DSCI
PROMOTING DATA PROTECTION

Brief on

RBI'S DRAFT GUIDANCE ON REGULATORY EXPECTATIONS FOR DATA GOVERNANCE

Brief: The Reserve Bank of India's Draft Guidance on Regulatory Expectations for Data Governance

The Reserve Bank of India (RBI) released the draft Guidance on Regulatory Expectations for Data Governance (Draft Guidance) in July 2026. The Draft Guidance provides a framework for Regulated Entities (REs)[1] to manage data as a vital asset, addressing information management weaknesses and outlining expectations for data governance, including governance structures, roles, life cycle, architecture, and third-party arrangements.

Applicability

The Draft Guidance applies to Commercial Banks (including Foreign Banks), Small Finance Banks, Payments Banks, Local Area Banks, Regional Rural Banks, Urban and Rural Co-operative Banks, Non-Banking Financial Companies across all four layers (Base, Middle, Upper, and Top), the All-India Financial Institutions (Export-Import Bank of India, National Bank for Agriculture and Rural Development, National Bank for Financing Infrastructure and Development, National Housing Bank, and Small Industries Development Bank of India), Asset Reconstruction Companies registered under the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002, and Credit Information Companies under the Credit Information Companies (Regulation) Act, 2005.

Key Definitions

- **Data Governance:** The policies, roles, standards, structures, processes, and controls put in place to ensure accountability, integrity, quality, accessibility, traceability, protection, and appropriate usage of data across its lifecycle.
- **Data Architecture:** The structural design of data assets, systems, repositories, interfaces, and flows supporting the creation, collection, processing, integration, aggregation, transformation, storage, and reporting of data, including technology infrastructure.
- **Data Classification:** The systematic categorization of data according to criteria laid out in the Data Governance Framework (DGF), reflecting its criticality, sensitivity and confidentiality, potential business and financial impact, and governance requirements.
- **Data Lineage:** The documented traceability of data from its origin, through aggregation, transformation, and usage, to its final destination.
- **Data Risk:** The risk of adverse outcomes arising from deficiencies in data, or in its management across the lifecycle, including data architecture.
- **Single Source of Truth:** A single designated authoritative source for a specific data element within the RE.

Governance

The Draft Guidance proposes that REs implement a DGF that is proportionate to their size and complexity, aligned with their risk management framework, and compliant with the Digital

[1] Any financial institution that is licensed, registered, and overseen by the Reserve Bank of India.

Personal Data Protection Act, 2023 (DPDP Act) and the DPDP Rules, 2025. The DGF is to be reviewed annually or more frequently as required.

- **Board Oversight:** The Board should oversee the DGF, while a Board-level Data Governance Committee (DGC), or an existing Board committee assigned the responsibility, formulates policies covering the scope of data governance, data architecture, data risk, ownership and accountability across the lifecycle, data quality, classification, and third-party arrangements. Material issues, such as breaches and conflicts, are to be presented to the Board.
- **Data Governance Executive Committee:** A Data Governance Executive Committee, with representation from the Data Function, IT, Information Security, business verticals, Risk Management, and Compliance, is responsible for implementing and operationalizing the DGF. It reviews instances of non-compliance, addresses structural gaps and inter-functional conflicts, oversees classification methodology and the identification of critical data elements, and approves material exceptions.
- **Data Risk Management:** REs must manage data risk as part of their overall risk framework, on the stated principles of accountability, integrity, auditability, transparency, traceability, proportionality, and standardization. Risk assessment should extend to third-party arrangements and to cross-border processing, storage, transfer, and use, with the expectation that cross-border operations do not impair the RE's ability to access, retrieve, and manage its data.

The Draft Guidance states that the DGF must undergo periodic internal and external audits, including, where applicable, by auditors empaneled by the Indian Computer Emergency Response Team (CERT-In), on a risk-based approach to frequency, scope, and depth, with reports placed before the Audit Committee of the Board.

Organisational Structure - Data Roles and Responsibilities

Under the Draft Guidance, the following organisational structure is proposed along with the responsibilities that each role must undertake:

- **Data Function:** A central coordination unit headed by an officer of at least Chief General Manager rank. It develops metrics to monitor DGF effectiveness, resolves conflicts on data definitions, classification, SSOT designation, metadata, lineage, and consent management, and ensures documentation of standards, processes, and taxonomies.
- **Data Owner:** Accountable for a specific data domain, including its definition, classification, and quality, as well as intended use and sharing, key data rules, oversight of metadata and lineage, designation of the SSOT, and approval of changes, exceptions, and remediation plans. The role applies even where a domain spans multiple functions, units, or systems.
- **Data Steward:** Positioned within business units to handle day-to-day operations and connect business logic to technical systems, monitor data flows, and report domain-specific metrics and material issues to the Data Owner.

