GOVERNANCE

The Group recognises its duty to ensure its business is conducted responsibly with a view to avoiding adverse impacts from direct and indirect operations and promoting sustainable development. Good governance underpins the overall direction, effectiveness, supervision, and accountability of the Group, guiding its business units to act with integrity and in the best interests of stakeholders through informed, effective, open, and ethical decision-making.

This section also covers governance approaches to specific cross-cutting sustainability topics that the Group identifies as important and should be integrated and mainstreamed under the governance framework to ensure all business units across the Group operate responsibly with integrity. These include: Data Privacy and Cyber Security, Labour and Human Rights, and Supply Chain Responsibility. How the Group allocates capital to ensure the achievement of its sustainability goals and targets is also important to effective governance and therefore covered in this section.

GROUP GOALS

- EMBED RIGOROUS & EFFECTIVE GOVERNANCE
- OPERATE RESPONSIBLY WITH INTEGRITY

CONTENT IN THIS SECTION

- INTEGRATED GOVERNANCE STRUCTURE
- INTERNAL CONTROL FRAMEWORK
- DATA PRIVACY AND CYBER SECURITY
- LABOUR AND HUMAN RIGHTS
- SUPPLY CHAIN RESPONSIBILITY
- SUSTAINABLE INVESTING

Linked SDGs

8 DECENT WORK AND ECONOMIC GROWTH

**16 PEACE, JUSTICE AND STRONG INSTITUTIONS**

INTEGRATED GOVERNANCE STRUCTURE

The Group integrates environmental and social governance into its corporate governance structure, providing a solid foundation for sustainability strategy, management, monitoring and assurance to be embedded throughout its operations.

This section of the report should be read in conjunction with the Corporate Governance Report of the Annual Report ⧉, which is the primary source of information about the Group's corporate governance framework and practices. For more information about governance roles and mechanisms specifically in relation to climate change, please refer the Group's TCFD Report ⧉.

Figure 6 CKHH's Integrated Governance Structure
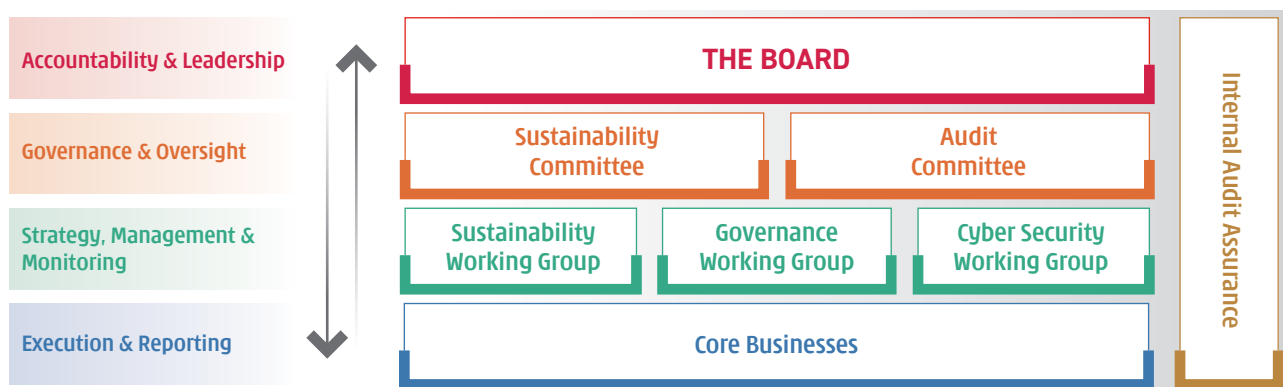
The Board

The Board has oversight and ultimate accountability for the sustainability strategy of the Group, as well as its management, performance and reporting with the support of the Sustainability Committee and the Audit Committee which play complementary roles in sustainability management. Directors are charged with the task of promoting the long term sustainable success of the Company and making decisions in the best interests of the Company with due regard to sustainability considerations.

The Board examines and approves the sustainability goals, objectives, policies and frameworks and reviews progress towards their implementation and achievement, while ensuring alignment with the Group's business strategy.

