Risk Committee report

Helen Gordon Chair of the Risk Committee

2026 focus areas

- Receive regular updates on central London market trends which may impact the portfolio
- Ensure health and safety risks continue to be managed effectively
- Receive updates on the Group's main developments and compliance with the Building Safety Act
- Monitor the Group's ongoing strategy in mitigating cyber risk
- Continue to monitor the Group's principal and emerging risks

Committee membership during 2025

	Independent	Number of meetings	Attendance[1]
Helen Gordon	Yes	3	100%
Lucinda Bell	Yes	3	100%
Sanjeev Sharma	Yes	3	100%
Cilla Snowball[2]	Yes	1	100%
Madeleine McDougall	Yes	3	100%

1 Percentages are based on the meeting entitled to attend for the 12 months ended 31 December 2025.

2 Cilla Snowball stepped down from the Board at the AGM on 16 May 2025.

Dear Shareholder,

I am pleased to provide a report on the activities and focus areas of the Risk Committee during 2025.

Risk profile of the Group

As a predominantly London-based Group, we are particularly sensitive to factors that impact central London's growth and demand for office space. The Group's risk profile has continued to be elevated in 2025 characterised by uncertainty in the macroenvironment and cost inflation.

Managing risks / See pages 100 to 111

Key activities of the Committee

During the year, the Committee has overseen four principal areas: property and market, cyber security, people and environment and compliance.

A particular focus of the Committee has been to continue to monitor the emerging and market risks and how they might impact the Group in the short to medium-term. In response to this, the Committee has held in-depth discussions around the potential impact of the UK Government's current policy agenda and the proposal to abolish upward only rent review clauses in commercial leases.

The Committee also received training on the Building Safety Act 2022 with the objective of raising awareness at Board level. The training related to two of the Group's major developments, 25 and 50 Baker Street, and it was pleasing to note the Group's progress and compliance with the Building Safety Act.

Key activities of the Committee / See pages 156 and 157

Cyber security

During the year, the Committee continued to remain vigilant to the ongoing risk of cyber crime and dedicated a significant proportion of its meeting in August to receiving a thorough update on cyber security, which provided an overview of the Group's cyber posture and strategy. Although no cyber-related issues have arisen during 2025, cyber insurance has been acquired to further support the Group in mitigating the risk of cyber attacks.

Our disclosures on the work completed in respect of cyber security have been expanded in this report to reflect the volume of work that has been undertaken during the year.

Cyber security / See page 156

Health and safety

The Committee remains committed to prioritising the safety of our people, contractors and occupiers. At each meeting a detailed update on health and safety is provided and includes a forward look at the potential risks across the managed portfolio and major developments, including how they will be mitigated. During the year, the Group's ongoing commitment to health and safety was reinforced through the delivery of health and safety training by Mishcon de Reya to Executive Directors, Non-Executive Directors and senior management.

Health and safety / See pages 80 and 81

Key risk indicators

The Committee monitors a schedule of key risk indicators which works to provide early warning signs of potential risks, helping organisations to anticipate and mitigate risks before they escalate. During the year, a comprehensive internal review of the key risk indicators schedule was conducted. The review ensured the indicators remain forward looking and continue to support the Committee in identifying early warning signs of potential risks approaching or exceeding tolerance levels. As part of the review, enhancements were made to broaden the scope of the schedule, with new areas identified for inclusion to strengthen the overall risk monitoring framework.

Further engagement

The forthcoming AGM is on 15 May 2026 and I will be available to answer any questions on the Committee's activities that you may have. If you wish to contact me, I am available via our Company Secretary, David Lawler.

Telephone: **+44 (0)20 7659 3000** or
Email: **company.secretary@derwentlondon.com**

Helen Gordon
Chair of the Risk Committee

25 February 2026

Committee composition and performance

The Committee's membership for the year under review is detailed in the table on page 154. In addition to the Committee members, the Board Chairman, other Directors, senior management and the internal and external advisers, are often invited to attend all or part of any meeting as and when appropriate or necessary.

In 2025, the Risk Committee met three times (2024: three meetings). The meetings in August and November included a joint session with the Audit Committee to review the outcome of internal audits (see page 147).

The 2025 evaluation of the Board, its committees and individual Directors was externally facilitated by the third party Independent Audit Limited, in accordance with our three-year cycle of evaluations (see page 137). The review raised no significant matters or areas of concern in respect to the operation of the Committee.

