Recommendations on

Discussion Paper on 'Governance in Commercial Banks in India'

Submitted by:

Bridge Policy Think Tank

C 18, Third Floor, Local Shopping Centre 1, Above IndusInd Bank, C Block Market, Vasant Vihar, New Delhi 110057

director@bridgemediation.in | +91 9560439503 | +91 8586074575

C 18, Third Floor, C Block Market, Vasant Vihar, New Delhi 110057
Anuroop Omkar | director@bridgemediation.in | +91 9560439503

Recommendations | RBI Discussion Paper on Governance of Commercial Banks in India

1. Para no. –

5.1.2. **Risk Management Committee of the Board (RMCB)**

3. The role of the RMCB is to assist the board, inter alia, in the following:

xxv. ensure a sufficiently robust data infrastructure, data architecture, information technology infrastructure – that is in sync with developments such as balance sheet and revenue growth; increasing complexity of the business, risk configuration or operating structure; geographical expansion; mergers and acquisitions; or the introduction of new products or business lines.

1.1. Background

The Discussion paper on Governance in Commercial Banks in India released on 11 June 2020 [hereinafter referred to as **'Discussion Paper'**] released by the Department of Regulation , Reserve Bank of India [hereinafter referred to as **'RBI'**] under para 5.1.2 establishes the Risk Management Committee of the Board [hereinafter referred to as '**RMCB**'] made up only of the non-executive directors of the Bank.[1] The **Discussion Paper** further elaborates upon the composition of the **RMCB** to include at least three non-executive directors and two-thirds independent directors out of which at least one such independent director to have risk management expertise.[2] The said para lays down the eligibility of the members of **RMCB** and that the **RMCB** shall be chaired by the independent director who does not chair any other committee of the Board.[3]

The **roles and responsibilities** of **RMCB** includes, amongst other things, to discuss all risk strategy and make recommendations on such strategy and the risk appetite of the bank this further includes to assist the board in ensuring a robust data infrastructure, data architecture, information technology infrastructure which is in synchronisation with developments of the bank including the following:

i. Balance sheet and revenue growth;
ii. Increasing complexity of the business;

[1] Para 5.1.2 (1), Discussion Paper
[2] Ibid
[3] Para 5.1.2 (2), Discussion Paper

iii. Risk configuration or operating structure;

iv. Geographical expansion;

v. *Mergers and acquisitions; [Emphasis supplied]*

vi. Introduction of new business in the business line.

1.2. Background research / International best practices / Interpretation of statute

We understand that the above para 5.1.2 (3) (xxv) of the **Discussion Paper** is the only para which addresses the issue of mergers and acquisition of the Bank. However, such addressing is only limited to the responsibility of RCMB in ensuring a robust data infrastructure, data architecture and information technology framework is in place which syncs with the mergers and acquisition of the Bank. Therefore, the said para only fixates on the information technology framework to be suitable in case any merger or acquisition is proposed for the Bank and such framework smoothly enables the transition. The para does not address the specific risk evaluation in case of any proposed merger, amalgamation or acquisition of the Bank.

To further draw attention to the need of a dedicated para for evaluation of any proposed merger, acquisition or any other scheme of restructuring, a need is felt to refer to the **Paragraph 125** of the **Basel Committee on Banking Supervision's Guidelines on Corporate Governance Principles for Banks, July, 2015**, which states:

> *"Mergers and acquisitions, divestitures and other changes to a bank's organisational structure can pose special risk management challenges to the bank. In particular, risks can arise from conducting due diligence that fails to identify post-merger risks or activities conflicting with the bank's strategic objectives or risk appetite. The risk management function should be actively involved in assessing risks that could arise from mergers and acquisitions and inform the board and senior management of its findings"*

Therefore, various risks emanate from the merger and acquisition or any other changes to the organizational structure of banks especially with respect to the post-merger risks which may not be in consonance with the risk-appetite of the merged or restructured entity. Additionally, there are probabilities of overlooking such risks even during the due diligence of the proposed restructuring transaction. The restructured entity's internal structure

should be sound in terms of generally accepted management principles,[4] and the proposed merged structure should not be detrimental to the merged entity or to the effective supervision of the merged entity.

