RISK MANAGEMENT REPORT

RISK POLICY STATEMENT

Robust and effective management of risks is an essential and integral part of corporate governance. It helps to ensure that the risks encountered in the course of achieving the Group's strategic objectives are managed within the Group's risk appetite.

To achieve this, an Enterprise Risk Management ("ERM") approach is adopted for identifying, assessing, responding to and reporting on risks that might affect the Group in pursuit of its objectives and goals. The purposes of the implementation of ERM are as follows:

- to establish a structured and comprehensive process for identifying, assessing, reporting and managing risks;
- to define roles and responsibilities within a "Three Lines of Defence" framework;
- to increase risk awareness at all levels;
- to enhance constructive discussion, effective communication and timely escalation of risks by adopting a common platform for risk management;
- to focus on risks that are relevant to the Group's business and reputation, the Board's requirements and stakeholders' expectations;
- to provide senior management and the Board with a holistic view of the Group's material risk exposures and steps taken to manage and monitor such exposures;
- to provide senior management and the Board with the best available risk information and facilitate the making of informed decisions;
- to ensure compliance with the relevant laws and regulations, and the best practices in corporate governance; and
- to help creating and protecting the value of the Group.

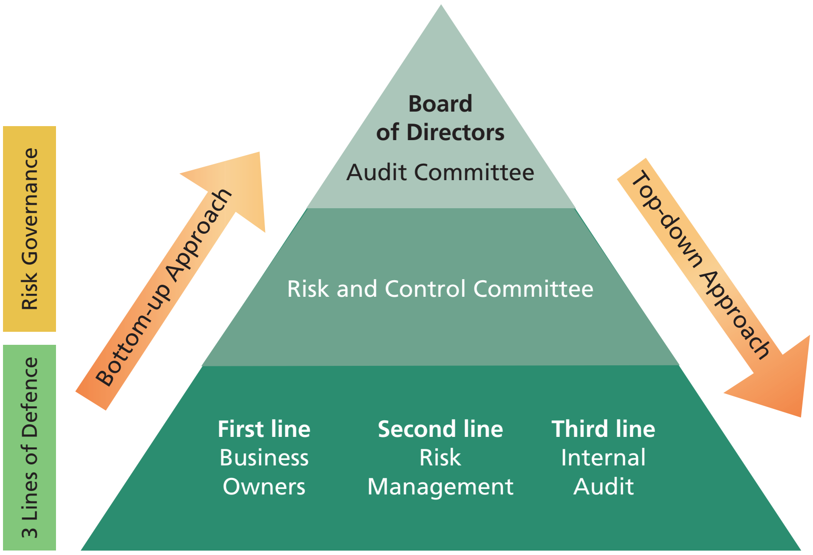
The Group is committed to continuously improving its ERM framework and processes and building a risk-aware culture across the Group with a view to achieving a sustainable and balanced development.

RISK GOVERNANCE AND MANAGEMENT

In August 2016, the Audit Committee approved the ERM Policy and Framework, which was based on the International Standard ISO 31000:2009 Risk Management – Principles and Guidelines, proposed by the Risk Management function of the Internal Audit Department. To ensure continued relevance and for continuous improvement, the ERM Policy and Framework has been reviewed and updated with changes in the newly released ISO 31000:2018.

The Group adopts a "Three Lines of Defence" model in risk governance. This is manifested by the oversight and directions from the Board, the Audit Committee and the Risk and Control Committee (formerly known as Internal Audit Committee) of the Group. The risk management framework of the Group combines a top-down strategic view with a bottom-up operational assessment conducted by each division and department. Members of senior management discuss the top-tier risks escalated through the bottom-up process and deliberate on any other risk issues that they consider important. This combined approach ensures that all the significant risks which need to be considered are identified and managed properly.

The following diagram illustrates the Group's Risk Governance and Management Framework:



The Board has the overall responsibility for evaluating and determining the nature and extent of the risks it is willing to take in achieving the Group's strategic objectives, and ensuring that the Group establishes and maintains appropriate and effective risk management and internal control systems.

RISK GOVERNANCE AND MANAGEMENT *(Continued)*

The Audit Committee is delegated with the authority from the Board to oversee the Group's management in the design, implementation and monitoring of the risk management and internal control systems. The Audit Committee advises the Board on the Group's risk-related matters. The Audit Committee is also responsible for reviewing and approving the Group's ERM Policy and Framework and for ensuring the adequacy and effectiveness of the Group's risk management and internal control systems. The Head of Internal Audit Department reports regularly to the Audit Committee, which in turn reports to the Board, on the Group's overall risk position and key exposures, the actions planned or taken by management, and major emerging risks that require special attention.