The Committee's role and responsibilities are set out in the terms of reference, which were last updated in August 2024, and are available on the Company's website at: **www.derwentlondon.com/investors/governance/board-committees**

New 'failure to prevent fraud' offence

Alongside the Audit Committee, the Risk Committee is responsible for overseeing the Group's non-financial internal controls and risk management systems.

During the year, the Group has remained informed about the new corporate offence, 'failure to prevent fraud' under the Economic Crime and Corporate Transparency Act 2023 (the Act). The Act seeks to promote stronger anti-fraud governance and strengthens corporate integrity by placing an obligation on companies to ensure reasonable procedures are in place to prevent fraudulent activity.

To ensure both compliance with the Act and to demonstrate that the Group has reasonable procedures in place to protect against fraud, the following activities were undertaken during the year, in addition to the review and update of the Fraud Risk Management Framework and detailed Fraud Risk Assessment:

Gap analysis: An in-depth gap analysis was conducted using the Home Office's guidance to understand how the Group's existing fraud controls compared to the six key principles of a robust fraud prevention framework.

Training and awareness: The Executive Committee attended a training session hosted by Burges Salmon to understand their obligations, liability and role in preventing fraud within the organisation. Due to the positive feedback and high level of engagement received, the training session was extended to over 30 other employees who are involved in the procurement of goods and services.

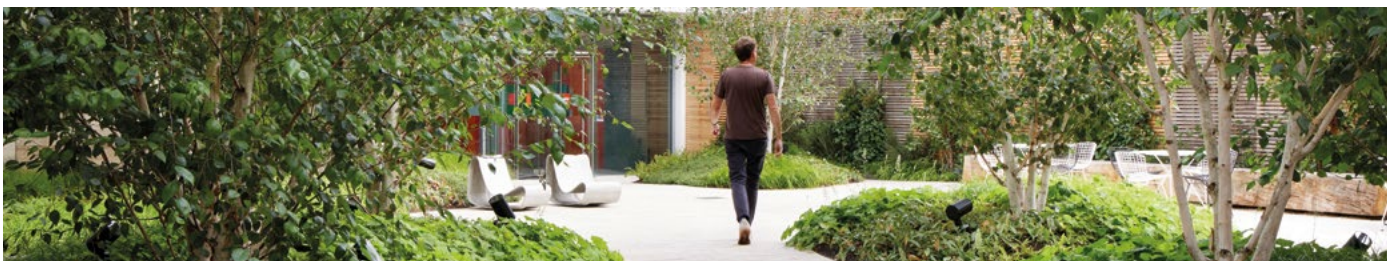
Independent review: The Group's compliance with the Act and the strength of existing 'reasonable procedures' were subject to independent review and assessment by Internal Audit. The review found a sound level of fraud prevention and detection controls to be in place, with only minor opportunities for continued improvement noted.

The Risk Committee will continue to monitor the legal developments under the Act and ensure that the Group's Fraud Risk Management Framework remains robust.

Director ID verification / See page 137

Fraud Risk Management / See page 148

Supplier whistleblowing line / See page 168



Oliver's Yard EC1

Key activities of the Committee

During 2025, the Committee focused on a variety of risks across four principal categories: property and market, cyber security, people and environment, and compliance.

Property and market

Impact of current Government's policies

Discussed the impact of the UK Government's current policy agenda on the central London property market and both the opportunities and risks faced by the Group.

A detailed discussion was held on the Government's proposal to abolish upward only rent review clauses in commercial leases.

Investment market

A comprehensive update on the London investment market with an overview of both opportunities and risks from CBRE.

Development risks

Regularly reviewed the key risks affecting the Group's major on-site developments. The Committee also received an update on the construction market with a focus on the supply chain challenges, tender price inflation and construction costs.

Construction Market

An update on the Construction Market was provided to the Committee and covered the following areas:

- Construction costs
- Supply chain challenges
- Tender price inflation

Reviewed valuation in business rates

An overview of the 2026 reviewed valuation of business rates was received and the Committee discussed how this could impact the Group.

Insurance claims

The Committee reviewed the number of insurance claims that have been incurred across the managed portfolio over the last five years and discussed the controls in place to continue to mitigate the risk.