The Sustainability Committee and the Audit Committee report to the Board on sustainability risks, opportunities and assurance, which the Board examines and reviews with the committees periodically, as well as their impact on business strategy and new investments.

Board diversity

As at 31 December 2022, the Board comprised 17 directors, including seven Executive Directors, four Non-executive Directors and six Independent Non-executive Directors. The Nomination Committee, chaired by Dr Rosanna Wong, an Independent Non-executive Director, with the Chairman Mr Victor T K Li and Independent Non-executive Director Mrs Sophie Leung as members, is responsible for reviewing the structure, size, diversity profile and skill set of members of the Board.

The Group values the benefits of a diverse Board that possesses a balance of skill set, expertise, experience and perspective. Appointment of Directors is based on attributes that the selected Director will bring to the Board. Gender diversity of the Board stands at 29.4% (up from 28% in 2021), a relatively high level amongst companies listed on The Stock Exchange of Hong Kong Limited.

Sustainability Committee

The Sustainability Committee, elevated as a Board-level committee in 2020, is chaired by Mr Frank Sixt (Group Finance Director and Deputy Managing Director), with Ms Edith Shih (Executive Director and Company Secretary) and Dr Rosanna Wong (Independent Non-executive Director) as members.

The key responsibilities of the Sustainability Committee are to make recommendations to the Board on the Group's sustainability goals, objectives and strategies. It oversees, reviews and evaluates actions taken by the Group to progress its sustainability priorities and goals. The Sustainability Committee also reviews and reports to the Board on sustainability risks and opportunities, and assesses emerging sustainability issues and trends that could impact the business operations and performance of the Group. Moreover, it considers the impact of the Group's sustainability initiatives on its stakeholders and advises the Board on external communication, disclosure and publications as regards to its sustainability performance.

During 2022, the Sustainability Committee focused on reviewing progress against the targets and actions committed to by the Group. It also reviewed and approved the 2021 Sustainability Report published in May 2022. The Sustainability Committee received a report on the allocation of the proceeds and the impact created from the green bond issued in October 2021. The adequacy of resources, staff qualifications and experience, training programmes and budget of the Group's sustainability performance and reporting function was also examined and considered satisfactory by the Sustainability Committee. Following each Sustainability Committee meeting, a progress report, signed off by the Chairman of the Committee, is submitted to the Board. An agenda item is also added to the Board meeting for Directors to receive the report from the Committee and ask questions as needed.

Audit Committee

The Audit Committee oversees the effectiveness and adequacy of the Group's risk management and internal control systems, covering financial, operational and compliance aspects, per the Audit Committee Terms of Reference.

The Audit Committee currently comprises three Independent Non-executive Directors. It is chaired by Mr Wong Kwai Lam with Ms Lee Wai Mun, Rose and Mr Paul Joseph Tighe as members.

Sustainability Working Group

Supporting the Sustainability Committee is the Sustainability Working Group, comprising two Executive Directors as Co-Chairs, as well as other senior executives from key departments that influence the material sustainability impacts of the Group.

Governance Working Group

To assist the Audit Committee and the Sustainability Committee in discharging its responsibilities, a Governance Working Group chaired by the Executive Director and Company Secretary, and comprising representatives from key departments of the Company, provides timely updates, identifies emerging matters of compliance, and establishes appropriate compliance policies and procedures for Group-wide adoption.

Cyber Security Working Group

The Cyber Security Working Group is chaired by the Group Finance Director and Deputy Managing Director and comprises technical specialists from the core businesses, as well as representatives from Internal Audit and the Group Information Services Department. It oversees the cyber security risks and defences of the Group to ensure they are effective, coherent, and well-coordinated, and make recommendations as it deems appropriate to the Audit Committee per the Cyber Security Working Group Terms of Reference.

Internal Audit Assurance

Internal Audit, reporting directly to the Audit Committee and administratively to the Group Finance Director and Deputy Managing Director, provides independent assurance as to the effectiveness of the risk management activities and controls of the Group, including those related to sustainability. Internal Audit also has an important role throughout the year in sustainability data quality oversight as well as performing ongoing audits of operations to ensure the effectiveness of sustainability-related controls.

