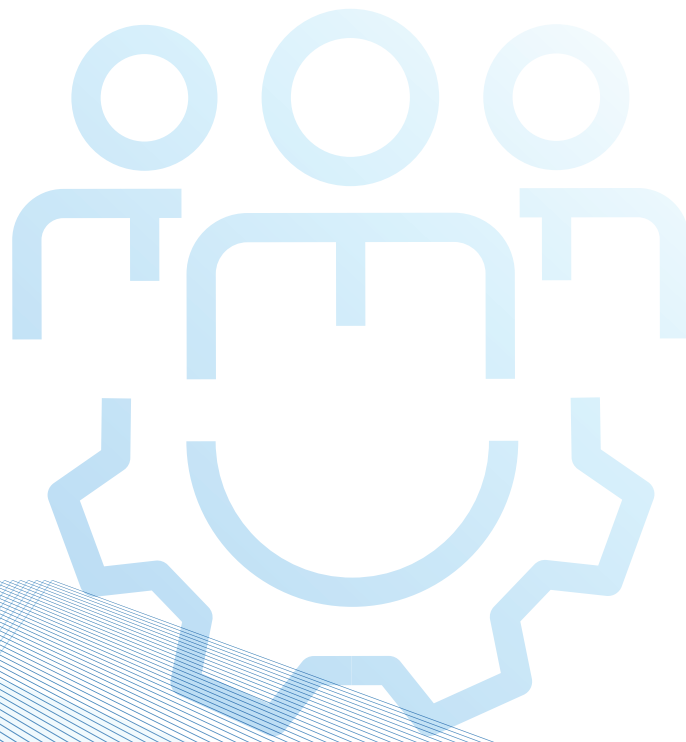


GOVERNANCE

Committed to responsible business conduct, the Group applies best-in-class practices to guide operations, minimise adverse impacts, and foster long-term sustainable growth that serves the best interests of stakeholders. Management regularly reviews developments across divisions and refines processes and mechanisms to ensure alignment with evolving market dynamics and regulatory requirements.

This section outlines the Group's governance approach and the material sustainability topics identified as priorities. These topics, such as Digital Responsibility and Information Security, Responsible Use of Artificial Intelligence, Labour and Human Rights, and Supply Chain Responsibility, are embedded within the Group's governance framework to uphold responsible and ethical practices across all business units.



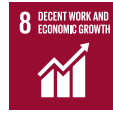
GROUP GOALS

- EMBED RIGOROUS AND EFFECTIVE GOVERNANCE
- OPERATE RESPONSIBLY WITH INTEGRITY

CONTENT IN THIS CHAPTER

- INTEGRATED GOVERNANCE STRUCTURE
- SUSTAINABILITY PERFORMANCE-LINKED APPRAISAL
- INTERNAL CONTROL FRAMEWORK
- DIGITAL RESPONSIBILITY AND INFORMATION SECURITY
- RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE
- SUPPLY CHAIN RESPONSIBILITY
- LABOUR AND HUMAN RIGHTS

Linked SDGs

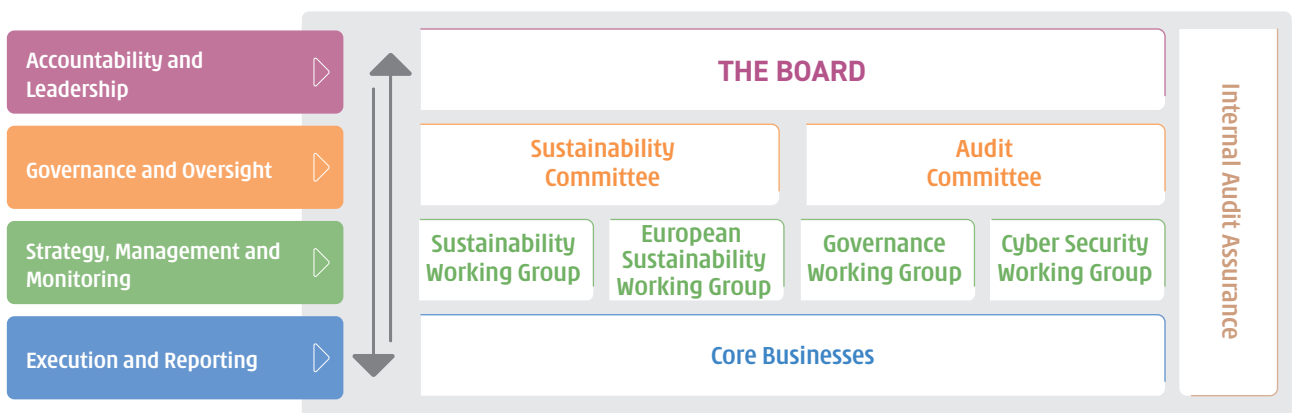


INTEGRATED GOVERNANCE STRUCTURE

The Group has implemented a comprehensive governance structure to oversee its sustainability strategy, monitor performance, and provide assurance across all divisions. This framework ensures that environmental and social considerations are fully integrated into the Group's corporate governance practices.

This section should be read alongside the Corporate Governance Report in the [2025 Annual Report](#), which serves as the primary reference for the Group's governance framework and practices. For details on governance roles and mechanisms specifically related to climate change, please refer to the Group's [TCFD Report](#) and the Climate Transition and Resilient Business section in this report.

CKHH's integrated governance structure



The Board

The Board provides oversight of the Group's sustainability strategy, management, performance, and reporting, supported by the Sustainability Committee and the Audit Committee. It reviews and approves sustainability goals, objectives, policies, and frameworks to ensure alignment with the overall business strategy. The Board monitors implementation and progress, with Directors accountable for driving long-term sustainable growth and making decisions with a strong sustainability focus.

The Sustainability Committee and Audit Committee report two and four times per year respectively to the Board, and covered topics including sustainability risks, opportunities, and assurance matters, which are assessed for their impact on business strategy and new investments.

Board Diversity

Following Board changes in 2025, female representation stands at 28% (five out of 18 Directors), maintaining a relatively high level compared to the average female representation percentage as stated by the HKEX in 2025. Upon the retirement of Mr Chow Kun Chee, Roland and Mr Lee Yeh Kwong, Charles from the Board with effect from the conclusion of the 2026 AGM, the female representation on the Board will increase to 31.2% (five out of 16 Directors). The Group remains committed to promoting gender diversity and continues to review and assess the appropriate level of diversity and Board composition to align with its strategic objectives. The Company has set a target of approximately 30% female representation on the Board, which is reviewed annually and periodically by the Nomination Committee as necessary.

To ensure a balanced mix of perspectives and experience, the Company pursues various initiatives that support its strategic priority of maintaining a diverse Board. Structured recruitment, selection, and training programmes across different levels of the Group are ongoing to develop a broader pool of skilled and experienced potential Board members.

Sustainability Committee

The Board-level Sustainability Committee is chaired by Mr. Frank John Sixt (Group Co-Managing Director & Group Finance Director), with Ms. Edith Shih (Executive Director & Company Secretary)⁽¹⁾ and Ms. Tsim Sin Ling, Ruth (Independent Non-Executive Director) as members. The Committee is responsible for recommending the Group's sustainability objectives, strategies, priorities, initiatives, and goals to the Board. It oversees, reviews, and evaluates actions taken to advance these priorities, including coordination with divisions to ensure that operations and practices align with established goals.

The Committee reports at least twice annually to the Board on sustainability risks and opportunities and monitors emerging issues and trends that may impact the Group's operations and performance. It also considers the implications of the Group's sustainability programmes for stakeholders, including employees, shareholders, investors, customers, business partners, suppliers, governments and regulators, local communities, NGOs, and the environment. Additionally, the Committee advises the Board on public communications, disclosures, and publications related to sustainability performance. It is authorised by the Board to obtain independent professional advice on matters within its remit when necessary.

Audit Committee

The Audit Committee is responsible for overseeing the effectiveness and adequacy of the Group's risk management and internal control systems, covering all material controls, including financial, operational, and compliance controls, in accordance with its Terms of Reference. The Committee currently comprises of five Independent Non-Executive Directors and is chaired by Mr. Wong Kwai Lam, with Ms. Chow Ching Yee, Cynthia, Mr. Graeme Allan Jack, Mr. Paul Joseph Tighe, and Ms. Tsim Sin Ling, Ruth as members. Please also refer to the [2025 Annual Report](#) for their respective professional backgrounds.