The Risk and Control Committee, with its formal terms of reference approved by the Audit Committee, is made up of members from senior management. The Risk and Control Committee assists the Audit Committee in discharging its corporate governance responsibilities for risk management and internal control. Regarding risk management, the Risk and Control Committee is responsible for ensuring that the ERM system is adequate and effective and that the ERM framework is implemented consistently throughout the Group. It monitors the Group's overall risk profiles by reviewing the key risks relating to individual business units and the key risks that are enterprise-wide, and ensures alignment with the approved risk appetite.

As the first line of defence, heads of individual divisions and departments manage risks faced by their business units/functions. As the risk owners, they identify and evaluate the risks which may potentially impact the achievement of their business objectives, mitigate and monitor the risks by designing and executing control procedures in their day-to-day operations. They conduct risk assessment and control self-assessment on a regular basis to evaluate the adequacy and effectiveness of controls that are in place to mitigate the identified risks.

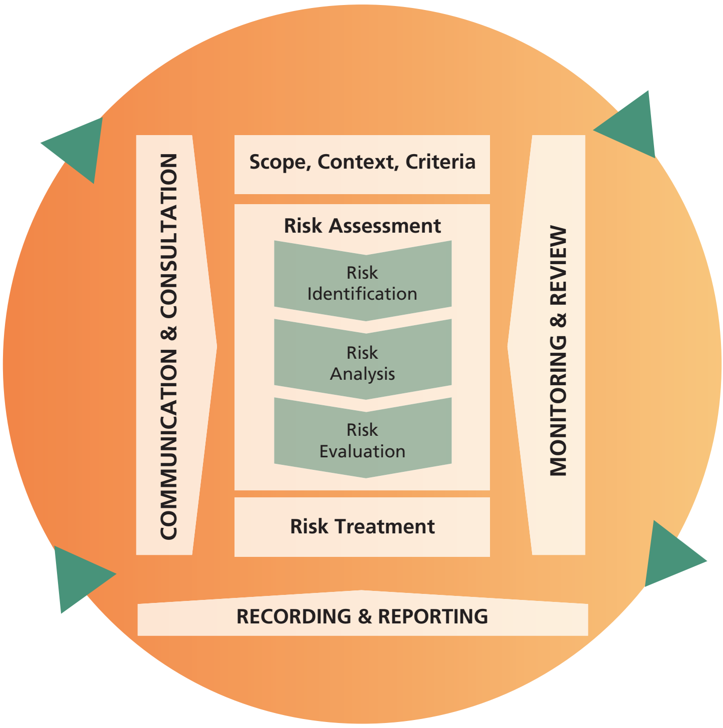
As the second line of defence, the Risk Management function is responsible for the ongoing maintenance of the ERM infrastructure and recommending changes to the Risk and Control Committee and the Audit Committee as appropriate. The Risk Management function collects and collates risk information to create an enterprise-wide view of risks and controls. In doing so, it critically reviews the risk assessment results of individual business units, constructively challenges their views so as to ensure that all the risks relevant to the Group are properly identified, consistently assessed and timely reported. It prepares reports for the Risk and Control Committee and the Audit Committee and escalates risk and control issues with reference to the risk appetite thresholds.

RISK GOVERNANCE AND MANAGEMENT *(Continued)*

As the third line of defence, the Internal Audit Department acts as an independent assessor. It conducts independent review and assessment of the adequacy and effectiveness of the risk management and internal control systems. The Internal Audit Department assesses if all the key risks are properly identified and evaluated according to the approved ERM Policy and Framework and whether the existing key controls are operating effectively. The risk assessment results are also mapped to the internal audit plan to ensure the audit performed by the Internal Audit Department systematically covers all the significant risks and the corresponding key controls. As such, the Internal Audit Department is able to provide independent assurance on the adequacy and effectiveness of the risk management and internal control systems and reports any deficiencies and room for improvement to the Risk and Control Committee and the Audit Committee.

RISK MANAGEMENT PROCESS

The ERM process is illustrated in the diagram below:



(Source: The ISO 31000:2018 Risk Management Process)

RISK MANAGEMENT PROCESS *(Continued)*

a) **Communication and consultation**

Communication and consultation with appropriate external and internal stakeholders takes place within and throughout all steps of the ERM process. For instance, the management team holds daily meeting to raise risk concerns, discuss emerging risks identified and formulate early response actions.

b) **Scope, context, criteria**

The risk management process applies to all business and decision-making processes, including the formulation of strategic objectives, business planning and day-to-day operations. The context of the ERM process is developed from the understanding of the external and internal environment in which the Group operates, taking into account the relevant external and internal factors, the relationships with the external and internal stakeholders and the contractual relationships and commitments to ensure that the risk management approach adopted is appropriate for the Group. To ensure a common assessment standard is adopted, risk criteria are defined to measure the relative significance of risk.

c) **Risk identification**

Divisions and departments analyze their respective business activities and main processes to identify operational risks, which forms a "bottom-up" approach. A "top-down" approach is also adopted by the senior management to identify business/strategic risks. Combining the output from the two approaches, a comprehensive list of risks for individual business units and hence for the Group can be generated. Risk classification system is used to facilitate the identification and accumulation of similar risks.

d) **Risk analysis**

The purpose of risk analysis is to comprehend the nature of risk and its characteristics. Risk analysis involves a detailed consideration of the risk sources, the consequences and likelihood, the existing controls and their effectiveness.

