is possible to improve the resilience to such events. In this rapidly developing environment, a robust, business-aligned NFR-management strategy is a core requirement not only for a sustainable growth and resiliency but also for a competitive advantage of banks. Size is not necessarily a good determinant of whether a bank gives a particular NFR due cognizance; banks of all sizes need to invest in their non-financial risk capabilities. Keeping pace with the risks manifesting faster, timely digitization and automation of risk management can ease the identifying, inventorying, and tracking of NFRs. Impact

of changes to internal and external conditions on a bank's risk situation require an adjustment to the organizational structure used for risk management.

I conclude with wishes for a very productive day ahead in deliberation of various aspects of Non-Financial Risk Management.

Xxx***xxX

=

[i] Pension Risk, Systemic Risk, Concertation Risk, Strategic Risk, Reputational Risk, Liquidity Risk and Legal Risk

[ii] 1.Internal Frauds; 2.External Frauds; 3.Employment Practices and Workplace Safety; 4.Clients, products, 5.Business practices; 6.Damage to physical assets; 7.Business disruption and system failures

[iii] The Social Amplification of Risk: Theoretical Foundations and Empirical Applications by Ortwin Renn, Clark Univerrsity; William J. Burns, University of Iowa, Jeanne X. Kasperson and Roger E. Kasperson, Clark University; Paul Siovic, University of Oregon, 1980