

---

# Information Technology Committee Charter

# Contents

- 1. INTRODUCTION ..... 3
- 2. PURPOSE ..... 3
- 3. IT GOVERNANCE FRAMEWORK ..... 3
- 4. RESPONSIBILITIES OF THE INFORMATION TECHNOLOGY COMMITTEE ..... 4
  - 4.1. AUTHORITY ..... 4
  - 4.2. PROJECT OVERSIGNHT AND ADVOCACY ..... 4
  - 4.3. ACCOUNTABILITY ..... 4
  - 4.4. EXPLORE & SAFEGUARD ..... 4
- 5. COMPOSITION OF THE INFORMATION TECHNOLOGY COMMITEE ..... 4
- 6. QUORUM ..... 4

## 1. INTRODUCTION

---

The Board of Directors of the IBL Ltd ("IBL") acknowledges the critical role of IT governance in ensuring the effective and strategic management of technology across the Group. In line with **Principle 4 of the Code of Corporate Governance**, which states that "The Board is responsible for the governance of the organisation's information strategy, information technology and information security", the **IT Committee (ITC)** was established in February 2021 as a sub-committee of the **Finance, Audit & Risk Committee (FARC)** to monitor and evaluate significant IT investments, expenditures, and risks.

Over a 4 year period, the Group's IT governance maturity has significantly improved as a result of the stronger integration of IT governance into the overall governance structures of **IBL Operations (BU's)** at the management board level, and **IT Committees** have been established in IBL's subsidiaries and sub-subsidiaries (GC's). To align with this evolution, the **IT Committee's mandate has shifted from a policy-making and monitoring role to an explore and safeguard role**, ensuring a proactive approach to innovation while maintaining oversight on security and governance. As a consequence, the ITC's meeting frequency initially aligned to the FARC and Board will be reduced to twice annually.

## 2. PURPOSE

---

The IT Committee provides oversight on technology governance, ensuring that IT investments and digital initiatives are aligned with the Group's business strategy and risk management framework. The Committee's role encompasses **exploration of emerging technologies, promoting best practices, overseeing IT investments** while safeguarding **information security, and regulatory compliance**.

## 3. IT GOVERNANCE FRAMEWORK

---

The responsibility for the implementation of the IT governance framework should be delegated to management.

This framework should apply to :

- IBL Head Office
- IBL Operations (BU's)
- IBL Subsidiaries & sub-subsidiaries – with ownership from 50% to 100% (GC's). IBL Subsidiaries, being those companies falling under the definition of Section 3 of the Companies Act 2001 of Mauritius, as amended from time to time. IBL Subsidiaries shall include IBL Sub-Subsidiaries. (GCs)

This framework should ensure that:

- IT governance is embedded at all levels: IBL Head Office, Operations (BU's), and Subsidiaries & Sub-subsidiaries (GC's).
- IT internal controls are adequate. Independent assurance on the effectiveness of the IT internal controls are provided by the Internal services and External Auditors.
- IT strategy should be aligned to the business strategy and the Board may identify opportunities and solutions to be implemented throughout the Group as a global IT improvement strategy.
- Suitably qualified and experienced Chief Information Officers (CIO)/ Head of Technology/IT Managers are duly appointed by the relevant CEO/COO/GM.
- IT goals and metrics are defined and communicated. The performance of IT processes and practices are monitored against the agreed objectives and reported regularly.
- The optimal investment is made in IT, costs are managed and the return on investment is measured by the relevant boards and oversight committees at BU's and GC's level. Where applicable synergies between IT initiatives are enabled and IT choices are in the best interest of the organisation as a whole.
- IT risks are identified and adequately addressed in line with IBL Ltd Risk Management framework. IBL ensures that it has adequate business resilience arrangements in place for disaster recovery and assurance has been provided to the Board.
- IT resources are sourced optimally and legitimately.
- Processes and procedures are in place to ensure that IBL's IT Assets are managed, maintained, replaced and disposed effectively and in accordance to applicable IT policies.
- Infrastructure, systems and policies are in place for the management of information which includes information security and information privacy.

## 4. RESPONSIBILITIES OF THE INFORMATION TECHNOLOGY COMMITTEE

---

The implementation, management and evolution of the IT governance framework is delegated to the Information Technology Committee's ('ITC's'). The terms of reference of the ITC are summarised as follows:

### 4.1. AUTHORITY

- Monitor IT governance maturity at BU and GC levels
- Guide the evolution of IT policies and governance charters
- Provide strategic direction for IT governance, aligning it with business needs
- Ensure that adequate resources are available to meet the IT governance framework objective/s
- Set up sub committees as required to respond to specific governance aspects

### 4.2. PROJECT OVERSIGHT AND ADVOCACY

- Oversee execution of projects identified as strategic for the Group
- Provide change leadership for the successful implementation of the Digital Transformation Programme
- Capture opportunities and reinforce the Digital Transformation Programme as a learning organisation, reflecting upon and improving on its performance on the basis of experience to date
- Appointment of any consultant or advisor to undertake any specific project or assignments at Group level in relation to the Digital Transformation Programme

### 4.3. ACCOUNTABILITY

- Mitigate business continuity and disaster recovery risk
- Communicate clear IT goals and objectives to BU's and GC's
- Ensure the objectives and policies are clear and disseminated to the relevant stakeholders
- Implement risk mitigation actions for critical risks and report to the Board.
- Review reports on the status of the IT governance and risk profile
  - Report to the FARC and the Board on
    - Strategic technological projects
    - Cybersecurity posture and risk mitigation strategies.
    - Technology related critical risks and incidents
    - Deviations from policies resulting from an «apply or explain» governance principle

### 4.4. EXPLORE & SAFEGUARD

- Explore and assess emerging technologies (AI, cloud computing, cybersecurity, etc.).
- Evaluate digital transformation opportunities and strategic IT investments.
- Safeguard IT security and regulatory compliance across the Group.
- Drive innovation while managing technology risks effectively.

## 5. COMPOSITION OF THE INFORMATION TECHNOLOGY COMMITTEE

---

Members of the ITC include:

- An IBL Ltd Non-Executive Director – Chairperson
- Group Head of Technology and Sustainability
- Head of Business Development M&A
- Group Head of Operations
- Group Head of Corporate Services
- Head of Financial Services
- Head of Technology & Transformation
- Heads of Business Units and other experts of business processes or technologies to be invited as and when required

## 6. QUORUM

---

A quorum is required to conduct an ITC meeting. The following members must be present:

- IBL Ltd Non-Executive Director (NED)
- Group Head of Operations
- Group Head of Technology & Sustainability
- Head of Technology & Transformation