Sustainability Working Group

The Sustainability Working Group, which supports the Sustainability Committee, is co-chaired by two Executive Directors and includes senior executives from key departments that influence the Group's sustainability impact. Members receive regular updates on emerging material sustainability topics, including disclosure and regulatory requirements, and provide guidance on the development, implementation, and strategic direction of the Group's sustainability plans.

European Sustainability Working Group

The European Sustainability Working Group is comprised of the Group and divisional senior sustainability leads, as well as European cross-functional, senior representation from Legal, Finance, Institutional and Corporate Affairs, and Group Management Services. It collaborates to monitor increasingly stringent regulatory developments, harmonise compliance approaches, and share best practices among sustainability leads. By fostering alignment and supporting the head office in implementing region-specific changes, the Working Group enhances the Group's ability to manage regulatory risks and maintain stakeholder confidence in its commitment to responsible and compliant operations.

Governance Working Group

The Governance Working Group, chaired by the Executive Director & Company Secretary, supports both the Audit Committee and the Sustainability Committee in fulfilling their oversight responsibilities. Comprising representatives from key departments, the Working Group promotes cross-functional collaboration to monitor regulatory developments, identify emerging compliance risks, and develop robust implementation frameworks across the Group. These efforts ensure strong governance, proactive risk management, and timely responses to evolving sustainability and regulatory challenges, reinforcing the Group's commitment to transparency and stakeholder trust.

Cyber Security Working Group

The Cyber Security Working Group, led by the Group Co-Managing Director & Group Finance Director, unites technical experts from core businesses with specialists from Internal Audit and the Group Information Services Department to advance the Group's digital resilience strategy. The Working Group ensures cybersecurity measures remain robust and adaptive to evolving threats, while prioritising employee awareness through targeted education and regular training programmes. These initiatives equip staff with the knowledge to identify risks and safeguard digital assets. By providing strategic recommendations to the Audit Committee, the Working Group reinforces strong governance and accountability over the Group's cyber security infrastructure, underscoring its commitment to protecting stakeholders and maintaining trust in a rapidly changing digital landscape.

Internal Audit Assurance

Internal Audit plays a key role in supporting corporate governance by providing objective insights into the Group's management of risks and effective control mechanisms. For detail please see Internal Audit and Enterprise Risks Management section.

(1) Ms. Edith Shih completed the University of Cambridge Business Sustainability Management programme at the University of Cambridge and obtained a certification of completion from the University of Cambridge Institute for Sustainability Leadership.

Sustainability in the Core Businesses

The Group's core businesses, operating across diverse sectors and geographies, maintain dedicated sustainability governance structures tailored to their operational contexts. Each business has established cross-functional sustainability working groups under the senior management's and the sustainability managers' leadership to ensure comprehensive oversight at the operational level. Periodic cross-divisional meetings align sustainability directives, targets, and goals across the Group, ensuring consistency and collaboration. During the reporting year, efforts focused on Group-wide initiatives such as decarbonisation and climate transition planning, with all divisions systematically reporting on progress. Further details on these initiatives are provided in the [Environment](#) chapter of this report.



SUSTAINABILITY PERFORMANCE-LINKED APPRAISAL

The Group adopts a strategic initiative to integrate ESG performance metrics into its remuneration framework, commencing with a phased rollout at the management level. This initiative strengthens the Group's existing division-wide performance appraisal system, which provides structured feedback to employees on their achievements and development opportunities. Regular performance evaluations continue to inform annual compensation decisions, which are being enhanced to incorporate sustainability-linked criteria. In 2025, the Ports and Telecommunications divisions began developing Short-Term Incentive Plans (STIPs) and Long-Term Incentive Plans (LTIPs) linked to sustainability performance. At the Retail division, Scope 1 and 2 GHG reduction performance against the 2018 baseline has been incorporated as an STIP/LTIP metric for nominated executives.

Ports



STIP AND LTIP INITIATIVES IN THE PORTS DIVISION

Hutchison Ports has begun incorporating sustainability-linked KPIs into both its STIP and LTIP for nominated executives. These KPIs cover four key areas:

1. Carbon intensity aligned with its decarbonisation pathway
2. Business continuity management
3. Safety
4. Diversity and inclusion

Performance against these metrics is assessed and validated on a semi-annual and annual basis, directly influencing incentive outcomes in accordance with the respective plan rules. Nominated executives primarily comprise department heads and senior leaders at

business unit and divisional levels. Other employees are encouraged to incorporate sustainability-related objectives into their performance goals where relevant to their roles.

For climate-related KPIs, carbon intensity is the core measure, defined as total Scope 1 and 2 emissions per TEU. Annual targets for each business unit are set based on the previous year's reductions relative to the 2021 baseline, ensuring goals are both tailored and progressively more ambitious across the division. By embedding sustainability into performance incentives, Hutchison Ports strengthens leadership accountability and drives measurable progress towards its environmental and social commitments.

Infrastructure



STIP AND LTIP INITIATIVES IN THE INFRASTRUCTURE DIVISION

At Northumbrian Water, performance evaluation is underpinned by a balanced scorecard: 60% of these metrics are non-financial, underscoring commitment to customer satisfaction, environmental stewardship, employee wellbeing, and community enrichment. To further bolster its environmental focus, since 2023, Northumbrian Water has included a stringent standard

within its scorecard framework, mandating a minimum 3* rating from the Environmental Performance Assessment (EPA) as a prerequisite for any reward linked to environmental metrics. 20% of the total STIP potential is linked to water related performance, including leakage, pollution and control of sewer flooding.

Telecommunications



STIP AND LTIP INITIATIVES IN THE TELECOMMUNICATIONS DIVISION

Across European business units, sustainability-linked KPIs were incorporated for the first time into leadership STIP plans. These covered the following topics:

- Scope 1 and 2 GHG emissions reduction
- Actions to support Scope 3 measurement and reduction, including supplier engagement
- Renewable electricity procurement
- Circular devices and networks
- Women in management
- Training hours
- Supplier sustainability assessment

This framework is being further refined, with sustainability-linked KPIs also embedded in the LTIP framework from 2026 onwards.



INTERNAL CONTROL FRAMEWORK

The Group upholds operational integrity through a comprehensive internal control framework encompassing governance policies, structured communication and training programmes, continuous assessments, rigorous due diligence processes, and systematic monitoring and review. This framework underpins the Group's commitment to ethical conduct, operational excellence, rigorous financial reporting, and full regulatory compliance throughout its daily operations.

The Board maintains oversight of business ethics and compliance through the Audit Committee, which conducts regular evaluations of the Group's risk management and internal control systems to ensure adherence to the highest corporate governance standards.

Internal Control Systems

The Group's financial control system underpins its internal control framework, incorporating segregation of duties, structured authorisation protocols, systematic record-keeping, comprehensive documentation requirements, and detailed audit trails. This system is subject to ongoing review and audit to ensure its effectiveness in preventing and detecting irregularities or misconduct.

Core businesses conduct semi-annual self-assessments of their internal control systems to drive continuous improvement. When material control deficiencies are identified, dedicated action plans are developed and closely monitored to ensure timely resolution. The outcomes of these self-assessments undergo thorough review, including management-level discussions, independent evaluation

by Internal Audit, and formal reporting to the Executive Directors and the Audit Committee. This process reinforces accountability and supports the Group's commitment to maintaining robust governance and risk management practices.

Governance Policies

The Group's commitment to high standards of business ethics is guided by governance policies accessible through the internal portal and corporate website. These policies are approved by the Board and are reviewed and updated as necessary to ensure continued relevance and effectiveness. To address specific industry or regional requirements, individual business units may adopt supplementary policies that align with the Group's overarching governance framework.

