Key Takeaways/Learnings

a) It was observed that human negligence and lack of awareness continue to constitute a significant vulnerability despite the presence of advanced technological controls. Generational variations in cyber hygiene were also identified, necessitating continuous capacity-building and awareness initiatives across all workforce levels.

b) A consensus emerged on the need to transition from traditional Endpoint Detection and Response (EDR) mechanisms to Extended Detection and Response (XDR) systems integrated with AI-driven SOAR solutions. The establishment of defined Recovery Time Objectives (RTOs) for cyber incidents was recommended to enhance operational preparedness.

c) Insider knowledge, even in the absence of direct collusion, was rated 4.5/5 by participants in perceived threat severity. It was emphasized that publicly available information—such as procurement notices and system specifications—can be exploited by adversaries, underscoring the necessity for controlled disclosure policies and the adoption of Zero Trust Architecture (ZTA).

d) Approximately 54% of participants identified AI-based behavioural monitoring as the most effective control for preventing insider-style financial fraud. The integration of such systems with ISO 42001 governance standards was strongly recommended to ensure transparency, accountability, and responsible AI deployment.

e) The exercise revealed that only 8% of participating institutions employ automatic API key rotation, while 49% rely solely on scope-limited permissions. This indicates a substantial gap in safeguarding block chain-integrated architectures and necessitates the implementation of multi-layered validation and centralized API gateway enforcement.

f) It was noted that 89% of the participating institutions favour a comprehensive incident response protocol encompassing account freezing, RTGS traffic blocking, and regulatory notifications. The absence of a standardized audit framework was identified as a challenge that may delay root-cause analysis and affect response uniformity.

g) The survey reflected that 59% of the participating organizations remain only partially prepared for AI-driven disinformation or deep fake incidents, while 5% reported complete unpreparedness. The adoption of AI-enabled social media scanners, rapid content takedown agreements, and digital identity protection for key personnel was recommended.

h) A significant 78% of participating organizations acknowledged the absence of real-time AI-based detection capabilities for deep fakes and synthetic media.

The establishment of centralized, cross-platform fact-checking mechanisms and the development of unified mandates with dedicated funding were suggested as corrective measures.

i) The need for uniform incident reporting norms, awareness checklists, and structured regulatory communication was reiterated. Early engagement with regulators was noted to reduce reputational risks, provided it does not hinder immediate containment measures.

j) It was emphasized that cybersecurity resilience must be achieved through a balanced integration of people, processes, and technology. Collaborative engagement among regulators, financial institutions, and technology partners was deemed essential to establish a sustainable defence-in-depth ecosystem.