Risk Management

As part of its enterprise risk management, the Group adopts a top-down and bottom-up approach to managing sustainability risks. The Sustainability Working Group seeks insights from the Group Executive Directors and the Board, via the Sustainability Committee, about the latest developments in the external and internal environment, and how the Group responds to these emerging risks and opportunities. Meanwhile, half-yearly, each core business is required to formally identify and self-assess its risks and necessary control procedures that are in place. Subject to independent audit assurance by Internal Audit, these self-assessment results are submitted to the Executive Directors and the Audit Committee and Sustainability Committee for review and approval. Relevant assessment results are also shared with external auditors.

Full information on how the Group identifies, assesses, and manages climate-related risks is available in the latest TCFD Report ⌐.

Sustainability at the Core Businesses

Each of the core businesses operates in unique sectors and geographies and are therefore supported by their own sustainability leads, governance structures and programmes. As a common standard, each core business has set up its own cross-departmental Sustainability Working Group which is chaired by senior management.

INTERNAL CONTROL FRAMEWORK

The internal control framework, which encompasses governance policies, communication and training, due diligence, ongoing assessment, and monitoring and review, guides and supports the Group's core businesses to act with integrity throughout all areas and aspects of daily operations.

Through the Audit Committee, the Board has ultimate oversight of business ethics and compliance efforts and also regularly reviews the effectiveness of the risk management and internal control systems of the Group on an ongoing basis.

Governance Policies

The Group's business ethics are guided by its governance policies which are available to download on the Group's corporate website. Where necessary to their industry and geography, additional policies are adopted by the core businesses to further complement the policies of the Group.

> **Figure 7** Internal Control Framework

⭕ **Governance Policies**

Sustainability

- Sustainability Policy ↗
- Environmental Policy ↗
- Health and Safety Policy ↗
- Human Rights Policy ↗
- Modern Slavery and Human Trafficking Statement ↗
- Supplier Code of Conduct ↗

Corporate Governance

- Anti-Fraud and Anti-Bribery Policy ↗
- Board Diversity Policy ↗
- Code of Conduct ↗
- Corporate Communications Policy ↗
- Director Nomination Policy ↗
- Information Security Policy ↗
- Policy on Appointment of Third-Party Representatives ↗
- Policy on Personal Data Governance ↗
- Policy on Securities Dealings and Handling of Confidential and Price-sensitive Inside Information ↗
- Whistleblowing Policy ↗
- Shareholders Communication Policy ↗

SA Power Networks team meeting

A zero tolerance approach to fraud and corruption

The Board sets a tone of zero tolerance towards fraud and corruption.
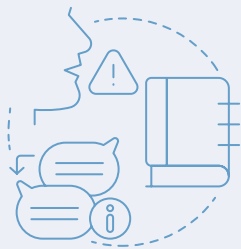
The Code of Conduct ⧉ (the "Code") sets out professional standards of the Group in all business dealings. It applies to subsidiaries and controlled affiliates, demanding strict adherence from every director and employee to the Code and applicable laws, rules, and regulations in the jurisdictions in which the Group operates. Employees serving as directors are also expected to encourage non-controlled affiliates to adopt and follow the Code.

The Anti-Fraud and Anti-Bribery Policy ⧉ provides guidance for employees on recognising and avoiding unethical behaviour in a range of business contexts, including procurement of goods and services, accepting and offering corporate gifts or hospitality, and making political or charitable contributions. The Group further promotes its commitment to anti-corruption through its selection of third party representatives via its Policy on Appointment of Third Party Representatives.

Communication and Training

The Group provides training to employees on its governance policies. Employees are required to self-declare their compliance with the Code of Conduct on an annual basis and new joiners receive training as part of their induction programmes. Training on specific governance topics, such as anti-fraud and anti-corruption, is provided to employees in accordance with their roles and areas of responsibility at least once every two years.

