Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is a member of the Technology senior leadership team reporting to the CTO, indirectly reporting to Company Secretary & Group Legal Counsel.

The CISO will be responsible for leading and managing the information and cyber security strategy, policies, and practices of C&C Group. You will ensure that our data, systems, and assets are protected from internal and external threats, and that we comply with relevant laws, regulations, and standards. You will also oversee the security operations, risk management, architecture, governance, and incident response functions, and collaborate with senior leadership, business units, and external partners to align security objectives with business goals.

Responsibilities:

- Develop, implement, and monitor a comprehensive and proactive information and cyber security program that covers all aspects of security, including people, process, and technology
- Establish and maintain security policies, standards, guidelines, and procedures that reflect best practices and industry benchmarks, and ensure compliance with legal and regulatory requirements
- Lead and manage any internal or external security teams, including performance evaluations in line with the Head of Supplier
- Work with Legal and Data Protection to ensure best practice is implemented and maintained.
- Provide strategic direction and guidance to the business units and Technology functions on security matters, and ensure security is integrated into the business processes and systems development life cycle
- Conduct regular risk assessments and audits to identify and mitigate security risks, vulnerabilities, and gaps, and report on the security posture and performance of the organisation
- Manage and allocate security resources effectively and efficiently
- Oversee any internal or external security operation functions and security incident response teams ensuring timely detection, containment, analysis, and resolution of security incidents and breaches
- Develop and maintain a security awareness and education program for all employees, contractors, and stakeholders
- Foster a culture of security and innovation, and promote security best practices and standards across the organisation
- Stay abreast of the latest security trends, threats, and technologies, and evaluate and implement new security solutions and tools as needed
- Represent the organisation in external forums and events, and build and maintain relationships with security peers, vendors, regulators, and law enforcement agencies

Behaviours required:

- **Strategic thinker**
  Strong strategic planning and critical and analytical thinking skills and can paint a compelling picture of the vision and strategy that inspires others and prioritises initiatives and efforts to have the greatest strategic impact.
- **Leadership**
  Able to motivate and inspire others and builds team capability and can build a collaborative workspace and influence cross- functional teams to achieve positive business outcomes.
- **Financial acumen**
  Uses data and metrics to inform business decisions and is able to interpret complexity and explain implications for business decisions.
- **Relationship builder**
  Builds strong and influential relationships both internally and externally. Demonstrates sophisticated influencing skills to gain support and commitment from others.

To be successful you will be able to demonstrate:

- Professional security certification, such as CISSP, CISM, CISA, or CRISC
- Proven experience in information and cyber security in a senior leadership role
- Being able to contribute at a senior level to the wider life of the department and a trusted partner
- In-depth knowledge and expertise in security frameworks, standards, and best practices
- Strong technical skills and experience in security technologies and tools
- Excellent communication, presentation, and interpersonal skills, and the ability to communicate complex security concepts and issues to technical and non-technical audiences
- Strong analytical, problem-solving, and decision-making skills, and the ability to balance security and business needs
- Strong business acumen and strategic thinking, and the ability to align security objectives with business goals and priorities
- High ethical standards and integrity, and the ability to handle sensitive and confidential information
- Bachelor's degree or higher in computer science, information systems, related field, or equivalent work experience