Authors: Subhojit Shome & Archisman Bhattacharjee
Email: finserv@vinodkothari.com
Date: May 09, 2024

Risk Management Function of NBFCs - A Need to Integrate Operational Risk Management & Resilience

An examination of the RBI Guidance Note on Operational Risk Management and Resilience

Contents

Introduction

Murphy's Laws:

- *Anything that can go wrong will go wrong, and at the worst possible time.*
- *If there is a possibility of several things going wrong, the one that will cause the most damage will be the one to go wrong.*

The BCBS defines operational risk as the *risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. It includes legal risk but not strategic and reputational risk.*

While NBFCs apply rigorous risk mitigation processes when it comes to credit, liquidity or market risks, operational risk generally gets relegated to the background. This may be attributed to the fact that, unlike other risks, such risk is implicit in the ordinary course of corporate activity and is not taken in return for expected reward. Further, the relative inherent likelihood of occurrence of operational risk is low. However, the consequence or impact that such risk may pose if materialised is high or even catastrophic. Recent shocks to the system, like the COVID pandemic and cybersecurity incidents, have exposed how operational disruptions can threaten the viability of an RE, impacting its customers and other market participants, and ultimately have an impact on financial stability.

Recently, the BCBS recognised that its 2011 Principles did not adequately capture operational risk sources such as those arising from information and communications technology (ICT). Additionally, it also perceived the need to develop principles for operational resilience for banks to withstand severe disruptions to their systems. To this end, the BCBS published its revised principles on sound management of operational risks in March 2021. The RBI, in its turn, issued the Guidance Note on Operational Risk Management and Operational Resilience ('Guidance Note'), vide its notification dated April 30 2024, in line with the BCBS's revised principles. In its remit the Guidance Note has gone beyond banks and has included NBFCs as well.

In terms of regulatory mandate, for NBFCs the evaluation of operational risks was solely limited to the process of identification of operational risks for determining the internal capital adequacy. Vide the Guidance Note, however, the RBI provides a holistic framework for treating operational risk exhorting NBFCs to implement specific risk management measures. Interestingly, the use of guidance notes is a novelty when it comes to the regulatory framework for NBFCs and there is conjecture on the regulator's expectations from NBFCs. In this article, we examine this uncertainty surrounding the enforceability of the Guidance Note and identify the action points for NBFCs arising from it.

Applicability

The guidance note is applicable to:

a. All Commercial Banks;
b. All Primary (Urban) Co-operative Banks/State Co-operative Banks/Central Co-operative Banks;
c. All All-India Financial Institutions (viz., Exim Bank, NABARD, NHB, SIDBI, and NaBFID); and

d. All Non-Banking Financial Companies including Housing Finance Companies.

Applicability on NBFCs

As has been provided above the guidance is applicable to all NBFCs. Prior to the notification of the guidance, NBFCs as a part of their internal assessment of capital commensurate with the risk had to factor operational risks in line with Pillar 2 of Master Circular – Basel III Capital Regulations. This requirement of ICAAP is only applicable to NBFC-ML and above, however, the evaluation and management of operational risks have also now been extended to NBFCs in the base layer (NBFC-BL).

Enforceability of the Guidance Note

Guidance notes, generally, do not have the same regulatory force as that of a master direction, circular, etc. The role of a guidance note is not to impose additional regulatory obligations on regulated entities, but rather to clarify existing regulations, i.e., provide guidance on the best practices that the regulator expects.

The current guidance issued by the RBI is aimed towards bolstering the overall risk management function of an NBFC. Under the SBR Directions, NBFCs are required to put in place a progressive risk management framework including policies and strategies to mitigate risks. Constituting the RMC and ALCO as part of an NBFC's governance framework also follows from the SBR Directions. The breach or failure to implement the guidance, per se, may not result in regulatory penalties or fines. NBFCs, however, would be ill-advised to turn a blind eye as non-adherence to the prescriptions in the Guidance Note may result in material gaps in their risk management framework and invite regulatory action.

Now that we have developed a broad idea of the applicability of the Guidance Note, we can go onto present a summarised view of its impact on NBFCs.

Impact on NBFCs

Regulatory Capital

The RBI Master Circular on Basel III Capital Regulations required SCBs to maintain Pillar - 1 capital against operational risk. Although the new SBR framework brought additional CET1 requirements for Upper Layer NBFCs, there was no mandate to maintain a capital charge against the NBFC's operational risk. This continues to be the case under the Guidance Note, with the footnote to para 1.8 of the preface to the Guidance Note explicitly stating that NBFCs are not required to maintain separate regulatory capital for operational risk.

Operational risk, however, is a material risk that an NBFC is exposed to. Consequently, as part of their internal capital adequacy process (ICAAP), NBFCs in the Upper and Middle Layer need to factor in such exposure when evaluating their capital requirement. Refer to the article on ICAAP for NBFCs available - *here*.

Operational Risk Management Function

The Guidance Note looks at incorporating an operational risk management function (ORMF) into an NBFC's existing risk governance structures. The Guidance Note recommends a governance structure consisting of the three lines of defence as well as specific responsibilities spread across functional management, senior management and the Board.

