Risk & **Internal Controls**

Maintaining a dynamic and effective risk management process is vital to supporting and strengthening business operations as we manage the impact of a challenging external environment.

We continue to operate in a challenging macroeconomic environment characterised by elevated inflation, rising energy prices and global supply chain disruptions. Our dynamic and effective risk management process has allowed us to proactively mitigate and manage our risks as well as embrace opportunities as they arise.

During the year under review, we remained constant in our efforts to strengthen and harmonise our risk management practices across the Group, whilst acknowledging that each cluster has its own business context and risk environment, with different risk management maturity levels. Our main actions were focused on the following aspects:

GOVERNANCE

- Updating the Group Risk Appetite Statements
- Revamping the Risk Governance structure of the Textile cluster
- Updating the Group Risk Register Please refer to Our Principal Risks Explained

PROCESS

- Revising the Group Enterprise Risk Management (ERM) manual to include useful tools and explanations to guide risk champions on the risk management process
- Issuing a playbook for cluster risk committees

PEOPLE

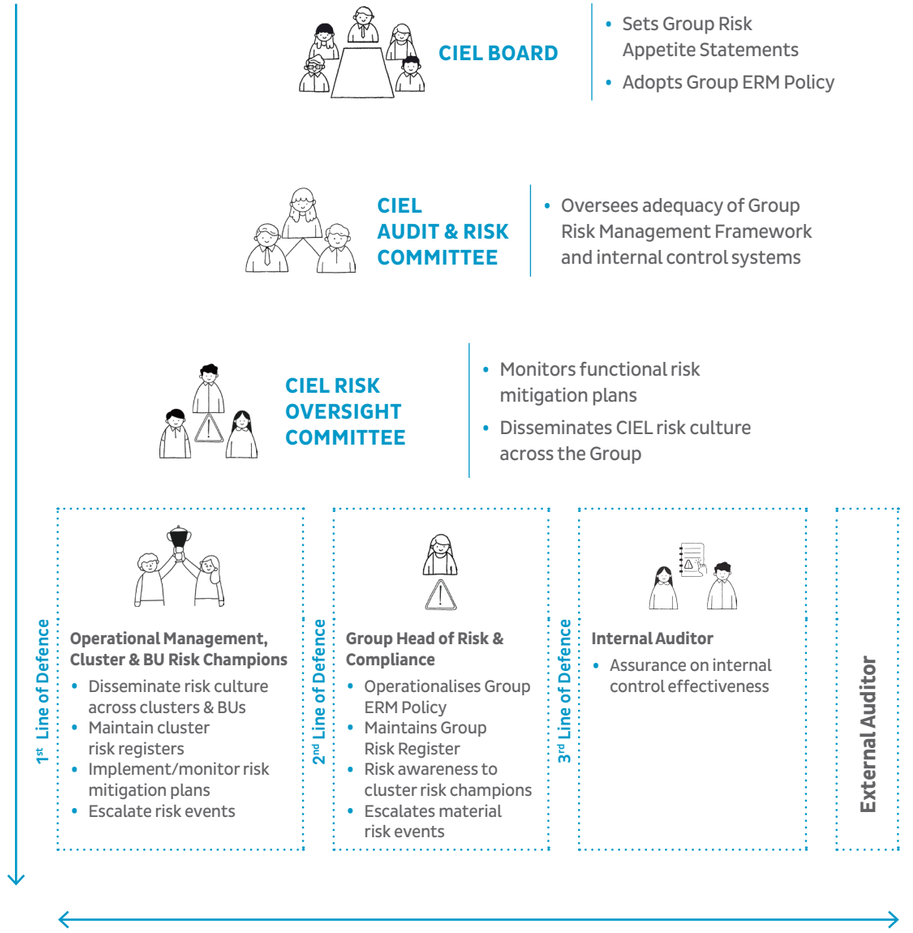
- Clearly articulating the roles and responsibilities of cluster and business unit (BU) risk champions
- Conducting risk awareness sessions with cluster and BU risk champions
- Regular interactions between Group Head of Risk and cluster risk champions to assist with the design and administration of cluster and BU risk functions

OUR RISK MANAGEMENT FRAMEWORK

We have a holistic approach to risk management, first building a picture of the top risks and corresponding controls at our cluster levels, then consolidating those risks alongside other material risks identified at Group level to arrive at a Group view. The Board sets the risk appetite for CIEL in line with the Group's strategic objectives, which is disseminated to our clusters to set the tone on the level of risk that we are willing to accept in the pursuit of our strategic objectives.

The Audit and Risk Committee (ARC), under delegated authority from the Board, oversees the effectiveness of the risk management framework, including the identification and rating of key risks faced by CIEL, together with the corresponding controls. To support the ARC in this responsibility, underlying processes are in place, which are fully aligned with CIEL's operating model where our clusters are each responsible to identify, assess and manage their risks autonomously. Additionally, key functions are accountable at Group level for the ongoing tracking of identified key risks and of changes in the business landscape. The ARC also receives assurance from the Internal Auditor on risk management and internal control effectiveness, along with agreed mitigating actions to resolve any weaknesses identified.

CIEL's risk governance structure is based on the three lines of defence model as illustrated on the right:



OUR RISK APPETITE STATEMENTS

Our Risk Appetite Statements set the level of risks that we are willing to accept in the pursuit of our strategic objectives.

