Data has become a critical governance and risk management asset for financial institutions, prompting regulators globally to adopt more structured approaches to data governance. On 15 July 2026, the Reserve Bank of India (RBI) released a draft 'Guidance on Regulatory Expectations for Data Governance' (Draft Guidance). Recognising data as a strategic organisational asset, the Draft Guidance draws on evolving international standards, including the Basel Committee on Banking Supervision's Principles for Effective Risk Data Aggregation and Risk Reporting, to establish broad regulatory expectations for data governance by RBI regulated entities (REs). It addresses key aspects of data governance, including governance frameworks, roles and responsibilities, data lifecycle management, architecture, and third-party arrangements. We analysis the key features of the Draft Guidance below.

1. Applicability

The Draft Guidance has a broad applicability and is proposed to apply to: (i) commercial banks (including foreign banks); (ii) small finance banks; (iii) payments banks; (iv) local area banks; (v) regional rural banks; (vi) urban co-operative banks; (vii) rural co-operative banks; (viii) all non-banking financial companies; (ix) all-India financial institutions (EXIM Bank, NABARD, NaBFID, NHB, and SIDBI); (x) asset reconstruction companies registered with the RBI; and (xi) credit information companies. It is to be read alongside other applicable RBI directions, which will prevail in the event of any inconsistency.

2. Definition of 'Data'

The Draft Guidance defines "data" broadly to include any recorded concepts, facts, information, opinion, or instructions, regardless of form or the medium on which they are recorded, that are capable of being communicated, interpreted, or processed by humans or automated means.

Comments: The breadth of this definition brings virtually all categories of information within the scope of the Draft Guidance. REs will therefore need review and, where necessary, strengthen their existing practices governing the aggregation, processing, storage, transformation and disposal of data.

3. Data Governance Requirements

(i) **Data Governance Framework**: Every RE must establish a Data Governance Framework (DGF) covering all data, proportionate to its size, complexity, business model, and information technology (IT) / information systems (IS) environment. Notably, the DGF must comply with the Digital Personal Data Protection Act, 2023 (DPDP Act) and be reviewed on an annual basis, or more frequently as required.

(ii) **Data Governance Committee**: Every RE must constitute a board-level Data Governance Committee (DGC) responsible for overseeing implementation of the DGF and formulating and reviewing data governance policies. Alternatively, the RE can assign these responsibilities to an existing board-level committee.

(iii) **Data Roles and Responsibilities**: REs must establish a dedicated Data Function headed by a sufficiently senior officer, not below the rank of Chief General Manager or its equivalent, to serve as the central point of coordination for implementing and interpreting the DGF. Furthermore, three distinct roles must be designated amongst individuals / functions / teams for governance, including – (a) Data Owners, accountable for governance outcomes within each data domain (such as customer, product, and financial data); (b) Data Stewards, responsible for operationalising governance requirements; and (c) Data Custodians, responsible for technical management of the data environment, including access controls, storage, backup, and disaster recovery.

Comments: These requirements represent a shift from viewing data as a technology or compliance concern to treating it as a governance asset with clearly defined ownership and accountability throughout its lifecycle. While many REs already maintain board-level IT governance structures under existing RBI directions, they are likely to integrate the DGC into those existing committees to avoid duplicative oversight, provided the committee has the expertise to discharge its expanded data governance responsibilities effectively.

4. Data Governance Obligations

(i) **Data Classification**: REs must establish a framework for classification of data based on factors such as risk, criticality to business operations, customer impact, and business and financial impact.

Comments: The proposed classification framework aligns RBI's approach with similar requirements prescribed by other financial sector regulators. For instance, the Insurance Regulatory and Development Authority of India requires insurers and insurance intermediaries to classify all data into four buckets – 'public', 'internal', 'restricted', or 'confidential'. While the Draft Guidance does not prescribe specific categories, it is likely to encourage greater consistency in data classification practices across the financial services sector.

(ii) **Data Risk Management**: REs must integrate data risk into their overall risk management framework, guided by principles of accountability, integrity, auditability, transparency, traceability, proportionality, and standardisation. Cross-border data operations, including processing, storage, transfer, and usage, must be assessed and managed to ensure they do not impair the RE's ability to access, retrieve, or manage its data.

Comments: Foreign banks and Indian banks with offshore operations / branches will need to review their data governance policies in order to comply with the Draft Guidance. REs will also be required to amend existing contractual arrangements with overseas group entities and offshore third-party service providers to ensure data retrieval, access and audit rights.

(iii) **Data Processing, Sharing and Transformation**: REs must ensure that all processing and sharing of data, whether internally or with third parties, is undertaken in accordance with approved rules, logic and standards.

Comments: Under the Draft Guidance, data should only be created, acquired, processed, retained and shared in alignment with clearly defined and legitimate business purposes. This requires REs to establish documented governance processes for intra-group and intra-organisational data sharing, supported by robust approval mechanisms and data minimisation practices throughout the data lifecycle.

