Summary of DSCI's Submissions on the Draft Guidance on Regulatory Expectations for Data Governance

The Data Security Council of India ("DSCI") has provided feedback on the Reserve Bank of India's Draft Guidance on Regulatory Expectations for Data Governance ("Draft Guidance"). DSCI appreciates the objective of establishing a coherent, accountable and auditable framework for data governance across the financial sector, including the proposed allocation of ownership and custodianship, data classification, lifecycle controls, metadata and lineage, data quality, and oversight of third-party arrangements. DSCI also welcomes the alignment with the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the recognition that data governance obligations extend to the service provider ecosystem on which Regulated Entities ("REs") increasingly depend.

While supporting these objectives, DSCI has offered targeted recommendations to provide greater clarity and proportionality, facilitate auditable implementation across REs of differing sizes and technological maturity, and avoid situations in which an RE could comply with the Draft Guidance while simultaneously falling short of another statutory or regulatory obligation.

Evolving Data Governance Considerations

Concern: The Draft Guidance is largely based on traditional concepts such as data elements, metadata, catalogues and lineage, which may not adequately address the contextual and semantic nature of data used by AI systems.

Recommendation: DSCI recommends adopting an AI-era approach that incorporates semantic metadata, knowledge structures, data relationships, and AI-enabled lineage and traceability, while retaining core requirements for data quality, security, privacy, and accountability.

Implementation Timelines

Concern: The Draft Guidance does not specify an effective date or transition period, even though requirements such as a Single Source of Truth ("SSOT") designation, metadata propagation, and lineage may necessitate substantial architectural changes, particularly for REs with legacy systems.

Recommendation: DSCI recommends a phased implementation schedule, with timelines calibrated to the nature and complexity of the requirement and entity category, and the option for REs to submit Board-approved implementation roadmaps during the transition.

Considerations for Unstructured Data

Concern: Although unstructured and semi-structured data are recognized, the Draft Guidance does not clearly explain how requirements such as classification, ownership, metadata and SSOT would apply to documents, emails, recordings and images.

Recommendation: DSCI recommends expressly bringing such data within the relevant governance requirements and permitting an authoritative repository or source where element-level SSOT is not practicable, while recognizing the role of AI and semantic technologies in identifying and consolidating data.

Third-Party System Considerations

Concern: Some REs, particularly smaller entities, may not have direct administrative control over data held on multi-tenant platforms operated by service providers, limiting their ability to conduct discovery, catalogue data or establish an SSOT.

Recommendation: DSCI recommends clarifying that accountability remains with the RE, while controls may be executed contractually by the service provider through defined deliverables such as catalogue extracts, lineage documentation, quality metrics and access logs.

Data Lifecycle Coverage and Non-Production Environments

Concern: The Draft Guidance addresses data at rest and in transit but does not expressly cover production data replicated into development, testing, user acceptance and analytics environments, where controls may be weaker, and copies may proliferate without adequate inventory.

Recommendation: DSCI recommends that production data used in non-production environments be masked, tokenized or synthesized, with exceptions appropriately approved, and that copies be inventoried and subjected to equivalent retention and disposal controls.

Audit of Third-Party Systems

Concern: The requirement for audits by auditors empaneled by the Indian Computer Emergency Response Team ("CERT-In") may be difficult to implement at scale, as CERT-In empanelment is focused on information security rather than the broader competencies required for data governance audits.

Recommendation: DSCI recommends allowing auditors with demonstrated qualifications and expertise in data governance, data protection, privacy, information security and audit and assurance, rather than making CERT-In empanelment the sole criterion.

Data Function and Organisational Proportionality

Concern: Requiring every RE to establish a separate Data Function headed by a senior officer may impose disproportionate organisational and resourcing requirements on smaller REs, including Regional Rural Banks and Urban Co-operative Banks.

Recommendation: DSCI recommends a proportionate, risk-based approach that allows REs to assign these responsibilities to an existing function, committee, or suitably senior officer, provided that clear accountability and authority are established.

Data Origination and Capture

Concern: The Draft Guidance does not expressly address data captured through Business Correspondents, agents, kiosks, and other assisted-service channels, which may involve offline connectivity, biometric authentication, and specific risks related to validation, consent, metadata, and lineage.

Recommendation: DSCI recommends explicit governance requirements at these points of capture, including validation, authentication, consent, secure transmission, reconciliation and controls to preserve data integrity and lineage through ingestion into the RE's systems.

Metadata and Inter-Entity Data Flows

Concern: Metadata requirements may work within individual institutions but break down when data moves between entities, as different organisations use separate catalogues and systems that do not exchange metadata in a standard form.

Recommendation: DSCI recommends a minimum common set of metadata attributes for material inter-entity data flows, covering source, classification, lawful basis, permitted use and retention, with phased implementation to account for existing technology architectures.