Further, this function to evaluate the risk on merger, acquisition or restructuring is attributable to the risk management function of the Board of the bank.

***Suo Moto* power to RBI to order restructuring**

To further draw attention to the need of a dedicated risk assessment framework to evaluate the risks emanating from proposed restructuring of banks, the President recently promulgated the **Banking Regulation (Amendment) Ordinance, 2020** which granted powers to the **RBI** to enforce reconstruction or amalgamation of a "banking company" even when the moratorium is not in force if such reconstruction or amalgamation is in the interest of public, depositors, to enforce proper management of the bank, or in the interest of the banking system of the company as a whole. For that purpose, Section 45 (4) of the Banking Regulation Act, 1949 has been amended to include:

> *(4) During the period of moratorium* ***or at any other time****, if the Reserve Bank is satisfied that:*
> *(a) in the public interest; or*
> *(b) in the interests of the depositors; or*
> *(c) in order to secure the proper management of the banking company; or*
> *(d) in the interests of the banking system of the country as a whole,*
> *it is necessary so to do, the Reserve Bank may prepare a scheme–*
> *(i) for the reconstruction of the banking company, or*
> *(ii) for the amalgamation of the banking company with any other banking institution (in this section referred to as "the transferee bank").*

The said provision in the **Banking Regulation (Amendment) Ordinance, 2020** has been promulgated, unless disapproved by the Parliament or not passed within 6 (six) weeks of reassemble of Parliament,[5] with the intention to resolve the banking stress without disrupting the bank's operations or withdrawals by depositors by putting it under moratorium. However, the process needs to include the risk measurement of the bank for

[4] Paragraph 4.4, Gill Marcus, Issues for consideration in mergers and takeovers from a regulatory perspective, Bank for International Settlement, July, 2000
[5] Article 123 (2), Constitution of India, 1950

which restructuring is proposed and the risks which the bank shall pose, in the current state of affairs, to its own operations and to the merged entity.

It is pertinent to mention here that a "hostile" merger could increase the difficulty of merging the cultures, especially at senior level. Perhaps the biggest mistake is to ignore the impact of a merger on employees and the senior management of the merged entity. [6]

1.3. Analysis & suggestions

Therefore, similar to paragraph 125 of the **Basel Committee on Banking Supervision's Guidelines on Corporate Governance Principles for Banks, July, 2015, RMCB** shall be made responsible to assess and oversee the risk emanating from any proposed restructuring, whether voluntary or statutory.

Moving a step ahead on the issue, **RMCB** shall further submit a detailed risk assessment report evaluating the cost benefit, performance, measures to manage stress, projected market and credit risks due to merger, amalgamation or restructuring, as the case may be, of the bank to the board. The board of the bank shall submit this report to **RBI** and taking into consideration the report, decide pragmatically upon the reconstruction or amalgamation as the case may be. Similarly, when a merger or acquisition is under consultation by the bank individually as well, the risk should be properly assessed and captured in a risk assessment report. Such risk assessment report shall be submitted with the **RBI** for approval of the proposed amalgamation of commercial banks.

---

2. Para No.

> *"5.1.2 Risk Management Committee of the Board (RMCB)*
>
> ***XXV.*** *Ensure a sufficiently robust* ***data infrastructure, data architecture, information technology infrastructure*** *– that is in sync with developments such as balance sheet and revenue growth; increasing complexity of the business, risk configuration or operating structure; geographical expansion; mergers and acquisitions; or the introduction of new products or business lines. "*

[6] Paragraph 4.10, Gill Marcus, Issues for consideration in mergers and takeovers from a regulatory perspective, Bank for International Settlement, July, 2000

2.1. Background

The **Discussion Paper** does not address a provision for a **Data Protection Officer** [hereinafter referred to as '**DPO**']. A mere mention under **RMCB** may not ensure an independent role is created within an organization that leads him/her to determine the purposes and means of processing personal data. There is a need for a clear defined role for a **DPO** in order to ensure compliance and a clear organizational position of a **DPO**.