As mentioned earlier, the Guidance Note recommends integrating an organisational operational risk management function (OORF) as part of its overall risk management framework as depicted in *Figure 1.*

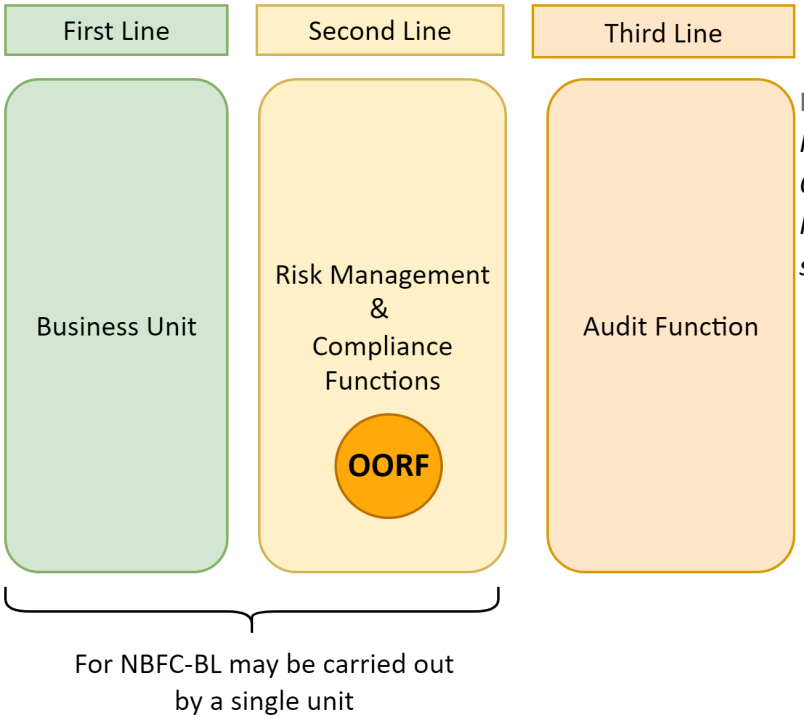

Figure 1. Three Lines of Defence *Incorporating the Organisational Operational Risk Management Function (OORF) within the second line.*

Business Unit	OORF	Audit Function
• Perform Operational Risk and control assessments of new products, services, activities, processes and systems • Identification and managing the risk which are inherent in the product services, activities, processes and systems for which the unit is responsible	• Review and challenge the control systems identified by the Business Unit(s) • Develop standard, guidelines, policies for operational risk management and resilience • Monitor the implementation of appropriate controls or remediation actions	• Reviewer of the entire Operational risk management governance structure

● Such responsibility also extends to all associated support, corporate and/or shared service functions, e.g., Finance, Human Resources, and Operations and Technology	● Provide operational risk-related training	

Table 1. Functions of the Three Lines of Defence

Significant Action Points

Highlighted below are some of the more significant changes that an NBFC will need to make to its existing risk management framework :

Action Points for NBFCs		
●Ensure existing risk management policy includes provisions with respect to identification, assessment and mitigation of operational risks inherent to the business (refer further to section on Risk Assessment and Identification Tools). ●Identify "Critical Operations"[1] of the NBFC. Define and document criteria for classifying operations as critical. ●Develop an Operational Risk Appetite and Tolerance Statement with tolerance for disruption specified at the critical operation level (refer section on Operational Risk Tolerance Metrics).	●Review and align compensation policies with its risk appetite and tolerance statement as well as overall soundness of risk management framework. ●Evaluate the effectiveness of the ORMF especially considering operation risks associated with new products, services, activities, processes or systems, including changes in risk profiles and priorities. ●Update ToR of the RMC to oversee operational risk.[2] ●Determine, and annually review, the maximum loss exposure the NBFC is willing to take and has the financial capacity to assume. Based on	●Manage third-party dependencies (refer section on Managing Third-party Dependencies). ●Develop and implement a change management system (refer section on Change Management). ●Document the company's operation risk management function. Having an inventory of risks, risk assessment tools, control library, inventory of incident response and recovery are requirements under the Guidance Note. ●ICT has been highlighted as a major risk source and NBFCs are expected to have a incident management plan to

[1] As per para 2.2 of the Guidance Note - "Critical operations" refers to critical functions, activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of the RE or its role in the financial system. Whether a particular operation is "critical" depends on the nature of the RE and its role in the financial system.

[2] For REs of substantial size and complexity having enterprise level risk committees, the Guidance Note recommends creating management level operational risk committees. While it is important for NBFCs in the Upper Layer to consider this advice, given the average size and complexity of Middle and Base Layer NBFCs they may reasonably leverage their existing RMC.

●Establish, and regularly review, a code of conduct and ethics policy to address conduct risk. The code should be made publicly available. The Board/ Board-level Committee or a separate ethics committee to monitor implementation of such policy.	such assessment evaluate the company's insurance or risk transfer needs.	handle such ICT-related incidents. ●Include succession planning and staff availability during extended periods of disruption as part of the company's BCP (refer section on Business Continuity & Incident Management). ●Develop a disclosure policy for informing stakeholders and the public.

