GOVERNANCE

The Group recognises its duty to ensure that 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. Reviews and updates on relevant procedures and mechanisms are also conducted regularly to ensure their effectiveness according to market changes and to comply with the latest regulatory requirements.

This section also covers governance approaches to specific cross-cutting sustainability topics that the Group identifies as important and that 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

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 should be read in conjunction with the Corporate Governance Report of the 2023 Annual Report ⤤, which is the primary source of information on 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 2021 TCFD Report ⤤.

Figure 6 CKHH's integrated governance structure
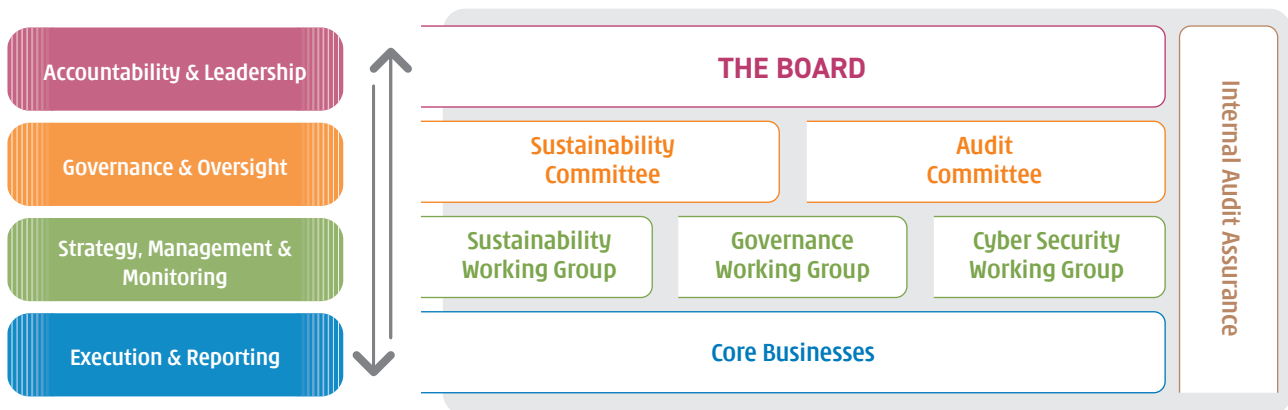
The Board

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 Group and making decisions in the best interests of the Group 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 the publication of this report, the Board comprises 19 directors, including eight Executive Directors, four Non-executive Directors and seven Independent Non-executive Directors. The Nomination Committee, chaired by Dr Wong Yick Ming, Rosanna, an Independent Non-executive Director, with the Chairman Mr Victor T K Li and Independent Non-executive Director Mrs Leung Lau Yau Fun, Sophie as members, is responsible for reviewing the structure, size, diversity profile and skillsets of members of the Board.

Female representation at the Board stands at a relatively high level (31.5%, six out of 19 Directors) amongst companies listed on The HKEX, increasing from 29.4% in 2022. Upon the retirement of Dr Rosanna Wong ⤤ from the Board at the conclusion of the annual general meeting of the Company to be held in May 2024, the female representation at the Board will decrease to 27.7% (five out of 18 Directors). The Company cements its commitment to gender diversity within its business so it continues to review and assess the appropriate level of gender diversity and composition that aligns with the strategy of the Company. The Company targets to maintain about 30% female directors on its Board. This target will be reviewed on an annual basis and from time to time by the Nomination Committee as warranted.

Sustainability Committee

The Board level Sustainability Committee is currently chaired by Mr Frank Sixt (Group Co-Managing Director and Group Finance Director), with Ms Edith Shih (Executive Director and Company Secretary) and Dr Rosanna Wong (Independent Non-executive Director) as members. With the retirement of Dr Rosanna Wong from the Broad at the conclusion of the annual general meeting of the Company to be held in May 2024, the composition of the Sustainability Committee will change, as Ms Ruth Tsim (Independent Non-executive Director) will be appointed as member. The Sustainability Committee oversees, reviews and evaluates actions taken by the Group to progress its sustainability priorities and goals, and it also drives and incorporates sustainability practices into the Group's strategy plans. 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 with regard to its sustainability performance.