2.2. Background research / International best practices / Interpretation of statute

The role of a **DPO** has been addressed in **General Data Protection Regulation** [hereinafter referred to as '**GDPR'**] and the **Personal Data Protection Bill, 2019.**

Under the **GDPR**, **Article 37(1)**[7] highlights the need of a **DPO** where the core activities of the controller or the processor consists of processing operation which require regular and systematic monitoring of data subjects on a large scale. Banks, in general fall under the ambit of undertaking these activities in their day-to-day activities.

Additionally, the **GDPR** recognizes the **DPO** as key player in the new data governance system and lays down conditions for his/her appointment, position and tasks.[8]

For the purpose of clarifying regular and systematic monitoring, the **Guidelines on Data Protection Officers, Data Protection Working Party Article 29** [hereinafter referred to as '**WP29**'] interprets '**regular'** as meaning one or more of the following –

- Ongoing or recurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

WP29 interprets '**systematic'** as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

[7] Article 37, General Data Protection Regulations - https://gdpr-info.eu/art-37-gdpr/
[8] Guidelines on Data Protection Officers, Data Protection Working Party Article 29 (WP29) - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Banks undertake the above mentioned activities, hence require a mandatory **DPO**.

Under the **Personal Data Protection Bill 2019**, section 30 addresses the function of a DPO.[9] The activities of a **DPO** is mentioned in a non-exhaustive manner while addressing important roles such as *conducting data impact assessments, development of internal mechanisms and grievance redressal.*

The **RBI** issued the **Master Direction - Know Your Customer (KYC) Direction, 2016**, under which clause 7 mandates for a principal office to be allocated to perform tasks such as ensuring compliance, monitoring transaction, sharing and reporting information as required under the law/regulations.

Additionally, Section 12 of Chapter IV of the **Prevention of Money Laundering Act 2002** highlights the role of officer to be designated to oversee, maintain and record information much like the role of a **DPO**. We believe the role of the designated officers in the above mentioned regulations lack uniformity and a clear clarification can be sought be addressing the same in the corporate governance guidelines.

For the purpose of this discussion paper, the role of a **DPO** can exceed the requirements of the above mentioned regulations. To enhance governance policies within the organization, additional roles can be adopted by the DPO. Some of these additional roles can include:

- Inform and advise the company (data controller or data processor) and employees how to be **GDPR** compliant and how to comply with other data protection laws
- Manage internal policies and make sure the company is following them through
- Raise awareness and provide staff training for any employees involved with processing activities
- Provide advice regarding the data protection impact assessment and monitor its performance
- Give advice and recommendations to the company about the interpretation or application of the data protection rules
- Handle complaints or requests by the institutions, the data controller, data subjects, or introduce improvements on their own initiative

[9] Personal Data Protection Bill 2019 - http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

- Report any failure to comply with the GDPR or applicable data protection rules
- Monitor compliance with GDPR or other data protection law
- Identify and evaluate the company's data processing activities
- Cooperate with the supervisory authority
- Maintain the records of processing operations

DPO is not personally responsible for compliance of the organization, it is always a fiduciary who is required to demonstrate compliance. The controller or the processor is obligated to provide all necessary tools, resources and personnel to enable **DPO** to perform tasks.

Certain Indian banks have already begun hiring personnel for this role such as State Bank of India.[10]

2.3. Analysis & suggestions

The **DPO**'s role in compliance with privacy rights and creating transparency might have a significant impact on IT implementation costs and time, product launching, marketing initiatives, etc. The proposed legislation also stipulates the independence of the **DPO**, in particular their freedom to discharge their responsibilities without fear of penalties. The relationship to information security is especially important since the two areas will have an overlap of systems, data and functions which will be visible in policies and monitoring functions.

It is necessary to draw guidelines for this new role in banks while keeping the needs of both internal relations and cooperation in mind, as well as the overall guidance of organisation setup and embedding as specified by the proposed regulation.

We are of the view of that both the data fiduciary and the **DPO** as monitoring authorities need to be supported by almost the whole organization in order to achieve compliance. We see strong overlaps at least at the beginning of the journey with existing data management networks and already established roles and responsibilities.