The Group's Investment Guidelines & Risk Appetite Statements (RAS) were revised during the reporting year and approved by the Board on 30 June 2023. The main approach was to factor in systemic risks inherent to countries and industries where we operate and adjust for top risks identified for CIEL and its clusters.

Our clusters are currently developping their own RAS and key performance indicators (KPIs), based, at a minimum, on the following statements:

Strategic Assertions
We invest responsibly and sustainably in order to create lasting value, outstanding returns and shared outcomes for our stakeholders. We have a preference to invest in industries where we have proven skills and competence, and primarily target Sub-Saharan African markets and Indian subcontinent markets for international expansion.

Sustainability
We recognise the importance of sustainability in meeting long-term business objectives and contributing to a healthier planet. As such we are committed to integrating the relevant environmental, social, and governance (ESG) factors in our investment decisions and throughout our operations and supply chain. This is with a view to improve our overall footprint and maximise positive environmental, social and economic outcomes.

We have no appetite for investments that conflict with our internal Sustainable Investment Policy, which is aligned with the harmonised European Development Finance Institution (EDFI) Exclusion List and International Finance Corporation (IFC) performance standards.

Presence in Selective Industries and Regional Markets
We have high appetite for investments in those industries and businesses in which we have proven skills and competences, but we may consider investments in other industries that will fuel innovation and drive growth across the different clusters, substantiated by a robust business case. We primarily target Sub-Saharan African and Indian subcontinent markets for international expansion and where appropriate, we seek strategic partnerships with industry leaders with the right cultural fit.

Controlling Stake in Tier 1 Companies
We have high appetite for investments with controlling stakes in companies that are amongst the leaders in their respective markets (Tier 1 Companies). We may consider investments in niche markets with growth potential and substantiated by a robust business case.

Performance Review and Asset Allocation
We determine asset allocation and portfolio balance based on the performance of each cluster according to a set of financial and non-financial targets, which are reviewed on an annual basis.

Financial Assertions
We invest for reward and minimise the possibility of financial loss by managing the risks and bringing them to a tolerable level. Value and benefits are considered, whilst resources are allocated in order to capitalise on potential opportunities.

Return Expectations
We have set minimum financial and return KPIs for each cluster, taking into account its risk profile, to maintain performance at target levels.

Business Plan Projects and Sensitivity Analysis
For every business plan, we seek a sensitivity analysis on the key financial metrics, and we have low tolerance to actual values falling outside the lower or upper bound (as applicable) of our projections.

We expect a new business plan every 3 to 5 years, which needs to be revisited annually to provide a rolling forecast.

Target Debt Rating
We endeavour to maintain a long-term CARE debt rating of "AA" for CIEL and to ensure our clusters achieve a rating of "A" or better.

Operational Assertions
We embrace a culture of operational excellence, based on innovation, aiming at enhancing in a sustainable way, customer experience, employee engagement and organisational efficiency in order to deliver a consistently superior performance in revenue growth, profitability and EBITDA levels.

Business Continuity
We are committed to maintaining the continuity of our critical business operations in the face of disruptive events. We recognise that no organisation is completely immune to disruptions, but we are committed to identifying and managing risks that could impact our critical functions by ensuring that all our subsidiaries have implemented a robust business continuity program that includes regular risk assessments, contingency planning, and testing response capabilities.

Talent Management
Our people are central to our ability to create value for all our stakeholders. As such we are committed to attracting, nurturing, and retaining the best talent to deliver sustainable growth by implementing a comprehensive management program that includes regular assessments of our needs, bespoke and tailor-made development opportunities, and a compelling employee value proposition.

Innovation
Innovation and digitalisation are key drivers of operational excellence, growth and competitive advantage, and we are committed to fostering a culture of learning, creativity and experimentation.

Data Management
We recognise data as a valuable and strategic asset but also understand that there are risks associated with it. Our approach to data management allows us to reap the benefits of data whilst ensuring that it is managed securely and ethically in compliance with data protection laws.

Reputation
Our reputation is a critical asset, central to our success and ability to maintain the trust of our stakeholders.

We have no appetite for situations and actions which may negatively impact our brand and reputation. We are committed to protecting our reputation through high operational excellence together with strict adherence to legal and ethical standards. We ensure open and transparent communication with our stakeholders, including customers, employees, shareholders, regulatory authorities and communities.

Cyber Threats
We recognise that cyber threats pose a significant risk to our operations, reputation, and financial stability. We are resolute to implementing a comprehensive cyber security program that includes regular vulnerability assessments and penetration testing, employee awareness and training programs, and an adequate response plan in the event of cyber security incidents.