In 2023, the Sustainability Committee continued to assess progress on sustainability targets and actions committed by the Group. It reviewed and approved the sustainability report published in April 2023. The Sustainability Committee also closely monitored changes on global and regional sustainability-related regulatory requirements and implemented necessary actions to ensure the Group's full compliance. In addition, the Sustainability Committee examined, and considered satisfactory, the adequacy of resources, staff qualifications and experience, training programmes and budget of the Group's sustainability performance and reporting. 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 in 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, as per the Audit Committee Terms of Reference.

The Audit Committee currently comprises four Independent Non-executive Directors. It is chaired by Mr Wong Kwai Lam with Ms Chow Ching Yee, Cynthia (appointed on 14 December 2023), Mr Paul Joseph Tighe and Ms Tsim Sin Ling, Ruth (appointed on 2 January 2024) as members. Ms Lee Wai Mun, Rose ceased to be a member of the Audit Committee upon her resignation from the Board on 14 December 2023.

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 materials sustainability impact of the Group. Members are updated with trends on the latest sustainability topics that are material to the Group (i.e. disclosure standards and regulatory requirements), and potential implementation and strategy sustainability plans would be guided with professional input.

Governance Working Group

To assist the Audit Committee and the Sustainability Committee in discharging their 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 Co-Managing Director and Group Finance 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 defences of the Group to ensure that the Group's tools and measures in managing cyber risks are effective, coherent and well-coordinated. Employee education and ongoing training in cyber security are arranged to increase knowledge of cyber threats and the best practices for safeguarding digital assets and data. It also makes recommendations as it deems appropriate to the Audit Committee as 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 Co-Managing Director and Group Finance 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 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 the 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 in 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. Periodic cross-business divisions meetings are also arranged, ensuring that the Group's sustainability directive, targets and goals are fully explained. During the year, Group-wide initiatives on the pursuit of net-zero targets and transition plans were discussed and progress was reported from all divisions. Details of which can be found in the "Environment ⤤" section of this report.

Sustainability team meeting, SA Power Networks

INTERNAL CONTROL FRAMEWORK

The internal control framework, which encompasses governance policies, communication and training, ongoing assessment, due diligence, 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 internal portal or 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 ⬀
- Biodiversity 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 ⬀

A zero-tolerance approach to fraud and corruption

The Board sets a tone of zero-tolerance towards fraud and corruption.
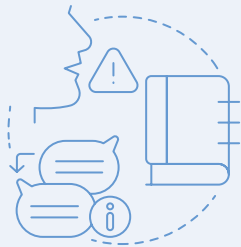
The Code of Conduct ⤢ (the Code) sets out professional standards of the Group in all business dealings. It applies to subsidiaries and controlled affiliates, demanding strict adherence from every director and employee to the Code and applicable laws, rules and regulations in the jurisdictions in which 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. Other operational or functional training courses are also offered throughout the year, with topics from data analysis to leadership and career skills development. These are available for all levels of employees to subscribe to.

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 generally required before engagement of third-party representatives generally 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, any material control deficiencies identified will entail an action plan being formulated and progress monitored closely. The results of this self-assessment are discussed in meeting, 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 trails, 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 Co-Managing Director and Group Finance Director and Head of Internal Audit.

Reported incidents of fraud and corruption will receive a comprehensive investigation. Internal Audit is responsible for reviewing reported incidents, seeking 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.

Figure 8 Cyber security governance and oversight

Accountability & Leadership	**THE BOARD**
Governance & Oversight	**Sustainability Committee** **Audit Committee**
	The Board maintains oversight of cyber security via the 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 defences. Chaired by the Group Co-Managing Director and Group Finance 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 for 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 Co-Managing Director and Group Finance 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 that they are fully supported in identifying, reporting, and responding to cyber security threats.
	Internal Audit 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 that the findings receive the attention of senior management at the operational level.

Internal Audit Assurance

Personal Data Governance and Information Security

The Group recognises its responsibility to keep 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.

