Information Technology and Digital Risk Management Committee (ITDRMC)
Terms of Reference

1. Purpose

The Information Technology and Digital Risk Management Committee ("ITDRMC" or the "Committee") is established by the Board of Directors in compliance with the amended NBFC regulatory requirements. The purpose of ITDRMC is to assist the Board of Directors in overseeing and strengthening the Company's governance, risk management, control environment, operational resilience and strategic initiatives relating to:

- Information Technology and digital operations;
- Cybersecurity and technology resilience;
- Emerging technology adoption and associated risks; and
- Regulatory compliance in respect of IT and digital risk.

to ensure alignment with applicable SECP requirements (including Regulation 67AC of the NBFC & Notified Entities Regulations, 2008, as applicable) and leading industry practices.

2. Authority

The Committee is authorized by the Board to:

1. Request information: Seek any information, reports, records, including minutes of the IT Steering Committee of the management and presentations from management and/or external parties relevant to its mandate.
2. Commission independent reviews (as needed): Direct management to commission independent assessments (e.g., penetration testing, vulnerability assessments, IT security reviews, third-party/vendor assurance, independent IT audits) and require documented remediation plans with owners and timelines.
3. Review and recommend to the Board: Review and recommend for Board approval: (a) enterprise-level IT/cyber/digital risk governance policies and frameworks; (b) material risk appetite/tolerance proposals for technology and digital channels (where applicable); and (c) material outsourcing arrangements and significant strategic IT initiatives or investments.
4. Approve within delegated authority: Approve procedures, standards, and operating frameworks within the scope delegated by the Board (where such delegation is explicitly provided).
5. Co-opt external expertise: Co-opt external experts/advisors with relevant knowledge and experience, subject to Board approval and conflict-of-interest safeguards.
6. Oversee ongoing vendor efficiency and risk management for critical IT/Digital service providers.
7. Review and approve the formulation of Business Continuity Planning (BCP) and Disaster Recovery Strategy Plan (DRP) mechanisms.

3. Composition

3.1 Chair

- The Committee shall be chaired by an Independent Director of the Board.

3.2 Members

The Committee shall include:

A) Board members (voting members)

- The Independent Director (Chair); and
- Other Board member(s) as appointed by the Board, including at least one Board member meeting the applicable digital/emerging technology expertise requirement under Regulation 67AC(3)(b)(i), as applicable from time to time.

B) Senior management representatives (standing attendees / members as designated and mandatory)

- Chief Executive Officer (CEO);
- Head of Information Technology / CTO (or representative from outsourced IT service provider, where applicable);
- Head of Risk Management / CRO;
- Head of Compliance / CCO.

3.3 Invitees (non-voting, by invitation)

The Committee may invite any relevant individual(s) to attend meetings, including Internal Audit, Operations/Business owners for digital channels, Information Security/CISO function (if separate), Legal, Finance, and key vendor representatives (as needed).

Where co-opted experts are included as members, their role shall be advisory in nature unless otherwise approved by the Board.

3.4 Secretariat

- The Company Secretary (or nominee) shall act as the Committee Secretary and be responsible for agenda preparation, paper circulation, minutes, and action tracking.

4. Roles and Responsibilities

The Committee shall oversee the following areas:

4.1 IT & Digital Strategy Oversight

- Review and provide input on IT strategy, digital initiatives, and emerging technology adoption; ensure alignment with business objectives, risk appetite, and regulatory expectations.
- Review material technology roadmaps and significant changes affecting customer channels, critical systems, data architecture, and security posture.

4.2 Cybersecurity Oversight

- Oversee the cybersecurity governance framework, including policies/standards for access management, privileged access, endpoint security, patching, logging/monitoring, encryption, and secure configuration baselines.
- Review results of independent security testing (e.g., penetration tests, vulnerability assessments) and track closure of high/critical findings.
- Review key cybersecurity risk indicators and trends (e.g., incidents, phishing metrics, patch compliance, endpoint health, critical vulnerabilities, security exceptions).

4.3 Digital/IT Risk Management

- Identify, assess, and monitor IT/digital risks (cybersecurity, operational resilience, emerging technology risks) and review mitigation plans and residual risk.
- Ensure that IT/digital risk is integrated with the enterprise risk management framework and reported consistently.

4.4 BCP/DRP and Operational Resilience

- Oversee the design, adequacy, and implementation of BCP/DRP policies and mechanisms, including:
  - Business impact analysis and recovery objectives (RTO/RPO) for critical services;
  - At least annual DR testing (or more frequently for critical changes), and review of test results and remediation plans.

4.5 Vendor Efficiency and Third-Party Risk Management

- Oversee vendor efficiency and risk management for technology and digital service providers, including:
  - Due diligence and risk assessment for critical vendors (including outsourced IT);
  - Contract safeguards (security requirements, audit rights, incident notification, data protection, subcontracting controls);
  - Performance against SLAs, concentration risk, and exit/transition planning for critical providers.

4.6 Incident Response Planning and Escalation

- Oversee incident response planning for material IT/cyber incidents, including review of incident response playbooks and crisis escalation protocols.
- Review post-incident reviews ("lessons learned") for material incidents and track corrective actions.
- Require prompt escalation to the Committee Chair for any material incident, with an appropriate special meeting where warranted.

4.7 Regulatory Compliance (IT/Digital)

- Ensure oversight of compliance with applicable SECP requirements and other relevant legal/regulatory obligations impacting IT/digital operations.
- Review key regulatory observations relating to IT/cyber/digital operations and management's remediation status.

4.8 IT Controls and Assurance

- Review the adequacy of IT general controls (ITGCs) and technology-related internal controls supporting financial reporting, investor services, and operational reliability.
- Coordinate with Internal Audit to ensure appropriate IT audit coverage and review closure status of high-risk audit observations.

4.9 Reporting to the Board

- Provide quarterly reporting to the Board (or more frequently if required) on IT/digital risk matters, including material incidents, top risks, key remediation items, and any Board approvals/recommendations required.

5. Meetings

5.1 Frequency

- The Committee shall meet at least quarterly, and additionally as required (including following a material IT/cyber incident).

5.2 Agenda and Papers

- Agenda and papers should be circulated sufficiently in advance to enable effective review, except in urgent circumstances.
- A standing action log shall be maintained and reviewed at each meeting.

5.3 Quorum

- Quorum shall be a majority of voting (Board) members, including the Committee Chair (Independent Director) or, in the Chair's absence, another Independent Director designated by the Board for that meeting.

5.4 Minutes

- Minutes shall be documented by the Secretary, approved by the Chair, and tabled at the next Committee meeting and/or shared with the Board as appropriate.

6. Conflicts of Interest and Confidentiality

- Members and invitees (including any co-opted experts) shall maintain strict confidentiality of Committee materials and deliberations.
- Any actual or potential conflict of interest shall be disclosed promptly; the Chair may require recusal from relevant agenda items, particularly for co-opted experts or vendor-linked attendees.

7. Review of Terms of Reference

- These Terms of Reference shall be reviewed at least annually by the Committee and submitted to the Board for approval and updated as required to reflect evolving regulatory requirements and industry practices.