5. Data Quality Management

(i) **Data Quality Management Processes**: The Draft Guidance requires REs to establish data quality management processes proportionate to the criticality, sensitivity and classification of data, ensuring that deficiencies in data quality do not compromise decision-making, risk management or regulatory reporting. Data quality metrics and persistent quality issues must be reported to the DGC at quarterly or more frequent intervals as needed.

(ii) **Single Source of Truth (SSOT)**: REs must identify and maintain a single authoritative source for each data element to avoid inconsistent or duplicative records across systems. All downstream systems, models, reports and business processes must rely on this authoritative source to preserve consistency and accuracy throughout the data lifecycle. REs must also implement reconciliation mechanisms to identify and correct discrepancies between the SSOT and downstream data.

(iii) **Metadata and Data Lineage**: REs must maintain key metadata for all data, including its source, purpose, owner, classification, permitted use and retention requirements, from the point at which it is first captured or generated. This metadata must accompany the data as it moves across systems and be updated whenever the data is modified, combined or used to generate new data.

Comments: These requirements reflect RBI's recognition that the quality of underlying data is fundamental to sound decision-making, effective risk management and accurate regulatory reporting. Accordingly, REs should incorporate these requirements into their DGF by defining measurable data quality standards (such as accuracy, completeness, consistency and timeliness) and implementing processes to monitor and remediate deficiencies on an ongoing basis. REs should also ensure that their management information systems can generate reliable and auditable data quality metrics for reporting to the DGC.

6. Third-Party Arrangements

REs remain responsible for the governance of data shared with third parties, including group entities. Data may be shared only for defined and approved purposes by designated personnel, with access restricted on a 'need to know' basis. REs must also ensure traceability to the single source of truth (SSOT), safeguards against unauthorised reuse or duplication, appropriate non-disclosure obligations in third-party agreements, and ongoing monitoring and periodic audits of third-party systems, including by CERT-In empanelled auditors.

Comments: These requirements are likely to have the greatest impact on lending service providers (LSPs), digital lending platforms and other technology vendors that process or supply data to REs. The Draft Guidance also requires that externally sourced data must meet the same governance standards as internal data belonging to REs. Therefore, LSPs which were previously subject to relatively limited data governance requirements, will need to upgrade their technical capabilities. Existing agreements with third-party service providers will need to be amended, and technology service providers will become subject to these flow-down obligations. Further, the proposed mandates relating to non-disclosure clauses, periodic audits of third-party systems, and ongoing monitoring will necessitate a thorough review of existing data-sharing arrangements and LSP agreements, including those within group entities. Fintechs that supply alternative data for credit scoring, including social media analytics, transaction data, and device data, should expect increased due diligence from RE partners.

7. Alignment with the DPDP Act

While the Draft Guidance is broader than the DPDP Act, applying to all types of data and data touchpoints, the DGF formulated by REs must also comply with the DPDP Act. Furthermore, the Draft Guidance's focus on consent management, permissible usage, data classification, retention and secure disposal maps closely to the concepts of lawful purpose, consent or legitimate use, storage limitation and accountability under the DPDP Act. A practical approach for REs would be to build a common data governance control layer, with DPDP-specific controls embedded within it for personal data.

8. Overlap with RBI Cyber Security and IT Governance Requirements

RBI's existing cyber security and information technology framework already require banks to maintain a board-approved cyber security policy calibrated to the complexity of their business and acceptable risk levels. It also addresses IT governance, controls, assurance, business continuity and cyber resilience. The Draft Guidance does not replace these requirements and instead creates a bridge between cyber controls and organisation-level data management. A potential area of overlap is role duplication, since existing RBI directions already address access controls, encryption, audit, incident reporting, third-party monitoring, business continuity, and disaster recovery from a cybersecurity perspective. REs should therefore integrate the mandatory requirements of the DGF into their existing cyber security, IT risk, outsourcing, business continuity and information security policies, rather than create a standalone framework that could result in inconsistent ownership, duplicative committee reporting or conflicting remediation timelines.

Concluding Remarks

The Draft Guidance proposes a broader, more holistic framework that covers all data touchpoints across the entire data lifecycle, going beyond existing cyber security requirements. While this creates room for duplication between cyber security and data governance obligations, it also presents an opportunity for

REs to consolidate overlapping cyber, IT, outsourcing and privacy compliance requirements into a single, coherent framework.

As the Draft Guidance is currently open for public consultation, REs may consider submitting comments on areas of concern, including regulatory overlaps, the application of proportionality to smaller institutions, transition timelines, and the practical feasibility of ensuring accuracy of data and metadata at all stages of the data lifecycle.

- *Smita Jha (Partner); Viti Bansal (Associate) and Sameep Baral (Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 340+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**