Key Takeaways/Learnings

a. It was emphasized that regulatory advisories spanning multiple control domains require a correspondingly comprehensive, multi-domain response with clear ownership and timelines — a patching-only, governance-only, or detection-only response, however well executed, is insufficient on its own.

b. Frontier AI compresses response windows to hours. Participants understood that reconnaissance, exploit development and source-code analysis that previously took days to weeks can now occur in minutes to hours, requiring organizations to match adversary speed with AI-enabled defensive tooling and pre-approved emergency remediation timelines.

c. It was highlighted that simultaneous but seemingly disparate signals — reconnaissance, phishing, malware, identity anomalies and data staging — occurring within a short window should trigger enterprise-level crisis governance immediately, rather than being managed as isolated technical events by separate teams.

d. The exercise also highlighted the growing significance of identity security as a foundational element of cyber defence. Privileged identities continue to represent high-value targets for sophisticated adversaries, particularly when combined with AI-generated phishing campaigns and deepfake-enabled social engineering. Participants recognised that phishing-resistant authentication mechanisms, Privileged Access Management (PAM), continuous authentication monitoring and rigorous identity governance should form integral components of enterprise cybersecurity strategies.

e. Participants recognized that reducing the public digital footprint of the organization (technical documentation, staff information, project details) is a necessary structural defense against LLM-enabled, hyper-personalized social engineering — not a substitute for, but a complement to, phishing simulations and staff training.

f. Crisis communication and regulatory disclosure are parallel, not sequential. It was underscored that coordinated public communication and LODR Regulation 30 materiality assessment must proceed simultaneously and cannot be deferred until an incident is fully understood or resolved.

g. Business continuity and disaster recovery planning emerged as another significant area of focus. The exercise demonstrated that successful restoration of services requires careful validation of system integrity, phased recovery, enhanced monitoring and structured executive oversight. Organisations should avoid prioritising rapid restoration at the expense of long-term security assurance.

h. Participants converged on the view that restoring operations should follow verified integrity checks, credential resets and telemetry validation in stages, with explicit executive risk acceptance, rather than either premature full resumption or indefinite, uncoordinated delay.

i. Log retention and data localization are live compliance risks. Discussion surfaced that reliance on foreign cloud providers for historical log storage, without assured India-based retrievability within a reasonable time, can itself constitute non-compliance with CERT-In's 180-day retention and localization requirements — a gap organization should proactively assess ahead of any incident.

j. It was clarified that the “harvest now, decrypt later” threat model must be addressed today — through cryptographic inventory, PQC readiness assessment and board-level briefing, rather than deferred to a future technology refresh cycle.

k. Participants noted that Regulated Entities frequently share common vendors and infrastructure providers, such that a vulnerability or compromise at one entity can propagate across the sector; this reinforced the value of information sharing among REs, MIIs and regulators, and of exercises of this nature in building a cohesive, sector-wide defensive posture.