RISK MANAGEMENT

RISK MANAGEMENT CHAPTER IN ANNUAL REPORT 2024

The VICOM Group's Risk Management Framework provides a systematic process for the Group and its Business Units (BUs) to identify and review the nature and complexity of the risks involved in their business operations and to prioritise resources to manage them. The Group is committed to enhancing shareholder value through growth that is sustainable and profitable while taking measured and well-considered risks.

The Group's approach to risk management is underpinned by several key principles:

- The risk management process is a continuous and iterative one, as the Group's businesses and operating environments are dynamic. Risk identification, assessment, and risk management practices are reviewed and updated regularly to manage risks proactively.

- We promote and inculcate risk awareness among all our employees by embedding risk management processes into day-to-day business operations and setting an appropriate tone at the top. Regular briefings, continuous education and training, as well as communications through various forums on risk management are carried out to sustain a risk-informed and risk-aware culture in the Group.

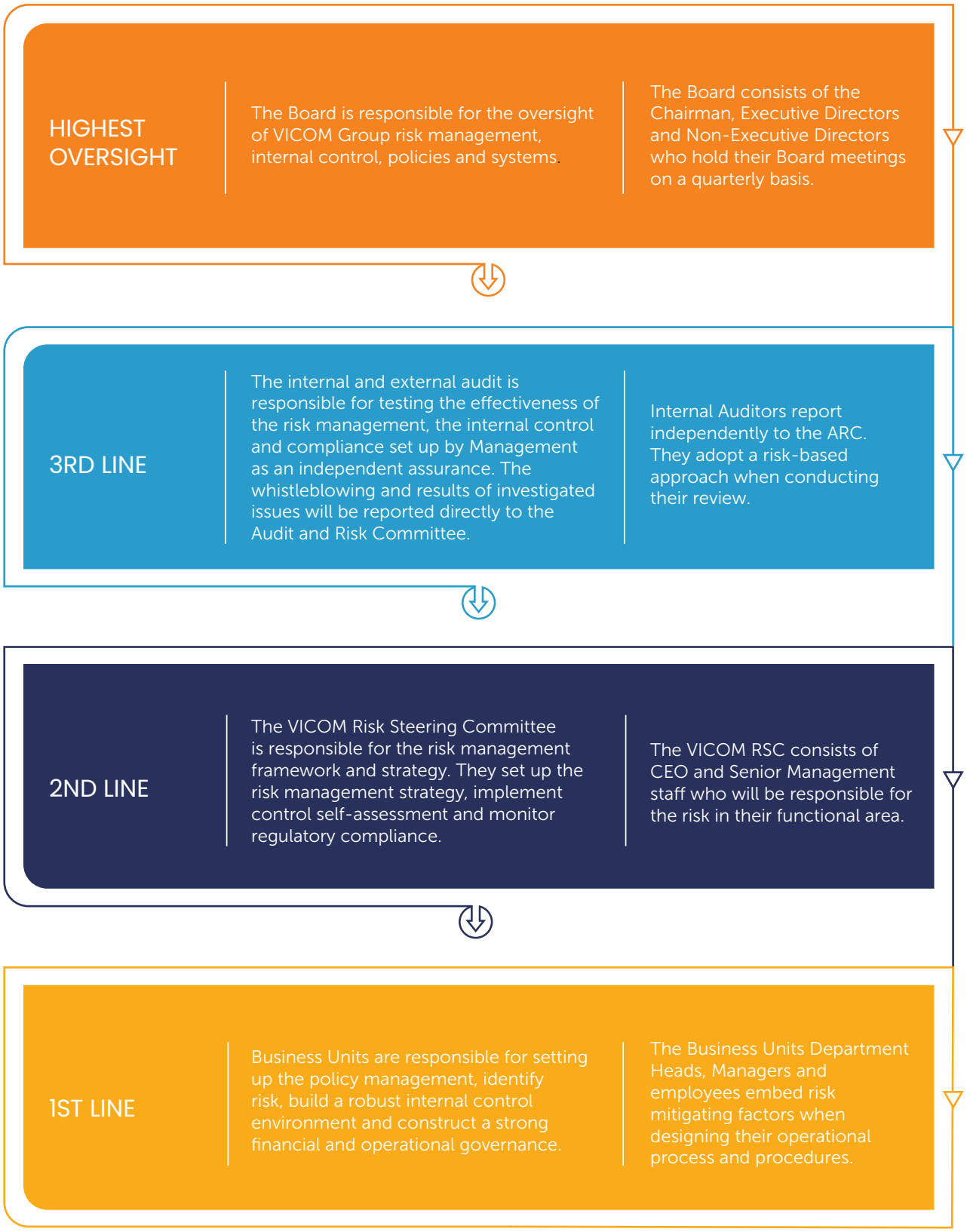
- Ownership and accountability for the risk management process are clearly defined and assigned to the BUs, departments, and individuals. Managers at each level have intimate knowledge of their businesses and take ownership of risk management, with stewardship retained at Senior Management.