Strategic objectives

1 2 4

Principal risks (see page 104)

1 3 4 5

Cyber security

Cyber security

In August 2025, the Digital, Innovation & Technology team provided an in-depth presentation on the Group's cyber posture, layered defence model and strategy.

Cyber Governance Code of Practice

Following the publication of the Cyber Governance Code of Practice in April 2025, the Committee received a comprehensive gap analysis undertaken by the Digital, Innovation and Technology (DIT) team and discussed the timeline to implement the remaining recommendations.

Phishing tests

Updates were provided on the phishing tests conducted by the Cyber and Infrastructure team.

Security penetration tests

Internal and external penetration tests were carried out by an independent security adviser.

Software vulnerability tests

Manual and automated vulnerability testing of our internally developed apps and solutions.

Employee risk score

During the year, we implemented a new employee risk score feature to ensure that our training and prevention measures are aligned with risk levels.

Crisis Management Team

The Crisis Management Team, reviewed its incident playbooks with the assistance of external experts and initiated a comprehensive revision of its Business Continuity Plan (BCP).

Cyber insurance

Obtained cyber insurance cover and discussed how this additional cover will supplement the existing cover in place.

Strategic objectives

3 4

Principal risks

6 7

Strategic objectives

1 To optimise returns and create value from a balanced portfolio

2 To grow recurring earnings and cash flow

3 To attract, retain and develop talented employees

4 To design, deliver and operate our buildings responsibly

5 To maintain strong and flexible financing

People and environment

Health and safety (H&S)

A detailed update on health and safety matters was provided with key risks identified. During the year the following areas were covered:

Key health and safety risks

An overview of the key health and safety risks across the managed portfolio, construction sites and the Scottish land, as well as a forward look at the Group's major projects were outlined and discussed by the Committee.

Health and safety training

Senior management received training on health and safety management from Mishcon de Reya, as well as attending health and safety leadership tours across the Group's major developments. The engagement of the Board in health and safety matters reinforces the Board's commitment and visibility to health and safety.

Building Safety Act 2022

An in-depth training session on the Building Safety Act took place which supported raising awareness across the business.

Occupier health risk

The Committee received an update on the Group's occupiers' covenant and financial 'health' as well as assurance that the process which assesses proposed occupier covenant strength remains robust.

Service charge

Discussed the market factors contributing to the rates of service charges and benchmarked the Group's service charge expenditure.

Environmental risk

Environmental risks are reserved for the Board and two of its principal committees; the Responsible Business and Audit Committees. Further details are included on page 94.

Strategic objectives

3 4

Principal risks

8 9 10

Compliance

Internal audits

Alongside the Audit Committee, the Committee received regular updates on the work performed by internal audit, including the Fraud Risk Management Framework and Fraud Risk Assessment.

Legal updates

The Committee reviewed the Group's status against recent legislation developments and received updates from management on the preparation for any upcoming legal developments. In particular, the Committee has monitored the developments of the Economic Crime and Corporate Transparency Act 2023.

Key risk indicators

The key risk indicators were subject to a thorough review to ensure they remain forward looking and provide a holistic overview of all key areas across the business.

Group risk registers

The Committee reviewed the Schedules of Principal and Emerging Risks and in particular discussed whether the risk registers sufficiently cover:

- geopolitical risks; and
- the ability to sell assets in a challenging market.

Anti-bribery and corruption

The Committee continued to review the Hospitality & Gift Register at each meeting. The Register provides an overview of the returns of all employees each quarter.

Compliance training

The Committee continued to monitor the completion rates and engagement received with the compliance training programme. During the year, c.99.6% of employees completed quarterly compliance training (see page 163).

Strategic objectives

3 4

Principal risks

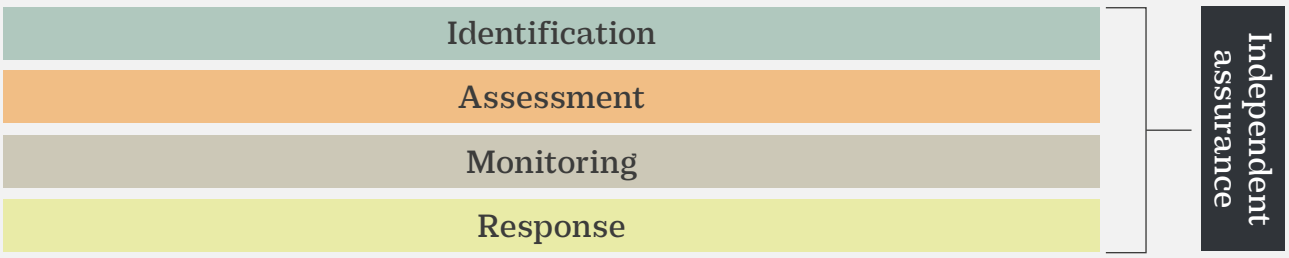
10

Risk Committee report continued

Risk management framework

Our risk management procedures seek to ensure that all foreseeable and emerging risks are identified, understood and managed.

