Summary of DSCI Submission on RBI's Draft Guidance on Regulatory Principles for Model Risk Management, 2026

The Data Security Council of India (DSCI) submitted a comprehensive set of recommendations in the month of July 2026 to the Reserve Bank of India (RBI) in response to the RBI's Draft Guidance on Model Risk Management (MRM) for **AI/ML deployments by regulated entities (REs)**, including banks, non-banking financial companies (NBFCs), and cooperative banks.

The submission, prepared with the support of our banking members and other relevant industry stakeholders across the Financial Services, Artificial Intelligence and Cybersecurity Ecosystem, identified significant areas where the Draft Guidance may offer clarity, consistency, or operational specificity and corresponding recommendations to strengthen the framework ahead of implementation.

Key Highlights

1. DSCI highlighted the opportunity to bring both the RBI's FREE-AI Report and the Draft Guidance closer together on some of the operational detail - committee structures and the triggers for red-teaming, for instance, are framed slightly differently across the two. That's a natural outcome of two frameworks evolving in parallel rather than any real divergence in intent. Our submission suggests that **a shared taxonomy and governance architecture** across both would make it easier for institutions and enterprises implementing them side by side, and we'd see that as a useful refinement RBI can build in as the guidance is finalized, not a gap that needs fixing.
2. **Terms** such as "material impact," "foundational AI models," "frontier AI models," and "high or equivalent risk" appear in the draft **without clear definition**, which may lead smaller institutions to under-classify - and larger institutions to over-classify - the AI systems that fall under regulatory scope.
3. **Third-party and vendor accountability** may need recalibration. With most regulated entities (REs) sourcing AI capabilities from third-party and foundational model providers rather than building in-house capabilities, we note that the current draft holds REs fully accountable for model outcomes even where vendors may restrict access to model internals or contractually limit liability. The submission recommends a shift toward proportionate obligations tied to demonstrated governance diligence, along with clarity on who qualifies as an "independent validator" for closed or black-box models.
4. Our submission covers **critical safety mechanisms, i.e., human oversight protocols, AI kill-switches, cybersecurity controls, and incident reporting** which are named in the draft but does not specify on defined timelines, personnel competency standards, and AI-specific threat coverage, including risks such as model inversion, data poisoning, and prompt injection. We further note that kill-switch mechanisms themselves currently carry no prescribed security safeguards despite being high-value targets for compromise.
5. **Model inventory security** is an unaddressed gap. While the Draft Guidance mandates ten-year retention of decommissioned models, DSCI notes it does not classify the model inventory

which maps an institution's entire analytical infrastructure as sensitive data requiring access controls or encryption.

6. **Smaller institutions need a proportional compliance path.** The submission recommends that RBI may introduce scalability provisions so that smaller regulated entities, such as urban cooperative banks, are not held to the same governance and validation rigor as large banks operating hundreds of models, while preserving strong safeguards for high-risk deployments across the board.