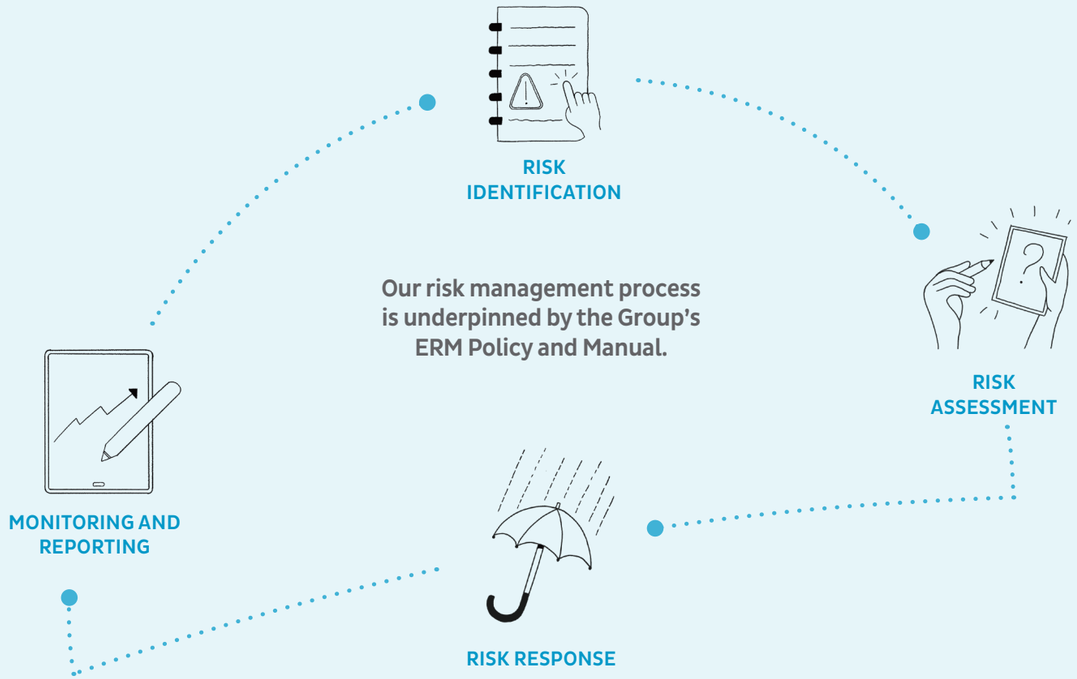
Fraud
Fraud is a significant risk that can have serious financial, legal, and reputational consequences for our Group and our stakeholders.
We have zero tolerance for fraud, and ensure strong prevention and detection measures across all our operations.

Compliance Assertions
We have zero tolerance for non-compliance with applicable laws, regulations and ethical standards.

Laws, Regulations and Ethics
Compliance with laws, regulations, and ethical standards is critical to our business success and reputation.

We maintain a strong culture of compliance across all our operations through robust compliance programmes and controls including employee awareness and education to promote ethical behaviour.

OUR RISK MANAGEMENT PROCESS



Risk identification is an integral part of CIEL's risk management process, and is based on a comprehensive review of the clusters' risk registers, from which a list of the key risks faced by the Group is drawn up to consider:

- **Systemic risks** which are the top risks that repeat across at least three clusters and merit elevation to Group level
- **Material risks** which although non-systemic, merit elevation to Group level based on the materiality of the related cluster or activity within the Group and
- **Other risks** which although not identified at cluster level, are important at Group level, such as transversal risks, risks affecting the CIEL brand and emerging risks

To establish context, internal and external factors which may influence the achievement of strategic objectives are also taken into consideration in the identification process.

The risk identification phase is an iterative and dynamic process whereby new risks and changes to the risk landscape, are identified through an on-going monitoring process of the cluster operations and annual review of the Group's Risk Register.

Risks are assessed both at inherent and residual levels, that is before and after application of internal controls respectively, based on an evaluation of the effectiveness of the control environments. This approach provides the extent to which the risks are mitigated by existing controls. The evaluation of control effectiveness is also dynamic as it accounts for changes in the control environments, and outcomes of control assessments performed by assurance providers such as internal and external auditors.

The output of the risk assessments is compared with established risk indicators as set by the RAS to determine the required **risk responses**, based on the following options:

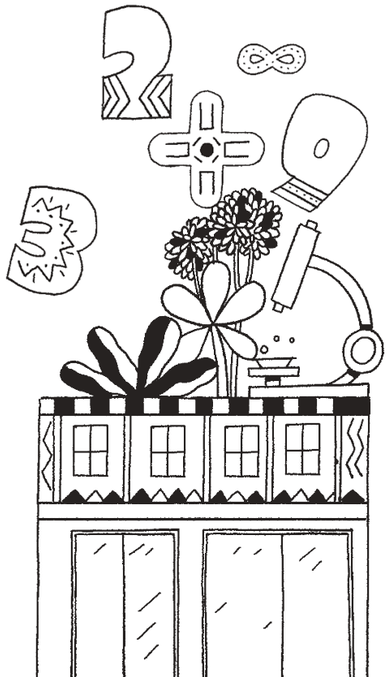
- **Terminate:** Eliminate the risk by not starting, discontinuing, terminating an activity that gives rise to the risk
- **Transfer:** Transfer the risk to a third-party (e.g subcontracting, joint venture, partnership, outsowurcing or insurance). This would usually involve a cost or risk premium
- **Treat:** Consider implementing additional controls to reduce the likelihood and/or impact of the risk
- **Tolerate:** Tolerate or accept the risk on the basis of satisfactory cost-benefit analysis

Monitoring and reporting includes providing assurance on the quality and effectiveness of risk management process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management processes and their outcomes is integrated into the risk management practices of CIEL, with clearly defined roles and responsibilities.