Due Diligence

The Group's commitment to anti-fraud and anti-corruption is also reflected in its management of business partners, suppliers, and third party representatives such as advisers, agents, and consultants. The Group conducts due diligence on the selection and renewal of new and existing business partners or suppliers based on an assessment of risk factors including transaction size, product or service nature, financial and compliance status, qualification, potential conflict of interest, and country risk.

Further, the Group adopts a comprehensive set of procurement and tendering procedures to ensure that related activities are carried out in a fair and transparent manner. Approval from the Head Office is required before engagement of third party representatives, with some exceptions, and material capital expenditure projects (in excess of predefined thresholds) also requires Head Office review and approval prior to any binding commitment.

Ongoing Assessment

Core businesses are also required to self-assess their control measures at least bi-annually to further drive improvement. In particular, for any material control deficiencies identified, they will formulate an action plan and monitor the progress closely. The results of this self-assessment are reviewed by Internal Audit and reported to the Executive Directors and the Audit Committee.

Monitoring and Review

The Group has implemented sound financial controls, including adequate segregation of duties, authorisation controls, records logging, supporting documentation, and audit trail, to prevent and detect irregularities or misconduct. This control system is subject to regular review and audit. In particular, Internal Audit, which is responsible for assessing the effectiveness and adequacy of the internal control system of the Group, conducts independent audits of the Group's ethical standards and policies in the areas of anti-corruption, fraud incident management, supplier code of conduct, fair dealing with suppliers, donations/sponsorships, handling of confidential/inside information, personal data governance, anti-trust, workplace safety, and accuracy of books and records. The audits run in a typical three-year cycle and are Group-wide. Business units exposed to higher fraud and corruption risks are subject to more frequent and intensive audits, generally once per year. All audit findings are reported to the Audit Committee and the Executive Directors and are also shared with external auditors.

Whistleblowing

The Group encourages its employees and other stakeholders, including customers, suppliers, creditors, and debtors, to raise concerns about suspected improprieties, misconduct, or malpractice. It operates various confidential reporting channels in local languages via the Group's corporate websites.

In accordance with the Whistleblowing Policy ⤢, the Group responds to each reported incident in strict confidence, and provides reassurances on protection for whistleblowers against unfair dismissal, victimisation or unwarranted disciplinary action. Each core business has internal procedures for handling reports. All core businesses must report any actual or suspected material incidents within one working day to the Group Finance Director, Deputy Managing Director, and Head of Internal Audit.

Reported incidents of fraud and corruption will be investigated. Internal Audit is responsible for reviewing reported incidents, seeking out relevant stakeholders for direction or comment, determining which incidents require in-depth investigation, and escalating its findings to the Executive Directors and the Audit Committee, as applicable.

The Executive Directors receive a summary of reported incidents and relevant statistics, including results of independent investigations and actions taken every quarter and at Audit Committee meetings. Substantiated complaints will result in disciplinary action following due management consideration, including verbal or written warnings and termination of employment. Violation of laws and regulations will be reported to law enforcement authorities, as applicable.

DATA PRIVACY AND CYBER SECURITY

Digitalisation is a powerful megatrend creating opportunities for automation, integration, data analytics, and innovation across all business areas. Ensuring data protection and effective control of cyber security risks are of paramount importance for the Group, as reflected in its comprehensive governance structure and mechanisms.

Personal Data Governance and Information Security

The Group recognises its responsibility for keeping personal data and sensitive information safe by implementing technical and organisational measures that demonstrate its compliance with legislation in relevant jurisdictions, including the EU's General Data Protection Regulation (GDPR).

The Group's Policy on Personal Data Governance ⬀ protects consumers and employees by enshrining the principles of respect for individual rights, procedural transparency, lawful processing, use and retention, and information security. It contains provisions on legitimate purposes for data collection, data usage and retention, sharing and transferring personal data, and safeguards for data processing by third parties. The Information Security Policy ⬀ outlines the Group's approach to protecting data confidentiality, integrity and availability, including personal data, as well as managing and escalating security incidents. It forms the basis for core businesses to formulate supplementary policies and procedures at the operational level.