Although the **Personal Data Protection Bill 2019** is yet to be passed in the parliament, we suggest a pre-study or implementation project to be adopted by banks in order to be prepared for compliance in the coming months. More importantly, regulations already been issued in *the KYC and the PMLA guidelines* in the past that require a position of a

[10] Recruitment of Data Protection Officer - https://recruitment.bank.sbi/crpd-sco-dpo-2020-21-02/apply

DPO. We recommend that the organisational positioning and collaboration model should be defined early in the implementation phase to in order to prevent a lack of guidance and support by the nominated board members, especially during first steps of implementation. We regard this as even more important because several strategic decisions will have to be that require the backing of senior management.

---

3. Para no. –

4.3.1. As part of overall governance framework, the board is responsible for overseeing a strong risk governance framework. A risk governance framework shall include well defined organisational responsibilities for risk management, typically referred to as ***'three lines of defence'*** viz.,

(a) First line of defence - the business line;
(b) Second line of defence - a risk management function and a compliance function independent from the first line of defence; and
(c) Third line of defence - an internal audit and vigilance function independent from the first and second lines of defence.

3.1. Background

The **Discussion Paper** by **RBI** under paragraph 4.3.1. provides for a risk governance framework for the commercial banks comprised of defined organisational responsibilities for better risk management. In this regard, reference is made for incorporating the **'three line of defence'** model within the organization wherein the responsibilities for each line of defence shall be well defined for better risk management. However, depending on the nature, size, complexity and risk profile of the bank the structure of the three lines of defence may vary.

The **Basel Committee on Banking Supervision** [hereinafter referred to as **'BCBS'**] in its guidelines on corporate governance in commercial banks dated October 2014 [hereinafter referred to as **'BCBS Guidelines'**] provided for incorporation of a risk governance framework within the organization comprised of well-defined organisational responsibilities for risk management as the 'three lines of defence'.[11] Business units namely the promoters and board of directors form the first line of defence. They take risks

[11] Paragraph 11, Report of the Based Committee on Banking Supervision on Corporate Governance principles of Banks (July, 2015)

and shall be responsible and accountable for the ongoing management of such risks. Their functions shall include identifying, assessing and reporting such exposures, taking into account the bank's risk appetite, policies, procedures and controls. The second line of defence shall be comprised of independent and effective risk management function to complements the business line's risk activities through monitoring and reporting responsibilities. The third line of defence shall consist of independent and effective internal audit function. Among other things, it shall provide independent review. As per Principle 9 of the **BCBS Guidelines** the internal auditors must be competent and appropriately trained.

3.2. Background research / International best practices / Interpretation of statute

The **Occasional paper 11** by Financial Stability Institute (FSI) on the **four lines of defence model for financial institutions** dated December, 2015 [hereinafter referred to as '**Occasional Paper**'], focused on governance and internal control mechanism of the banking institutions provides for a **'four lines of defence'** model. The paper endows a model providing for incorporation of external auditors and supervisors with a specific role in the organisational structure as the fourth line to enhance the internal control and risk management system.

Certain loopholes associated with the three line of defence model highlighted in the **Occasional Paper** are as follows:

i. The reports and accounts prepared by internal auditors tend to provide inadequate or subjective assessment by succumbing to hindsight bias associated with allegiance to board of directors, and often lacks independent and autonomous assessment.
ii. Lack of skills and expertise in the second line of defence.
iii. Lack of organisational independence of functions in second line of defence.

Incorporating external auditor into the defence and risk management framework shall mitigate the shortcomings within the traditional three-lines-of-defence model and increase the soundness and reliability of the risk management framework. Further, the existing structure shall benefit from enhanced information, knowledge and expertise of the external auditor. Thus, three-lines-of-defence model could be strengthened by making

supervisors and external auditors an inherent part of the internal control and risk monitoring systems as the fourth line of defence.

Additionally, in the absence of any underlying bias the external auditor shall prove to be effective in providing an autonomous assessment and to establish credibility of the financial statements presented by the internal auditing committee.