We continuously monitor and review our risks to ensure that our risk registers and action plans remain relevant within the fast-changing business environment. Any alteration of risk profiles due to any changing circumstances is properly documented.

OUR RISK PROFILE

An annual review of the Group's Risk Register was performed with due consideration to the local and global macroeconomic trends, the risks identified and escalated at cluster levels as well as new risks identified for the Group. The top 10 Principal Risks of the Group are explained on the following pages.



Amidst persisting economic instability and geopolitical tensions, CIEL, like other organisations in Mauritius and worldwide, continues to be vulnerable to external factors such as inflation, rising energy prices, exchange rate volatility and global supply chain disruptions. Our inherent risk rating pertaining to External Shocks was increased to reflect the declining growth observed in advanced economies.

Cyber-attacks continue to increase exponentially across the globe, catalysed by increased interconnectedness and dependency, and access to sophisticated digital technology. Malware and ransomware attacks are expected to target more enterprises and vulnerable sectors where there are perceived cybersecurity skill shortages. Over the past year, CIEL and its clusters have invested significantly in maturing their ability to prevent, detect and respond to cyber risks. This has resulted in a slight improvement in our cyber control effectiveness rating, with further improvements expected as and when remaining remedial actions are successfully delivered.

Attracting and retaining the right talent has emerged as one of the biggest challenges of organisations worldwide since the pandemic. During the reporting year, our local operations in Healthcare, Hotels & Resorts and Textile clusters have been impacted by the shortage of a skilled and qualified workforce, aggravated by increased competition and tighter migration laws. Our inherent risk rating under Talent Retention & Recruitment was accordingly increased, whilst our recruitment, retention and training strategies continue to be reinforced across the Group.

Climate change and associated risks will have a large impact on global risk perceptions over the next decade. The increased frequency and intensity of extreme weather events have been hitting headlines and costing lives and livelihoods around the world, whilst globally we are off track from meeting climate goals according to the United in Science 2023 Report. Mauritius being particularly exposed to rising temperatures and sea levels, accelerated coral erosion, volatile and extreme weather patterns, climate risk assessments are necessary for identifying potential hazards from climate-related events, trends, forecasts and projections, and for developing adequate climate mitigation and adaptation strategies. Our inherent risk rating was increased to reflect the growing external risks posed by climate change, as we continue to deploy our Sustainability Strategy 2020-2030.

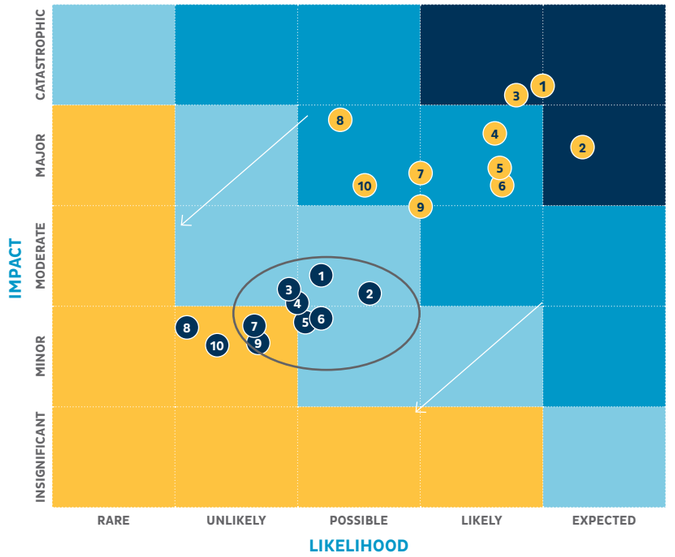
The ratings of other top risks identified at Group level have not changed over the past year.

Please refer to Our Principal Risks Explained on subsequent pages.

OUR PRINCIPAL RISKS EXPLAINED

Risk Heat Map

The following heat map shows the 10 Principal Risks of CIEL Group as they evolve from an inherent to a residual level after application of mitigating controls in place.



RISK LEVEL	MANAGEMENT APPROACH
EXTREME	PROACTIVELY MANAGED
HIGH	ACTIVE ATTENTION & PREPARATION
MEDIUM	CONTINUOUS MONITORING
LOW	PERIODIC ASSESSMENT

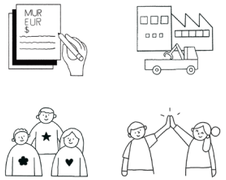
RISK VARIATIONS FY23

1	External Shocks	▲	6	Fraud	–
2	Cyber Threats	▼	7	Business Continuity	–
3	Talent Retention & Recruitment	▲	8	Liquidity & Funding	–
4	Compliance	–	9	Climate Change & ESG	▲
5	Competition Threats	–	10	Internal & External Communication	–

OUR PRINCIPAL RISKS EXPLAINED (CONT'D)

Risk has Increased | Risk has Decreased | Risk is Constant

Financial Capital | Human Capital | Intellectual Capital | Manufactured Capital | Social & Relationship Capital | Natural Capital