Recognising that customers face many cyber security challenges such as phishing emails, malware, and inappropriate websites, the Group's businesses have also developed a range of resources and services to help keep them safe.

Retail

TRUST-BASED MODEL FOR PERSONALISED CUSTOMER PROMOTIONS

The Retail division's O+O (Offline plus Online) worldwide platform strategy builds on a trust-based model underpinned by its highly advanced IT systems and Cyber Security Service. Privacy data is maintained in dedicated and encrypted environments where access is under strictly-controlled regulation. All modern Cyber Security Technologies, including advanced AI threat detection mechanisms, are applied to further protect data from unauthorised usage. As an example, data on the shopping behaviour of A.S. Watson's 141 million loyalty customers is used to design and deliver personalised promotions. These are highly effective at encouraging and enabling participating O+O customers to spend on average up to three times more than customers who shop through only one channel.

141 million

Data on the shopping behaviour of A.S. Watson's 141 million loyalty customers is used to design and deliver personalised promotions.

Telecommunications

SAFER BROWSING WITH PROTECTION FROM WINDTRE

WINDTRE, in the Telecommunications division, offers a range of services to help protect its customers from emerging threats to their safety online. Its monthly subscription service for landline customers, WINDTRE Home Protect, secures home networks and connected devices from threats such as malicious links. WINDTRE Security Pro app, powered by leading IT security firm Avast, also provides comprehensive protection for smartphone customers browsing the internet on the WINDTRE network, when roaming, or in Wi-Fi. It detects viruses, malware, spyware and trojans to limit tracking and keep passwords and personal credentials safe.

WINDTRE has also introduced NeoConnessi, its education platform in Italy to help parents and children navigate the online world safely together. The platform provides articles, insights, technical tips, and advice on how to create a healthy tension of control and trust with one's child as they begin their online introduction. NeoConnessi is also an educational programme helping primary school teachers to introduce children to using the internet safely. With its fourth edition released in 2022, the educational programme has reached more than 800,000 children since its inception.

WINDTRE helps protect its customers from emerging threats to their safety online.

Cyber Security Strategy and Performance

Digitalisation increases the scope, scale, and frequency of opportunities for intruders to penetrate the Group's IT networks as more and more applications and devices go online. The Cyber Security Working Group assists the Audit Committee in fulfilling its duties in cyber security and related areas. The principal mandates of the Cyber Security Working Group is to oversee the Group's cyber security defences, monitor the cyber threat landscape and provide strategic oversight. It also ensures that the Group's efforts in managing cyber risks are effective, coherent and well-coordinated, in addition to reviewing reports on material breaches/attempted breaches of the Group's information security measures and the adequacy of actions proposed or taken.

Figure 8   Monitoring to inform continuous evolution of the Group's Cyber Security Strategy

Root cause analysis of cyber-attacks when they occur (as needed)

Active threat hunting by security log analysis, active endpoint and server cyber defence as well as network monitoring on suspicious behaviour

Comprehensive vulnerability assessments on Group IT infrastructure and applications (quarterly)

THE GROUP'S CYBER SECURITY STRATEGY

Risk assessments of various security domains among all business units (twice per year)

Ad hoc independent cyber security assessments e.g., "ethical hacking"

Threat intelligence from trusted external sources to identify potential security loopholes or incidents