Corporate integrity framework



○ Sustainability Policies

- [Sustainability Policy](#) ↗
- [Biodiversity Policy](#) ↗
- [Environmental Policy](#) ↗
- [Health and Safety Policy](#) ↗
- [Human Rights Policy](#) ↗
- [Modern Slavery and Human Trafficking Statement](#) ↗
- [Supplier Code of Conduct](#) ↗
- [Workforce Diversity Policy](#) ↗

Corporate Governance Policies

- [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](#) ↗

Internal Audit and Enterprise Risks Management

Internal Audit, reporting directly to the Audit Committee with administrative oversight from the Group Co-Managing Director & Group Finance Director, provides independent assurance on the effectiveness and adequacy of the Group's risk management and internal control systems, including sustainability-related processes. Using a risk-based methodology, Internal Audit develops and continuously reassesses its audit plan, accounting for both internal and external factors. The scope of audits includes ethical standards and policy compliance across critical areas such as anti-corruption, fraud incident management, supplier code of conduct, fair dealings, donations and sponsorships, handling of confidential and inside information, personal data governance, antitrust compliance, workplace safety, and accuracy of books and records, as well as sustainability data quality. These efforts reinforce the Group's commitment to strong governance and transparency, while supporting its long-term sustainability objectives.

Audits are conducted on a three-year cycle across the Group, with business units exposed to higher fraud and corruption risks subject to more frequent audits, typically annually. All audit findings are reported to the Audit Committee, Executive Directors, and senior management, and are shared with external auditors. Internal Audit maintains close dialogue with external auditors to ensure alignment and awareness of significant factors that may influence their respective scopes of work.

In parallel, the Group's enterprise risk management framework facilitates identification, assessment, and monitoring of significant sustainability risks through a structured "top-down and bottom-up" approach. Regular stakeholder input and management reviews ensure comprehensive oversight, with outcomes compiled into a composite risk register submitted to the Board via the Audit Committee. This analysis feeds into the annual enterprise risk management review, aligning sustainability insights with strategic risk governance. Additionally, each division conducts semi-annual self-assessments to evaluate mitigation effectiveness.

External Audit on Management Systems

External audits of management systems provide an independent assessment of alignment of the Group's processes with internationally recognised best practice standards such as Quality Management System ISO 9001, Environmental Management System ISO 14001, or Occupational Health and Safety Management System ISO 45001. Conducted by accredited third-party auditors, these reviews evaluate compliance, identify gaps, and highlight opportunities for improvement. The results help the Group and its core businesses strengthen governance, enhance operational performance, and maintain or achieve certification, assuring stakeholders that the systems in place are effective, reliable, and continuously improving. Details on the Group's certifications can be found in the corresponding sections.

A Zero-Tolerance Approach to Fraud and Corruption

The Board maintains a zero-tolerance stance on fraud and corruption across all levels of the organisation.



The Group's [Code of Conduct](#) is the central tool through which the Group sets the conduct expectations for employees underscoring the strong commitment of the Group to upholding high standards of business integrity, honestly and transparency in all its business dealings. Directors and employees must comply with the Code of Conduct and all applicable laws, rules, and regulations in the jurisdictions where the Group operates.



The Group's [Anti-Fraud and Anti-Bribery Policy](#) provides clear guidance on identifying and preventing unethical behaviour across various business contexts, including procurement, gift and hospitality protocols, and political or charitable contributions. The Group further reinforces its commitment to ethical business practices through the [Policy on Appointment of Third-Party Representatives](#), which ensures rigorous due diligence and consistent anti-corruption standards in the selection and engagement of external representatives.

Whistleblowing

The Group maintains an accessible and confidential reporting system for employees and stakeholders, including customers, suppliers, creditors, and debtors, to raise concerns about suspected improprieties, misconduct, or malpractice.

In accordance with the [Whistleblowing Policy](#), all reported cases are handled with strict confidentiality, and whistleblowers are protected against unfair dismissal, victimisation, and unwarranted disciplinary action. Each core business has formal procedures for managing reports and must escalate any actual or suspected material incidents to the Group Co-Managing Director & Group Finance Director and Head of Internal Audit within one working day.

Reported incidents of fraud and corruption are subject to thorough investigation. The Internal Audit function reviews all reported cases, consults relevant stakeholders, determines the need for in-depth investigation, and escalates findings to the Executive Directors and the Audit Committee as appropriate. The Executive Directors receive quarterly updates summarising reported incidents, investigation outcomes, and actions taken.

Substantiated complaints result in disciplinary action following due management review, which may include verbal or written warnings or termination of employment. Violations of laws and regulations are reported to the relevant law enforcement authorities as required.

Proactive Communication and Mandatory Training

The Group implements a structured governance training framework to ensure a strong understanding of ethical standards and regulatory compliance across all levels of the organisation. All headoffice employees are required to complete an annual e-learning course on business ethics (covering topics such as anti-bribery, fraud and corruption), and must also submit a declaration confirming that no acts of non-compliance were committed during the year.

In 2025, the Group supplemented its Anti-Fraud and Anti-Bribery Policy, the Policy on Appointment of Third Party Representatives and the Whistleblowing Policy upon the introduction of the UK Economic Crime and Corporate Transparency Act as part of the ongoing efforts to enhance fraud prevention procedure. The internal annual training module on the CKHH Code of Conduct, applicable to all CKHH's full-time and part-time employees, was also enhanced to further strengthen employee alignment with the Group's ethical standards. It provides comprehensive guidance on the assuring aspects of business ethics, including the whistleblowing mechanism, procedures and reporting of potential unethical issues.

Infrastructure



REINFORCING DIVISION-WIDE COMMITMENT TO ETHICAL CONDUCT

To further reinforce the commitment to combating corruption, individual business units within the Infrastructure division have introduced tailored educational initiatives. For example, in June 2025, HK Electric's Internal Audit Department, in collaboration with the division's Legal Counsel & Company Secretarial Department, launched a mandatory online training

programme titled "Integrity in the Workplace: Say 'No' to Corruption and Fraudulent Activities". This programme was designed to enhance employees' awareness and understanding of anti-corruption practices. The initiative delivered positive outcomes, with all participants successfully completing the training and passing the assessment.

Retail



BUILDING A CULTURE OF COMPLIANCE THROUGH MANDATORY, ADVANCED, AND ROLE-SPECIFIC TRAINING

Compliance training at the Retail division is delivered through a structured programme that includes mandatory eLearning modules on the "RECHARGE" platform, live workshops for advanced topics, and targeted sessions for specific roles. The training covers key areas such as code

of conduct, anti-bribery, anti-fraud and anti-corruption, cybersecurity, competition law, modern slavery, personal data governance, trade descriptions ordinance, internal controls, privacy basics and sustainability.

Value Chain Due Diligence and Ongoing Assessment

The Group extends its anti-fraud and anti-corruption commitment throughout its value chain, encompassing business partners, suppliers, and third-party representatives such as advisers, agents, and consultants. Comprehensive due diligence is conducted during the selection and renewal of partners and suppliers, assessing risk factors including transaction size, nature of products or services, financial and compliance standing, professional qualifications, potential conflicts of interest, and jurisdiction-specific risks.