Reference to external experts in the Discussion Paper

The **Discussion Paper** on many occasions makes reference to external assessment but nowhere provides as to who shall be endowed with the responsibility of carrying the external assessment. The **Discussion Paper** on page 26 para 4 provides that:

> *"4. To support its own performance, the board shall carry out regular assessments – alone or with the assistance of external experts – of the board, its committees and individual board members."*

Further, the **Discussion Paper** on page 62 in para 11, provide for independent assessment with respect to compliance function to assure quality as follows:

> *"11. Incorporating all the above requirements, the board of the bank, through the RMCB, is responsible for establishing a compliance policy. This policy inter alia shall contain basic principles and shall explain the processes by which compliance risks are to be identified and thereafter managed across the organisation. The effectiveness of the compliance function will be subject to independent review by the RMCB at least annually. This will be in addition to the annual independent assessment of the compliance function by the internal audit function. Further, as part of quality assurance, once in three years an external assessment shall also be undertaken."*

3.3. Analysis & suggestions

Considering the loopholes associated with the three line of defence model, it is evident that commercial banks require a sound four-lines-of-defence model with an emphasis on the relationship between internal audit (third line of defence) and external audit and supervisors (both comprising the fourth line of defence). The close interaction between the internal audit function, external audit and supervisors is crucially important for better control of the internal system and manage the risk arising out of any loopholes created under the three line of defence model in a better and efficient manner.

Further, to maintain objectivity and independence of the external experts including external auditors and supervisors, the external experts shall be appointed for a short tenure ranging from three to five years. Further, the external auditor can be nominated by the Audit Committee, which shall then be approved by the Board after considering the credentials.

Apart from external auditors there shall be external supervising expert with respect to each committee for conducting policy and performance related regulatory audit in relation to each committee. The external experts shall be nominated by each committee in consultation with the regulator.

The roles performed by the external experts shall include the following:

i. To conduct ongoing supervision.
ii. To regularly examine the report submitted by the risk management committee and inform the board about any irregularities or risks. In case, the board does not remedy the situation within reasonable time then the expert shall be given the liberty to submit a report stating the emerging irregularities and risk before the regulator.
iii. To provide autonomous status of the affairs of things at various levels of the organizational risk management framework.
iv. External expert shall provide for assurance to the credibility of assessments done and reports submitted by the internal committees, thereby providing for a robust internal control mechanism to mitigate and manage the risks.

Recent significant risk incidents and bank frauds caused by misconduct in financial market operations indicate that banks need to further enhance corporate governance measures. But, most importantly, such incidents have led to a further prioritisation of governmental and supervisory agendas relating to the potential systemic implications of weak internal control systems. This calls for a prominence of external assessment mechanism. It also calls for closer cooperation between regulators, and external and internal auditors, so as to win back public trust in commercial banks.

4. Para no. –

"4.1. Responsibilities of the board - culture and values

2. *To put all the above into practice the board shall have oversight of:*

(iii) A whistle-blower policy which shall be well operationalised and widely communicated:

a. so that all stakeholders, including employees, shall be encouraged and are able to communicate bona fide concerns about illegal, unethical or questionable practices;

b. with adequate procedures and processes that allows bona fide concerns to be registered in a confidential manner;

c. with the board taking responsibility for ensuring that those who raise concerns are protected from detrimental treatment or reprisals;

d. with board oversight including approval of how, by whom legitimate material concerns shall be investigated and addressed by an objective independent internal or external body or the board itself"

4.1. Background

Under the **Discussion Paper,** it shall be the responsibility of the Board [as defined under paragraph 3 (1) (i)] to ensure *inter alia* to exercise oversight on the issue of complaints filed by whistleblowers, including the manner in which the investigation shall be carried out, who shall carry out this investigation [whether by an (i) independent internal body; (ii) external body or (iii) by the board itself].