PRINCIPAL RISK	DESCRIPTION	INHERENT LEVEL	CONTRIBUTING FACTORS	CAPITALS IMPACTED	HOW WE MANAGE THE RISK	RESIDUAL LEVEL
▲ 1 EXTERNAL SHOCKS **RISK CATEGORY:** STRATEGIC **RISK TYPE:** SYSTEMIC	The risk that CIEL Group is unable to sustain growth due to external shocks to the economies where it operates or where material revenues are coming from, resulting in missed performance targets and shareholder dissatisfaction. ***DETERIORATION IN INHERENT RISK:*** *global recovery slowing down amidst persistent geopolitical and economic challenges.*	EXTREME LOW	• Geopolitical tensions (Russia-Ukraine conflict, US/China political and trade tensions) • Emergence of new viruses or diseases • Rising costs and inflation • Declining global growth, mainly in advanced economies, affecting our main markets • Global supply chain disruptions • Sovereign debt crisis • Interest rate volatility • Foreign exchange volatility • Food crisis and poverty in developing countries due to extreme weather events • Political instability and social unrest in the countries where CIEL operates **Opportunities:** • Recovery of local tourism sector having positive spillover effects on other sectors of the local economy • Mauritius positioned as the only International Financial Centre with an "investment grade" in the African region		• Cost mitigation measures across all operations • Rationalisation of suppliers • Managing relationship with critical suppliers • Alternative sourcing options • Close monitoring of forex fluctuations with hedging strategies • Close monitoring of geopolitical situation in the countries where CIEL operates • Regular scenario/what if analysis in management and Board discussions • (Updated) Risk Appetite Statements aligned with systemic risks inherent to countries and industries where CIEL operates and top risks identified for the Group *Our Risk Appetite Statements* ***Extent to which the risk is mitigated: Medium***	EXTREME LOW

OUR PRINCIPAL RISKS EXPLAINED (CONT'D)

Risk has Increased | Risk has Decreased | Risk is Constant

Financial Capital | Human Capital | Intellectual Capital | Manufactured Capital | Social & Relationship Capital | Natural Capital

PRINCIPAL RISK	DESCRIPTION	INHERENT LEVEL	CONTRIBUTING FACTORS	CAPITALS IMPACTED	HOW WE MANAGE THE RISK	RESIDUAL LEVEL
▼ **2 CYBER THREATS** **RISK CATEGORY:** OPERATIONAL **RISK TYPE:** SYSTEMIC	The risk that CIEL Group is exposed to cyber-attacks, resulting in disruptions to activities, financial losses and client dissatisfaction. ***Minor improvement in control effectiveness:*** *action plans have been adopted across all clusters to strengthen cybersecurity capabilities, including recruitment of cybersecurity experts. Further improvements are expected as and when ongoing remedial actions are successfully delivered.*	EXTREME LOW	• Increase in the incidence of cybercrime following the COVID-19 pandemic and the Russia-Ukraine war • Malware/ ransomware attacks are expected to target more enterprises and vulnerable sectors like healthcare where there are cybersecurity skills shortages • Increasing dependency of CIEL on technology as it is infused in day-to-day operations • Increasing vulnerability of CIEL and its operations as more (data sensitive) activities are outsourced to third party service providers		• Action plans adopted across all clusters to strengthen cybersecurity capabilities, including recruitment of cybersecurity experts • Vulnerability Assessments and Penetration Testing performed on critical IT systems to identify vulnerabilities (extended to third party service providers for critical activities) • Enhanced monitoring and reporting of effectiveness of cybersecurity framework through tracking of KPIs organised around three main pillars (Prevention, Detection and Response) • Group level cybersecurity forum for sharing of best practices, lessons learnt from cyber incidents and insights on cyber trends • Frequent awareness sessions provided to staff • Regular phishing simulation exercises ***Extent to which the risk is mitigated: Medium***	EXTREME LOW

OUR PRINCIPAL RISKS EXPLAINED (CONT'D)

Risk has Increased | Risk has Decreased | Risk is Constant

Financial Capital | Human Capital | Intellectual Capital | Manufactured Capital | Social & Relationship Capital | Natural Capital

PRINCIPAL RISK	DESCRIPTION	INHERENT LEVEL	CONTRIBUTING FACTORS	CAPITALS IMPACTED	HOW WE MANAGE THE RISK	RESIDUAL LEVEL
3 TALENT RETENTION & RECRUITMENT **RISK CATEGORY:** OPERATIONAL **RISK TYPE:** SYSTEMIC	The risk that CIEL Group is unable to recruit, develop and retain talent to instill appropriate behaviours and service levels, resulting in client dissatisfaction, disruption in operations and significant costs and efforts associated with replacing former staff and training new ones. ***Deterioration In Inherent Risk:*** *shortage of skilled and qualified workforce, particularly in Healthcare, Hotels & Resorts and Textile clusters, aggravated in certain sectors, by increased competition and tighter migration laws.*	EXTREME LOW	• Change of mindset amongst working population post COVID-19 pandemic whereby a number of professions/jobs are no longer attractive, particularly in Hotels & Resorts, Healthcare & Textile • Poaching of competent resources by competitors • Lack of qualified or trained resources in Mauritius (e.g. nurses, doctors) and in other countries where we operate **Opportunity:** • Intra cluster and intra Group mobility for support functions		• Succession plan for key and critical roles developed for clusters Business Units management • Strong employee retention and employee value proposition strategies across all clusters and operations (e.g. employee engagement surveys, recognition and reward schemes, professional development schemes, employee wellness and welfare programmes, flexible hours) • Investment in bespoke leadership development programmes for Top Talent • Expatriate recruitment where expertise is not available locally, however limited by migration laws ***Extent to which the risk is mitigated: High***	EXTREME LOW
4 COMPLIANCE **RISK CATEGORY:** COMPLIANCE **RISK TYPE:** MATERIAL	The risk that CIEL Group is unable to manage the ever-evolving regulatory and compliance requirements, resulting in fines, revocation of relevant licences and reputational damage. ***No change:*** *the Group continues to be exposed to compliance risk, which is inherently high in certain sectors where it operates. Whilst robust compliance risk management plans are in place in our highly regulated operations, other operations are also reinforcing their compliance plans to ensure that their compliance risks are adequately identified, assessed and mitigated.*	EXTREME LOW	• Anti-Money Laundering (AML)/Combatting the Financing of Terrorism (CFT) related regulations particularly affecting Finance and Property clusters • Coming wave of ESG related regulations • Data privacy compliance regarding sensitive information • Entities of CIEL Group operate in multiple jurisdictions and/or sectors with different regulatory frameworks		• Strong compliance culture embedded across the Group along a "zero tolerance" policy to non-compliance • Compliance experts at Group, cluster and BU levels where applicable • Regular monitoring (second line of defence) and compliance audits (third line of defence) • Regulatory watch to keep track of regulatory changes ***Extent to which the risk is mitigated: Medium***	EXTREME LOW

