

RISK COMMITTEE REPORT



Helen Gordon Chair of the Risk Committee

2025 focus areas

- Monitor emerging and market risks and how they might impact on the Group in the short to medium-term
- Ensure health and safety risks are being effectively managed across the Group
- Receive training on the Building Safety Act 2022 during 2025
- Review the Group's response to the ongoing risk posed by cyber attacks
- Ongoing monitoring of the Group's principal and emerging risks

Committee membership during 2024

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

¹ Percentages are based on the number of meetings that each member is entitled to attend for the 12 months ended 31 December 2024.

² Madeleine McDougall was appointed as a member of the Risk Committee on 1 November 2024.

Dear Shareholder,

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

The Group's risk profile remained elevated during 2024, as the sector continued to be impacted by the wider macro environment. Further information can be found in the 'Managing risks' section on pages 90 to 101.

Key activities of the Committee during 2024

A focus for the Committee this year was to gain a deeper understanding of the emerging and market risks which could impact on the Group in the future, and to ascertain how the business was preparing and/or monitoring these risk areas. In particular, the Committee received presentations on changing occupation levels and tenant demand, in addition to how the Group is managing building obsolescence. Our emerging risk register is available on page 100.

The Committee has overseen a wide range of activities within four key categories (see pages 158 and 159):

- Property and market
- Technology
- People and environment
- Compliance

The Committee invited members of the senior management team to present on risks relevant to their departments. This allowed the Committee to delve deeper into management's approach to risk and compliance with key policies.

Health and safety

Due to the importance of ensuring our people and contractors are safe, at each Committee meeting, a detailed update is provided on health and safety matters and identified key risks, both in the managed portfolio and development pipeline.

During 2024, all Executive Directors conducted leadership tours to reinforce the Board's commitment to, and visibility of, health and safety. Further information on health and safety is available on pages 52 and 53.

The Committee received a presentation on the Scottish portfolio risks including operational and project-specific risks. The Committee noted that whilst the Scottish portfolio represents only c.2% of our assets, the risks associated with the large acreage and varied uses are principally focused on health & safety, and reputation. The Committee discussed the key controls being implemented and their effectiveness.

Supply chain insolvency

The trend of rising insolvencies has continued over the last year with the most notable insolvency being ISG in September 2024. Although ISG was not engaged on any Derwent London projects, checks were carried out with our main contractors to determine if they could be impacted by the ISG insolvency. It was pleasing to note that none were affected. The Committee received updates on the risk of insolvencies and how we are seeking to monitor the financial solvency of contractors and consultants.

Cyber security

Due to the ongoing and rising risk of cyber crime, the Committee dedicated a significant portion of its November meeting to receiving a detailed update on cyber security from members of the Digital Innovation & Technology (DIT) team. The Committee was advised of our cyber posture and how we are seeking to mitigate risks.

In November, the Group achieved the government-backed Cyber Essentials Plus accreditation which provides greater assurance to stakeholders on the strength of our cyber posture. Further information on cyber security is on pages 162 and 163.

Changes to our risk registers

Change management systems has been added as a principal risk for 2025. Additionally, the Board and Risk Committee identified opportunities to consolidate and simplify the Group's principal risks and uncertainties. As a result, the number of standalone principal risks identified by the Group has reduced from 15 to 11 (see page 92). Further information can be found in the Managing risks section on pages 90 to 101.

Further engagement

The forthcoming AGM is on 16 May 2025 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

26 February 2025

Committee composition and performance

The Committee's membership for the year under review is detailed in the table on page 156. In addition to the Committee members, the Board Chairman, other Directors, senior management and the internal and/or external Auditors, are often invited to attend all or part of any meeting as and when appropriate or necessary.

In 2024, the Risk Committee met three times (2023: four meetings). The meetings in August and November included a joint session with the Audit Committee to review the outcome of internal audits (see page 150).

The 2024 evaluation of the Board, its committees and individual Directors was internally facilitated, in accordance with our three-year cycle of evaluations (see page 139). The review confirmed that the Committee continues to operate effectively, with no significant matters raised.

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

Insolvencies within the construction industry

Our construction contracts place the risk of subcontractor insolvency with the main contractor. Whilst subcontractor insolvency remains a significant risk, we work with our contractors and consultant teams to monitor it closely.

