RISK COMMITTEE REPORT CONTINUED

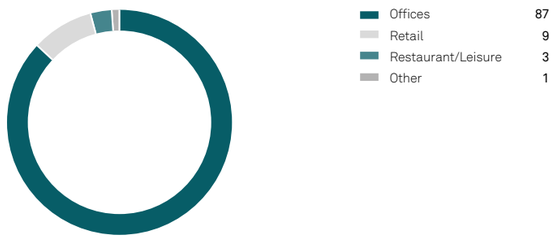
Tenant covenant review

Due to the uncertain economic environment, with a number of large retail businesses going into administration, the Committee conducted a review of how Derwent London assesses and monitors the financial strength of potential and existing tenants. The chart below illustrates that Derwent London has limited exposure to retail or restaurants within our portfolio.

At its meeting in November, the Committee received a detailed overview from the Head of Asset & Property Management and the Group Financial Controller on the workings of the credit committee and how it decides whether potential and existing tenants are financially sound to transact. The Committee was satisfied with the extensive due diligence process undertaken by the credit committee.

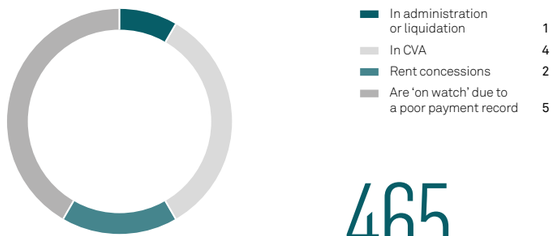
Portfolio income

Percentage



Analysis of the 'tenants at risk' register

Tenants



465

Tenants of which only 12 are on the 'at risk' register

Failure to prevent the facilitation of tax evasion

The Company will not tolerate any facilitation of tax evasion by staff, subcontractors or any other of its associates. To address these risks, the Company has established procedures which are designed to prevent its associated persons from deliberately and fraudulently facilitating tax evasion.

All staff have attended compulsory training sessions on our policies and procedures. The training was hosted by our Head of Tax, David Westgate, and included practical examples of how facilitation of fraudulent tax evasion could occur and guidance on how these should be addressed.

General Data Protection Regulations (GDPR)

The GDPR, which came into force on 25 May 2018, require a tougher approach to the handling and using of personal data. Derwent London holds relatively limited personal data, relating mainly to human resources, CCTV and private residential lettings.

The Company's project plan for GDPR commenced well in advance of 25 May 2018 with the establishment of a GDPR Steering Group which met weekly, dedicated Data Protection Champions from each department and compulsory training for all staff. The project to ensure our compliance continued throughout 2018 and included:

GDPR Steering Group	The GDPR Steering Group initially met weekly (for 18 weeks) and now meets fortnightly.
Guidance and training	Ongoing training and support to staff, including compulsory induction training. The creation of a dedicated GDPR intranet page. Short internal video explaining the employee privacy notice.
Contract remediation	Conducted risk assessments of all contracts followed by thorough contract remediation for those processing personal data.
Policies, documentation and procedures	All policies, procedures, guidance notes, contracts of employment, offer letters and consultancy agreements have been updated to be GDPR compliant. New procedures created for subject access requests and Data Protection Impact Assessments (DPIAs). The removal of historical data from our shared drives (soft copies) and the destruction of printed documents (hard copies) is an ongoing exercise.

Since 25 May 2018, all new projects or changes to processes involving data processing are subject to DPIA screening assessments to determine the level of risk. A total of 19 DPIAs have been completed during the year.

The Committee and Board have been routinely updated on the project's progress and, to date, are satisfied that management have undertaken all necessary steps to ensure the Group's ongoing compliance with GDPR. A gap analysis will be performed in 2019 to review our progress and identify areas for further improvement.

CCTV

Our CCTV system is intended to provide an increased level of security for the benefit of those who work in or visit Derwent London properties by acting as a deterrent against crime and protecting our buildings and assets from damage, disruption and vandalism. CCTV images are not released unless satisfactory evidence has been obtained by us that the third party requesting the personal data has a legal and justifiable need.

Since May 2018, we have received 14 access requests for CCTV footage. Requests are authorised in accordance with our CCTV policy and CCTV disclosure procedures. Prior to disclosing CCTV images, we redact any third-party personal data and images (for example, by blurring the images) before saving the images to disc and placing them in a sealed evidence bag.