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 protect 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.

With the ever-increasing cyber security challenges, such as phishing emails, text messages, malware and inappropriate websites, the Group's businesses will continue to work hand-in-hand with its customers, offering a range of resources and solutions to safeguard their businesses.

Retail

CYBER SECURITY AND ENCRYPTED CUSTOMER DATA

The Retail division's O+O (Offline plus Online) worldwide platform strategy is built on a trust-based model underpinned by its highly advanced IT systems and cyber security service. For instance, data on the shopping behaviour of AS Watson's 159 million loyal customers is maintained in dedicated and encrypted environments where access is strictly controlled. The data is only made available for the design and delivery of personalised promotions. To further protect data from unauthorised usage, all modern cyber security technologies, including advanced AI threat detection mechanisms, are applied.

159 million

Data on the shopping behaviour of the 159 million AS Watson loyal customers are maintained in dedicated and encrypted environments where access is strictly controlled.

Telecommunications

SAFER BROWSING WITH THE SENIORS

The first cyber security internal faculty, #Cyber4Seniors, was built and dedicated to the parents and grandparents of Wind Tre employees. In line with Wind Tre's value of responsibility, it is the intention to contribute through this initiative to breaking down the digital gap, placing a particular focus on the issues of

IT security, which are increasingly important in the digital world, but at the same time exposed to cyber security issues. The programme was launched in 2023, through which 221 seniors received training from experts and gained understanding on topics such as scams and other forms of online dangers.

Infrastructure

CYBER SECURITY INCIDENT RESPONSE PLAN AND DISASTER RECOVERY TEST

United Energy and Victoria Power Networks have implemented the "Cyber security Incident Response Plan" demonstrating commitment to enhancing cyber security measures within business operations. This plan provides operational guidelines for effectively identifying and promptly addressing cyber security incidents.

Disaster recovery tests are also carried out by United Energy and Victoria Power Networks to mitigate potential disruptions and ensure the continuity of business operations. By regularly evaluating their disaster recovery plans, United Energy and Victoria Power Networks can identify any weaknesses or gaps in systems and processes and make necessary improvements to maintain the integrity of their information assets.

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 reviewing and managing cyber security and related areas.

The principal mandates of the Cyber Security Working Group are to oversee the Group's cyber security defences, monitor the cyber security threat landscape and provide strategic oversight. The Group "Cyber Security Policy" provides a framework for defining the baseline for cyber security practices, and managing cyber

security risks to ensure that the Group's tools and measures in this area are effective, coherent and well-coordinated. The Group Cyber Security Incident Reporting Policy provides guidelines for reporting and responding to cyber security incidents, in order to minimise impact and prevent future occurrences. These frameworks elevate the Group's information security measures and the adequacy of actions proposed or taken to protect against cyber security threats.

Experts from the Group's Cyber Security team will remain vigilant in monitoring and addressing external cyber security threats to ensure operations are free from disturbance.

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

GROUP CYBER SECURITY POLICY ──────

Defines the baseline for protection against cyber security threats and supports development of protection controls and programmes to strengthen the Group's cyber security maturity

Group Cyber Security Incident Reporting Policy

Provides guidelines on reporting cyber security incidents to minimise impact and prevent future occurrence by feeding intelligence to Risk Assessments and Threat Intelligence

GROUP 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 campaigns

Infrastructure

CYBER SECURITY AWARENESS STRATEGY, DELIVERY PLAN AND TRAINING

Similar to other business divisions across the Group, SA Power Networks has in place a cyber security awareness strategy and delivery plan, including regularly disseminating at least one article per fortnight through electronic media channels and twice-yearly refreshments of posters at various sites. A monthly online awareness session and monthly phishing exercises are organised for all employees. Employees are also required to complete an annual training course online. The primary objective of implementing these comprehensive measures is to enhance its employees' awareness regarding cyber security threats and best practices and emphasise users' critical role in preventing them.