Causes of insolvency

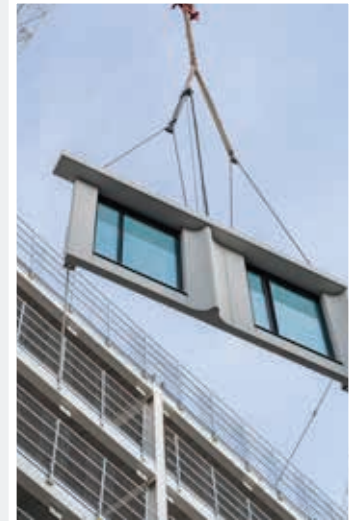
- Poor financial management
- Inflation
- Economic downturns
- Over-reliance on a single client/project
- Inadequate risk assessment
- Low margin bidding
- Over investment

Consequences

- Project delays
- Increased costs
- Legal disputes
- Reputational damage
- Supply chain disruptions

Mitigation strategies

- Financial due diligence
- Parent company guarantees or performance bonds
- Insurance
- Warranties
- Advance payments
- Contractual protections
- Monitoring and auditing
- Factory visits



Even with the above protections in place, we remain vigilant to early indicators that may indicate strain within the subcontractor supply chain. This includes maintaining good relationships in the industry to raise awareness about contractor finances, late financial returns, project team members leaving, project programmes slipping, under-resourced projects, increasing defects, subcontractors not being paid on time and inflated applications. We meet with our subcontractors to review performance and carry out visits of factory facilities to assure the quality of the outputs and that the necessary staffing levels are maintained. During 2024, Derwent London was not materially impacted by supply chain insolvencies.

s.172 factors (see page 132)



Key activities of the Committee

During 2024, the Committee has focused its attention on a variety of risks within four key categories.

Property and market

Development risks

The Committee regularly reviewed the key risks affecting our major on-site developments. In addition, the Committee received updates on the wider factors which could impact our developments, including construction cost inflation, supply chain disruption, site security and material/labour shortages (see page 96).

Planning risk

The Development team joined Committee meetings to provide updates on the progress of planning applications for all major projects.

Insolvency risk

The Committee received a presentation on the causes of contractor and consultant insolvency and its consequences. The Committee received assurances that neither Derwent London nor its supply chain had been impacted by the insolvency of ISG (see page 157).

Building Safety Act 2022

The Committee received an update on our responsibilities and how we are ensuring our compliance. It was agreed that in-depth training on the Building Safety Act 2022 would be provided to the Committee in 2025.

Building obsolescence

The Committee were advised of the steps being taken to ensure longevity of assets and discussed obsolescence risk from a physical, functional and locational viewpoint.

Fire safety

The Committee received an update on the frequency and robustness of the Group's fire risk assessments, system testing and strategies.

Strategic objectives

1 2 4

Principal risks (see page 94)

1 3 4 5

Technology

Cyber security

Our cyber security controls have been strengthened considerably in recent years in response to the increasing threat this poses to businesses, and it remains an area that the Committee keeps under continuous review (see pages 162 and 163). In November 2024, the Committee received a detailed presentation on cyber security which covered:

- our cyber posture;
- our cyber strategy;
- future trends; and
- third party dependencies.

Crisis Management Team (CMT)

The Committee received updates on technical testing that was completed in July to ensure key IT disaster recovery failover mechanisms were operating effectively.

Phishing tests

The Committee received updates on the phishing tests conducted by the Digital Innovation and Technology (DIT) team throughout the year, which sought to test the robustness of our training programme.

Security penetration tests

The Committee received summarised reports of the independent security penetration tests that were carried out in 2024.

Cyber Essentials Plus

In November, the Group achieved the government-backed Cyber Essentials Plus accreditation which provides greater assurance to stakeholders on the strength of our cyber posture.

Strategic objectives

3 4

Principal risks

6 7 11

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)

At each Committee meeting, a detailed update is provided on health and safety matters and identified key risks, both in the managed portfolio and development pipeline. During 2024, all Executive Directors conducted leadership tours to reinforce the Board’s commitment and visibility to health and safety.

H&S system and reporting

The Committee reviewed the systems utilised to monitor our health and safety compliance, reporting and management.

Asbestos management

The Committee receives updates on asbestos management at least annually. The Committee gained assurance that the risk was being adequately managed.

Lift entrapment

The Committee reviewed the number of instances of lift entrapment across the portfolio. The Committee gained an understanding of why lift entrapments occur and how we seek to rectify the issues. It was pleasing to note that there had been no injuries or harm to individuals from the lift entrapments.

Scotland solar panel procurement

The Committee reviewed the risks associated with the procurement of solar panels for our 100-acre Solar Park in Lochfaulds (see page 161).

Terrorism risk

The Committee received an update on the security provision across the portfolio to ensure our assets and occupiers are protected, with plans in place to respond to terrorism risks should they occur.