Risk & **Internal Controls** (Cont'd)

OUR PRINCIPAL RISKS EXPLAINED (CONT'D)

Risk has Increased | Risk has Decreased | Risk is Constant

Financial Capital | Human Capital | Intellectual Capital | Manufactured Capital | Social & Relationship Capital | Natural Capital

PRINCIPAL RISK	DESCRIPTION	INHERENT LEVEL	CONTRIBUTING FACTORS	CAPITALS IMPACTED	HOW WE MANAGE THE RISK	RESIDUAL LEVEL
5 COMPETITION THREATS **RISK CATEGORY:** STRATEGIC **RISK TYPE:** MATERIAL	The risk that CIEL Group does not anticipate and respond to competitive threats or new entrants, affecting its ability to maintain and grow its market share. ***No change :*** *competition risk remains amongst the group's top 5 risks given that it operates in highly competitive sectors. Strategic reviews are prioritised in management and board meetings where market trends are tracked and analysed.*	EXTREME LOW	• Risk of disruption from more innovative products/ organisations with enhanced customer experience • Threats of new entrants in the sectors where we operate (e.g. Healthcare) • Highly competitive markets in the sectors where we operate (e.g. Textile, Finance, Hospitality) **Opportunities:** • Disruptive technologies such as blockchain and artificial intelligence • Mauritius well positioned as a financial hub between Asia and Africa • Pan African Healthcare strategy • Yielding of Group land assets • AgriTech		• Strategic discussions at management and board levels to analyse customer/market trends and competition • Product innovation • Developing unique value propositions • Impact investing • Enhancing brand value ***Extent to which the risk is mitigated: Medium***	EXTREME LOW
6 FRAUD & UNETHICAL PRACTICES **RISK CATEGORY:** OPERATIONAL **RISK TYPE:** OTHER	The risk that CIEL Group does not adopt appropriate measures and internal procedures to prevent and detect fraud, bribery and unethical behaviours, leading to financial losses, reputation damage and erosion of stakeholder trust. ***No change :*** *the Group remains exposed to the risk of fraud, which is inherently high in certain sectors and countries where it operates. Efforts are constantly employed across the group to strengthen internal control systems with a view to mitigate the risk further.*	EXTREME LOW	• Fraud risk is inherently high in the banking and financial services cluster • Corruption is inherently high in certain countries where CIEL operates • Heightened risk of fraud post COVID pandemic and current economic conditions		• Formalised processes and controls • Segregation of duties • Incident reporting • Whistleblowing channel at BU and Group levels • Disciplinary measures in case of unethical behaviours • Frequent audit of operations inherently exposed to fraud risk ***Extent to which the risk is mitigated: Medium***	EXTREME LOW

Risk & **Internal Controls** (Cont'd)

OUR PRINCIPAL RISKS EXPLAINED (CONT'D)

Risk has Increased | Risk has Decreased | Risk is Constant

Financial Capital | Human Capital | Intellectual Capital | Manufactured Capital | Social & Relationship Capital | Natural Capital