As part of its cyber security programme, Alliance Construction Materials and Wales & West Utilities also provides regular online awareness training to all its employees, and it is compulsory for every employee to attend the training and complete an assessment. The objective is to equip employees with the knowledge and ability to identify and respond to cyber security incidents proficiently. The online cyber security awareness course offered by Wales & West Utilities is also a UK National Cyber Security Centre accredited course and is a mandatory course for all employees upon joining the organisation.

Group

PHISHING AWARENESS

Phishing poses a significant threat by tricking individuals into revealing sensitive information such as passwords and confidential data. It could lead to identity theft, financial losses and unauthorised access to personal and corporate accounts through malicious emails and exploits human vulnerability through social engineering techniques to deceive unsuspecting victims.

The Group understands the cyber security threats that arise from phishing attacks and maintains a high awareness level among all employees by conducting regular phishing simulations and training campaigns. The Group Cyber Security team manages related activities on a monthly basis and measures their effectiveness through dedicated metrics. The team also shares information or articles with all employees on the latest cyber security trends and best practices on a regular basis. By doing so, general cyber security awareness to defend against cyber criminals is upheld.

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.

Responsible use of AI

While AI, such as OpenAI and ChatGPT can reduce time and efforts spent on producing work-related content, it should be used responsibly and in compliance with applicable laws and regulations to avoid legal issues and information leakage. The Group has reviewed and updated the internal "Group Cyber Security Acceptable Use Policy", providing guiding principles of use and responsibilities for senior management and employees in business units in general. The Group will continue to monitor progress regularly and update the relevant policy to ensure its effectiveness.

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 in its operations and engagement with stakeholders, as it values the diversity and inclusion of the individuals with whom it works. It is committed to equal opportunity and to maintaining workplaces that are free from discrimination or harassment. Its Human Rights Policy **affirms the following priorities and approaches throughout its direct operations and supply chains as 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 re-deployment 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

Employee at work, Northern Gas Networks

SUPPLY CHAIN RESPONSIBILITY

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

Supplier Code of Conduct

The Group has implemented a Supplier Code of Conduct which is enforced across our business, requesting its business partners to uphold the same ethical standards as the Group. Under the Group's Supplier Code of Conduct ⤤, business partners working with the Group are expected to comply fully with local laws and regulations, promote ethical standards, protect the rights of all employees and operate responsibly.

Core businesses implement tailored codes of conduct for suppliers based on the model provided by the Group and incorporate detailed operational protocols relevant to their respective industries. The Retail division has launched an enhanced Supplier Code of Conduct, including an improved due diligence screening process for new suppliers, evaluating 23 risk indicators across five categories, including reputation and sanctions, financial, environmental, social and governance. As of 2023, more than 8,600 suppliers have completed the process. The Ports division has also launched similar initiatives across business units, pre-screening business partners' compliance according to its sustainable procurement guideline.

The Group implements effective systems and controls to ensure slavery and human trafficking are 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

As the Group operates across industries and regions, its overall consumption footprint can be significant. A comprehensive sustainable procurement guideline that assesses suppliers' performance, such as product safety and quality, can be of great assistance to the Group's approach in sustainable material sourcing. Business divisions have been implementing additional measures and leveraging on external platforms to further implement supply chain screening. For example, **3** UK and **3** Ireland have been working with EcoVadis since 2022, the global leader in independent supply chain sustainability ratings, to support the understanding of supply chain practices across a broad range of sustainability topics. As a result, over 90% of total third-party sourcing activities are currently covered by the EcoVadis assessment in the UK, as compared to 55% in 2022, and both the **3** UK and **3** Ireland target to achieve 95% of coverage in the near future.

As a significant procurer of goods and services, the largest supplier assessment programme within the Group belongs to the Retail division, which has been a member of amfori, working towards improving working conditions and environmental management in global supply chains. As part of its supplier assessment programme, all Exclusive Brands 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. The AS Watson sustainable supply chain programme continued the audits in 2023 covering 308 factories worldwide.

