Comments to the Draft Guidance on Regulatory Expectations for Data Governance.

On 15 July 2026, the Reserve Bank of India (RBI) released the **"Draft Guidance on Regulatory Expectations for Data Governance"** (hereafter **"the Guidance"**). This Guidance establishes expectations for data governance across banks, NBFCs, cooperative banks, financial institutions, asset reconstruction companies and credit information companies. It requires a Board-approved Data Governance Framework (DGF) aligned with risk management, supported by Board oversight, Executive Committee and assigned Data Owners, Stewards and Custodians. Data must be governed throughout its lifecycle, from origination, processing to retention and deletion.

Summary of Recommendations

1. **Despite multiple frameworks, customer harms from data misuse may remain unaddressed.** Typically, the data protection frameworks and authorities oversee the issue of redressing and compensating customers for privacy-led financial harms. However, the Digital Personal Data Protection Act, 2023 and the attendant Data Protection Board, do not allow for compensating customers on account of data-driven financial losses. Under such circumstances, the RBI Integrated Ombudsman Scheme, 2026 promises to be a viable channel. However, it may be prohibitively onerous for an aggrieved customer to establish data-driven harms such as discriminatory loan pricing. These outcomes often become intricately linked to the lender's "commercial judgment", which (rightly) remains out of the scope of the Integrated Ombudsman. As such, it is currently unclear how and if at all, customers can be compensated for data-related harms that result in financial losses such as in discriminatory loan pricing, losses due to financial breach etc. The Guidance could consider defining "harm", consistently across this and the model risk management framework, categorically empower and equip the Ombudsman to accept complaints of harm, assess them through appropriate technological tools and share the burden of proof more symmetrically between the Ombudsman and the complainant.

2. **Proportionate regulations may be complemented with minimum standards.** It is very welcome that the Guidance is anchored in a strong notion of proportionality. It recommends that the safeguards be proportionate to the size, complexity, IT infrastructure of the organisation and the criticality of the data. However, advances in artificial intelligence (AI) have rendered cyber-offensive strategies cheap and easily accessible. These attacks often pry on the weakest link in the value chain. An employee email, for instance or shared drives that do not necessarily strike as critical may become easy targets for AI-led cyber-attacks. The Guidance could, therefore, consider laying out minimum, baseline safeguards for all organisations, assets and data types, and any safeguards beyond the baseline should be in tandem with the risk carried by the organisation or the asset or the data type. Where smaller organisations struggle for monetary or tech resources to meet the baseline safeguards, development funds and meaningful capacity building exercises could be considered to help them bridge the gap. A readily exploitable vulnerability anywhere has the potential to cascade into a grave system-wide threat.

3. **Harmonizing related and adjacent frameworks to build an integrated data risk management framework.** We appreciate that the Guidance is one of the many instruments in the suite of frameworks designed to address data-related risks. It is essential that the different frameworks operate in harmony, do not pose conflicts or require duplication of efforts. For instance, incidents' are likely to be interconnected, exhibiting dual properties of cyber and data incidents. In those circumstances, it is important for Regulated Entities (REs) to understand the integrated protocol to enable thorough investigation, timely communication to regulators and customers, and customer remediation.

Key Recommendations

1. Despite multiple frameworks, customer harms from data misuse may remain unaddressed.

We welcome the emphasis on factoring in customer harm in determining the criticality of data. However, we note that this implicit recognition does not translate into express redress pathways for customers to seek redress when they suffer data-driven financial harm. Under the current regulatory structure, data-related harms can fall between the responsibilities of the Data Protection Board, financial service providers, and the RBI Ombudsman.

In principle, claims arising from misuse of personal data would be handled under the privacy and data protection regime. In India, however, the Data Protection Board is not empowered to compensate affected customers or order direct payouts. Section 34 of the Digital Personal Data Protection Act, 2023 requires all penalties imposed by the Board to be transferred to the Consolidated Fund of India. As a result, the enforcement framework may penalise non-compliance without addressing the financial loss suffered by individual customers.