Table 2. Action Points for NBFCs

While the above table provides a summarised view of the action points, certain items require a more granular analysis and the following sections examine these items.

Managing Third-party Dependencies

There are already guidelines[3] laid down by the RBI with respect to managing risks arising out of outsourcing of IT and financial services by NBFC. The Guidance Note goes beyond the limited perimeter of outsourced financial or IT services and advises NBFC to develop operational resilience for all third-party arrangements, especially, when they are material to its Critical Operations[4].

Consequently, other than outsourced financial and IT service providers, NBFCs are also expected to manage operational risks arising out of their dependence on external consultants, advertising partners, payment system providers, legal service providers, etc.

NBFCs should make note of the following action items when it comes to managing third-party dependencies:

Managing Third-party Dependencies	
● Develop procedures to identify the need for entering into third-party arrangements ● Augment their risk management policies and procedures to include additional third-party relationships and include contingency/ business continuity plans and exit strategies as part of their risk mitigation processes ● Perform due diligence of the third-party to satisfy itself that such party has, at least, an	●Identify and manage risks arising from any further downstream service provider (say, sub-contractors - a "fourth party") in case they play a role in the NBFC's ability to maintain its critical operations ●Review their contractual agreements/ SLAs with third-parties to ensure that they include provisions with respect to ownership and confidentiality of data, termination

[3] A new framework for financial services outsourcing is also in the pipeline. We have examined the question of what constitutes outsourcing in our article - here.
[4] *Supra*

equivalent level of operational resilience as the NBFC	rights, clear allocation of responsibilities including their service provider's liability towards performance and risk management practices of its sub-contractors.

Table 3. Managing Third-party Dependencies

It can be reasonably contended that the need for contractual agreements/ SLAs does not arise in case of the NBFCs use of public utilities including payment infrastructure.

Operational Risk Tolerance Metrics

NBFC are expected to set at least one impact tolerance metric for each of its critical operations. Impact tolerance metrics may be of the following types:

Time-based	Quantity-based	Service Level
E.g. Maximum acceptable duration of service disruption/ maximum tolerable downtime (MTD)	E.g. - Maximum tolerable data loss (MTDL) - Maximum tolerable number of customers affected - Maximum tolerable number of transactions impacted	E.g. Minimum services that th NBFC should continue to support during a disruption

Table 4. Operation Risk Tolerance Metrics

Change Management

The IT Master Direction mandates applicable REs to establish documented policies for change and patch management, ensuring secure and timely implementation, justified changes with approvals, and mechanisms for recovery from failures. However, the Guidance Note not only covers operational risk due to changes in IT applications and processes but also extend to cover all operational changes, including new activities, product modifications, the introduction of new products and geographical risks[5]. The Guidance Note emphasises change management through the three lines of defence structure.

Action points for NBFCs to note:

Change Management	
● NBFCs are required to maintain a central record of products and services to ease the monitoring of risks associated with change ● NBFCs should establish policies and processes for identifying, managing, challenging, approving, and monitoring change.	● NBFC's review and approval process should consider - inherent risks (legal, ICT, and model risks), changes to its operational risk profile, appetite and tolerance limits, necessary controls and risk management

[5] Risks associated with RE operating from branches far from its head office

●NBFCs should have policies and procedures for the review and approval of new products, services, activities, processes, and systems.	processes, residual risk remaining with the company.

Table 5. Change Management

Business Continuity & Incident Management

The prescriptions contained in the Guidance Note largely echo the compliance requirements under the recently introduced IT Master Directions. The Guidance Note further requires the NBFCs to have succession planning in place in case of disruptions that impact key personnel. Furthermore, the RE's are also required under their business continuity plan to take into account the impact of pandemic since it has the capability of disrupting the activities of an RE for a prolonged period.

Further, it should also be noted that the business continuity as envisaged under the IT Master Directions is related to risks that may arise due to failure or compromise of IT systems and processes, however, the guidance note covers a larger ambit which requires the framing of Business Continuity Plan for all operational risks.

Operational Risk Identification & Assessment Tools

The Guidance Note suggests a number of tools that a NBFC may use for the purpose of its risk identification and assessment. The term "tool" does not necessitate the implementation of risk-related software or application; rather these are the techniques that an NBFC may use, often in conjunction, for the purposes of assessing operational risk level.

NBFCs may, inter alia, consider using metrics capturing incidents of disruption, self-assessment by business units, control monitoring and assurance as operational risk assessment techniques.

Conclusion

The Guidance Note impresses upon NBFC to pay particular attention to its operational risks, which in an NBFCs risk management framework gets overshadowed by credit, liquidity and market risks. As noted earlier, the aim of this Note is not to prescribe additional structures and framework but rather to have NBFCs integrate operational risk in their existing risk management framework. The Guidance Note also broadens the scope of certain elements in an NBFCs governance framework such as change management, managing third-party dependencies, vetting and monitoring of new products and services, use of impact tolerance metrics, BCP and treatment of ICT-related risks. In light of this Note, Board and Senior Management of NBFCs will be well advised to re-evaluate their existing risk management practices.