Irish Continental Group

2019 ANNUAL REPORT & FINANCIAL STATEMENTS

RISK MANAGEMENT

Risk Management

Overview

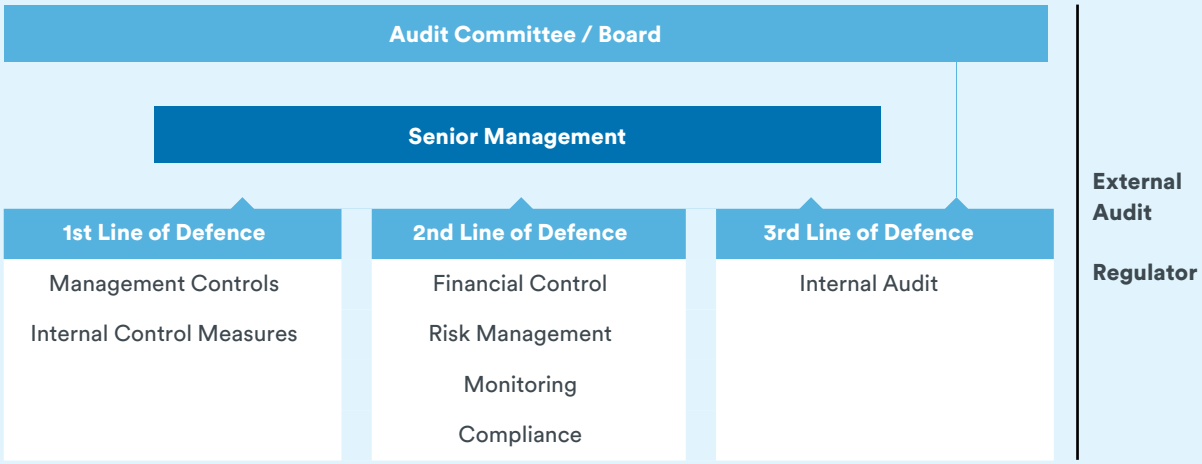
Exposure to risk is an inherent element to carrying out the business activities of the Group; the operation of ships and provision of related services. Effective risk management and internal control systems are therefore necessary to protect the Group from exposure to unnecessary risks and ensure the sustainability of the Group's business.

The Board has overall responsibility for establishing procedures to manage risk, oversight of the internal control framework and determining the nature and extent of the principal risks the Group is willing to take in order to achieve its long-term objectives. The Board has created a culture of risk awareness throughout the organisation whereby risk consideration is built into decision making processes.

This Board has delegated the monitoring of the Group's risk management and internal control systems to the Audit Committee. This assessment is carried out through the review of reports and presentations made by the Risk Management Committee (RMC) and Group Internal Audit. Further information on the Audit Committee activities is set out in its report on pages 83 to 87.

Risk Management Framework

The Group has adopted a three lines of defence framework to provide assurance that appropriate control and mitigation measures are in place for identified risks.



The first line of defence rests with management acting through their staffs who are responsible for the design, implementation and monitoring of internal control measures within their respective business areas.

The second line of defence comprises of oversight functions such as Group Finance and Group Marine and Safety. These functions are involved in policy setting and provide assurance over first line activities.

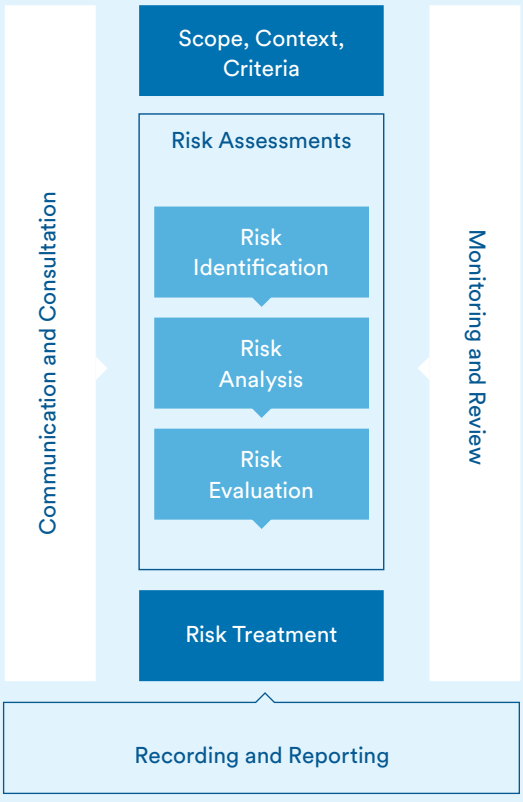
The third line of defence consists of the Group Internal Audit function, which performs independent oversight of the first two lines and reports directly to the Audit Committee on matters of internal control, compliance and governance.