PRINCIPAL RISK	DESCRIPTION	INHERENT LEVEL	CONTRIBUTING FACTORS	CAPITALS IMPACTED	HOW WE MANAGE THE RISK	RESIDUAL LEVEL
7 BUSINESS CONTINUITY **RISK CATEGORY:** STRATEGIC **RISK TYPE:** SYSTEMIC	The risk that CIEL Group is not able to carry out or resume its operations timeously in the event of interruptions/disasters, resulting in significant losses, reputational damage and in extreme cases, loss of life ***No change:*** *business continuity remains a principal risk for the group and its clusters. Actions are on-going to ensure that business continuity plans remain pertinent to changes in operating environments.*	EXTREME LOW	• Impact of climate change on Mauritius, including beach erosion, coral death, volatile and extreme weather patterns, droughts, floods etc • Mauritius is particularly exposed to the impact of climate change (Small Islands Developing States) and disasters to its natural resources (e.g. oil spills) • Disease outbreak • Risks associated with connectivity issues to IT systems and internet, given increasing dependency		• Business continuity plans, disaster recovery plans and crisis management plans implemented across BUs • Drills to assess the readiness of the clusters/BUs to recover in specific situations • Frequent awareness sessions to staff ***Extent to which the risk is mitigated: Medium***	EXTREME LOW
8 LIQUIDITY & FUNDING **RISK CATEGORY:** OPERATIONAL **RISK TYPE:** MATERIAL	The risk that CIEL Group is unable to access internal or external funds to cover obligations and/or operations or excessive borrowing to cover current operating obligations, resulting in cash flow constraints and missed targets. ***No change:*** *strong revenue growth, mainly on account of hotels performing well above expectations and all other clusters posting double-digit growth.*	EXTREME LOW	• Persistent geopolitical and economic challenges • Ability to secure funding at an attractive cost of capital		• Stress test analysis • Robust cash flow management • Robust cost control and business optimisation measures • Leveraging on financial support and schemes • Nurturing investor relationships ***Extent to which the risk is mitigated: High***	EXTREME LOW

OUR PRINCIPAL RISKS EXPLAINED (CONT'D)

Risk has Increased | Risk has Decreased | Risk is Constant

Financial Capital | Human Capital | Intellectual Capital | Manufactured Capital | Social & Relationship Capital | Natural Capital

PRINCIPAL RISK	DESCRIPTION	INHERENT LEVEL	CONTRIBUTING FACTORS	CAPITALS IMPACTED	HOW WE MANAGE THE RISK	RESIDUAL LEVEL
▲ 9 **CLIMATE CHANGE & ESG** **RISK CATEGORY:** STRATEGIC **RISK TYPE:** OTHER	The risk that CIEL Group does not factor the impact of its activities and decisions on the environment and society at large, resulting in unsustainable business operations and reputation damage. ***Deterioration in inherent risk:*** *increased frequency and intensity of extreme weather events around the world with Mauritius being particularly exposed to rising temperatures and sea levels, accelerated coral erosion, volatile and extreme weather patterns. Whilst the group continues to invest considerably in deploying its sustainability strategy 2020-2030, inherent risk was increased to reflect the increasing external risks posed by climate change.*	EXTREME LOW	• Increased frequency and intensity of extreme weather events around the world with record breaking storms, floods, heatwaves, wildfires • Climate mitigation and transition plans are off-track largely due to insufficient collective actions and geopolitical tensions • Mauritius is exposed to rising temperatures and sea levels, accelerated coral erosion, volatile and extreme weather patterns (droughts, floods), with impacts already being felt in our operations (Properties)	Financial, Manufactured, Human, Social & Relationship, Natural	• Group Sustainability Strategy 2020-2030 around three main pillars (workforce, inclusive growth and climate response) • Roadmap devised at cluster levels to deliver the Group's sustainability goals • Dedicated teams of sustainability experts and champions to drive action plans across the Group • Group-wide internal reporting for measuring sustainability progress • Regular awareness & training sessions to staff on ESG and climate change *Please refer to the Activate Climate Response Section* ***Extent to which the risk is mitigated: Medium***	EXTREME LOW
— 10 **INTERNAL & EXTERNAL COMMUNICATION** **RISK CATEGORY:** OPERATIONAL **RISK TYPE:** OTHER	The risk that CIEL Group does not effectively manage its internal and external communication, leading to internal dysfunctionality, stakeholder dissatisfaction, and brand & image damage. ***No change:*** *the Group continues to be exposed to high reputational risks which are inherent to certain sectors where it operates. Adequate crisis communication plans are in place at Group and cluster levels.*	EXTREME LOW	• CIEL Group operates in critical sectors with high societal impact and exposure to reputational risk (e.g. healthcare, hospitality, financial services & banking). Effective internal and external communication is key in case of material incidents • Long lasting effects that media coverage can have on the BU brands and Group brand	Financial, Manufactured, Human, Social & Relationship	• Crisis communication strategy • Incident reporting/raising concerns • Media strategy & protocols • On-going sharing of Group strategy and overall vision with employees • Group level department monitoring internal and external communication ***Extent to which the risk is mitigated: High***	EXTREME LOW

Audit

INTERNAL AUDIT

The internal audit function is outsourced to EY, which has a dedicated team of qualified auditors servicing the Group at CIEL and cluster levels.

As a third level of defence, the internal audit function provides independent and objective assurance on the effectiveness of governance, risk management and control processes across the Group. To ensure that the function remains independent and sufficiently objective, internal audit teams report functionally to the ARC of CIEL and of the clusters, and administratively to the respective executive teams. The internal auditor teams have unrestricted access to company records and information, employees, and management teams as required, to enable them to deliver effectively.

The primary source of internal assurance is through delivery of the internal audit plan, which involves conducting a risk assessment exercise at company level to identify and rank the main risks faced by the company, and determine what areas need to be audited and in what order of priority. High-ranked risks that have corresponding auditable controls are typically prioritised for review. This exercise involves collaboration amongst the internal audit function, the members of the ARC, and the management to draw out consensus on the material risk areas that warrant attention. The same process is replicated across the Group by EY.