Strategic objectives

- 3**
- 4**

Principal risks

- 8**
- 9**
- 10**

Compliance

Key risk indicators

The Committee has identified, and reviews at each meeting, key risk indicators and whether they have exceeded the agreed risk tolerances.

Legal updates

The Committee received assurances from the business that we are preparing for any upcoming legal developments.

Anti-bribery and corruption

At each meeting, the Committee reviews the Hospitality & Gift Register which contains the returns prepared by all employees (including Directors) on a quarterly basis.

Litigation risk

The Committee received updates on a series of ‘mock trials’ undertaken with assistance from expert barristers, which aimed to understand how Derwent London was seeking to avoid regulatory action and how it would respond to litigation risks.

Compliance training

The Risk Committee agreed the 2025 training programme and monitored completion rates. Engagement with the training continues to be high with on average c.96% of employees completing quarterly training (see page 165).

Internal audits

Alongside the Audit Committee, the Risk Committee received updates on the work performed by internal audit. Further information on the audits conducted during 2024 is on page 150.

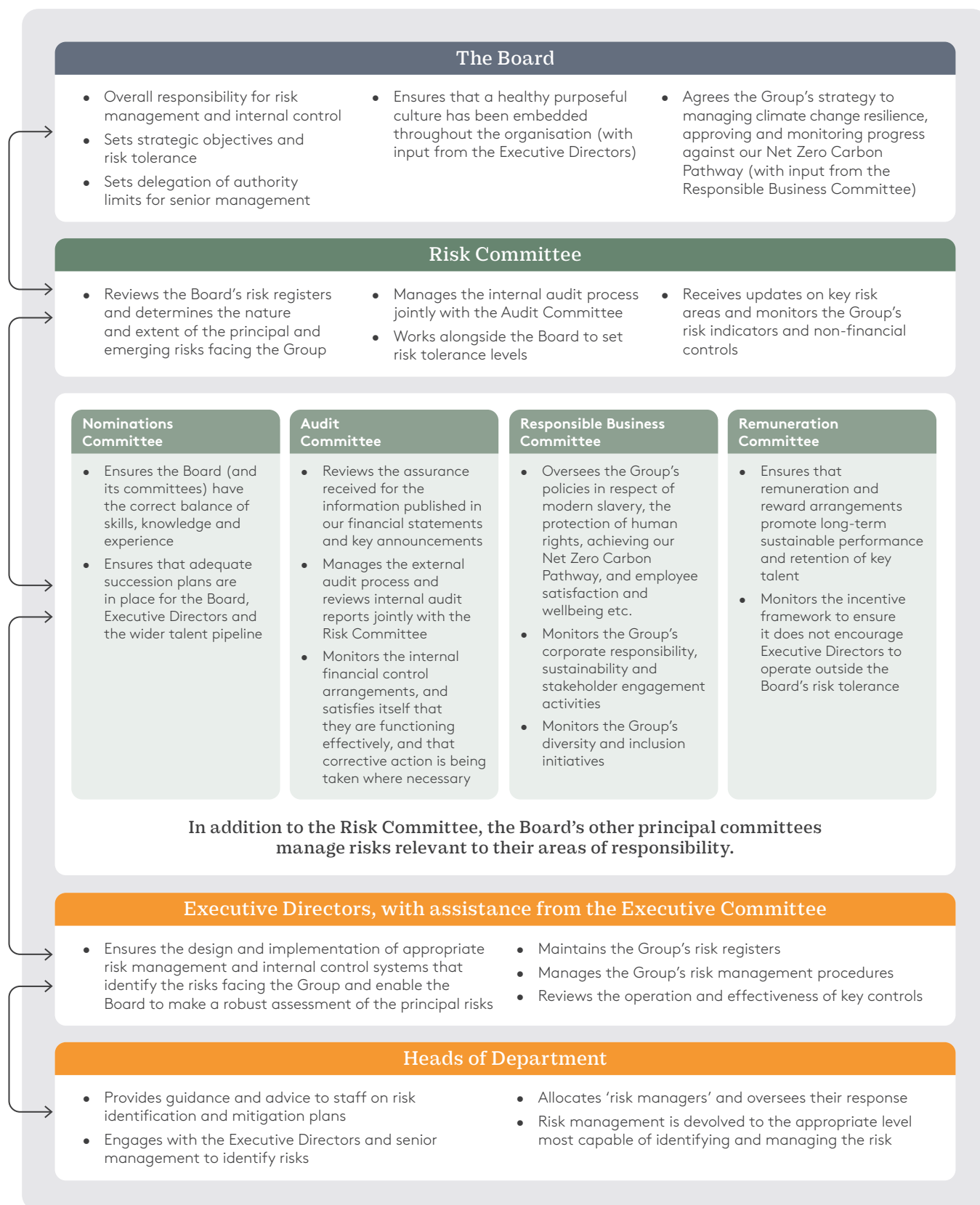
Strategic objectives

- 3**
- 4**

Principal risks

- 10**

Risk management structure



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 judge 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 94 to 99) 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 (changes made to our principal risks during 2024 are on page 92). Further information on the Group’s risk registers subject to review by the Risk Committee are detailed in the table below.