Our risk management framework is summarised below:



Identification

- **Top down approach to identify the principal risks that could threaten the delivery of our strategy:** At the Board's annual strategy review, scenarios for the future are considered which assist with the identification of principal and emerging risks and how they could impact our strategy. The continuous review of strategy and our environment ensures that we do not become complacent and that we respond in a timely manner to any changes.
- **Bottom up approach at a departmental and functional level:** Risks are principally identified by the Executive Committee and members of senior management, through analysis, independent reviews and use of historical data and experience. Risk registers are maintained at a departmental/functional level to ensure detailed monitoring of risks, where necessary. Risks contained on the departmental registers are fed into the main Group Risk Register depending on the individual risk probability and potential impact.

Assessment

Following the identification of a potential risk, the Executive Committee seeks to:

- gain sufficient understanding of the risk to allow an effective and efficient mitigation strategy to be determined;
- allow the root cause of the risk to be identified;
- estimate the probability of the risk occurring and the potential quantitative and qualitative impacts; and
- understand the Group's current exposure to the risk and the 'target residual risk profile' (in accordance with the Board's risk tolerance) which will be achieved following the completion of mitigation plans.

Where necessary, external assistance is sought to assess potential risks and advise on mitigation strategies. Emerging risks are kept under review at each Risk Committee meeting and are reassessed during the Board's annual strategy review.

Monitoring

As part of our risk management procedures, the Executive Committee and Risk Committee routinely conduct monitoring exercises to ensure that risk management activities are being consistently applied across the Group, that they remain sufficiently robust and identify any weaknesses or enhancements which could be made to controls. Monitoring activities include:

- the regular review and updating of the Schedule of Principal Risks, Schedule of Emerging Risks and the Group's Risk Register;
- alerting the Board to new emerging risks and changes to existing risks;
- monitoring how the risk profile is changing for the Group; and
- providing assurance that risks are being managed effectively and, where any assurance gaps exist, identifiable action plans are being implemented.

Response

We implement controls and procedures in response to identified risks with the aim of reducing our risk exposure, so that it is aligned or below our risk tolerance. The successful management of risk cannot be done in isolation without understanding how risks relate and impact upon each other. The mitigation plans in place for our principal risks are described on pages 104 to 109. We use insurance to transfer risks which we cannot fully mitigate.

Insurance

The Group has a comprehensive insurance programme. We are advised by insurance brokers, who provide a regular report to the Risk Committee. We have a long-standing relationship with our property insurers, who perform regular reviews of our properties that aim to identify risk improvement areas. Due to our proactive risk management processes, Derwent London has a low claims record which makes us attractive to insurers.

Risk management

At Derwent London, the management of risk is treated as a critical and core aspect of our business activities. Although the Board has ultimate responsibility for the Group's risk identification and management procedures, certain risk management activities are delegated to the level that the Board judges is most capable of overseeing and managing the risks. In order to gain a comprehensive understanding of the risks facing the business and the management thereof, the Risk Committee invites senior managers and external advisers to present at its meetings.

A robust assessment of the principal risks facing the Group is regularly performed by the Directors, taking into account the risks that could threaten our business model, future performance, solvency or liquidity, as well as the Group's strategic objectives over the coming 12 months.

Our principal risks are documented in the Schedule of Principal Risks (see pages 104 to 109) which includes a comprehensive overview of the key (financial and non-financial) internal controls in place to mitigate each risk and the potential impact. The Directors also review an assurance framework which evidences how each internal control is managed, overseen and (where appropriate) independently assured.

Due to its importance, material changes to the Schedule of Principal Risks can only be made with approval from the Risk Committee or Board. Further information on the Group's risk registers subject to review by the Risk Committee are detailed in the table below.