Employee cyber security awareness raising campaigns

Infrastructure

INVESTING CONTINUALLY TO MITIGATE CYBER THREATS

As the utilities sector continues to digitalise, it must invest continually to mitigate cyber security risks. In 2022, EDL conducted a third-party review of its cyber security practices and information security management system against guidelines from the National Institute of Standards and Technology (NIST) and the Australian Energy Sector Cyber Security Framework (AESCSF). The review provided an overview of EDL's cyber security controls in the information technology and operational technology environment and made recommendations on how to improve its cyber security practices.
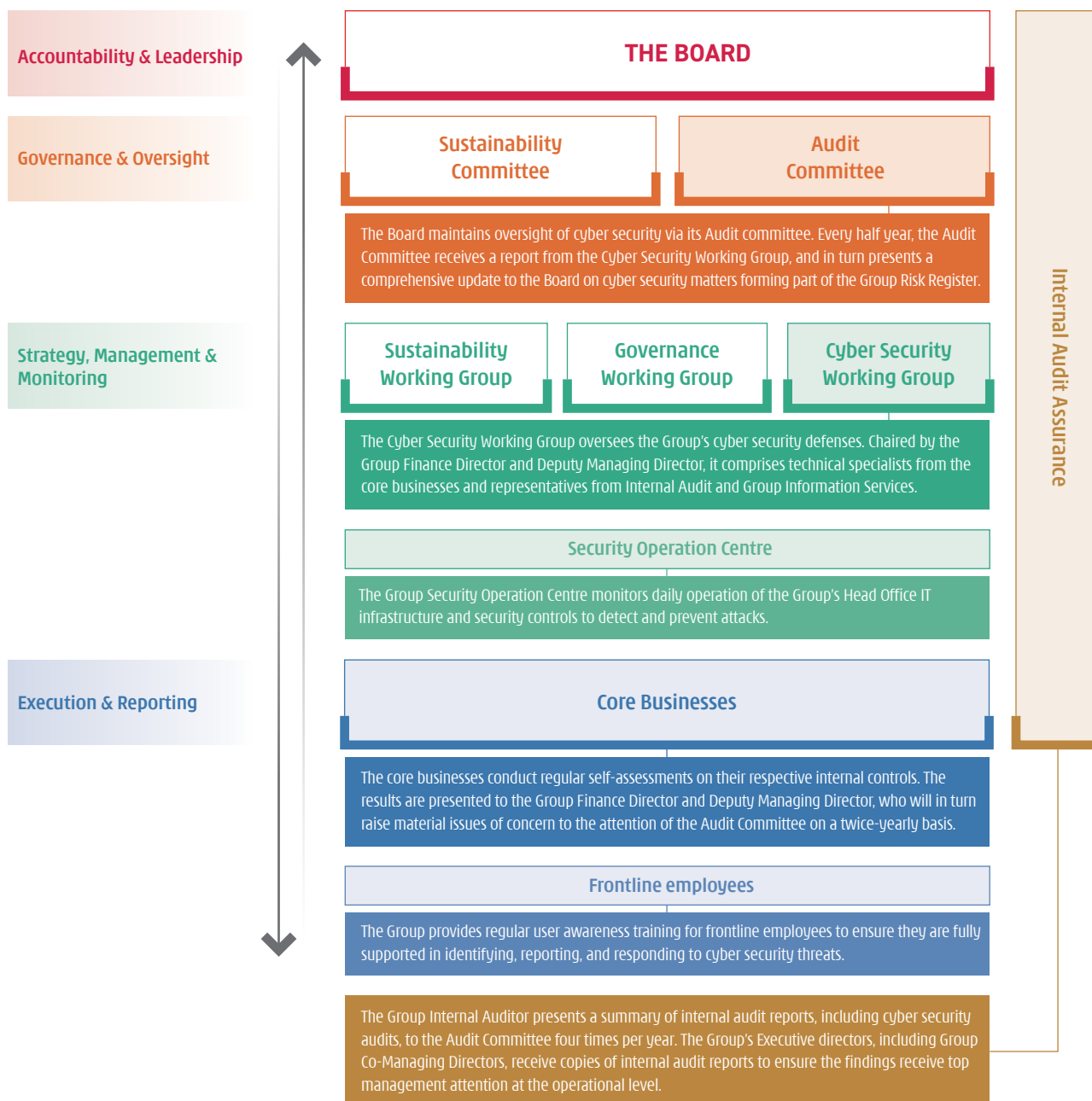
Cyber Security Risks

The Group's cyber security risk governance structure collects, consolidates, verifies, and escalates information from the operational level with additional assurance provided by Internal Audit.