Sourcing Guidelines

As a major consumer of goods and services, the Group seeks to leverage on its purchasing power in support of sustainable consumption and production by choosing environmentally and socially preferable options. In 2023, to facilitate the achievement of the vision of Hutchison Ports to be "the preferred partner for a sustainable supply chain", a group-wide initiative was rolled out by requesting suppliers and business partners to complete a "Supplier Sustainability Self-Assessment Questionnaire" for assessing their conformance on the Supplier Code of Conduct (covering sound environmental performance, social well-being and governance practices) and developing corrective plans for any non-conformances. In addition, the Procurement and Shared Services team at SA Power Networks also regularly reviews summary reports to evaluate the risk of modern slavery within its supply chain. These reports are subsequently utilised to refresh the organisation's internal dashboard, enabling the continuous monitoring of suppliers and the corresponding levels of risk.

Since 2022, Wind Tre from the Telecommunications division has implemented sourcing guidelines that align procurement decisions with its decarbonisation targets. In 2023, the tendering rules regarding energy consumption in the selection of microwave network equipment have been tested, formalised and applied to other similar tenders. Wind Tre will continue to explore similar tendering rule applications with other kinds of purchases in the future.

Warehouse, PARKnSHOP

SUSTAINABLE INVESTING

Capital allocation is crucial to effective sustainability governance. Sustainable investing can deliver strategic benefits such as enhanced financial returns while providing tangible positive impact for society and the environment. The Group identified "Focusing on Sustainability" as one of its key corporate strategic pillars and considered the elements of sustainability during investment decision-making, capital and operating expenditure and debt financing.

New Investments

Sustainability considerations play an integral role in determining the Group's approach to new investments, particularly with regard to advancing its low-carbon transition plans. Having committed to becoming a net-zero port operator by 2050, Hutchison Ports will opt for electric models for equipment and/or truck replacement and for any approved new purchase, which will be supplemented with other forms of clean energy such as green hydrogen. As a result, over 25% of the division's equipment and trucks are powered either by electric or hybrid source up until the end of 2023. 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. For further details, please refer to the "Sustainable Business Model and Innovation – Climate Resilient Business ⧉" section of this report.

Capital and Operating Expenditure

The Group has enhanced the tracking mechanisms for monitoring and reporting capital and operating expenditure aligned with the Group's sustainability objectives. The numbers and analysis are regularly reported to senior management to ensure effective monitoring. Details can be found in the "Disclosure on Green Spendings" section below.

Disclosure on Green Spending

During 2023, the Group's subsidiaries and associates spent over US$1.8 billion in green spending. The spend categories include energy efficiency, renewable and other clean energy, sustainable transport, sustainable water management, circular economy and design, biodiversity protection and small amounts in the sustainable supply chain. To enable stakeholders to understand the potential implication of climate change on the Group's operations, the Group will progressively disclose the anticipated material impact from climate-related risks and opportunities, the expected financial impact over the short, medium and long term, and strategy and resource required to pursue its net-zero transition plans. More descriptive and quantitative disclosures will be available in the Group's subsequent sustainability reports as appropriate. Details are set out below:

Table 1   Green Spending in 2023

Project Category	Amount in 2023 (US$, million)	Accumulated Amount 2019 to 2023 (US$, million)
Energy Efficiency	920.52	2,024.35
Renewable and Other Clean Energy	546.92	2,995.86
Sustainable Transport	156.90	365.81
Sustainable Water Management	113.77	372.05
Circular Economy and Design	56.47	148.02
Biodiversity Protection	46.58	93.00
Sustainable Supply Chain	0.07	0.07
Total Green Spendings	**1,841.23**	**5,999.16**

Debt Financing

Under the CKHH Sustainable Finance Framework, the Group and its subsidiaries may raise bonds, loans 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 from leading standards such as the EU Taxonomy and Climate Bonds Standard. Sustainalytics was contracted to provide a Second Party Opinion on the Sustainable Finance Framework and complete an Annual Review in May 2023.

The Group will regularly review its position on green financing against the prevailing market conditions. 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 published its first Green Bond Report which provides an overview of capital allocation and expected impact and will continue to monitor market conditions for further activity in the future.

Ports equipment electrification, Hutchison Ports UK