Health and safety training at Board level

During the year, the Board's ongoing engagement in, and commitment to, health and safety was reinforced through the delivery of health and safety training to Executive Directors, Non-Executive Directors and senior management. The training session was led by Mishcon de Reya, with the objective of updating and refreshing senior management's understanding of evolving health and safety obligations, responsibilities and the importance of proactive risk management.

The training session focused on:

- recent developments in health and safety legislation;
- contractual implications of health and safety compliance;
- identification and mitigation of workplace risks;
- corporate and director's duties under current regulations;
- best practice guidance tailored for executive and non-executive roles; and
- a review of Derwent London's health and safety governance structure.

"To see so much active participation at both sessions was a credit to all those involved."

Matt Peaty
Head of Health and Safety

Risk documentation and monitoring

Schedule of Principal Risks **(See page 104)**	Contains the risks which are classified as the Group's main risks which do or could impact the Group over the next 12 months. The Schedule of Principal Risks also includes an assurance framework to evidence how each control is managed, overseen and independently verified. As at 31 December 2025, the Schedule of Principal Risks contains 11 risks (2024: 11 risks).
Schedule of Emerging Risks **(See page 110)**	Contains the internal and external emerging risks that could significantly impact the Group's financial strength, competitive position or reputation within the next five plus years. Emerging risks could involve a high degree of uncertainty. As at 31 December 2025, the Schedule of Emerging Risks contains four risks (2024: five risks).
Group Risk Register	Risks not deemed to be principal to the Group are documented within the Group Risk Register, which is maintained by the Executive Directors, with assistance from the Executive Committee. The Board reviews and approves the Group Risk Register and it is reviewed by the Risk Committee on an annual basis. As at 31 December 2025, the Group Risk Register contains 50 risks (2024: 48 risks).
Key risk indicators	The Risk Committee has identified risk areas which could indicate an increase in the Group's risk profile. These indicators are reviewed at each Risk Committee meeting and are compared against the Board's Risk Appetite Statement (see page 103). During the year, the key risk indicators were subject to a thorough internal review to ensure the indicators remain forward looking and continue to support the Committee in identifying early warning signs of potential risks approaching or exceeding tolerance levels. Any deviance or significant increase is subject to challenge by the Risk Committee.
Functional/ departmental risk registers	Risk registers are maintained at a departmental/functional level to ensure detailed monitoring of risks, where necessary. These registers are the responsibility of each department and are periodically reviewed by the Risk Committee during risk-specific presentations. Examples of these registers are the development risk registers for each building project and the 'tenants on watch' register.

Risk Committee report continued

Digital security risks

We adopt a layered defence approach to cyber security which provides multiple levels of security controls to protect against cyber attacks.

The Group's cyber security framework is subject to regular independent review and testing, the outcomes of which are reported to the Risk Committee. During H1 2025, engagement was sought with a CREST-accredited security consultant for a comprehensive penetration test to be conducted across all of the Group's infrastructure. The scope of this testing included both external and internal assessments and encouragingly, no critical vulnerabilities were identified. We operate a layered defence model that applies multiple, complementary security controls across our technology environment, reducing reliance on any single control and mitigating single points of failure.

Our Security Information and Event Management (SIEM) platform continuously aggregates and analyses telemetry from across our systems and infrastructure, providing real time visibility of security events. This capability is supported by a 24/7 Security Operations Centre (SOC), which proactively monitors for indicators of compromise and anomalous activity. Potential incidents are investigated promptly, and confirmed events are managed in accordance with established incident response playbooks to ensure timely containment, remediation and recovery. To maintain preparedness, we regularly review and update these incident response playbooks and participate in table-top exercises designed to test decision making, escalation processes and recovery arrangements. These activities help ensure that our response capabilities remain effective and aligned to evolving threats. These preventative, detective and responsive controls are complemented by regular vulnerability assessments, independent penetration testing and ongoing control assurance activities. Together, they strengthen our ability to identify emerging risks, minimise potential impact and enhance our overall cyber resilience.

In June 2025, following the publication by RICS on 'Digital Risk in Buildings', the Group commissioned WiredScore to pilot the newly developed Cyber Foundations Assessment at one of its flagship properties. The assessment, conducted through an on-site review supported by documentation, evaluated 16 criteria across four key domains: Governance, Building Systems, Cyber Controls, and System Vulnerabilities. The outcome demonstrated an overall maturity level of 'advanced' across the categories assessed, underscoring the Group's commitment to maintaining high standards of digital resilience within the portfolio. Opportunities for further enhancement identified during the process will be reviewed and considered for application across the wider portfolio.