In line with the current dynamics in the global and local economies, the Group also reviewed its risk management policies and processes and refreshed the risk registers for the Group and its BUs. These refreshed risk registers reflect the current risk portfolios of the Group in mitigating business and operational risks while exploiting opportunities in the present technology-driven economy.

Risk Management Model

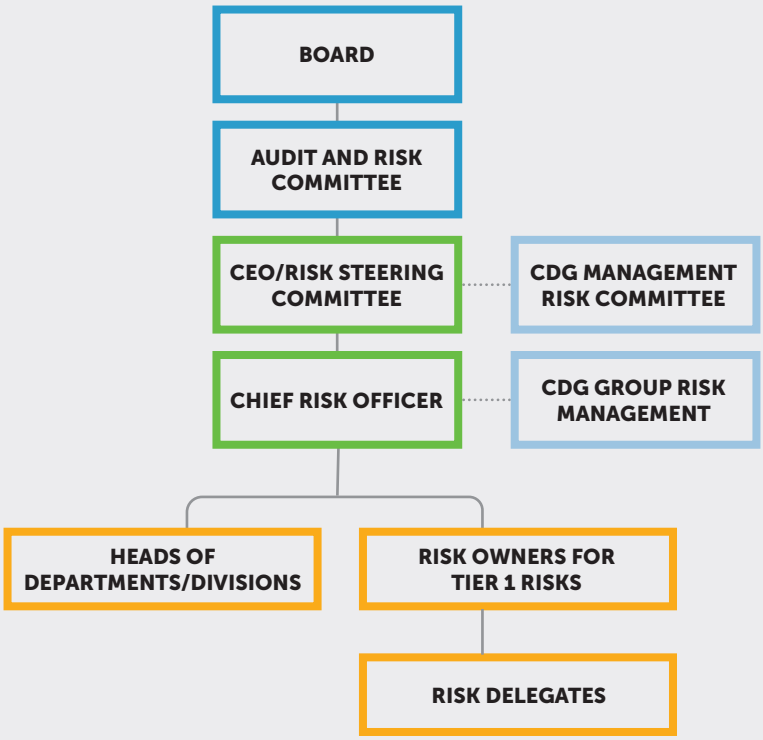
The Group has adopted the "Four Lines of Defence" as our assurance framework in risk management. The Board has the ultimate responsibility for the governance of risk and sets the tone and direction for the Group. It delegates the oversight of risk management and internal control to the Audit and Risk Committee (ARC). The ARC helps the Board ensure that the Management establishes and enforces a sound system of risk management and internal controls to safeguard the Group's assets and shareholders' interests and that a robust system and processes are in place to identify and manage risks enterprise-wide.

Sharing Risk Management Responsibilities Through The "Four Lines Of Defence" (LOD)



RISK MANAGEMENT

Vicom Group Risk Management Structure



The Group CEO chairs the Risk Steering Committee (RSC), and members are drawn from BUs' senior management staff. He is also a member of ComfortDelGro's Management Risk Committee and has appointed a Risk Officer to work closely with ComfortDelGro's Group Risk Management to ensure alignment and that the Risk Management Framework is diligently implemented. Key risks for the Group are identified and presented to the ARC and the Board annually.

The Group RSC meetings serve as the platform where Group and BU-level risks are shared and discussed, including the progress of the respective risk treatment action plans and the key risk indicators. Different BUs will have different risk profiles but the risk assessment methodology, approach and processes are aligned with that of the Group, including the risk taxonomy. BUs are expected to continually refine and review their risk profiles and to detect and report any emerging risks promptly. This is to prevent unexpected risks and disruptions to our business operations and growth.

Group Risk Profile

The key risks faced by the Group, the relevant mitigating factors, and how they are managed are set out in the paragraphs below. The risks are categorised into Operational, Financial, Compliance, and Information Technology risks.

