RISK MANAGEMENT

Effective risk management is key to ensuring that the Group achieves its strategic objectives and protects its reputation, market position and financial strength. The Company itself and its operating companies follow the Group's Enterprise Risk Management (ERM) policy. The ERM policy requires continuous identification, assessment, management, monitoring and reporting of current and emerging risks.

Group Risk Governance Structure

The Board of Directors and the management of each division are responsible for identifying, analysing and, reporting on the risks for which they are responsible and for optimising the profile of such risks. Risks are mitigated and, where practicable and economic, eliminated. Where risks cannot be eliminated, the related returns should reflect the level of risk being taken.

The Board has adopted the three lines of defence model of risk governance which is designed to minimise conflicts of interest and ensure independent oversight of risk management. There are two key management committees with responsibility for risk management, both of which report to the Audit Committee:

Finance Committee – a first line committee which determines the parameters within which financial risk is managed and oversees the management by the operating companies of financial risk within those parameters. Membership of the Finance Committee includes all the senior finance officers of the Group and its operating companies.

Group Risk Management Committee (GRMC) – a second line committee which is responsible for overseeing the management of non-financial risks and for providing assurance to the Board and the Audit Committee that risk is being managed effectively. The GRMC comprises the Finance Director, an Executive Director and five heads of operating businesses. The GRMC (i) regularly reviews the Group's risk profile, (ii) oversees the management of major risks at Group and operating company levels, (iii) identifies emerging risks and potential sources of future risk and (iv) analyses risk events which materialise, with a view to their resolution and to learning from them. In these activities the GRMC is supported by four risk forums.

In addition, the Company has its own risk management committee, the Swire Pacific Risk Management Committee (SPACRMC). The SPACRMC oversees risks specific to the Company itself, identifies risks which have a Group dimension and proposes approaches to the management of such risks to the GRMC.

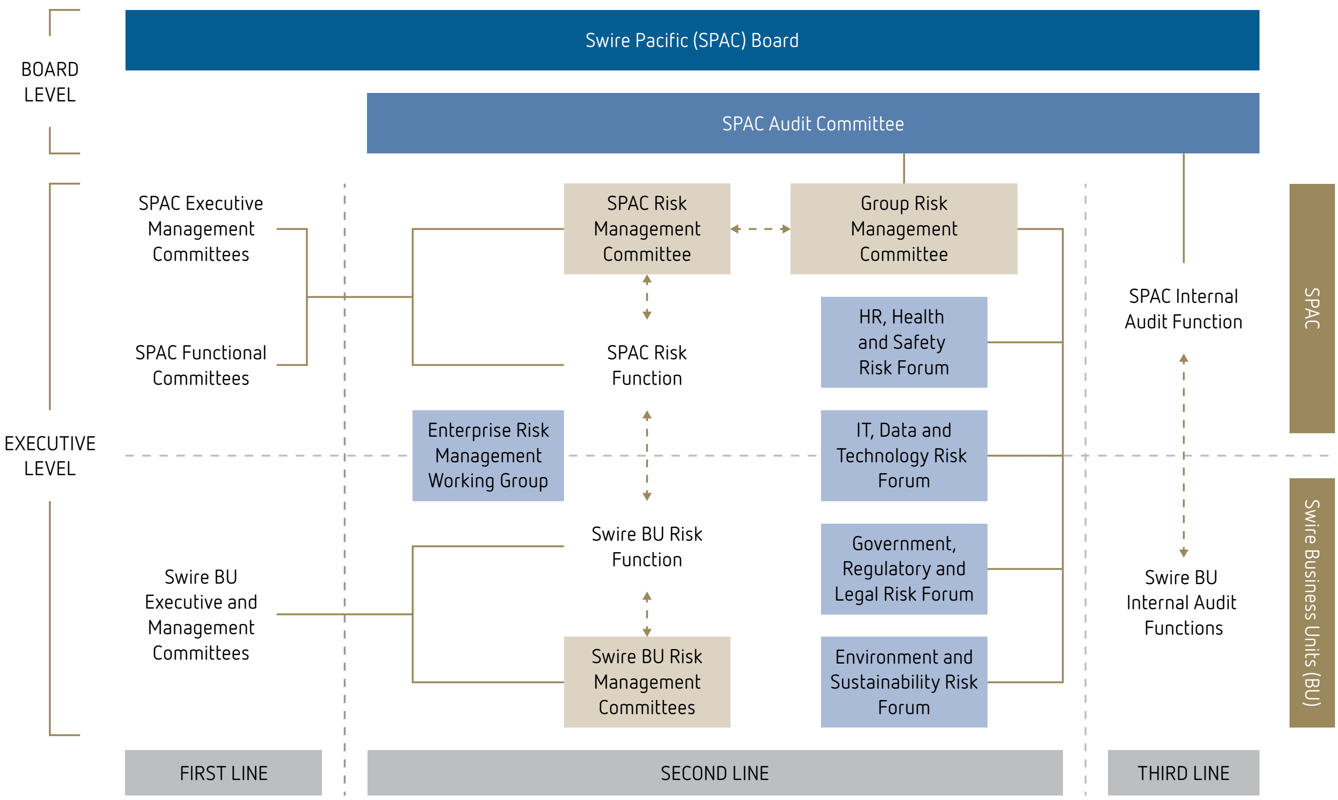
All three of these committees are chaired by the Finance Director, who is also the Company's senior risk officer.

The boards and management of operating companies are responsible for the management of risk at those companies. Risk management governance varies between operating companies. Some have risk committees and dedicated risk functions. Others manage risk through audit or executive committees, supported by individual risk officers.