Role of the Risk Management Committee

The RMC established by the Group comprises members from across the three lines of defence, as well as having Board representation. The RMC is tasked with driving the Group's risk management process including the maintenance of the Group Risk Register and coordination of risk management activities. The RMC role is one of facilitator rather than assessor. The RMC makes presentations to the Audit Committee and Board during the year outlining its work and reporting on key risk areas.

Risk Management Process

The Group's Risk Management Process is underpinned by the Risk Management Framework and is led by the RMC. The Group's process is based on the revised international standard ISO 31000 (2018), 'Risk Management – Guidelines', and provides a systematic approach to managing risks throughout the Group.



Risk identification and monitoring

The Board sets the Group's risk appetite and has identified four principal risk categories; strategic, operational, financial and IT and cyber. The Group's appetite for various risk areas is communicated through the adoption of Risk Appetite Statements. These provide context to how the Group's strategy is pursued and to which risks are assessed. The Board has a low tolerance for risks that may impact reputation in terms of safety of vessels and customers and compliance with relevant laws and regulations. The ICG Risk Code contains the Group's risk policy and details the Group's framework and risk activities.

Each business owner is responsible for ensuring comprehensive risk identification and assessment is carried out covering their sphere of responsibility. Risks are identified through various means, including the use of an identification tool guiding risk assessors through several internal and external factors in identifying potential barriers to respective objectives. Risks are assigned to risk owners whom are those persons with responsibility for the activity generating the risk. Where a risk contains multiple causes and consequences, risk owners are required to collaborate in performing a cause and consequence analysis.

Risk owners are ultimately responsible for the completion and maintenance of risk assessments across their respective risk areas. Risks are measured in terms of the likelihood of occurrence and estimated impact using a standardised scoring model. All evaluations are made from a Group perspective and are relative to Group risk appetite. Guidance tools are in place to ensure consistency is achieved across risk assessments and the Group.

Existing control measures are documented and assessed within the risk assessment forms in determining net risk scores. All risk assessments are reviewed by members of the RMC before they are released to the Group Risk Register. The RMC and risk owners can prescribe the implementation of further control measures at the review stage.

Risk Management
Continued

The Group Risk Register is the central online repository for documenting, assessing and prioritising risks, and for documenting and prescribing control measures. The Register forms a significant portion of the Group's risk management process.

The Group Risk Register is reviewed on a regular basis by the RMC. Any necessary changes to the Group Risk Register are identified throughout the year through the occurrence of a risk event, via quarterly RMC meetings, from Internal Audit reviews or through new risk assessments completed. The RMC will in time develop metrics to monitor changing exposure to key risks.

Risk information within the Group Risk Register is analysed and used for reporting principal risks to the Board and for Internal Audit planning. A presentation of the Group's principal and emerging risks is made to the Board at least annually or more frequently if warranted by developments. At these presentations the Board challenges the RMC is their processes and evaluations of the principal and emerging risks identified in the context of the Group's own risk policy, risk appetite and general market developments both within and outside the industry sector.

Emerging Risks

Risk monitoring is an ongoing process to reflect the dynamic nature of the environment in which the Group operates.

The Group acknowledges two types of emerging risks that can arise. The first type are new risks that emerge in the external environment in which the Group operates. These are identified through the ongoing Group risk identification process. The second type are previously identified risks recorded in the Group Risk Register whose impact on Group activities has changed, prompting a reassessment. Emerging risks are closely monitored and assessed as their uncertain nature can result in the risks becoming significant within a short timeframe. Emerging risks currently under review at the date of this report relate to greater employer responsibility for employee welfare, greater environmental and climate awareness driving increased regulation and the potential disruption to travel and trade from the developing situation around Covid-19.

Viability assessment

The principal risks identified through the Group's risk processes have been considered by the Directors when preparing the Viability Statement on page 67, as part of their assessment of the prospects for the Group.

Principal Risks

Strategic Risks

	Description	Potential Impact	Examples of Mitigation
Commercial & Market Service disruption	The Group operates in a highly competitive environment where service reliability is a key attribute and where brand damage can be caused through mismanagement of service disruption however caused.	Loss of revenue and reputational damage.	The Group has standard processes in place for managing various types of disruptive events, including clear and timely communications with customers. Vessels have access to high resolution professional weather forecasts and regular contact is maintained with ship managers.