Figure 9   Cyber security governance and oversight

Accountability & Leadership	**THE BOARD**	Internal Audit Assurance
Governance & Oversight	**Sustainability Committee** / **Audit Committee**	
	The Board maintains oversight of cyber security via its Audit committee. Every half year, the Audit Committee receives a report from the Cyber Security Working Group, and in turn presents a comprehensive update to the Board on cyber security matters forming part of the Group Risk Register.	
Strategy, Management & Monitoring	**Sustainability Working Group** / **Governance Working Group** / **Cyber Security Working Group**	
	The Cyber Security Working Group oversees the Group's cyber security defenses. Chaired by the Group Finance Director and Deputy Managing Director, it comprises technical specialists from the core businesses and representatives from Internal Audit and Group Information Services.	
	Security Operation Centre	
	The Group Security Operation Centre monitors daily operation of the Group's Head Office IT infrastructure and security controls to detect and prevent attacks.	
Execution & Reporting	**Core Businesses**	
	The core businesses conduct regular self-assessments on their respective internal controls. The results are presented to the Group Finance Director and Deputy Managing Director, who will in turn raise material issues of concern to the attention of the Audit Committee on a twice-yearly basis.	
	Frontline employees	
	The Group provides regular user awareness training for frontline employees to ensure they are fully supported in identifying, reporting, and responding to cyber security threats.	

The Group Internal Auditor presents a summary of internal audit reports, including cyber security audits, to the Audit Committee four times per year. The Group's Executive directors, including Group Co-Managing Directors, receive copies of internal audit reports to ensure the findings receive top management attention at the operational level.

Cyber Security Collaboration

The Cyber Security Working Group has a sub-working group focused on operational technology to enhance collaboration and leverage the deep knowledge offered by specialists working in different areas across the Group. Colleagues further exchange ideas and experiences through the Global Cyber Security Collaboration Platform.

LABOUR AND HUMAN RIGHTS

The Group respects and promotes human rights as a fundamental principle to how it operates and engages with all stakeholders. Its Human Rights Policy ⤤ **affirms the following priorities and approaches throughout its direct operations and supply chains guided by the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights:**

Treat people with dignity and respect, free from discrimination and fear of harm or abuse

Prohibit unlawful child labour or any kind of forced or bonded labour (see also the Group's Modern Slavery and Human Trafficking Statement ⤤)

Adhere to local laws and regulations governing working hours, equal and fair compensation, and rights to freedom of association and collective bargaining

Prevent and limit redundancies and include respect for human rights considerations in transition planning such as redeployment and outplacement services for impacted workers

Engage with communities on human rights, including indigenous people and other vulnerable or disadvantaged groups

This topic of Labour and Human Rights is closely linked with other material topics in the Group Sustainability Framework, including:
- Social Inclusion ⤤
- Inclusion and Diversity ⤤

SA Power Networks team members in the field

SUPPLY CHAIN RESPONSIBILITY

The Group's efforts to embed rigorous and effective governance also extends to its supply chain engagement.

Supplier Code of Conduct

Under the Group's Supplier Code of Conduct ⌐, business partners working with the Group are expected to uphold ethical standards on compliance with law and avoidance of corruption, respect for and implementation of the rights of employees, and environmental protection.

Core businesses implement tailored codes of conduct for their suppliers based on the model provided by the Group and incorporate detailed operational protocols relevant to their respective industries. In 2022, the Retail division refreshed its Supplier Code of Conduct and launched an enhanced due diligence screening process for new suppliers evaluating 23 risk indicators across five categories, including reputation and sanctions, financial, environmental, social, and governance. The Ports division has also launched an initiative across all business units to assess supply chain partners' compliance with its Supplier Code of Conduct and to develop plans for corrective action in 2023.

The Group implements effective systems and controls to ensure slavery and human trafficking is not taking place in its supply chains. It has various measures in place to ensure third parties implement anti-corruption policies and compliance programmes in accordance with relevant provisions in the Group's procurement contracts.

