Bombay Chamber of Commerce & Industry

Suggestions and Comments on RBI Discussion Paper on 'Governance in Commercial Banks in India' by the Bombay Chamber of Commerce and Industry

15 July, 2020

We thank the Reserve Bank of India (the "**RBI**") for this opportunity to present our views and suggestions on the Discussion Paper on 'Governance in Commercial Banks in India' released on June 11, 2020. We understand that the discussion paper has been released in response to the recent instances of fallouts in the governance and management of several Indian commercial banks, and appreciate that it seeks to compensate the legislative drawbacks by aligning the management and governance principles as well as rules with established global standards on the subject. Set out below are our inputs on certain specific recommendations in the discussion paper.

Sl. No	Subject	Rationale / Recommendations
1.	**Strengthening Governance Standards in Banks**	**Rationale**: Regulations should predominantly be 'principle based' and not 'rule based.' **Recommendation**: The Regulations should primarily be in sync with the governance framework prescribed by the Securities and Exchange Board of India, including the corporate governance standards, especially in terms of the role and responsibilities of the board of directors (the "**Board**") and the Independent Directors as distinct from the operating / whole-time management responsibilities.
2.	**Role and Responsibilities of the Board**	**Rationale**: The role of the Board is to: (a) collectively supervise and provide broad direction including strategic inputs; and (b)

Sl. No	Subject	Rationale / Recommendations
		monitor the performance, and holding the operating management accountable and responsible for the results. The Board is also responsible for ensuring the public's trust and prevents any wrong doings that impact its reputation. It is also of course responsible for selecting and appointing the CEO / MD / whole-time directors with prior approval of the RBI and also assessing their performance. **<u>Recommendation (1)</u>:** The CEO and the whole-time directors (collectively, the "**Operating Management**") needs to be accountable for the affairs of the bank. The role and accountability of the Operating Management needs to be specified. Operations related functions, including Internal Audit, Compliance, Risk Management, Vigilance and HR need to report to the Operating Management, and the managers responsible for such functions needs to have a direct line of responsibility towards the Operating Management alone, and only a dotted line responsibility to the heads of their functional committees who may be independent directors. **<u>Recommendation (2)</u>:** In respect of appointment of the CEO / MD / whole- time directors, there should be no distinction between owner managers and professional managers and each of them should be appointed solely for their competence, experience and integrity by the Board which in any case is approved by the RBI at present. The only restriction on tenure of the CEO / MD should be the upper age limit that should apply to all whole-time directors. The Board or RBI should have the power for early termination in case on non-performance.

Sl. No	Subject	Rationale / Recommendations
		It may be noted that the earlier age limit of 65 (sixty five) years was only recently raised to 70 (seventy) years and the RBI may specify an upper age limit as it deems fit. The CEO must not overstay and needs to ensure proper succession planning, ahead of the scheduled retirement date. Succession planning in any case is an important role of the Board. If, however a term limit is felt necessary it may be set at 12 (twelve) years given the size and complexity of the Banks. In respect of Board Committees, while they may be headed by Independent Directors, there must be management representation at the senior most levels in all Committees to ensure implementation of its recommendations. The heads of Committees in case they are not happy with the persons in charge of the functions can ask management to replace / train / develop them but need not have a single point reporting to the heads of Committees alone, as this will result in dysfunctional governance, and create parallel levels of power and accountability. In addition, the Company Secretary should be responsible for recording the deliberations of all the Committees to ensure uniformity and information to the Board. Independent Directors may be members of more than one committee including the non-executive Chairman to enable proper discussions of the Committee deliberations at the full Board.
3.	**On the overall governance**	**Rationale**: It is imperative that the governance norms also apply to **public sector banks** which are around 65-70% of the

Sl. No	Subject	Rationale / Recommendations
		Banking Industry to ensure requirement of the overall governance improvements. **Recommendation (1)**: All Banks and NBFCs must have at least two Whole- time Directors – one Managing Director (MD) and one Executive Director (ED). Operational and staff heads must report to one of them in a heterogeneous format, i.e. a mix of some staff, operational and business roles. **Recommendation (2)**: A MD should not be permitted to have more than 2 (two) terms, with each term being limited to 5 (five) years and the total permissible tenure for an individual be limited to 10 (ten) years. The tenures of NEDs and the CEO should be preferably asynchronous. An ED promoted as the CEO should be permitted to have a total tenure of 12 (twelve) years on the Board. The advantage of having asynchronous tenures is twofold – (i) seamless transition in the event of a mishap; and (ii) having at least one internal candidate in the fray, (subject to performance and other criteria), in a planned succession scenario.
4.	**Compliance, Internal Audit and Vigilance**	**Rationale**: Similar tenure restrictions of a total not exceeding 10/12 years for the Chief Financial Officer and the Chief Risk Officer positions always held by different people as mandated by RBI. (Beyond such tenures, people become overconfident or at least blind-sided). **Recommendation (1)**: The following roles should always be held by separate persons – Compliance, Internal Audit and Vigilance, Fraud