Operational Risks

Safety Risk
The safety of our customers and employees has always been our top priority. To achieve assurance, we regularly update and revisit our safety policies and procedures. We apply zero tolerance to non-compliance with these policies. We also carry out risk assessment and safety inspections on our premises and conduct fire drills as part of our preventive measures.

The Group will continue to comply with the latest requirements imposed by the Ministry of Manpower (MOM).

Competition Risk
Competition remains keen in the Testing, Inspection, and Certification (TIC) industry, as evidenced by the 487 accredited laboratories, 138 accredited Inspection Bodies, and 203 accredited Certification Bodies. To remain relevant, the Group and its BUs will have to improve our offerings and services, enhance efficiency and productivity through digitalisation and automation, and leverage on partnerships and collaborations to enhance our value propositions. The Group must also continue to exploit technology to diversify its revenue stream and venture into a business that is still in its infancy.

Economic cycle
Changes in economic conditions may impact the businesses in terms of customer demand and the cost of providing the services. We manage these risks by continuously scanning and monitoring the economic climate and its impact across industries. We also monitor demand trends, cost structures, and operating margins closely. Expenses are managed in the light of revenue patterns and changing market conditions. Where possible, revenue risks are mitigated by diversifying revenue streams and reducing dependency on a specific industrial sector.

Operational Performance Risk
The Group and its BUs have established the requisite frameworks, standard operating procedures and Business Continuity Plans (BCPs) to ensure operational effectiveness and enable compliance and control of our various business operations and services. The BCPs are to mitigate the risks of disruption and catastrophic loss to our operations, people, information databases and other assets. Such risks can arise from adverse natural events like flooding, fires, or pandemic outbreaks. The BCPs include identification and planning of alternate operation centres, operational procedures to maintain communication, measures to ensure continuity of critical business functions, protection of our employees and customers, and recovery of information databases. We update and test the BCP regularly. Drills and emergency response exercises are conducted to familiarise employees with the various incident management plans. The BCPs enhance the Group's operational readiness and resilience to potential business disruptions.

The Group also seeks to adopt the best industry practices, harmonise and streamline our processes, and attain 3rd party accreditation from the Singapore Accreditation Council (SAC) as an attestation to our technical competency and professionalism. Besides this, the Group works closely with the various regulatory bodies to keep abreast of the latest regulatory requirements and ensure compliance. Ensuring high standards and operational excellence will enable us to deliver the desired outcomes and mitigate the risk of operating licences, certifications, and accreditations being revoked.

Manpower Risk
The Group's ability to develop and grow the business depends on the quality of its people, and it is committed to investing in developing its talent pool. We believe in developing a strong workforce by putting in place various programmes and processes. These include talent management, building management bench strength, succession planning, performance management, compensation and benefits, training and development, and employee conduct and supervision. We ensure that our employees are selected and promoted based on merit and that they understand their responsibilities and are given access to the necessary training. At all times, a positive, constructive and productive working climate based on strong tripartite relations is fostered. We work with the Authorities and the Unions to ensure that our people are fairly recognised, remunerated and taken care of.

Property and Liability
The Group's exposure to property damage, business interruption and other liability risks is constantly monitored and reviewed with ComfortDelGro's wholly-owned insurance broking subsidiary. We ensure the sufficiency of insurance coverage and maintain an optimal balance between risks that are internal and risks that are placed out with underwriters.

RISK MANAGEMENT

Financial Risks

Budgetary Control
A robust and comprehensive Annual Budget is prepared and approved by the Board prior to the commencement of each financial year. Material variations between actual and budgeted performance are reviewed on a monthly basis. The capital expenditure budget is approved in principle by the Board as part of the Annual Budget. Each capital expenditure is subjected to rigorous justification and review before it is incurred in accordance with the Group's financial authority limits. Specific approvals must be sought for unbudgeted expenditures. Tight control of manpower is exercised through the headcount budget.

Financial Management Risk
The Group upholds the highest integrity in financial statement disclosure. Financial Authority Limits are put in place for capital expenditure, operating expenses, treasury matters, direct investments, revenue tender participation, and disposal and write-off of assets. These authority limits are delegated based on the organisational hierarchy with the Board retaining the ultimate authority.

Fraud Risk
Committed to shareholder value and strategic growth, the Group prioritises proactive fraud prevention through comprehensive internal controls and audits, ensuring compliance and transparency. Vigilant risk awareness and ethical conduct are ingrained in our culture, securing our future through unwavering vigilance and integrity.

