Effectiveness review

To ensure focused oversight, the Board operates a separate Risk Committee (see pages 154 to 163). The Risk Committee reviews the effectiveness of the Group's risk management policies and practices. This effectiveness review is conducted through speaking with senior management directly, third party assurance reviews, reports from internal and external audits, and independent testing of our key controls.

The Audit Committee reviews the adequacy and effectiveness of the Group's system of internal financial controls (see page 149). The Audit Committee remains satisfied that the review of internal financial controls did not reveal any significant weaknesses or failures, and that they continue to operate effectively.

Following the Audit and Risk Committee's reviews, the Chairs of each Committee confirmed to the Board that they were satisfied that the Group's internal control framework (financial and non-financial) and risk management procedures:

- operated effectively throughout the period; and
- are in accordance with the guidance contained within the FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.

Risk appetite

Risk is inherent in running any business. At Derwent London we aim to deliver on our strategic objectives for the benefit of our shareholders and other stakeholders, whilst operating within the risk tolerance levels set by our Board.

The Group's risk appetite is set by the Board and is the level of risk we are willing to accept to achieve our strategic objectives. Our overall risk appetite is low with varying levels of risk tolerance. This, alongside our culture, informs how our staff respond to risk. Due to our open and collaborative working style, any potential problem, risk or issue is identified quickly so appropriate action can be taken.

The use of inherent and residual 'risk ratings' within our Schedule of Principal Risks makes it easier for the Board to identify which risks are not aligned with its tolerance on a residual basis (after controls):

- When assessing our health and safety risks, we consider all of our core activities, including the work of our contractors on site at our developments. Due to the nature of these activities, health and safety is classified as a 'medium risk' at residual level, which requires further contractor-led controls to be implemented and the adoption of best practice standards. As the Board is committed to promoting the highest health and safety standards, its tolerance for health and safety risks is set at zero. Further information on health and safety is on pages 80 and 81.
- Similarly, the Board's tolerance for cyber threats is low. The Board recognises that due to the pervasive nature of the threat, it is difficult to reduce the residual risk from medium to low. To provide the Board with comfort that our Digital Innovation & Technology (DIT) team have adopted a continuous improvement strategy towards our cyber security posture, we commission regular independent reviews and assessments as well as ongoing monitoring by the Risk Committee. Further information is on pages 160 and 161.

Risk Appetite Statement
Summary of risk tolerance

Operational	
Health and safety	Zero
IT continuity (including cyber attacks)	Low
Staff retention	Medium
Climate change resilience	Low
Other operational risks	Medium
Financial*	
REIT status	Low
Credit rating	Low
Decrease in asset value (>£100m)	Medium
Profits (>£5m)	Medium
Cost overruns (>5%)	Medium
Interest cover (<20%)	Medium
Reputational	
Brand value	Low
Regulatory	
Statutory	Zero
Governance	Low

* Financial amounts are measures of deviation from Group annual budget.

Key

Zero	The Board has a zero-tolerance approach and is committed to promoting full health and safety and statutory compliance
Low	The Board is risk averse and is reluctant to take risks
Medium	The Board is willing to take measured risks if they are identified, assessed and controlled
High	The Board is willing to take significant risks

Additional risk disclosures	Page
Double materiality assessment	68
Health and safety	80 and 81
Risk management structure	162
Risk documentation and monitoring	159
Digital security and strategy risks	160 and 161
Risk management framework	158