Customers may approach the RBI Ombudsman where data misuse leads to a clear financial loss—for example, when discriminatory profiling results in a higher interest rate. In practice, however, this route faces two major challenges:

First, data-driven harms such as data breaches and misuse are often not visible to customers. Even when they become aware of a breach, customers may struggle to link it to a specific financial loss.[1] As a result, many harms may never reach the formal grievance system.

Second, even when a customer first raises a complaint with the financial service provider and then approaches the Ombudsman, it is often unclear whether the issue reflects a commercial decision or actionable customer harm. For instance, a customer may show that they were charged a higher, discriminatory interest rate, conduct that is prohibited under the Fair Practices Code and may amount to a deficiency in service. However, the provider could argue that the pricing decision falls within commercial discretion and is therefore outside the Ombudsman's jurisdiction. Experience from other jurisdictions also suggests that establishing discrimination places a prohibitively high burden of proof on the customer. It may require the complainant to use advanced statistics and proprietary data to establish the discrimination. These are unattainable for ordinary customers and risk rendering the grievance redress mechanisms redundant.[2] These challenges risk excluding precisely the types of data-driven harms that the DGF aims to address.

Thus, we recommend:

- **Defining 'harms' as used in the Draft Model Risk Management guidelines and this Guidance**. As opposed to deficiency of service, harms may be outcome-based, specifying the adverse outcomes that customers may have encountered even when they are unable to establish their cause. The burden of proof needs also to be symmetrically distributed between the customer and the system. The Consumer Financial Protection Bureau of the USA, for instance,

[1] https://www.proquest.com/openview/ce9f514a7d96978b46bc13d9ffd05e5c/1?pq-origsite=gscholar&cbl=36043
[2] https://arxiv.org/html/2512.20753v2

can bring enforcement actions under fair lending laws like the Equal Credit Opportunity Act without requiring an individual consumer to prove personal, quantifiable financial harm.[3,4,5]

- **Affording non-monetary reliefs during data incidents**. While dispensing monetary compensation for breaches may be long-drawn processes, requiring high threshold of causality, temporary relief measures can help contain losses more effectively and instantaneously. REs could also introduce an additional layer of authentication for transactions or other communications with customers until they have taken adequate measures to mitigate the harms arising from a data breach or other cybercrime affecting the RE. Such authentication measures could include an additional layer of password checks or biometric systems, or specific telephone numbers for the customer to authenticate or verify transactions with the RE. These measures - while temporary - can serve as a critical enabler of trust by providing customers with greater assurance and helping to address concerns or hesitations regarding the risks or harms they may face as a result of the breach or cybercrime. Additionally, the Monetary Authority of Singapore, for instances, offers a kill switch that customers can activate when they suspect malicious activity.[6]

2. Proportionate regulations may be complemented with minimum standards.

We appreciate that the Guidance adopts a proportionate approach to data governance expectations given its application to a diverse range of REs including cooperative banks, regional rural banks, smaller banks and NBFCs. Specifically, it recognises that a) the DGF is proportionate to the size, complexity, business model, and IT set-up of the RE and b) the controls in place are commensurate with the criticality, risk, and reliance placed upon the data.

However, advancements in AI-enabled cyber offensive strategies are stress-testing the principle of proportionality in cybersecurity.[7]This is particularly significant because when considered from a supply-chain perspective, data risk presents an inherent asymmetry between the defenders (REs) and potential attackers. The rapid growth in digital financial services has significantly expanded the volume, velocity and complexity of data being generated, processed, shared and stored by an RE. While an RE may be required to manage the operational, financial and customer risks arising across its data environment, an attacker may need to identify and exploit a single point of weakness or vulnerability. Consequently, counterintuitive to the logic of proportionality, data assessed or treated as low risk may become an attractive target precisely because it is subject to weaker safeguards.

For instance, an RE may have a mature DGF for core banking data, while sensitive information residing in places such as, digital conversations, shared drives, emails, data lakes or other peripheral repositories may remain less governed and turn out to be the attack vector. Such data repositories may include sensitive customer information or operational business information that may not have been initially classified as high risk, but which can nevertheless provide surface area for a breach. Thus, a narrow application of a risk-based proportionality approach may create inadvertent weak links within an RE's data environment. This is especially relevant in context of AI advancements, where the barriers for attackers have been lowered and AI can be used to autonomously expose vulnerabilities in operating systems, browsers and network services.