Procurement of solar panels

There are global concerns over the possible use of forced labour in the production of solar panels. At its meeting in August 2024, the Committee sought to understand the risks associated with the procurement of solar panels for our 100-acre Solar Park in Lochfalds. To aid in finding an appropriate supplier, Derwent London appointed The Greenspan Agency at the conception of the project. To aid in its understanding, the Committee reviewed background reports on the preferred supplier shortlist, a risk exposure report and research information. It was agreed that to avoid human rights abuses, all potential suppliers would be required to confirm the origins of the materials used and their manufacturing during the tender process.

s.172 factors (see page 132)

C D E

Risk documentation and monitoring

<p>Schedule of Principal Risks</p> <p>➔ See page 94</p>	<p>Contains the risks which are classified as the Group’s main risks which impact on the Group 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. During 2024, the Board and Risk Committee identified opportunities to consolidate and simplify the Group’s principal risks and uncertainties. As at 31 December 2024, the Schedule of Principal Risks contains 11 risks (2023: 15 risks).</p>
<p>Schedule of Emerging Risks</p> <p>➔ See page 100</p>	<p>Contains the internal and external emerging risks that could significantly impact the Group’s financial strength, competitive position or reputation within the next five years. Emerging risks could involve a high degree of uncertainty. As at 31 December 2024, the Schedule of Emerging Risks contains five risks (2023: five risks).</p>
<p>Group Risk Register</p>	<p>Risks not deemed to be principal to the Group are documented within the Group’s Risk Register, which is maintained by the Executive Directors, with assistance from the Executive Committee. The Board reviews and approves the Group’s Risk Register on an annual basis and it is reviewed by the Risk Committee at each of its meetings. As at 31 December 2024, the Group Risk Register contains 48 risks (2023: 47 risks).</p>
<p>Key risk indicators</p>	<p>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 93). Any deviance or significant increase is subject to challenge by the Risk Committee. The risk indicator contains 10 risk areas including cyber security, cost inflation, project status, data protection, and health and safety incidents etc.</p>
<p>Functional/departmental risk registers</p>	<p>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.</p>

RISK COMMITTEE REPORT continued

Digital security risks

Cyber and information security

We adopt a layered defence approach to cyber security which provides multiple levels of security controls to protect against cyber attacks. This eliminates single points of failure and provides multiple opportunities for threats to be identified, contained and remediated before they can cause harm.

Our cyber security controls and procedures are subject to regular independent reviews and tests, the results of which are presented to the Risk Committee, which monitors the implementation of any arising actions. The Committee reviews a dashboard of key risk indicators at each meeting which includes information security and cyber risk-related KPIs.

In H1 2024, multiple security penetration tests were conducted by a UK-based CREST accredited security consultancy and in November, our government-backed Cyber Essentials accreditation was upgraded to Cyber Essentials Plus. This provides greater assurance to stakeholders on our security posture as it involves an independent technical audit of our cyber controls and vulnerability tests performed by the certification body, IASME.

During 2024, there was a 15% increase in the total number of potential attacks when compared to 2023, none of which resulted in a security incident. 99.98% of the attempts were stopped before they reached the intended targets, with the remaining attempts immediately being reported to our Digital Innovation and Technology (DIT) team. This highlights the robustness of our cyber security posture and awareness campaigns.

As part of our compliance training programme in 2024, the DIT team highlighted the dangers of video and audio 'deep fakes' to perpetrate realistic cyber attacks by generating voice clones of our Executive Directors. With the rise of sophisticated technology available to threat actors and the enhanced effectiveness of AI in executing attacks, it is critical that our staff remain abreast of the latest threats.

- Cyber attack on our buildings/See page 97
- Cyber attack on our IT systems/See page 97



Members of the Digital Innovation & Technology team

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 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 security posture 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.

Digital strategy risks

As we increase the digitalisation of our business model through our Intelligent Building Programme, our potential exposure to digital risks will increase. 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 97.