Audit plans are reviewed throughout the year to ensure that they remain relevant for new and emerging circumstances, both internal and external. The findings and remedial actions, including business improvements from internal audit reviews are discussed with the relevant business areas, are communicated to the respective management and ARCs, and tracked through to completion.

As a recurrent item on the agenda of the ARC meetings of CIEL and of the clusters, the members are updated on the audit findings arising from the previous internal audit reports which remain to be addressed and closed. The internal auditor also conducts follow-up reviews on previous audits to ensure that the necessary remedial action points have been duly implemented. In addition to areas covered by the annual internal audit plan, the ARCs may request internal auditors to perform special audits on other areas requiring attention.

Please refer to the Ensuring Good Governance section for the composition, organisation and responsibilities of the ARC.

The internal audit function typically executes its internal audit assignments through the following 5 main phases, which are aligned with the Institute of Internal Auditors (IIA) standards and leading internal audit practices.

Continuous project management and status updates as agreed in communication protocol

PHASES	APPROACH	DELIVERABLES
1 PLAN AND SCOPE	• Meet with appointed contact person to agree on audit project scope, objective and communication protocols • Confirm appropriate resources required to execute the audit program • Agree audit timelines	• Mobilise the project team and assign roles • Confirmed scope and objectives • Project schedule, plan and timelines
2 CONDUCT FIELDWORK	• Conduct understanding interviews and review key business documentation • Formulate audit programs including risk and control matrices (RACM) • Assess the design of controls through interviews with relevant personnel, review of process documentation and 'walkthrough' of the control • Assess the effectiveness of controls in operation via execution of the test work program	• Audit program including RACM • Audit Working Papers and supporting documents
3 REVIEW FINDINGS	• Review and analyse findings from fieldwork conducted • For issues identified, perform root cause analysis and impact analvsis to understand the materiality and 'why' the issue has occurred • Identify any compensating controls associated with the preliminary findings • Draft the report in a pre-agreed format and structure • Submit draft report to management for preliminary comments and validation	• Preliminary List of Issues • Draft Audit Report
4 ISSUE REPORT	• Close comments and agree with management on content of draft report • Collect management comments and remediation actions, and include these in the internal audit report • Finalise the report and release	• Final Audit Report including management actions
5 CONDUCT FOLLOW UP	• Agree with management timing for follow up audits • Agree which remediation actions have been implemented to date and plan to independently confirm that these are operating effectively • Interview relevant management for status update inquiry and determine required test • Verify that action plans for each finding have been implemented • Verify reasons for failing to implement any action plans and recommend way forward to close out any remaining issues	• Follow-up Report including the status for each action plan within the issued reports

Audit (Cont'd)

INTERNAL AUDIT (CONT'D)

EY has a specialist team of internal auditors who hold recognised international qualifications in their respective fields (e.g. ACCA, Institute of Chartered Accountants of England & Wales, Certified Internal Auditors (CIA), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC)). EY maintains the independence and objectivity of its staff by ensuring their strict adherence to professional and ethical standards and by providing them with regular training and awareness on these subjects.

For the financial year ended 30 June 2023, the major processes that were covered in the audit reviews are detailed below per cluster:

AUDITED AREAS	HEAD OFFICE	HOTELS & RESORTS	TEXTILE	FINANCE	HEALTHCARE	PROPERTIES
Payroll processing	●	●			●	
Revenue & debtors management				●	●	
Procurement & Inventory		●			●	
Food & Beverage (F&B)		●				
Sampling & Product development process			●			
Project costs & expenses monitoring process						●
Maintenance & Facilities		●				●
Contract Management			●		●	
Archiving system			●			
Risk Management system					●	

Other high-risk areas have been or will be covered as part of the 3-year audit cycle ending 2023/2024.

EXTERNAL AUDIT

PricewaterhouseCoopers (PwC) was appointed by the shareholders as the external auditor for a mandate of seven years, ending 30 June 2024. A formal tender process will be initiated during the next financial year for the rotation of the external auditors. Advanced planning and ongoing communication between the external auditors and the Finance teams across the Group on certain aspects of the audit cycle have created opportunities for improvement on audit areas in advance of the year end.

Throughout the year, our Finance teams have worked with PwC to ensure that the financial statements present a true and fair view of the financial performance and position of our businesses with the required level of disclosures regarding significant issues.

At the closing of the year-end audit exercise, PwC reports on the significant risks and control deficiencies identified at Group level to the ARC, together with recommended actions. Significant risks pertaining to each cluster are also reported at the respective cluster ARC, following which remedial action plans are promptly implemented by management and monitored by the ARC until closure.

The Executive and the Finance teams of the Group work together with the external auditor in an environment of constructive challenge whilst ensuring that the auditors' independence and objectivity is maintained. PwC also ensures that its teams adhere to the Code of Ethics of the International Ethics Standards Board for Accountants (IESBA).

The ARC regularly meets the auditors in the presence of management since it has no impact on the objectivity of the meeting. However, if the need arises, the ARC meets with the external auditors without management.

The fees paid to the auditors for audit and other services for the financial year are described under ***Other Statutory Disclosures***. The non-audit services provided by the auditors relate mainly to tax computation, compliance, and transaction advisory. Hence, the objectivity and independence of the auditors are safeguarded since the teams involved are not the same as the one providing audit services.