Our key deterrent and mitigation actions include:

- Commitment, Oversight, and Tone from Top: The Management sets the tone from the top in promoting ethical culture and having zero tolerance to fraud. Our employees are required to declare any conflicts of interest annually. They undergo frequent trainings on Anti-corruption, Anti-bribery, Ethics, and Competition Law. To ensure our supply chain partners maintain the same level of rigour we set internally, our suppliers are required to comply with our Supplier Code of Conduct.
- The Group has established a Whistle Blowing Policy that provides a whistleblowing alert line that empowers our employees to report any misconduct or fraud directly to the Chairman of ARC and/or the Group Chief Internal Audit Officer. The policy is communicated to all employees twice yearly through Electronic Distribution Mails (EDMs) with their acknowledgment. The ARC provides independent oversight on the investigations conducted by Group Internal Audit. Reported incidents will be dealt with promptly and thoroughly.
- Proactive Risk Identification and Mitigation: Our commitment in preventing and detecting fraud extends beyond robust internal controls, including checks and balances and multi-step approvals. We leverage our comprehensive Minimum Acceptable Controls Self-Assessment (MACSA) to establish consistent baseline controls across the Group, enhancing the effectiveness of our finance and business processes.
- The Group has continually attained the ISO370001:2016 Anti-Bribery Management System (ABMS) certification to further attest and strengthen its policies, internal processes, and procedures in preventing and mitigating the risk of fraud and bribery. Such certification demonstrates the Group's uncompromising commitment to combating fraud and bribery and its policy of zero tolerance for corruption.

Compliance Risks

Compliance & Regulatory Risk
The Group is committed to ensuring that all BUs comply with the laws and regulations in the country they operate in. These laws and regulations include, but are not limited to, labour, taxation, and environmental laws. As part of the risk management process, we maintain a compliance framework to monitor closely for any changes in the laws and regulations. Any changes are disseminated and updated in the respective compliance registers. We proactively engage the regulatory authorities for any updated policies. As and where necessary, our BUs will also provide feedback on proposed regulatory changes during industry or public consultation exercises.

Information Technology Risks

Cybersecurity Risk
Cybersecurity remains a key risk for the Group, given the trend of increasing cyber-attacks globally, and that our digital footprint has grown with increased digitalisation. Coupled with the ever-evolving digital terrain, it is pertinent that the Group put in place a comprehensive and robust security framework, with regular reviews to ensure continuing relevance in the face of changing threats.

The Group's information technology security management framework complies with the latest industry standards. We have put in place various controls and data recovery measures to mitigate the risks, including the use of intrusion prevention systems, multi-level firewalls, server protection, software code hardening, and data loss prevention controls to manage internet security and cyber threats. Penetration tests are carried out regularly to test the systems, identify potential vulnerabilities and to strengthen the security hardening of our websites. Information security policies and procedures, including education and training for all staff, are reviewed and enhanced regularly.

Data Confidentiality Risk
As a data custodian for our employees' and customers' personal data, the Group has implemented various policies, practices, and controls to protect the confidentiality of these data. We regularly review our means of collecting, managing, safekeeping, sharing, and disposal of such data to ensure compliance with the personal data protection regulations. The Group and the BUs also evaluate and update our data inventory map bi-annually. Data Protection Officers and other organisational representatives involved in the management of personal data are also sent for training to ensure that they are equipped with the required competencies.

The Group has attained the Data Protection Trust Mark (DPTM) from the Infocomm and Media Development Authority (IMDA) since 2020 as a testament to the adequacy and effectiveness of its policies, internal processes, and procedures in preventing personal data breaches.