Operational Risks

	Description	Potential Impact	Examples of Mitigation
Health and Safety Hazardous cargo	As a pivotal supplier of maritime transport services within Ireland's external logistics chain there is potential for incidents involving hazardous cargoes during handling or shipping.	Pollution, serious personal injury and reputational damage.	Hazardous cargoes are stowed in accordance with the International Maritime Dangerous Goods Code. The Group relies on quality customers and partners to ensure cargo is adequately packed, secured and declared. Crews are trained in the response to any hazardous incident. All hazardous paperwork requirements are strictly enforced by trained personnel.
Health and Safety Risk of injury	Given the nature of the Group's activities there is risk of accidents causing serious personal injury.	Loss of life and/or serious personal injury and reputational damage.	All companies within the Group maintain up to date Safety Policies. Safety audits are carried out on all Group locations. Information, instruction, training and supervision is provided to all personnel as appropriate. The Group has put in place major incident response plans and regularly conducts drills.
Operational Compliance People trafficking	As the Group operates international maritime services there is a risk that our services are used for people trafficking within cargo transport units.	Serious health risks to refugees or stowaways and reputational damage.	The Group complies with the International Ship and Port Facility Security (ISPS) Code. There is CCTV and 24-hour security at terminals. There is close liaison in place with the relevant port authorities on security measures. Additional private security is deployed at shore locations where warranted. Shore staff and crews are also given training in identifying suspicious traffic.

Risk Management
Continued

Financial Risks

	Description	Potential Impact	Examples of Mitigation
Financial Loss Major project failure	Where the Group contracts the construction of significant assets including vessels with long construction leadtimes there is risk of budget overrun arising from underestimation of costs, excess spending, or by failure in the performance of contractors.	Business interruption resulting in financial loss. Reputational damage.	Elements and objectives of major projects are clearly defined. External expertise is sought where appropriate. Any divergences from spending plans are investigated and reported to Executives. Due diligence is performed in advance on potential contractors. Contract guarantees are sought. Key milestone dates are set and monitored.
Financial Loss Inadequate insurance	The Group activities are capital intensive and concentrated in a small number of significant high value complex assets which increases the risk of inadequate insurance on new and existing assets, or on emerging risks.	Damage to assets resulting in irrecoverable losses and service disruption.	Management of insurance is performed by experienced and knowledgeable personnel. All insurances including insured values are reviewed timely prior to renewal. The Group maintains close liaison with its brokers regarding emerging risks and insurance trends.
Fraud Payment diversion	The Group incurs significant liabilities to a small number of suppliers which generates the risk that payments might be diverted to incorrect bank accounts.	Financial loss and potential reputational damage.	All invoices are reviewed by the relevant managers. All vendor bank account details are subject to a documented callback verification. Dual management authorisation is required for all payments in banking systems. There is a Group Social Engineering Policy in place which is circulated to relevant personnel, who are also required to undertake online awareness modules.
Volatility Fuel costs	The Group consumes fuel oils (accounting for 20% of 2019 operating costs) which are traded commodities and subject to significant unpredictable price fluctuation.	Increase in cost base, reducing profitability.	Group policy has been to purchase these commodities in the spot markets and to remain unhedged. The Group operates a dynamic surcharge mechanism with the Group's freight customers which allows for prearranged price adjustments in line with Euro fuel costs. In the passenger sector, in addition to fixed environmental surcharges changes in bunker costs are included in the ticket price to the extent that market conditions will allow.

IT Systems and Cyber Risks

	Description	Potential Impact	Examples of Mitigation
Information Security	By nature of the services offered the Group requires to capture and retain personal data which creates the risk of personal data breach by whatever means.	Heavy fines imposed under GDPR and reputational damage.	The Group has documented data protection impact assessments on all activities. Personal data is maintained in accordance with retention requirements. All mobile devices are encrypted. Compliance is assessed by the Group's Data Protection Officer and Group Internal Audit.
Cyber Threats	The Group relies on information technology systems to support its business activities. These systems are connected to customers and the internet generally which makes the Group susceptible to cyber-attacks affecting the availability of systems.	Business interruption resulting from spread of virus to critical systems and reputational damage.	Group policy is to only use licensed software providers. Anti-virus software is in place on all PCs. Security information and event management (SIEM) system is in place to detect infections quickly. All staff are required to undertake security awareness training. The Group has documented and rehearsed incident response plans in place.

IRISH CONTINENTAL GROUP

Irish Continental Group plc , Ferryport
Alexandra Road, Dublin 1, Ireland, D01W2F5.