- **Data Custodian:** Responsible for technical management, including access controls and user entitlements, storage, transmission, backups, reconciliation and root cause analysis, retention and disposal processes, and business continuity and disaster recovery.
- **Mapping of Roles and Responsibilities:** REs should maintain a documented mapping of roles to processes and lifecycle stages, covering accountability, execution responsibility, points of consultation, and escalation, updated on material internal or regulatory change.

Data Lifecycle

Governance should be applied across the entire data lifecycle, from origination to disposal, covering metadata, lineage, data rules and logic, dependencies between data elements and systems, and consent management for customer data.

- **Data Origination and Capture:** Data should be captured for legitimate purposes with foundational attributes (ownership, classification, usage intent, and consent for customer data) established at the point of origination. Capture systems should be capable of enforcing validation, completeness, and consistency checks commensurate with the criticality and classification of the data, and externally sourced data should meet governance standards equivalent to those applied to internally generated data.
- **Data Processing, Sharing, and Transformation:** Transformations should use approved rules and preserve data meaning, with security controls such as encryption, tokenization, data loss prevention, and anonymization protecting data at rest and in transit. Transformation logic should be subject to impact assessment prior to implementation, and outputs should remain traceable to the source and appropriately classified.
- **Data Retention, Archival, and Disposal:** REs should have a formal Data Retention and Archival Policy ensuring data remains usable throughout its retention period and is disposed of securely. Retention periods should be justified by business, legal, regulatory, or audit requirements. Archival systems should preserve links to data definitions, classifications, and lineage and should not impede timely retrieval for supervisory, audit, or investigative purposes.

Data Architecture

- **Single Source of Truth:** REs should designate one authoritative source for every data element, with no parallel or competing sources for the same element, and all downstream systems, models, and business processes deriving from it. The architectural model may be centralized, federated, or hybrid. Designations and changes require approval by the executive committee, documentation, reporting to the DGC for information, and a reconciliation mechanism to resolve inconsistencies with downstream data.
- **Metadata and Data Lineage:** Minimum foundational metadata (source system, purpose of collection, owner, classification, retention and permitted usage) should be created at capture and move downstream without loss of attributes created at source. Metadata should be updated on transformation to record the source-to-derived relationship, the

purpose and nature of the transformation, and any change in classification or accessibility. For high-volume system-generated data, such as logs and audit trails, metadata may be maintained in proportion to the volume.

- **Data Classification:** Data should be categorized based on its criticality to business operations, criticality to customers, sensitivity (including personal data), confidentiality, and legal and regulatory relevance. The DGF should address the impact of aggregation, enrichment, and derivation on materiality, risk profile, or sensitivity.
- **Data Quality Management:** REs should develop metrics across multiple dimensions to ensure data is fit for use and to identify trends, emerging risks, and control gaps, and report persistent quality issues to the DGC at least quarterly.

Third-Party Arrangements

The Draft Guidance proposes the following, with respect to third-party arrangements for sharing data:

- **Responsibility and Accountability:** REs remain fully responsible for the governance of data shared with third parties, including group entities.[2]
- **Permitted Sharing of Data:** Sharing must be for defined and approved purposes only, effected by designated personnel, on a 'need to know' basis via secure channels that employ encryption, authentication, and access controls, auto-deletion, and de-duplication controls, with agreements that include non-disclosure clauses.
- **Access Controls:** Controls over access, use, and deletion must account for the classification and criticality of the data, whether it comprises personal or customer-related information, the nature and extent of third-party use, the potential impact in the event of misuse or loss, and consent when customer data is involved.
- **Oversight:** Shared data must remain traceable to the internal SSOT, and entities must conduct periodic audits of third-party systems, either directly or through external auditors, including CERT-In empaneled auditors, with ongoing monitoring and periodic reassessment where data is critical.

[2] "Group" carries the same meaning assigned under the Reserve Bank of India (Commercial Banks - Concentration Risk Management) Directions, 2025, which means an arrangement of two or more entities linked together through relationships like subsidiaries, associates, joint ventures, or related parties.