Sl. No	Subject	Rationale / Recommendations
		Control Unit ("**FCU**") & Investigation. (This is akin to a similar separation mandated by RBI for the Chief Information Officer (the "**CIO**") and Chief Information Security Officer (the "**CISO**")). **<u>Recommendation (2)</u>**: Personnel at banks who undertake vigilance, fraud control and investigation functions should be duly qualified personnel who are trained in *Forensics and Fraud Investigation*. For instance, he / she can be a certified fraud examiner, alumnus of the Gujarat State Forensic University or equivalent, or worked in the government in a similar role etc. **<u>Recommendation (3)</u>**: The Supervision Department of RBI must conduct 'surprise' audits occasionally in addition to the annual 'Inspection'. The Supervision Department of RBI must meet the following people on a one on one basis at least once a year, (in addition to the routine post inspection closure meeting with the leadership team and the Audit Committee Chair), - (a) Statutory Auditor, (b) Audit Committee Chair (annual), (c) Risk Committee Chair (annual), (d) Internal Audit Head (biannual), (e) Others such as Vigilance Head, CFO, CRO, CIO, CISO etc. (on a random basis). **<u>Recommendation (4)</u>**: Breaking the precedent of approving the first named, (required to be submitted in order of preference) choice of Statutory Auditor. **<u>Recommendation (5)</u>**:

Sl. No	Subject	Rationale / Recommendations
		Given that Companies (Auditor's Report) Order, 2016 (CARO) does not apply to banks, certain matters must be identified to be compulsorily addressed by statutory auditors of banks as a part of the annual financial statements. Some of these matters could be capital adequacy ratio, cash liquidity ratio, credit appraisal, restructuring, recovery and resolution. **<u>Recommendation (6)</u>**: Making an independent IT and Data Security audit mandatory once every 2 (two) years. **<u>Recommendation (7)</u>**: Regarding Audit Committee (AC) – The MD / CEO is not permitted to be a member of the Audit Committee Meeting (in line with regulations), but to suggest that the default position should be his/her non-attendance in the Audit Committee Meetings, is too far-fetched and completely preposterous. On the contrary, presence of the CEO / MD should be mandatory unless for a certain matter the Committee feels that a discussion should happen to his/her exclusion. The Audit Committee should have the freedom to meet anyone in camera. And, there must be minutes for these, which is presently not the practice. **<u>Recommendation (8)</u>**: Regarding Risk Management Committee (RMC) - Most RMC focus on non-financial risks as the financial risks are exhaustively covered by AC; they do not do a deep dive on people risks as they are covered by the nomination and remuneration committee (the "**NRC**") and IT Risks as they are covered by the IT Committee. The RMC needs to deal with aggregation of risks and get the big picture right; it needs to focus on external risks, business strategy and

Sl. No	Subject	Rationale / Recommendations
		model risks, compliance risks, operational risks. Therefore, RMC cannot be complete without the membership of the MD/ CEO. Chairpersonship of the RMC has to be of an Independent Director; its membership can comprise of members from AC, NRC, IT and Credit Committee, so that the entire range of risks are represented in a common forum; (common members can be inducted to avoid an unwieldy committee). **<u>Recommendation (9)</u>**: Regarding Executive Accountability - (i) All executive positions must ultimately report to the MD / CEO. (ii) All operational managers of critical functions (such as: internal audit, compliance, risk management, vigilance and HR) should have a direct reporting line to the MD / CEO or any designated whole-time directors along with only a dotted line responsibility to the heads of their relevant functional committees of the Board (who may, in some cases, such as the audit committee be Independent Directors). (iii) All appointments for the critical function heads such as: certified internal auditor, chief financial officer or chief risk officer should be cleared by the NRC and the respective committee of the Board. For instance, by the RMC for chief risk officer and by the audit committee for certified internal auditor and chief financial officer. (iv) Similarly, appraisals and exits for such critical function heads should be monitored and even signed off, if necessary, by the NRC and the relevant committees as well.