Key risk indicators

The Committee reviews a dashboard of key risk indicators at each meeting, incorporating information security and cyber risk related KPIs. During the year, an in-depth review was undertaken to ensure the indicators remain forward looking and continue to support the Committee in identifying early warning signs of potential risks or tolerance levels being exceeded.

As part of this review, cyber risk indicators were updated to reflect the evolving threat landscape. A significant enhancement was the introduction of employee risk scores within the Group's security training platform, enabling a data-driven approach to identifying and mitigating potential vulnerabilities among employees. This strengthens the Group's cyber resilience by directing training at employees with the greatest need. Risk scores are derived from engagement with training modules, performance in cyber security assessments, and responses to simulated phishing exercises. Employees identified as higher risk are now monitored with targeted interventions including additional training and phishing simulations where necessary, until their risk levels fall within acceptable thresholds. To reinforce these measures, all employees were required to complete mandatory compliance training during the year, which included a Cyber Security and Data Protection module.

Disaster recovery and business continuity

Derwent London has formal procedures in place for use in the event of an emergency that disrupts normal business operations. These consist of:

Business Continuity Plan (BCP)	Crisis Management Team (CMT)	Off-site disaster recovery	Testing and review
The BCP serves as the centralised repository for the information, tasks and procedures that would be necessary to facilitate Derwent London's decision making process and its timely response to any disruption or prolonged interruption to our normal activities. The aim of the BCP is to enable the recovery of prioritised business operations as soon as practicable.	The CMT is composed of key personnel deemed necessary to assist with the recovery of business. The BCP empowers the CMT to make strategic and effective decisions to support the recovery of business until we are able to return to normal working.	An off-site disaster recovery data centre is available in the event of an emergency, to provide continued access to IT services and data to our staff.	The strength of our business continuity and disaster recovery plans are regularly tested and continually refined to reduce the potential for failure.

Digital strategy risks

As we increase the digitalisation of our business model through our Intelligent Building programme, our potential exposure to digital risks also increases. A cyber attack on our buildings has been identified as a principal risk for the Group, and our key controls to mitigate these risks are detailed on page 107.

Artificial Intelligence (AI)

Technological advancements, particularly in the form of AI, are an emerging risk for the Group (see page 110). While the rapid pace of change offers the potential for efficiency gains across the business, AI can introduce new cyber security vulnerabilities and amplify data privacy concerns. Our Acceptable Use policy has been amended to reference the responsible use of AI and during 2026 we are looking to develop a responsible AI framework based on transparency, security, human oversight and ethical use. We continually review emerging AI tools and platforms to identify those that can safely and meaningfully add value across the business.

Intelligent Building programme

The Derwent London Intelligent Building programme aims to improve building performance through enhanced monitoring, reduced equipment faults, and lower energy use and operational carbon. In 2025, the Executive Committee continued to oversee the programme and received ongoing updates on its progress and impact.

AI is being harnessed to enhance efficiency across our portfolio by improving energy management, predictive maintenance and operational decision making. It enables richer data insight to support design, leasing and customer experience, while automation can free teams to focus on higher-value, creative and strategic work.

Cyber Governance Code

In April 2025 the Cyber Governance Code of Practice (the Code of Practice) was published by the UK Government with the aim of demonstrating to boards how to manage digital risks and how to protect their organisations from cyber attacks. The Code of Practice outlines recommendations across five categories:

- Risk management
- Strategy
- People
- Incident planning, response and recovery
- Assurance and oversight

Following the publication of the Code of Practice, a comprehensive gap analysis was undertaken by the Digital, Innovation and Technology (DIT) team with a discussion held on the timeline to implement the remaining recommendations.

Data protection

Derwent London is perceived as being relatively low risk from a data protection perspective, as the amount of personal data that we hold and process is limited. We have robust procedures in place to safeguard the security and privacy of information entrusted to us. As part of the Committee's key risk indicator schedule, we monitor the number of 'near miss' data breaches and how these have been addressed.