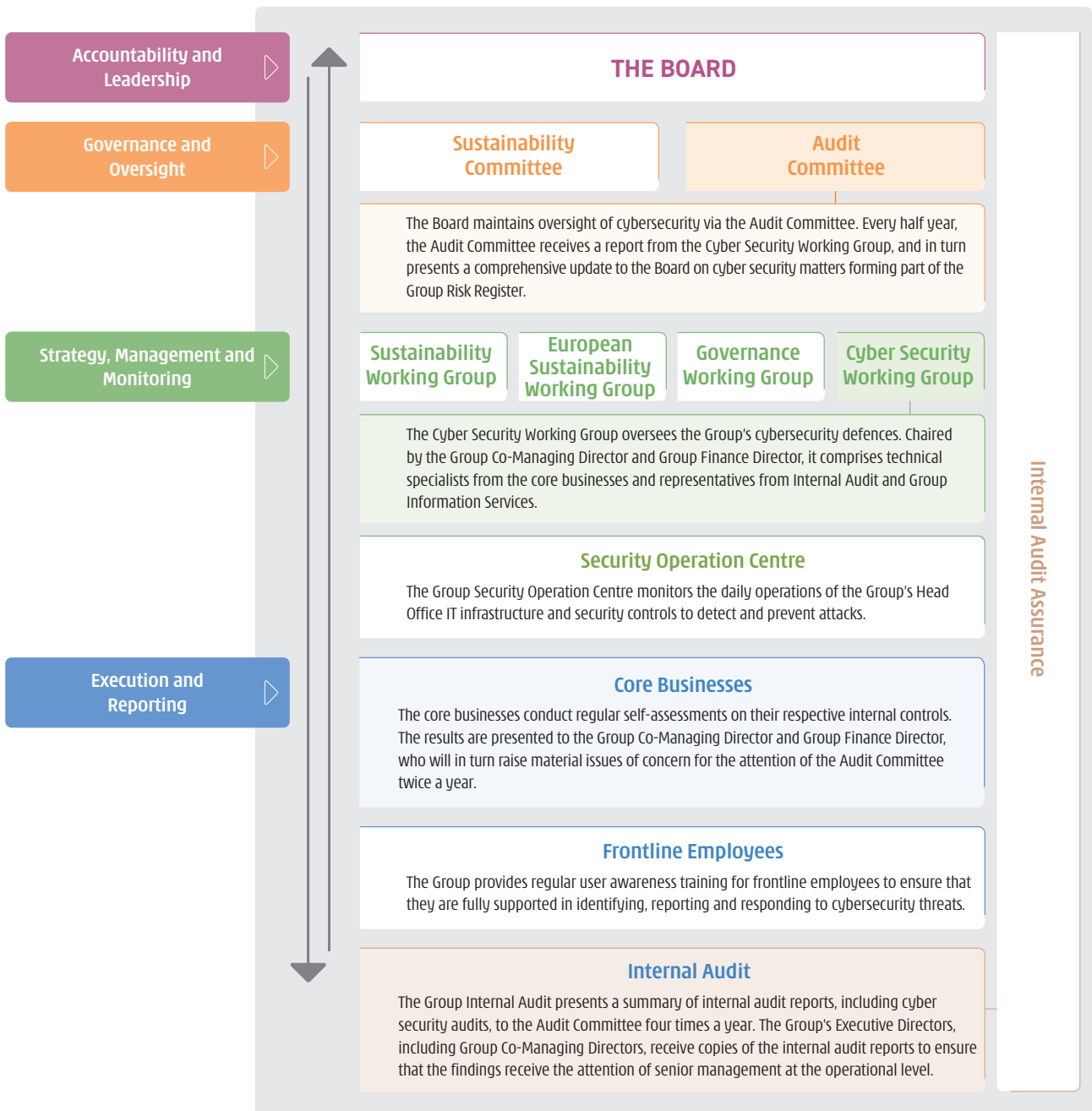
To uphold procurement integrity, the Group enforces transparent and systematic tendering procedures. Material capital expenditure projects exceeding predefined thresholds and generally the engagement of third party representatives requires head office review and approval prior to binding commitment. Divisions conduct supplier pre-screening based on sustainability performance and internal sustainability procurement policies. Further details are provided in the [Supply Chain Responsibility](#) section of this report.



DIGITAL RESPONSIBILITY AND INFORMATION SECURITY

In response to ongoing digital transformation across the global business landscape, the Group has strategically adopted digitalisation to foster sustainable growth through automation, seamless system integration, advanced data analytics, and innovative solutions across its diverse operations. The Group remains committed to data protection and cybersecurity, supported by a robust governance framework and comprehensive security protocols that ensure secure and resilient digital transformation.

Cybersecurity governance and oversight



Personal Data Governance and Information Security

The Group continues to uphold the highest standards in personal data protection and cybersecurity, reinforcing its commitment through enhanced governance, advanced safeguards, and proactive risk management.

The [Personal Data Governance Policy](#) remains a foundation of the Group's approach, protecting the rights of employees and customers through rigorous principles of transparency, lawful processing, purposeful data usage and retention, and robust information security. The policy addresses emerging regulatory requirements and evolving operational needs, including enhanced oversight of third-party data processing and cross-border data transfers. The [Information Security Policy](#) establishes Group-wide standards for maintaining information confidentiality, integrity, and availability. This framework expands to incorporate

adaptive security protocols and real-time threat intelligence, enabling business units to implement tailored procedures that meet increasingly complex security demands.

Senior management of each business unit is accountable for the effective implementation of these policies and the data privacy principles and procedures. All employees should understand and comply with the procedures and guidelines implemented by the Group and divisions. Non-compliance in personal data processing may lead to disciplinary action, and could result in dismissal in serious cases.

Alongside the annual compulsory Group's Code of Conduct training, all employees are required to complete the integrated module on data privacy.

Infrastructure



PROACTIVE COMMUNICATION AND AWARENESS PROGRAMME

As part of Northumbrian Water's commitment to responsible business practices and sustainability, the business has embedded robust measures, including a comprehensive training and awareness programme for all employees, to safeguard customer data and uphold privacy standards.

Mandatory data protection training along with annual refresher courses are delivered to all employees via e-learning platforms. In addition, bespoke training sessions are provided to colleagues in higher-risk roles, including customer directorate, human resources, data analytics, and designated data champions to address

specific responsibilities and risks associated with handling sensitive information.

To ensure accountability and transparency, all training activities are tracked and logged via the Human Resources system, enabling the business to monitor compliance and identify areas for improvement. Data champions also play a pivotal role by disseminating monthly newsletters across teams. These communications share updates on best practices, regulatory changes, and practical guidance, fostering a culture of vigilance and continuous improvement.

Cybersecurity Governance and Oversight

The Group continues to strengthen its cyber resilience in response to the expanding digital landscape and increasingly sophisticated cyber threats. The Cyber Security Working Group plays a pivotal role in supporting the Audit Committee by providing strategic oversight and ensuring the effectiveness of the Group's cyber defence capabilities. The Working Group's mandate encompasses four key areas: reinforcing cyber security infrastructure, conducting real-time threat intelligence monitoring, guiding digital security strategy, and ensuring cross-business unit alignment in cyber risk management. This ensures a coherent and agile response to emerging threats across the Group's operations.

The Group's Cyber Security Policy provides a comprehensive framework for establishing baseline practices and managing cyber risks, while the Cyber Security Incident Reporting Policy outlines clear protocols for incident reporting, response, and recovery. These policies incorporate predictive analytics and automated response mechanisms, enabling faster containment and mitigation of cyber incidents.

Cybersecurity experts across the Group remain vigilant, leveraging advanced tools and collaborative platforms to monitor external threats and safeguard digital assets. The Group continues to work closely with customers and partners to deliver innovative solutions that protect privacy and ensure operational continuity in an increasingly complex threat environment.

Monitoring to inform: the continuous evolution of the Group's cybersecurity 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 and handling cyber security incidents to minimise impact and prevent future occurrences by incorporating intelligence to risk assessments and threat intelligence



GROUP CYBER SECURITY STRATEGY



Risk assessments of various security domains among all business units (twice a 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

The Group also places great importance on empowering its employees with the knowledge and skills to safeguard its digital environment. All staff are required to complete annual Code of Conduct training, which includes comprehensive cybersecurity modules designed to strengthen awareness and resilience. To reinforce this learning, bi-monthly phishing simulations help

employees recognise and respond to suspicious emails, ensuring that vigilance becomes second nature across the organisation.

Looking ahead, a comprehensive awareness campaign, including interactive workshops, informative posters, and other initiatives, will be rolled out in the coming year, to keep security top of agenda.

Group



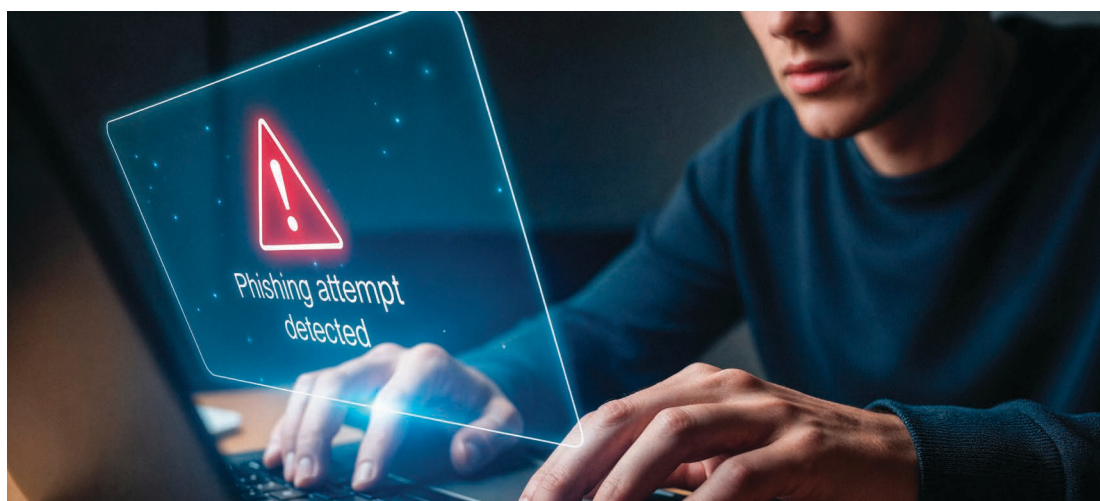
BUILDING CYBER RESILIENCE THROUGH PHISHING AWARENESS

Phishing remains one of the most significant cybersecurity risks for organisations, with malicious emails continuing to be a preferred tactic for infiltrating IT systems and networks. To address this growing threat, the Group Security Service continued to roll out a series of comprehensive phishing awareness campaigns throughout 2025, reinforced by regular security digests and educational messages to keep employees informed about emerging risks and the potential impact of phishing attacks on the Group.