Privacy notice

Derwent London respects privacy and is committed to protecting personal data. Our privacy notice, which sets out how we use personal data, is available on our website here: www.derwentlondon.com/texts/privacy-policy

We also have tailored privacy notices for employees, recruitment candidates and tenants, which are available upon request from the Company Secretary.

Business continuity and disaster recovery

Information and cyber security

To safeguard the security and privacy of information entrusted to us, we have robust procedures in place. The procedures ensure that we:

- safeguard the security and 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.

Our cyber security procedures have been strengthened considerably in recent years in response to the increasing threat this poses to businesses, and it remains an area that we keep under continuous review.

During 2018, we requested that Capgemini conduct a benchmarking review of our cyber security procedures. In November, the Committee reviewed the outcome of the audit and were pleased that Capgemini had noted the improvements made since the prior audit. The Committee agreed the responses and timeframes for implementing the audit recommendations. Management will be required to provide the Committee with a status update on the implementation of the recommendations at the Committee's August 2019 meeting.

The Committee reviews a dashboard of key risk indicators at each meeting which includes information security and cyber-risk-related KPIs. During 2018, there were 474 attempted attacks on our systems, none of which resulted in a security breach and 99.9% of the attempts were stopped before they reached the intended targets – this highlights the robustness of our cyber security posture. Our IT team tested the effectiveness of our ongoing security awareness programme by sending fake phishing emails to staff and monitoring their response. Any staff member who clicked on the links contained in the test emails was provided with further training on the dangers.

All staff attend mandatory information security workshops each year which focus on our policies and procedures, cyber and personal security. Our Group intranet also includes a 'tips and tricks' section for our staff with guidance on issues such as cyber security, social media and general security awareness.

Disaster recovery procedures

Derwent London has formal procedures for use in the event of an emergency that disrupts our normal business operations which 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 the business. The BCP empowers the CMT to make strategic and effective decisions to support the recovery of the business until we are able to return to normal working.
- **Off-site disaster recovery suite:** An off-site disaster recovery suite is available in the event of an emergency, to provide IT and data facilities to our staff who either work on site at the suite or via our 'agile' working capabilities.
- **Testing and review:** The strength of our business continuity and disaster recovery plans are regularly tested to ensure they are continually refined and to reduce the potential for failure. An overview of the disaster recovery tests due to take place during 2019 are provided in the adjacent table.

FULL BUSINESS CONTINUITY TEST

At 5pm on Friday 21 September, our disaster recovery procedures were tested by staging a complete loss of power at our head office building at 25 Savile Row. The test required the evacuation of the building and the transfer of key systems and personnel to our disaster recovery suite.

The migration was overseen by independent verifiers, IT Governance Limited, who assessed our procedures and efficiency.

The Committee was pleased to note that the test was successful and well managed with no major issues identified and no downtime reported. A number of minor suggestions were raised by IT Governance Limited to further strengthen our robust Business Continuity Plan (BCP) which included:

- using the disaster recovery tests as an exercise to raise the awareness, competence and capability of the CMT;
- appoint an individual responsible for noting all actions taken and logging time-delayed actions; and
- monitor the UPS load as systems migrate to the disaster recovery suite.

The entire process from the loss of primary power, transfer to our disaster recovery suite and roll back to Savile Row took 6 hours and 45 minutes (a 3 hour and 20-minute improvement on our last full test completed in October 2016).

Business continuity tests planned for 2019/2020

Test	Purpose	Date
Business Continuity Plan review	The CMT meet to review and update the business continuity plan, review current threat levels and agree on any action points.	Q1 2019
IT Component test	A technical test of the individual components required to carry out a failover of IT services to our disaster recovery suite.	Q1 2019
Desktop review	A desktop exercise which uses a series of scenarios to rehearse decision making and familiarise the CMT members with their roles.	Q2 2019
IT disaster recovery test	A technical test to carry out a full IT systems failover from our offices to the disaster recovery suite.	Q3 2019
Full business continuity test	A full plan invocation exercise covering one disaster scenario and testing all contingency functions at the disaster recovering suite. Representatives from each department will confirm all business-critical functions are still available.	Q4 2020