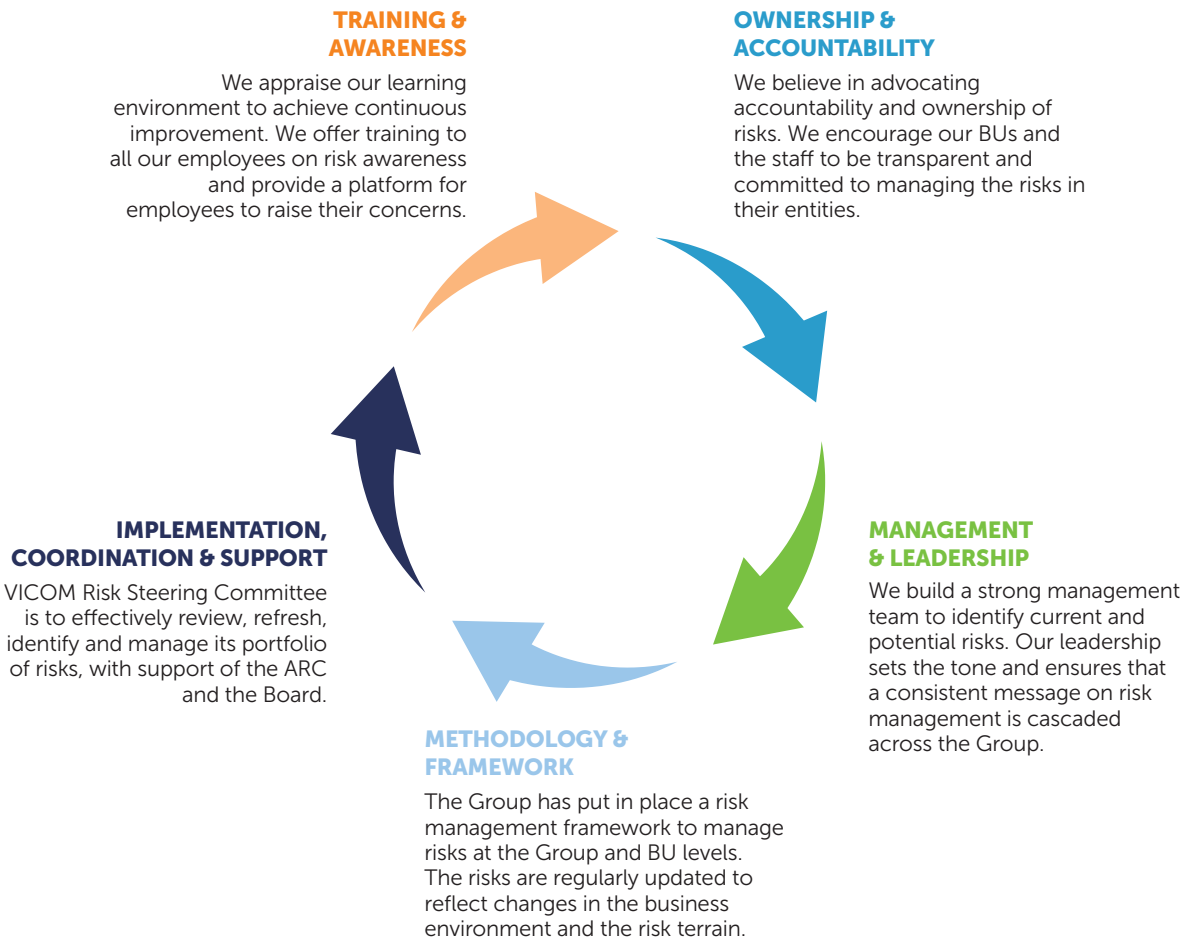
Audit Process

The Internal and External Auditors conduct reviews in accordance with their audit plans to assess the adequacy of the internal controls that are in place. A risk-based approach has been adopted for the annual internal audit plan, which extends to the auditable universe of the Group. In the course of their audits, the Internal and External Auditors will highlight to the Management and the ARC the areas with material deficiencies, non-compliance, weaknesses or occurrences or potential occurrence of significant risk events. The auditors will also propose mitigating measures and treatment plans. The audit recommendations are to be followed up as part of the Group's continuous review of its system of internal controls, and the implementation status is reported to the ARC. The Group Internal Audit is independent of the activities it audits, and has unfettered access to the ARC, the Board and the Management. In line with best practices, Group Internal Audit has a Quality Assurance Programme that covers all aspects of its audit activities and conforms to international standards of auditing. The Group Internal Audit successfully completed its external Quality Assurance Review in 2023 by Protiviti Pte Ltd and continues to meet or exceed the IIA Standards in all key aspects. The Quality Assurance Review is conducted every 5 years.

RISK MANAGEMENT

Risk Culture

The Group believes in setting a robust risk management culture by ensuring good awareness, attitudes and behaviour toward risk management. We aim for continuous improvement by aligning ourselves with best practices and lessons learnt. The diagram below best describes the processes that the Group advocates to sustain continuous improvement in our risk management.



Code of Business Conduct

The Group has adopted a Code of Business Conduct that sets out the principles and policies upon which businesses are conducted. The Code of Business Conduct includes anti-corruption and anti-bribery policies that stress on zero tolerance for fraud, and improper use of monetary favours, gifts, or entertainment. In addition, employees should not put themselves in a position of conflict of interest with the Group. If there is a potential conflict of interest, employees should declare to their immediate supervisors and recuse themselves from the decision process.