The policy of dealing with whistleblower complaints find mention in various other paragraphs of the **Discussion Paper** as well. These include the following:

Where the board shall oversee integrity, independence and effectiveness of the bank's whistle-blower policies/procedures [para 4.5 (4) (ix)];

Where the Audit Committee of the Board (ACB) shall assist the board to ensure implementation of a credible whistle blower mechanism that allows employees, directors or any other person to report concerns about unethical behavior, violation of code of conduct, actual or suspected fraud. This mechanism (a) shall also include acceptance of anonymous complaints that appear prima facie bona-fide and (b)

shall deny protection to whistleblowers if the disclosures are made directly to the media. [para 5.1.1 (5) xxix.];

Where the RMCB will be responsible to introduce oversight of a risk culture dash board with reports to track progress across key culture attributes, indicators to track the frequency along with the treatment of both self-reported control and risk problems as well as whistle-blowing incidents [para 5.1.2 (3) xvi.];

Where a senior management functionary shall provide the board with information it needs to carry out its responsibilities, including to supervise senior management and to assess the quality of performance of a senior management functionary. In this regard, the concerned senior management functionary shall keep the board regularly and adequately informed of material matters, including issues raised because of the bank's whistleblowing procedure. [para 7.1 (8) (f)]

Where the bank shall formulate a vigil/whistle blower policy for directors, employees and third parties to report genuine concerns. The vigil mechanism shall provide for adequate safeguards against victimisation of director(s) or employee(s) or any other person who avail the mechanism and in appropriate or exceptional cases provide for direct access to the chair of the ACB/ chair of the board. [para 12 (2)]

The bank shall in case of breaches by staff: through an independent internal whistleblowing procedure in addition to instructions issued by the RBI under the Protected Disclosures Scheme for Private Sector and Foreign banks vide DO DBS. FrMC No. BC 5 /23.02.011 /2006-07 dated April 18, 2007 updated from time to time inform; [para 12 (3) (ii)]

4.2. Background research / International best practices / Interpretation of statute

Barclays Whistleblowing Case

In May 2018, the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) jointly fined Barclays CEO Jez Staley £642,430 for violating a conduct rule requiring individuals to act with due skill, care and diligence. The penalty related to his two attempts to identify whistleblowers who had raised concerns to Barclay's executives. The New York

State Department of Financial Services noted senior executives and members of the board of directors had failed to act properly and not proactively supervising the case.[12]

In addition to this, there have been various scams in India where senior officials are involved in execution.

In September 2015, US Deputy Attorney General Sally Quillian Yates issued a memorandum, **Individual Accountability for Corporate Wrongdoing (Yates Memo).**[13] The Yates Memo does not change fiduciary duties, but it is part of the framework that a board should consider in connection with its good faith obligation to see that the company has in place appropriate compliance systems and related information systems, reporting systems, and internal controls. Among other things, it also discusses the role of board members in dealing with whistleblower complaints. It states that the board must consider:

- risks to the company,
- the level of potential involvement in the misconduct by senior decision-makers,
- the substance of the allegations, and
- the way the allegations arise will influence decisions regarding the most efficient and effective way to conduct the investigation.

These decisions include whether the board should provide general oversight of a management-directed investigation or should itself be actively engaged in supervising the investigation with the assistance of outside counsel. While there are no absolute rules for when a board-driven investigation is required, as a general matter active board oversight and control of an internal investigation regarding allegations of misconduct is typically called for if the allegations:

- Relate to actions of the board members, in which case consideration needs to be given to whether comprising a board committee of disinterested directors is appropriate.
- Relate to actions of the CEO, the CFO, the general counsel, or other key executive officer.
- Involve conduct that could reasonably implicate one or more executive officers.

[12] DFS fines Barclays Bank PLC and New York branch $15 million following whistleblower investigation, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1812181

[13] Memorandum on 'Individual Accountability for Corporate Wrongdoing', https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations

In organizing a board-driven investigation, it is typical for a standing or special committee to provide oversight to the outside counsel hired for the matter. In such instances, the composition of the board committee should be independent of the company and the potential investigation targets and key witnesses. In addition to this, the directors should be disinterested to the extent possible. They should not be directly involved in the actions that are the subject of the investigation.

4.3. Analysis & suggestions

Hence, there is requirement to install similar safeguards in board-driven internal investigation, especially for those with involvement of a senior management or a board member. The commercial banks may be required to specifically provide a protocol to deal with such cases and how the board may be able to maintain a distance from the details of the proceedings.