RISK MANAGEMENT PROCESS *(Continued)*

e) **Risk evaluation**

Divisions and departments use the predefined criteria to assign scores for the risks identified. With reference to the risk matrix (i.e. a combination of the consequence and likelihood scores), the risk ratings are determined (i.e. low risk, moderate risk, high risk and extreme risk). The risk ratings reflect the management attention and risk treatment effort required, taking into account the Group's risk appetite.

f) **Risk treatment**

The adequacy of existing controls is assessed in order to determine if additional measures are required to bring the remaining risks to an acceptable level. When determining the appropriate risk treatment plans, one or more of the following four types of risk response will generally be adopted:

- avoid (not to start or not to continue with the activity that gives rise to the risk);
- reduce (lessening the likelihood or consequences);
- transfer (sharing the risk with another party, e.g. insurance); and
- accept (retaining the risk by making an informed decision).

g) **Monitoring and review**

Annual risk assessment is conducted to effectively manage the Group's risk profile. A half-yearly review is also conducted to update the progress of risk treatment plans and incorporate changes in the external and internal environment. Key risks and emerging risks are reviewed at least quarterly and at the situation may require.

h) **Recording and reporting**

The results of risk assessment are documented in the risk registers in a consistent manner. All the identified risks, risk scoring and ratings, together with the details of existing controls and proposed treatment plan (if any) are recorded in the risk registers.

Quarterly ERM report is prepared for the Risk and Control Committee and the Audit Committee. The Group's top tier risks are presented in a heat map which provides a dynamic and forward-looking picture of the Group's risk position. The changes in risk profile since the last review, the corresponding key controls and risk treatment plans, as well as the targeted risk positions upon the completion of risk treatment plans with specified time frame are highlighted in the ERM reports. The potential/expected trend of certain risks, such as emerging risk, is also indicated on the heat map.

PRINCIPAL RISKS TO THE GROUP

The principal risks faced by the Group include the following:

Risk Category	Risk Description	Risk Movement*	Key Controls/ Mitigation Measures
Strategic Risk	Changes in macro-economic outlook and government policies resulting in decrease in number of visitor/tourist/customer	↓	• Closely monitoring changes in global and local economic outlook as well as Mainland China policy, and making appropriate responses promptly • Constantly monitoring business performance and adjusting our pricing and marketing strategies accordingly • Continuous effort on market diversification to attract visitors from different countries • Regular review of the conditions of our properties to determine if hotel facilities upgrade or renovation is necessary • Continuously improving the quality of our services to strengthen our brand and market position
Operational Risk	Human resources – tight labour market	↔	• Regular review of compensation and benefit package to ensure competitiveness • Continuous and strong focus on staff development, e.g. providing in-house training and development programmes to retain our staff • Succession planning
	Cyber security	↑	• Implementation of security measures such as firewall, anti-spam and anti-virus protection • Ongoing review of IT infrastructure and systems and the need for upgrade/ enhancement • Internal communication and training on cyber-attack threats

PRINCIPAL RISKS TO THE GROUP *(Continued)*

Risk Category	Risk Description	Risk Movement*	Key Controls/ Mitigation Measures
Operational Risk *(Continued)*	Disaster event, e.g. epidemic, terrorist attack	↔	• Comprehensive insurance coverage for our properties and business operations • Contingency plans developed for critical business processes/ functions • Taking immediate response actions, e.g. stepping up hygiene measures when potential threat of epidemic increases

For the financial risks of the Group, please refer to "Notes to the Consolidated Financial Statements" on pages 138 to 141.

* *Key – Risk Movement (change from last year)*

↑ *Risk rating increased*

↔ *Risk rating remained broadly the same*

↓ *Risk rating decreased*

INTEGRATION OF RISK MANAGEMENT WITH INTERNAL CONTROL SYSTEM

Risk management is closely linked to the Group's Internal Control Framework. Key controls for mitigating high risk items identified in the ERM process are subject to independent reviews and tests by the Internal Audit Department in order to assess their adequacy and effectiveness. Details of the internal control system are set out in the "Corporate Governance Report" on pages 26 to 30.

REVIEW OF THE EFFECTIVENESS OF RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

During the year, the Audit Committee, on behalf of the Board, has reviewed the effectiveness of the Group's risk management and internal control systems. Details of the aforesaid review of effectiveness are described in the "Corporate Governance Report" on pages 29 to 30.