As part of these efforts, 2,709 simulated phishing emails were sent to head office staff during the year, prompting employees to identify and report 1,822 potentially dangerous messages. This response has improved cyber threats detection and reporting rates, reflecting

heightened awareness and vigilance among staff and highlighting the effectiveness of continuous education and engagement. Employees who failed the phishing simulation email initiative were required to conduct mandatory training to ensure proper awareness.

Beyond strengthening technical defences, these campaigns have fostered a culture of cybersecurity mindfulness across the organisation. Employees are now more alert to suspicious communications and better equipped to act swiftly, reducing the likelihood of successful phishing attempts. By prioritising ongoing training and awareness, the Group reinforces its commitment to safeguarding critical data and systems against evolving cyber threats.



Telecommunications



BUILDING A CYBER-RESILIENT CULTURE

The Telecommunications division deploys a coordinated, division-wide programme to reduce cyber risk by strengthening employees' security awareness and behaviour.

Wind Tre applies a comprehensive model, combining mandatory Learning Management System-based cyber courses (covering phishing, social engineering, mobile security, AI risks, incidents, and internal policy refreshers) with targeted awareness for critical roles such as C-suite, privileged users, assistants, sales teams, agents, and franchisees. This includes webinars, on-site awareness roadshows, short "training pills", mystery calls to retail points of sale, and quarterly phishing simulations to test and improve real-world responses. Continuous updates via the WeCyber intranet portal and security bulletins act as a "digital first-aid manual", giving timely guidance on new threats and reinforcing responsible use of company systems. In 2025, SECURITYLAB, an Information Security Faculty delivered cybersecurity education to 2,000+ technology professionals involved in the creation and

management of technological services and systems. This internal security expert-led training strengthened skills in digital identity, data protection, risk, and cyber threats guided by the most advanced security principles and techniques.

3 Sweden runs mandatory annual e-learning for all staff, supported by additional intranet content and bi-weekly "nano-learning" modules to keep security foremost.

3 Ireland maintains a formal security awareness programme, including compulsory cyber awareness training at onboarding and yearly thereafter, plus secure coding courses for developers, and uses quarterly phishing simulations with remedial training. **3** Hong Kong requires all employees, including part-time staff, to complete vendor-delivered online cyber courses and participates in regular phishing drills. **3** Austria ensures annual interactive online training with knowledge checks, maintaining a consistent baseline of cyber hygiene across the workforce.

Managing Cybersecurity Risks

By reinforcing the cybersecurity risk governance structure, the Group ensures timely and accurate escalation of risks from the operational level. This structure systematically collects, consolidates, and validates cyber-related information across business units, enabling informed decision-making and strategic oversight. Internal Audit provides independent assurance, validating the effectiveness of controls and the adequacy of responses to emerging threats. The governance framework supports a proactive and coordinated approach to managing cyber risks, aligned with the Group's broader resilience and compliance objectives.

A comprehensive IT audit of the Group's operations, supported by external experts, is conducted annually. Beyond the audit, independent experts are engaged to rigorously test and validate defences through annual red teaming exercises and penetration testing, ensuring that potential vulnerabilities are identified and addressed proactively. These external assessments provide assurance that systems adhere to the highest standards of security and compliance, reinforcing the commitment to transparency and continuous improvement in protecting stakeholders. Management procedures are also established at division level.

Ports



GOVERNING CYBERSECURITY ISSUES

The Ports division has aligned its data security strategies with industry best practices. For instance, both Hutchison Ports HIT and Hutchison Ports Yantian have obtained ISO 27001 Information Security Management certification and underwent an annual external audit in 2025. Additionally, the Ports division has implemented the Information Security Policy, Operational Technology Policy, and AI-Governance and Code of Conduct which outline standard procedures for employees, partners, and suppliers to ensure the security of IT infrastructure and customer data.

Governance Structure

The Cyber Security Working Group at the Ports division works on standardising security strategies, monitoring cyber resilience across business units, supporting units that lack resources for security management and enforcing various regulatory and compliance requirements to ensure the security and integrity of the organisation's operations.

- **Semi-annual Cybersecurity Committee (CYBERCOM)** To promote cybersecurity awareness and reduce cybersecurity threats across the group in all IT and operational technology environments through the development and maintenance of standards and guidelines, and sharing of best practices.
- **Quarterly information security custodians meeting** To cover crucial updates across various security domains. The agenda includes discussions on key security updates, emphasising the latest developments in security governance practices. Furthermore, the meeting explores insights regarding security management strategies and provides updates on the ongoing security programme enhancements. This comprehensive session aims to align stakeholders, foster collaboration, and reinforce the Port's division commitment to maintaining a robust and adaptive security posture.

Assessment and Identification of Potential Threats

The Ports division regularly scans for vulnerabilities in the terminals' IT systems to identify weaknesses in systems, networks, and applications. It analyses the security posture of the division, providing insights into potential risks and generating detailed reports with remediation suggestions. By automating the process, it regularly checks for new vulnerabilities, helping the division to proactively address security issues before they can be exploited.

Cyber detection and response tools are deployed to ensure the readiness of detection and containment actions upon attack scenarios. Security alerts are sent to the 24/7 Service Desk for maintaining a holistic situational awareness across the IT environment.

Training and Regular Drills

All business units conduct regular phishing simulations and security awareness exercises to strengthen cybersecurity vigilance across their workforces. These activities help employees recognise and respond to social engineering threats more effectively, reinforcing a strong security culture throughout the organisation. Additionally, cybersecurity drills are performed to improve employees' ability to handle cybersecurity incidents promptly and effectively. Collaborative information security drills with local law enforcement agencies are also conducted to address critical infrastructure vulnerabilities.