The Group's risk governance structure was reviewed in 2021. This resulted in the creation of the SPACRMC and the four GRMC risk forums, the movement of committees with executive authority to the first line of defence and the disbanding of the GRMC working committee.

The revised structure is shown below.

Risk Governance Structure



Group ERM Process

The operating companies have adopted a common approach to ERM based on the development and management of their risk registers. This involves:

- **Identification:** Risks are identified by senior executives and categorised by reference to a common risk taxonomy.
- **Assessment:** Each major identified risk is assessed by two or more senior executives. Plausible scenarios are considered in which the risk could eventuate and the impact of the risk rated in six dimensions. The vulnerability of the entity to the risk is then rated according to a) the controls in place to prevent an occurrence, b) the readiness of the organisation to respond to any risk event and c) the degree to which the impact cannot be mitigated.
- **Mitigation:** Designated risk owners then consider the potential for further mitigation and propose action plans. These plans will be expected to reduce the Company's vulnerability to this risk and improve its overall risk profile.

The results of this process are used to update the Company's risk registers.

The SPACRMC also follows the above process. Risks which it identifies which have a Group dimension may be considered by the GRMC, the Audit Committee and/or the Board and passed to operating companies who are then responsible for mitigating these risks in their businesses.

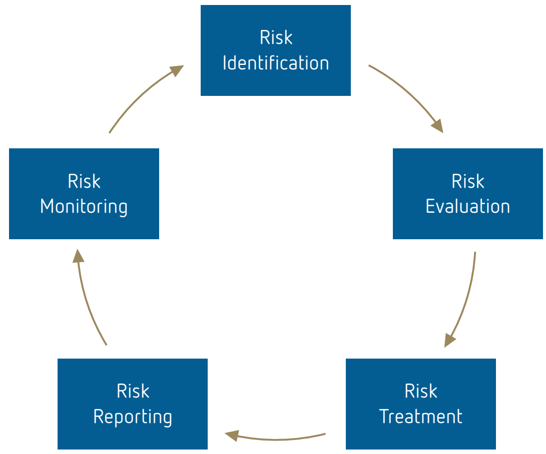
The risk forums of the GRMC provide specialist oversight and support to the operating companies, assisting them in the ERM process and providing additional challenge where appropriate. They also advise the GRMC on emerging risks which may affect the Group, help to analyse risk events that have materialised and develop best practices for managing risks, in each case in areas within their respective remits.

The GRMC reviews Group and divisional risk registers and considers how effectively risks are managed. It issues policies to the operating companies and promotes risk culture across the Group. The GRMC reports to the Audit Committee, which reports to the Board. The Board may itself identify risks, providing an independent perspective of what concerns them. These risks are passed to the GRMC and to the operating companies for incorporation into their risk registers.

The ERM process is thus both top down and bottom up. The Board gives guidance on its risk priorities, the operating companies assess their own risks and the SPACRMC group risks. All of these are reported to the GRMC and consolidated into the Group risk register which is then presented to the Audit Committee and the Board.

Risk management is an integral part of each stage of the business management process:

- Strategic planning is informed by the risk identification process which looks for opportunities as well as threats.
- Improving the risk profile is part of the budgeting and planning process.
- Delivery of action plans is included in the performance management process.
- Monitoring changes in the risk profile and its likely impact on the Company's risk profile is part of the ongoing reporting process.
- A risk assessment is also conducted as part of due diligence for any major investment or transaction.



Key Risk Management Focus Areas

The Group is exposed to a broad range of risks. The following table deals with the current key areas of focus. Note that significant risks specific to our operating companies are highlighted in their risk registers.

Key Focus Areas	Mitigation
Evolution of Hong Kong	– Regular review of strategy and investments by the Board. – Gradual rebalancing of business operations within the region with a particular focus on the Greater Bay Area. – Recruitment and training of more leaders with appropriate Chinese Mainland experience. – Enhancing corporate affairs capabilities and reinforcing relationships with government in order to contribute to public policy development.
Regulatory changes	– Through contacts with relevant authorities, understanding planned regulatory changes which may affect the Group's businesses. – Obtaining and acting on external legal and other professional advice.
Political – international tensions	– Monitoring of news, media reports, trends and prevailing public and government opinions. – Having crisis management and business continuity plans in place, with a focus on responding to 'high velocity' risk events. – Systematic management of relationships with key third parties. – Regular reviews of capital allocation to major countries.
Climate change	– Dedicated governance including a GRMC risk forum to oversee environment and sustainability risks and to recommend best practice. – Adopting appropriate targets. – Having contingency plans in place to respond to extreme weather events.
Crisis management	– Having an escalation and reporting protocol in place. – Regularly updating and testing crisis management and business continuity plans. – Bringing in specialist resources as required.
Protection and use of data	– Having the right policies (including relating to personal data), training programmes and penetration testing in place. – Adoption of NIST cybersecurity maturity standard. – Appointment of Chief Information Security Officer. – Dedicated governance including a GRMC risk forum to oversee IT, data and technology risks and to recommend best practice. – Using external service providers for cybersecurity solutions and system testing. – Having cyber incident response plans in place.
Portfolio discipline	– Having in place 10-year capital budgets. Consideration by the Board and management of the resulting make-up of the portfolio and of risks and alternatives. – Having in place formal processes for investment approval, including a dedicated investment committee. – Conducting risk and know your customer assessments of entities considered for investment and proposed joint venture partners. – Evaluating acquisitions after they have been made. Hiring more people who know about executing transactions.
People and culture	– Having in place policies and processes relating to recruitment, performance appraisal, learning and development, succession planning, staff wellness, diversity and inclusion, and compensation and benefits. – Developing digital capabilities by hiring appropriate staff and training existing staff. – Hiring external senior management where appropriate and putting local employees with high potential on a fast track for promotion.