Intelligent Building Programme

In alignment with our strategy and purpose, the Derwent London Intelligent Building Programme seeks to enable our buildings to be monitored and operated more efficiently, driving down equipment faults (and consequential maintenance) and delivering energy and operational carbon savings. During 2024, the Executive Committee continued to monitor the phased roll-out of the Intelligent Building Programme. The Committee will be kept updated on progress and its success. The key indicators of success will be the cost savings to our occupiers (due to early fault detection) and the operational carbon savings for the Group and our occupiers.

Artificial Intelligence (AI)

Technological advancements are an emerging risk for the Group. While the rapid pace of AI development offers potentially large efficiency gains throughout our business, it does introduce several risks. A group of users have been trialling Microsoft Copilot over recent months to see how it can assist their roles. It is expected that we will roll Microsoft Copilot out to the wider business in 2025, along with training. Our Acceptable Use Policy has been amended to reference AI and make clear to our users that it should be used responsibly and ethically and that users are accountable for reviewing any output generated for correctness.

→ Technological change/ See pages 100 and 101

Business continuity

In 2024, a Business Impact Analysis (BIA) was conducted to determine and evaluate the potential effects of an interruption to critical business operations.

During the analysis, we reviewed the Maximum Tolerable Outage (MTO) time for all critical business processes, the dependencies for each process in terms of people, technology and supply chains, as well as the expected process recovery times in the event of various major disruptive incident scenarios.

The output from the BIA will be used in 2025 to further develop our Business Continuity Plan (BCP) and prioritise recovery plans.

In July 2024, annual technical testing was completed to ensure key IT disaster recovery failover mechanisms were operational. Our next biennial full interruption test, including a failover of all IT systems and services to our backup data centre, will be conducted in 2025.

Disaster recovery

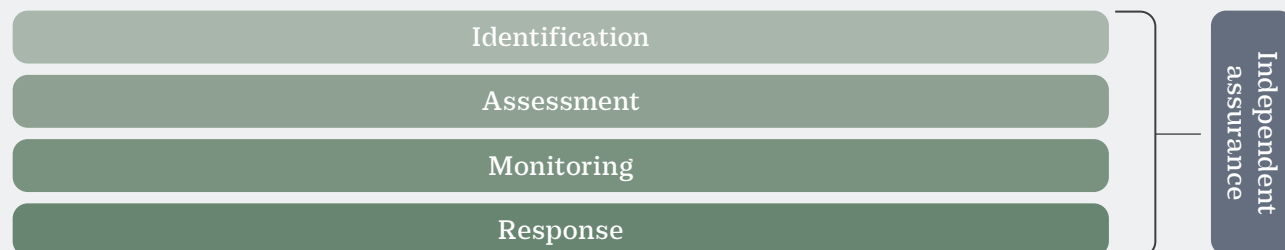
Derwent London has formal procedures for use in the event of an emergency that disrupts our normal business operations that consist of:

- **Business Continuity Plan (BCP):** 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.
- **Crisis Management Team (CMT):** 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.
- **Off-site disaster recovery data centre:** 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.
- **Testing and review:** The strength of our business continuity and disaster recovery plans are regularly tested and continually refined to reduce the potential for failure.

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 reviews, scenarios for the future are considered which assist with the identification of principal and emerging risks and how they could impact on 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 reviews.

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 the procedures. Monitoring activities include:

- the regular review and updating of the Schedule of Principal Risks, Schedule of Emerging Risks and the Group's Risk Register;
- independent third party reviews of the risk management process to provide further assurance of its effectiveness;
- 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 94 to 99. We use insurance to transfer risks which we cannot fully mitigate.

Insurance

Our comprehensive insurance programme covers all of our assets and insurable risks. We are advised by insurance brokers, who provide a report to the Risk Committee on an annual basis. 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.

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 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 practice 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, agrees 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 links to further information (including Company policies and guidance notes). The topics covered over the past two years are:

- anti-money laundering;
- prevention of tax evasion;
- modern slavery;
- competition law;
- conflicts of interest;
- anti-bribery and corruption; and
- cyber fraud awareness.

The Committee was pleased with the level of engagement from employees with, on average, c.96% of all employees completing each training module.

Policy and procedures 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 Sponsorships 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.
Contractors and suppliers	Our greatest potential risk area is in respect of our long supply chains, as detailed above.
Supply Chain Responsibility Standard	Contains the minimum standards we expect from major suppliers (further information is on page 171).
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 128 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 helpline is available for staff to report concerns anonymously (see page 128).