Telecommunications



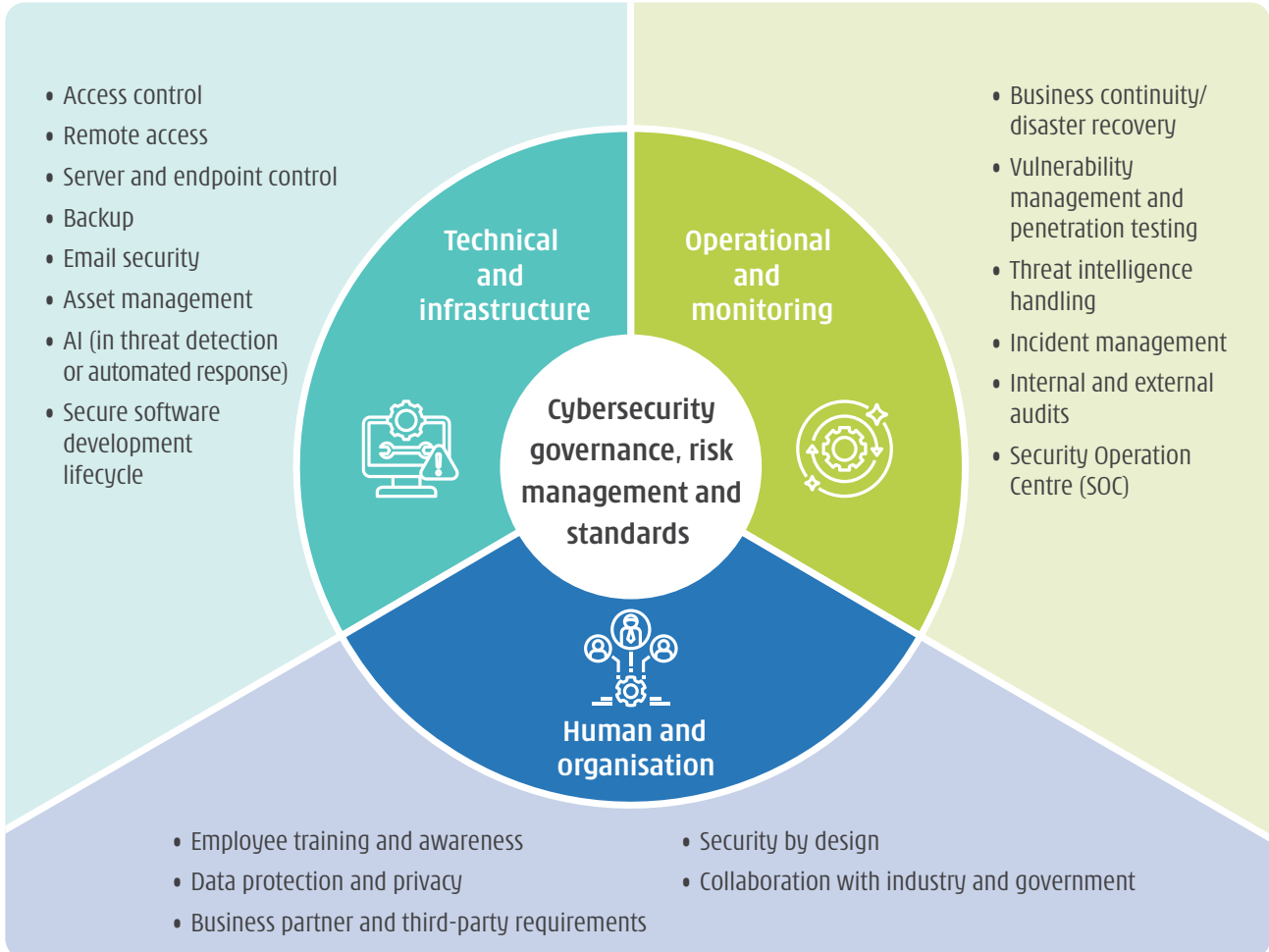
ROBUST MANAGEMENT SYSTEMS

Wind Tre and 3 Austria, representing a significant proportion of CKHGT's revenue, maintain ISO 27001 certification. The rest of the Telecommunications division's business units in the UK and Europe operate according to ISO 27001 minimum control standards, ensuring strong information security risk management practices. Security is embedded across all system lifecycle stages, from design and deployment to operations and decommissioning. Business units further enhance cyber resilience by integrating National Institute of Standards and Technology (NIST) guidance into

cybersecurity risk frameworks. 3 Sweden and 3 Denmark have progressed with NIS2 Directive readiness across shared IT and network technology functions. The implementation has included a unified risk management framework improving cybersecurity governance, revised cybersecurity policies aligned with corporate goals and regulatory developments, and the introduction of an information security management system tool to optimise risk assessment, incident management, and documentation workflows.

Cybersecurity risk management at CKHGT

The diagram below outlines CKHGT's cybersecurity framework, illustrating the governance structure, risk management approach and key standards that guide its cybersecurity practices.



Ensuring Business Resilience and Cyber Disaster Recovery Plan

Cyber Disaster is governed under a series of internal policies at the Group, including the Group Cyber Security Acceptable Use Policy, Group Cyber Security Standard and Group Cyber Security Incident Reporting Policy. During the year, the Group's internal Cyber Security Incident Reporting Policy has been updated and expanded to apply across all business units, ensuring consistent standards and coordinated action. The revised policy designates key contact persons at both the head office and business unit levels, and introduces an indicator-based rating system to help assess the potential impact and severity of cyber incidents, enabling timely escalation and more effective risk management.

Across core businesses, Cyber Disaster Recovery protocols are embedded as part of the broader business continuity planning, alongside other operational risk considerations. For further details on how these measures integrate into the Group's overall resilience framework, please refer to the Business Continuity Plan Section in the [Sustainable Business Model and Innovation Chapter](#).

Ports



CYBER INCIDENT RECOVERY STRATEGY

In the event of a Data Security Incident (DSI) involving personal data, business units must activate immediate containment and mitigation measures, secure affected data, and follow established rapid response protocols in strict alignment with regulatory obligations and Group standards. Notification to the relevant departments is mandatory upon identification of a DSI, and where applicable, formal communications with privacy authorities and affected individuals are executed in accordance with legal and procedural requirements.

The Cyber Incident Recovery (CIR) strategy includes a comprehensive Preparedness and Response Playbook to ensure swift action in the event of an incident. It sets clear Recovery Time and Point Objectives, with Recovery Time Objectives (RTO) at 24 hours and Recovery Point Objectives (RPO) at 15 to 30 minutes. Additionally, a Cloud-Based Disaster Recovery (CBDR) system is in place to support rapid recovery and maintain operational continuity. Business units conduct annual cyber incident recovery drills to ensure that they can recover from cyber incidents such as ransomware attacks.

Infrastructure



SA POWER NETWORKS CYBER SECURITY STRATEGY 2025-30 LAUNCHED

In 2025, SA Power Networks launched its first standalone "Cyber Security Strategy 2025-30", setting out a risk-based roadmap to strengthen resilience across its operations. The strategy identifies 10 key cyber risks, ranging from critical systems failure and supply-chain vulnerabilities to poor cyber culture, and maps them to

12 initiatives covering identity and access management, cloud security, supply chain monitoring, and cultural awareness. Unlike previous approaches, cybersecurity is now addressed in a dedicated framework with annual reviews, ensuring greater visibility, accountability, and adaptability to evolving threats.

Ports



EMPOWERING BUSINESS RESILIENCE WITH CLOUD BACKUP SOLUTIONS

In today's digital landscape, safeguarding critical system configurations and valuable data is essential for operational resilience. Traditional backup methods, while reliable, often face limitations in scalability, accessibility, and cost-efficiency. To address these challenges, Hutchison Ports has adopted cloud backup solutions for a proactive defence against data loss, system failures, and cyber attacks.

Cloud backup involves storing copies of data and system configurations on secure remote servers accessed via the internet. This approach offers multiple advantages over conventional methods. Enhanced security is achieved

through robust encryption protocols that protect data during transmission and storage, mitigating risks of unauthorised access and cyber threats. Scalability and flexibility allow business units to adjust storage capacity as needs evolve, eliminating physical constraints. Automated scheduling and incremental backups reduce manual intervention, ensuring consistent data protection while freeing IT resources for higher-value tasks. Furthermore, cloud backup delivers cost-efficiency without compromising reliability or performance by removing the need for on-premises hardware and maintenance.



Safeguarding the Community from Cyber Threats

Amid rising cyber threats including AI-driven phishing, deepfake scams, and sophisticated malware, the Group's businesses continue to collaborate closely with customers, offering innovative solutions to safeguard digital assets and privacy.

Telecommunications



STRENGTHENING MOBILE SECURITY AND PROTECTING CUSTOMERS FROM EMERGING CYBER THREATS

In partnership with award-winning cybersecurity company Corrata, **3** Ireland offers a business mobile security solution, "**3**Mobile Protect", that protects mobile devices from phishing and malware and prevents data loss on company smartphones and tablets. This responds to the increasing number of mobile phishing attacks occurring outside of email, and the importance of raising standards of mobile security - which is often given less attention than laptop computer security by businesses.

In 2025, **3** Ireland attained ISO 27001 certification for the IoT platform and solutions, providing its customers with the assurance that the solutions it provides them with are secured to the highest standards. In addition, various initiatives have been rolled out to protect customers from scam calls and text messages, such as the blocking of inbound international calls that "spoof" Irish numbers, marking untrusted SMS messages that have an alphanumeric header as "Likely Scam". The company is also preparing to introduce a Voice Firewall to filter or highlight untrusted voice calls.