Our procedures ensure that we:

- maintain the confidentiality, integrity and availability of data and safeguard the privacy of our customers and employees, to ensure that the business retains their trust and confidence;
- protect the Group's intellectual property rights, financial interests and competitive edge;
- maintain our reputation and brand value; and
- comply with applicable legal and regulatory requirements.

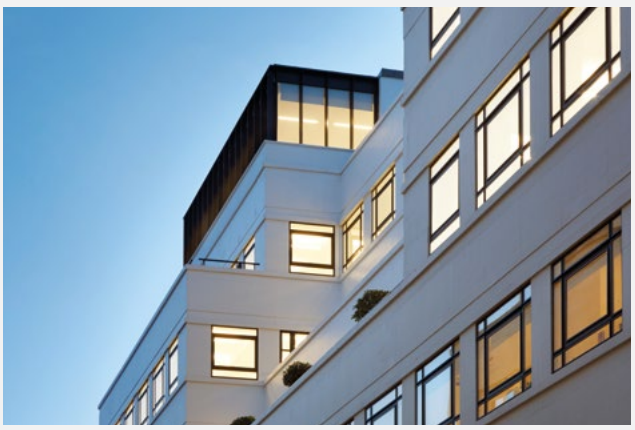
We operate a Data Protection Steering Committee which meets on a quarterly basis and comprises of Data Protection Champions from each department. Our DIT team routinely conducts supplier information security due diligence assessments as part of the onboarding process for all new suppliers of digital services to help provide assurance on the risk profile of our suppliers and reduce the risk of supply chain attacks. Data Protection Impact Assessments (DPIAs) are also completed for any new projects or changes to processes that involve data processing, to help identify and mitigate any data privacy risks.

Crisis Management Team

Derwent London operates a Crisis Management Team that is comprised of key personnel deemed necessary to assist with the recovery of the business.

During the year, the Group initiated a comprehensive revision of its Business Continuity Plan (BCP) to ensure it remains robust, modern, and aligned with industry best practice. As part of this update, we have introduced a formal Gold-Silver-Bronze (GSB) command structure. This framework provides clear strategic, tactical and operational roles during an incident, enabling more effective decision making and co-ordinated responses across the organisation.

The revised BCP is aligned with our separate building incident response plans and the DIT incident response plan and associated 'playbooks', ensuring that all response procedures are fully integrated and mutually supportive. This unified approach strengthens our overall resilience, enhances clarity during critical events, and ensures consistent communication and leadership throughout any disruption.



25 Savile Row W1

Risk Committee report continued

Risk management structure

The Board

- Overall responsibility for risk management and internal control
- Sets strategic objectives and risk tolerance
- Sets delegation of authority limits for senior management
- Ensures that a healthy purposeful culture has been embedded throughout the organisation (with input from the Executive Directors)
- Agrees the Group's strategy to managing climate change resilience, approving and monitoring progress against our Net Zero Carbon Pathway (with input from the Responsible Business Committee)

Risk Committee

- Reviews the Board's risk registers and determines the nature and extent of the principal and emerging risks facing the Group
- Manages the internal audit process jointly with the Audit Committee
- Works alongside the Board to set risk tolerance levels
- Receives updates on key risk areas and monitors the Group's risk indicators and non-financial controls

Nominations Committee

- Ensures the Board (and its committees) have the correct balance of skills, knowledge and experience
- Ensures that adequate succession plans are in place for the Board, Executive Directors and the wider talent pipeline

Audit Committee

- Reviews the assurance received for the information published in our financial statements and key announcements
- Manages the external audit process and reviews internal audit findings jointly with the Risk Committee
- Monitors the internal financial control arrangements, and satisfies itself that they are functioning effectively, and that corrective action is being taken where necessary

Responsible Business Committee

- Oversees the Group's policies in respect of modern slavery, the protection of human rights, achieving our Net Zero Carbon Pathway, and employee satisfaction and wellbeing etc.
- Monitors the Group's corporate responsibility, sustainability and stakeholder engagement activities
- Monitors the Group's diversity and inclusion initiatives

Remuneration Committee

- Ensures that remuneration and reward arrangements promote long-term sustainable performance and retention of key talent
- Monitors the incentive framework to ensure it does not encourage Executive Directors to operate outside the Board's risk tolerance

In addition to the Risk Committee, the Board's other principal committees manage risks relevant to their areas of responsibility.