Supplier Screening and Assessments

End-to-end supply chain visibility is important for business units to assess risks and avoid disruptions. Supplier assessments and detailed safety and quality guidelines tailored to specific product categories play an important role in the Group's management approach to ensuring product and service safety and quality. Business units are also using dedicated external platforms and partnerships to further implement supply chain screening. For example, in 2022, **3** UK and **3** Ireland partnered with EcoVadis, the global leader in independent supply chain sustainability ratings, to support their understanding of supply chain practices across a broad range of sustainability topics. In 2022, over 55% of **3** UK's total third party spend was covered by current EcoVadis assessments, with the aim to achieve 95% coverage by the end of 2023.

As a significant procurer of goods and services, the largest supplier assessment programme within the Group belongs to the Retail division. A.S. Watson is a member of amfori, an international organisation dedicated to improving working conditions and environmental management in global supply chains. As part of its supplier assessment programme, all Own Brand suppliers in high-risk countries undergo audits referencing amfori's social and environmental requirements or other leading frameworks such as Sedex Members Ethical Trade Audits or the Initiative for Compliance and Sustainability.

374

During 2022, audits of 374 factories worldwide were conducted under A.S. Watson's sustainable supply chain programme.

Sourcing Guidelines

As a major consumer of goods and services, the Group seeks to leverage it purchasing power in support of sustainable consumption and production by choosing environmentally and socially preferable options. During 2022, among other guidelines for sustainable sourcing, the Retail division re-published Watsons' Sustainable Choices guideline for suppliers specifying more stringent requirements. It also launched a new online platform to collect detailed information on product sustainability from suppliers. Northumbrian Water, in the Infrastructure division, also has an ambitious goal to spend at least 60p in every £1 with local suppliers in the regions of its operations.

In the Telecommunications division, WINDTRE has introduced new sourcing guidelines to align its procurement decisions with decarbonisation targets. In 2022, it applied new tendering rules regarding energy consumption in the selection of microwave network equipment and it will seek to adopt these rules for all network equipment in future.

SUSTAINABLE INVESTING

Another principle of effective sustainability governance pertains to capital allocation. Sustainable Investing can deliver strategic benefits such as enhanced financial returns while providing tangible positive impacts for society and the environment. With "Focusing on Sustainability" identified as a key corporate strategic pillar for the Group, the Group is therefore committed to integrating sustainability into its investment decision making, capital and operating expenditure and debt financing.

New Investments

Sustainability considerations play an integral role in informing the Group's approach to new investments, particularly with regards to advancing its low carbon transition plans. Having committed to becoming a net-zero port operator by 2050, the Ports division has mandated that all new investments will be fully electric, and/or supplemented with other forms of clean energy such as green hydrogen. The Infrastructure division has identified sustainability as one of its four key long-term development strategies and continues to grow its business both organically and inorganically with new investments in companies and assets that support the energy transition.

Capital and Operating Expenditure

The Group has implemented detailed tracking mechanisms for monitoring capital and operating expenditure aligned with the Group's sustainability objectives. During 2022, the Group's Subsidiaries and Associates spent over USD1 billion in green spend. The largest spend categories include renewable and other clean energy generation, energy efficiency, and clean transportation, with smaller amounts in the categories of circular economy and design, and sustainable water management.

Debt Financing

Under the CKHH Sustainable Finance Framework ⬈, the Group and its subsidiaries may raise bond, loan or related financing for specific assets, projects and investments that it believes will catalyse positive environmental and/or social impact. In developing and implementing this framework, the Group has engaged various stakeholders to solicit input and has taken reference to leading standards such as the EU Taxonomy and Climate Bonds Standard. Sustainalytics provided a Second Party Opinion ⬈ on the Sustainable Finance Framework in October 2021 and completed an Annual Review ⬈ in August 2022.

In November 2021, the Group issued its first green bond of EUR500 million guaranteed notes due in 2033 aimed at influencing the environmental footprint of its operations. As of 31 May 2022, net proceeds from the 2021 Green Bond were fully allocated towards financing new projects and refinancing existing projects. In determining the allocation of the proceeds, the Group conducted multiple meetings with debt investors to understand areas of focus and preferences towards allocation. The Group has published its first Green Bond Report ⬈ providing an overview of capital allocation and expected impacts.

Canadian Power Okanagan Wind farm