Telecommunications



ADVANCING NETWORK-LEVEL PROTECTIONS TO ENHANCE DIGITAL SAFETY FOR ALL USERS

3 Sweden offers network-level protection against spam, phishing, and malicious traffic, along with fraud monitoring and parental control tools that enhance online safety. Key target groups include private customers, families, and business users. **3** Sweden

continued to strengthen its digital safety offering through improved fraud detection, clearer customer guidance on safe online behaviour, and expanded access to content filtering solutions.

RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE

The Group recognises the transformative potential of artificial intelligence (AI) technologies to enhance operational efficiency and productivity across business functions. While embracing these opportunities, the Group remains committed to the responsible and ethical deployment of AI systems.

The Group's Cyber Security Acceptable Use Policy provides comprehensive guidance for management and employees, establishing standards for the responsible application of AI tools in compliance with regulatory requirements and data protection obligations. Building on this foundation, the Group Policy on Reasonable and Ethical Procurement, Implementation and Use of AI, introduced in 2024, establishes clear principles and protocols governing the procurement, implementation, and use of AI systems – whether internally developed, externally sourced, or commercially acquired. This policy ensures alignment with the Group's core values, corporate governance standards, and legal obligations.

Recognising the potential risks associated with AI in operations and customer-facing services, the Retail division has established a robust governance framework to ensure safe and ethical AI adoption. The approach includes comprehensive risk assessments and strict approval processes for all AI use cases. Every application must undergo review and receive formal approval before deployment, ensuring compliance with regulatory standards, data privacy requirements, and ethical principles. To date, 89 AI use cases have been assessed, reflecting the commitment to responsible innovation.

The Group maintains vigilant oversight of emerging AI developments and regularly reviews its governance frameworks to ensure continued effectiveness and alignment with evolving regulatory requirements and global best practices.



The Group hosts the online AI conference, sharing AI use cases on enhancing business operations.

Ports



EMBEDDING RESPONSIBLE AI GOVERNANCE ACROSS HUTCHISON PORTS

The Ports division has adopted the Group Policy on Reasonable and Ethical Procurement, Implementation and Use of Artificial Intelligence and embedded it across all business units through a robust governance framework. An AI Governance Committee has been established, comprising senior leaders, technical experts, and legal or compliance representatives to review AI systems prior to launch to ensure alignment with Group policies. An AI Questionnaire is completed for every use case for review and approval.

The AI governance framework operates alongside key Group policies, including those on information security, personal data governance, acceptable use of technology, and the handling of confidential and price-sensitive information, ensuring consistency across all risk domains.

To ensure the responsible use of AI in operations, Hutchison Ports enforces clear “dos and don’ts”. Ongoing post-deployment monitoring and incident readiness help maintain safe and reliable operation, while regular employee training builds awareness of ethical AI practices and reinforces a strong culture of compliance.



Automated equipment and AI systems are being deployed at the Ports division to advance digitalisation and smarter ports operation.



IMPLEMENTING AI MANAGEMENT POLICY FOR COMPLIANCE WITH THE EU AI ACT

AI is transforming the telecom industry, driving innovation in network optimisation, predictive maintenance, customer service automation, and fraud detection. For Wind Tre, effectively harnessing AI is essential to enhancing customer experience and operational efficiency, while ensuring full compliance with the EU AI Act and applicable national legislation.

To address these challenges, the company has established an AI Committee tasked with guiding the adaptation of Wind Tre's internal policies and procedures, as well as its contractual standards with third parties, and with overseeing compliance in relation to the adoption and use of AI systems.

Wind Tre has also adopted an AI Policy, aimed at regulating the behaviours to be followed – and those to be avoided – in order to mitigate the risks associated with the use of AI systems, whether developed internally or provided by external parties. The company recognises the opportunities offered by AI technologies and their significant potential to create value and drive efficiency within corporate activities and business processes. At the same time, it acknowledges that the deployment of AI systems may entail considerable risks, both in terms of regulatory liability and potential conflicts with Wind Tre's fundamental principles and internal procedures.

The Policy is built upon the following pillars:

- Security and reliability
- Value creation as a guiding principle
- Fairness
- Privacy and confidentiality
- Responsibility
- Governance
- Human oversight and intervention
- Transparency and interpretability

To ensure the implementation and effective management of these principles, an operational procedure has also been introduced. Its key objectives are the following:

- Built-in regulatory, ethical and security controls: ensuring that AI systems comply with company values and applicable regulations
- Full traceability of decisions: documenting each decision to enhance transparency and trust

This framework is supported by a multi-layered organisational structure involving multiple business functions and ensuring continuous alignment with the AI Act.

SUPPLY CHAIN RESPONSIBILITY

The Group has strengthened its governance practices by extending rigorous oversight to supply chain engagement. Through its policies and procedures, the Group promotes effective governance that incorporates active collaboration with suppliers and systematic evaluation of sustainability performance across the value chain.

Supplier Code of Conduct

The Group reinforces its commitment to ethical business practices across its supply chain through the implementation of the [Supplier Code of Conduct](#). Business partners and suppliers are expected to uphold the same high ethical standards as the Group, including full compliance with local laws and regulations, protection of employee rights, and responsible business conduct. Core business units apply tailored versions of the Supplier Code of Conduct, adapting its provisions to their specific operational contexts while maintaining consistency with Group-wide ethical expectations.

To safeguard human rights and uphold integrity across its value chain, the Group maintains robust systems and controls to prevent modern slavery and human trafficking. Procurement contracts include clauses requiring third-party partners to implement anti-corruption policies and compliance programmes, in alignment with the Group's Supplier Code of Conduct, governance standards and regulatory obligations.

Telecommunications



ENGAGING SUPPLIERS IN ENVIRONMENTAL COMMITMENTS

The Telecommunications division is committed to embedding sustainability and ethical practices across its supply chain through the Supplier Codes of Conduct and targeted engagement initiatives.

- **3** Sweden has aligned its supplier engagement strategy with its approved science-based targets, committing to reduce Scope 3 emissions by 42% by 2030 and achieve net zero by 2040. This includes proactive collaboration with suppliers to drive emissions reduction and sustainable practices.
- Wind Tre promotes responsible procurement by requiring all suppliers, and their sub-suppliers, to

adopt ESG principles. A dedicated clause in supplier contracts mandates compliance with the Supplier Code of Conduct, published on the company's official website. Non-compliance allows Wind Tre to terminate contracts, reinforcing accountability throughout the supply chain.

- **3** Hong Kong complements its sustainability questionnaire with a formal Supplier Code of Conduct, outlining environmental expectations, when purchasing exceeds a certain level. In cases of non-conformance, the company works with suppliers to develop corrective plans. Failure to comply may result in termination of the business relationship.

Retail 

ROBUST SUPPLIER MANAGEMENT MECHANISM

Supply chain governance in the Retail division is deeply integrated into the company's overall sustainability framework. Clear responsibilities and roles are assigned to relevant teams, ensuring that supply chain risks are proactively managed, and that the division's sustainability objectives are consistently applied across all business units and markets.

The Board

The division's board is responsible for approving key policies, such as the Supplier Code of Conduct, which sets out expectations for ethical sourcing, labour standards, and environmental stewardship.



Global Sustainability Committee

The division's global sustainability committee, chaired by the division's CEO, regularly reviews supply chain risks and progress, ensuring that sustainability considerations are embedded into procurement and supplier management.

Contracts and the Supplier Code of Conduct are key instruments to enforce the division's standard of ethical and sustainable practices. As a signatory of The Mekong Club Pledge and a member of amfori, the Retail division embeds the amfori's Business Social Compliance Initiative (BSCI) Code of Conduct into its Supplier Code of Conduct. This integration ensures that suppliers adhere to internationally recognised standards on labour rights, environmental performance, and responsible business conduct.

In 2025, all suppliers' of contracts included ESG clauses and the Supplier Code of Conduct has been acknowledged. The division also reported zero instances of child or forced labour, ensuring that all suppliers are held to high standards of ethical and sustainable practices.



In 2025, AS Watson's group supply chain department and Watsons China hosted the Health & Beauty Asia Supply Chain Conference.

Supplier Screening and Assessments

Given the Group's extensive operational footprint across diverse industries and jurisdictions, a robust approach to sustainable sourcing remains essential. The [Supplier Code of Conduct](#) continues to serve as a foundational framework for guiding supplier performance, with a strong emphasis on product safety, quality standards, and ethical business conduct.