---

[3] https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-files-amicus-brief-cfpb-action-opposing-efforts-weaken-equal-credit-opportunity-act
[4] https://www.consumerfinance.gov/archive/blog/addressing-credit-discrimination/
[5] https://www.nclc.org/cfpb-guts-fair-lending/
[6] https://www.mas.gov.sg/news/parliamentary-replies/2026/written-reply-to-pqs-on-srf-and-fraud-surveillance
[7] https://dvararesearch.com/mitigating-ai-related-harms-in-finance-from-model-governance-to-systemic-resilience-context-setting/

Thus, we recommend:

- **Proportionality should operate on top of a baseline of minimum data governance safeguards** applicable to all REs rather than determine whether baseline safeguards apply at all. While we recognise that investing in baseline resilience would require significant infrastructure, resources and capabilities from REs, and that REs differ considerably in terms of technological maturity, operational capacity and financial resources. There is scope for wider ecosystem, through the SROs, industry bodies and larger REs to play a role in supporting the smaller institutions institutional capacity. However, at the same time, a complete absence of baseline safeguards for data assessed as lower risk could create vulnerabilities and governance gaps, whose consequences are not necessarily commensurate with low-risk perception. Other jurisdictions are finding means to support smaller organisations in meeting the asks of data governance. For example, Japan's Ministry of Economy, Trade and Industry and the Small and Medium Enterprise Agency drive small business AI adoption primarily through the Digitalization & AI Introduction Subsidy, which provides grants ranging from JPY 50,000 to JPY 4.5 million to help small and medium enterprises purchase pre-registered.[8] The RBI also has adopted similar measures, most recently by instituting the Payment Infrastructure Development Fund in 2021 to subsidise deployment of payment infrastructure in Teir 3-6 cities. A similar fund with the mandate of helping less suave institutions meet the baseline safeguards could reap outsize dividends in terms of system-level defence.[9]

3. **Harmonizing related and adjacent frameworks to provide an integrated data risk management framework.** We appreciate that the Guidance is one of the many instruments in the suite of frameworks designed to address data-related risks. It is essential that the different frameworks operate in harmony, do not pose conflicts or require duplication of efforts. Specifically, we recommend:

   - **Recognizing the interconnectedness of risks and consolidating attendant frameworks**. Data and cyber incidents are closely interconnected and co-occur, for instance, cyber-attacks that cause data breaches. In these instances, both cybersecurity and data governance protocols would get activated. It is important that where such incidents co-occur, these protocols are consolidated, providing a seamless standard operating procedure (SoP) that avoids confusion, duplication, and ensures all stakeholders receive relevant information and relief. In the context of incident reporting, the Financial Stability Board has recognised siloed approaches as to incident reporting as ineffective, given the divergence in establishment of impact and severity thresholds, divergence in scope of what is an incident to be reported. It has come up with a Reporting Format that seeks to reduce duplication of an REs efforts while at the same time improving quality and consistency of information reported.[10]

   - **Rationalizing duplication and resolving tensions if any**. The Guidance mandates creating/ delegation of governance frameworks to a Board-level Data Governance Committee and Executive Committee. The Cybersecurity Directions mandate an IT Strategy Committee, IT Steering Committee, Information Security Committee and Audit Committee oversight of IS audit. Both frameworks also require recurring Board or committee reporting. Without coordination, and considering the interconnected nature of issues, the same issue could pass through several committees, or consolidation could inadvertently remove a mandatory cyber committee. European

[8] https://oecd.ai/en/dashboards/policy-initiatives/digitalization-and-ai-introduction-subsidy-2026
[9] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12009&Mode=0
[10] https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/

Union also provides a useful illustration in this regard. The Digital Operational and Resilience Act, consolidated and harmonised ICT risk management practices across EU for financial entities.[11] The European Banking Authority narrowed down the scope of its existing Guidelines on ICT and security risk management measures, to avoid duplication and rationalise requirements with regulatory instruments with overlapping scope.[12]

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A333%3AFULL&uri=uriserv%3AOJ.L_.2022.333.01.0001.01.ENG&utm

[12] https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application