Executive Directors, with assistance from the Executive Committee

- Ensures the design and implementation of appropriate risk management and internal control systems that identify the risks facing the Group and enable the Board to make a robust assessment of the principal risks
- Maintains the Group's risk registers
- Manages the Group's risk management procedures
- Reviews the operation and effectiveness of key controls

Heads of Department

- Provides guidance and advice to staff on risk identification and mitigation plans
- Engages with the Executive Directors and senior management to identify risks
- Allocates 'risk managers' and oversees their response
- Risk management is devolved to the appropriate level most capable of identifying and managing the risk

Anti-bribery and corruption

We are committed to the highest standards of ethical conduct and integrity in our business practices and adopt a zero-tolerance approach to bribery and corruption. The Company has assessed the nature and extent of its exposure to bribery and corrupt practices and, overall, considers our residual exposure to be low. To address the risk areas identified, and other risks that may arise from time to time, the Company has established procedures which are designed to prevent bribery and corrupt practices from occurring. An overview of our policies and procedures in this area is contained in the table below.

The greatest potential risk area for Derwent London is in respect of our long supply chains. Our zero-tolerance approach to any form of bribery or corruption is communicated to all of our suppliers, contractors and business partners. Before we enter into a new business relationship, our due diligence procedures determine if a third party has previous convictions under the Bribery Act. All contracts with suppliers or contractors prohibit the payment of bribes, or engaging in any corrupt practice, and we have the right to terminate agreements in the event a bribe is paid or other corrupt practices are undertaken.

Compliance training

The Group operates a compliance training programme which is mandatory for all employees and members of the Board. The Risk Committee oversees the programme, approves the topics to be covered and receives an update on completion rates. The programme covers a range of risk and compliance topics (including anti-bribery and corruption, diversity and inclusion, data protection, fraud and modern slavery).

At the launch of each training topic, an introductory email is sent to participants advising them why the training is important and providing links to further information (including Company policies and guidance notes). The topics covered over the past two years are:

- anti-money laundering;
- modern slavery transparency;
- tackling tax evasion;
- recognising sexual harassment in the workplace;
- fraud and market abuse;
- competition law;
- whistleblowing; and
- cyber security awareness.

The Committee was pleased with the level of engagement from employees with, on average, a c.99.6% completion rate for quarterly compliance training.

Procedures and controls to prevent bribery and corruption	
Corporate hospitality	Hospitality must be reasonable in value, appropriate to the occasion and provided openly and transparently. It must not compromise, nor appear to compromise, the Group nor the business judgement of our staff.
Business gifts	Generally, gifts should not be accepted unless valued at less than £50, are not cash or a cash equivalent (e.g. gift certificate), are appropriate to the circumstances and are not given with the intention of compromising or influencing the party to whom it is being given.
Hospitality and Gift Returns	All staff are required to complete quarterly Hospitality and Gift Returns which document all instances of third party hospitality or gifts (given or received) over that three-month period if the value is in excess of £50 for hospitality and £10 for gifts. The Hospitality and Gift Returns are subject to review by the Risk Committee.
Political donations	The Company strictly prohibits any political donations being made on its behalf.
Charitable donations	Charitable donations are handled by the Sponsorship and Donations Committee. 'Know your client' procedures are applied to charitable organisations to ensure we are dealing with a valid body acting in good faith and with charitable objectives.
Supply Chain Responsibility Standard	Our greatest potential risk area is in respect of our long supply chains. The Supply Chain Responsibility Standard contains the minimum standards we expect from major suppliers (further information is on page 168).
Payments and expenses	All payments made must be warranted, transparent and proper. All payments must be accurately recorded through the normal accounting and financial procedures without any deception or disguise as to the recipient's identity or the purpose of the payment in question. No one approves their own expense claim. All expense claims must be approved by a Director or senior manager.
Facilitation payments	Facilitation payments are bribes and are strictly prohibited.
Conflicts of interest	All conflicts of interest or potential conflicts of interest must be notified to the Company Secretary and a register of such notifications is maintained. The Corporate governance statement on page 124 explains our process for managing potential conflicts.
Training	We provide our employees with guidance notes and regular training on anti-bribery, corruption, fraud, ethical standards and the prevention of the facilitation of tax evasion.
'Speak up' procedures	A confidential hotline is available for staff and suppliers to report concerns anonymously (see page 124).
Fraud prevention	The Company strictly prohibits any type of fraud (see page 148).