Divisions have strengthened their supply chain oversight by implementing enhanced measures and leveraging external platforms to conduct comprehensive supplier screening. These efforts support the Group's commitment to responsible procurement and continuous improvement in sustainability performance across its value chain.

3 Ireland is committed to enhancing transparency and monitoring ethical and sustainable performance across its supply chain. Since 2022, the company has partnered with EcoVadis, a global leader in independent sustainability ratings, to assess suppliers' ESG practices. This initiative continued to expand in 2025, reached a coverage of 87% across supply chain by spend, reinforcing the commitment to responsible sourcing and supplier engagement.

Retail



SUPPLIER ASSESSMENT AND MONITORING

All suppliers of the Retail division are first screened via LSEG Data & Analytics, to flag any publicly available ESG risks. The comprehensive screening process enables AS Watson to identify high-risk suppliers, prioritise engagement, and drive improvements in supply chain sustainability. By maintaining high coverage of sustainability assessments, the company demonstrates its commitment to responsible sourcing and continuous improvement in supplier performance.

In 2025, over 90% of suppliers (across various brands) were screened using the LSEG Data & Analytics, resulting in over 104,000 screenings across about 31,500 suppliers, covering trade and non-trade items. For suppliers manufacturing Exclusive Brands products,

additional social and environmental assessments against amfori's BSCI and BEPI (Business Environmental Protection Initiative) would be required if their manufacturing is in high-risk countries, as defined by the Worldwide Governance Indicators. These assessments evaluate suppliers' practices across a range of ESG criteria, including environmental impact, labour standards, and human rights. It also endorses other reputable frameworks (for example, SA8000, Initiative for Compliance and Sustainability, Sedex Members Ethical Trade Audit, ISO 14001 management system). Approximately 60% of targeted factories underwent detailed sustainability assessments through on-site audits or self-assessments, with the remaining scheduled for assessment in 2026 and 2027.

Supplier Engagement

The Group leverages its significant purchasing power to promote sustainable consumption and production across its operations. By prioritising environmentally and socially responsible procurement practices, the Group actively supports the development of sustainable markets and drives positive impact throughout its supply chain. Please see also the Sustainable Product Choices

Section in the [Sustainable Business Model and Innovation Chapter](#) for more information.

Divisions have been actively engaging suppliers to communicate the Group's expectations in sustainability practices and embed sustainability values throughout the value chain.

Ports



PROACTIVE ENGAGEMENT WITH SUPPLIERS

In 2025, the Ports division engaged a third-party consultant to conduct two Supplier Training workshops. To accommodate suppliers from various regions, the workshops were held in both face-to-face and online

formats, attracting over 500 participants. The workshops aimed to strengthen ESG awareness and ensure collaboration on decarbonisation initiatives with the suppliers across the company's supply chain.

Telecommunications



SUPPLIER ENGAGEMENT ON GHG DISCLOSURE AND TARGET SETTING

The Telecommunications division views supplier engagement as a critical enabler of its climate strategy and a fundamental lever to achieve its science-based targets. As the majority of the division's GHG emissions arise in the value chain, meaningful progress towards decarbonisation depends on structured, data-driven collaboration with suppliers.

Building on initial engagement efforts in 2024, CKHGT transitioned in 2025 from a broad disclosure-based approach to a more targeted and tailored programme led by the procurement and sustainability teams. The 2025 programme segments suppliers based on strategic




importance, spend, carbon intensity and ESG maturity, allowing CKHGT to prioritise engagement where impact and influence are greatest.

As part of this programme, CKHGT conducted a dedicated supplier climate workshop. The session familiarised participants with the climate ambition of the Telecoms division, Scope 3 methodology, data requirements and decarbonisation expectations. It also clarified the role suppliers play in enabling the telecoms division to meet its GHG emissions reduction targets and provided practical guidance on measurement, disclosure and target setting.


LABOUR AND HUMAN RIGHTS

The Group embraces human rights as a foundational principle embedded within its corporate values and operational practices. This commitment informs stakeholder engagement and supports a workplace culture founded on respect, inclusion and equal opportunity. The Group is dedicated to maintaining work environments that are free from discrimination and harassment across all levels of its operations.

This topic of Labour and Human Rights is closely linked with other material topics in the Group Sustainability Framework, including the following:

- [Social Inclusion](#) 
- [Inclusion and Diversity](#) 
- [Employer of Choices](#) 

Responsible Employment Practices


The Group's [Human Rights Policy](#)  provides a comprehensive framework aligned with internationally recognised standards, including the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights. This policy guides the Group's approach to human rights protection throughout its value chain, encompassing direct operations and supply chain partnerships, and is underpinned by the following principles:

Group human rights principles



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

The Group's [Human Rights Policy](#)  forms the foundation of its employment practices, ensuring full compliance with labour laws and regulations across all jurisdictions and business units. Transparent communication channels are maintained to keep employees informed about policies, rights, and workplace practices. The Group also upholds freedom of association, allowing employees to join or form labour unions without fear of reprisal. Collective bargaining agreements reflecting this commitment,

cover 34% of employees in 2025. Regular dialogue with union representatives ensures employee interests are taken into account in decision-making processes. According to the [Whistleblowing Policy](#) , the Group processes and investigates all reports received through its confidential reporting channels, ensuring that each case is handled fairly, impartially and in a timely manner.

The Group offers full time employee 46 working hours averagely during the working week, in full compliance with all applicable local laws and regulations. Beyond statutory obligations, the Group underscores its commitment to employee welfare through a comprehensive suite of non-statutory benefits. These include enhanced maternity and shared parental leave provisions, substantial childcare support, and educational assistance programmes. The Group's employee policies are designed to comply with, and in certain cases exceed, applicable local statutory requirements in respect of parental benefits. For example, female employees at the Group's Hong Kong head office are entitled to 14 consecutive weeks of statutory maternity leave, with full pay for the first five weeks, exceeding the statutory requirement of 80% pay, while male employees are entitled to five days of

statutory paternity leave. Wind Tre in Italy provides a 100% pay supplement for optional maternity leave i.e. 4.5 months more than the statutory entitlement, and 3 Ireland offers four weeks of paid paternity leave for employees with one year's service, compared with the statutory entitlement of two weeks. Employees also enjoy competitive pension plans, performance-based bonuses, and long-service recognition.

Health and wellbeing remain a priority, and is supported by onsite medical clinics, employee assistance programmes offering mental health support, and flexible or hybrid working arrangements tailored to operational and regional needs. Additionally, the Group provides wellness initiatives designed to promote holistic wellbeing.

Infrastructure



SUPPORTING EMPLOYEES THROUGH INCLUSIVE BENEFITS AND FLEXIBLE POLICIES

The Infrastructure division prioritises employee wellbeing by implementing family-friendly policies that address diverse life stages and responsibilities. SA Power Networks and Victoria Power Networks strengthen financial and emotional support for new parents, offering up to 18 weeks of paid parental leave for primary carers and extending superannuation contributions during unpaid leave. Wales & West Utilities ensures inclusivity with adoption leave matching maternity leave, time off for fertility treatments, and flexible benefits schemes covering physical, mental, and financial wellbeing.

Northern Gas Networks provides compassionate support through emergency and carers leave, career breaks, and its commitment under the Dying to Work Charter, ensuring dignity and flexibility for employees with terminal illness. United Energy promotes work-life balance via flexible arrangements, including remote work, compressed weeks, and tailored schedules.

The Group is committed to identifying, preventing, and mitigating adverse human rights impacts arising from any business transaction, including restructuring decisions. This commitment is guided by the following principles:

- **Early identification:** Assess potential human rights impacts on employees as early as possible
- **Transparent communication:** Engage with employees and, where appropriate, labour unions at the earliest opportunity regarding potential impacts, ensuring respect for human rights considerations
- **Redundancy prevention:** Minimise redundancies wherever possible and provide severance packages at or above statutory requirements when redundancies occur

- **Transition planning:** Incorporate human rights considerations into transition plans, including redeployment and outplacement services for affected staff
- **Constructive dialogue:** Maintain meaningful engagement with employees and take proactive steps to mitigate adverse effects during ownership or structural changes

During organisational changes, the Group supports employees through severance packages aligned with industry standards, outplacement services, re-employment opportunities within the Group, skills retraining programmes, and extended health coverage during transition periods.