AAF 01/06 / ISAE 3402 Assurance report on internal controls for the period 1 January 2019 to 31 December 2019

Legal & General Investment Management (Holdings) Limited
Pooled Funds
One Coleman Street
London EC2R 5AA

Legal & General
INVESTMENT MANAGEMENT

Contents

The report on Legal & General Investment Management's description of its investment management services and on the suitability of the design and operating effectiveness of its controls is confidential. The report is intended solely for use by the management of LGIM(H), its user entities, and the independent auditors of its user entities.

If you are receiving this report on Legal & General Investment Management's description of its investment management services and the suitability of design and operating effectiveness of its controls, in your capacity as an institutional client or customer or a prospective or new customer (i.e., after December 31, 2019) of LGIM(H) then your attention is drawn to the disclaimer letter in Appendix 1 of this document, which outlines the basis on which you have received this report on Legal & General Investment Management's description of its investment management services, suitability of design and operating effectiveness of controls and the report of independent service auditors therein.

1. Introduction

As the directors of Legal & General Investment Management (Holdings) Limited (LGIM(H)) we are committed to maintaining a strong control environment throughout the organisation. We consider this to be a key objective, as effective control of business risk is a vital component of the quality service we continually strive to deliver to all of our clients.

We remain committed to managing the many regulatory changes currently impacting our industry and have continued to invest in our systems, infrastructure and people in order to ensure these are managed in a controlled manner.

This report describes the control environment and control objectives with regard to the management and administration of our pooled investment funds, and sets out the control procedures established to meet those objectives.

The intention of this report is to allow our clients and their auditors to understand the means by which we conduct our business and how we control and manage risks in the provision of investment management services. This report is based upon the framework set out in the technical releases International Standards for Assurance Engagements (ISAE) 3402 issued by the International Auditing and Assurance Standards Board (IAASB) and the Audit and Assurance Faculty (AAF) 01/06 on assurance reports on the internal controls of service organisations made available to third parties, issued by the Institute of Chartered Accountants in England and Wales (ICAEW)..

Return to top

2a. Statement by the directors of Legal & General Investment Management (Holdings) Limited (LGIM(H))

As directors we are responsible for the identification of control objectives relating to customers' assets and related transactions in the provision of investment management services and the design, implementation and operation of the control procedures of LGIM(H) to provide reasonable assurance that the control objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of customers but also to those of the owners of the business and the general effectiveness and efficiency of the relevant operations.

We have evaluated the effectiveness of LGIM(H)'s control procedures having regard to the Institute of Chartered Accountants in England and Wales Technical Release AAF 01/06 and the criteria for investment management set out therein.

We set out in this report a description of the relevant control procedures together with the related control objectives which operated during the period 1 January 2019 to 31 December 2019 and confirm that:

- The report describes fairly the control procedures that relate to the control objectives referred to above which were in place;
- The control procedures described are suitably designed such that there is reasonable assurance that the specified control objectives would be achieved if the described control procedures were complied with satisfactorily; and
- The control procedures described were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the specified period.

Richard Lee

Director

Date 20 February 2020

Signed on behalf of the Board of Directors

Return to top

2b. Statement by the directors of Legal & General Investment Management America Inc. (LGIMA)

As directors we are responsible for the identification of relevant control objectives relating to the provision of investment management services to Legal & General Investment Management (Holdings) Limited (LGIM(H)) and the design, implementation and operation of the respective control procedures of Legal & General Investment Management America Incorporated (LGIMA) to provide reasonable assurance that the relevant control objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of LGIM(H) but also to those of the owners of the business and the general effectiveness and efficiency of the relevant operations.

The following relevant control procedures supporting the related control objectives of LGIM(H) are performed by LGIMA:

- **2.2 Investment transactions are properly authorised, executed and allocated in a timely and accurate manner**

  Controls performed by LGIMA are 2.2.1, 2.2.7 and 2.2.8

We have evaluated the effectiveness of the relevant control procedures having regard to the Institute of Chartered Accountants in England and Wales Technical Release AAF 01/06 and the criteria for investment management set out therein.

We set out in this report a description of the relevant control procedures together with the related control objectives which operated during the period 1 January 2019 to 31 December 2019 and confirm that:

- The report describes fairly the control procedures that relate to the control objectives referred to above which were in place;
- The control procedures described are suitably designed such that there is reasonable assurance that the specified control objectives would be achieved if the described control procedures were complied with satisfactorily; and
- The control procedures described were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives were achieved during the specified period.

Director

Date 20 February 2020

Signed on behalf of the Board of Directors

Return to top

3. Service auditor's report on the internal controls of Legal & General Investment Management (Holdings) Limited

KPMG LLP
15 Canada Square
London E14 5GL
United Kingdom
KPMG LLP

Tel +44 (0) 20 7311 1000
Fax +44 (0) 20 7311 3311
zahra.kassam@kpmg.co.uk

Private & confidential
Legal & General Investment Management (Holdings) Limited
One Coleman Street
London,
EC2R 5AA

20 February 2020

Dear Directors,

AAF01/06 and ISAE 3402 Type II Reporting Accountant's Assurance Report

In accordance with our engagement letter dated 20 February 2020 (our "Engagement Letter"), we have examined the accompanying description at pages 21-61 of the controls in place at the service organisation called Legal & General Investment Management (Holdings) Limited

("LGIM(H)" or Client) and carried out procedures to enable us to form an independent opinion on whether the Client's management has fairly described the investment management services throughout the specified period 1 January 2019 to 31 December 2019 (the "Description"), and on the design and operation of controls related to the control objectives stated in the Description. Our opinion is set out below and should be read and considered in conjunction with this report in full.

Use of report

This report is made solely for the use of the directors, as a body, of LGIM(H), and solely for the purpose of reporting on the internal controls of LGIM(H), in accordance with the terms of our engagement letter dated 20 February 2020.

Our work has been undertaken so that we might report to the directors those matters that we have agreed to state to them in this report and for no other purpose. Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission.

We permit the disclosure of this report, in full only, by the directors at their discretion to customers of LGIM(H) using LGIM(H)'s investment management ('customers'), and to the auditors of such customers, to enable customers and their auditors to verify that a report by reporting accountants has been commissioned by the directors of LGIM(H) and issued in connection with the internal controls of LGIM(H), and without assuming or accepting any responsibility or liability to customers or their auditors on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the directors as a body and LGIM(H) for our work, for this report or for the conclusions we have formed.

Return to top

Service organisation's responsibilities

LGIM(H) is responsible for: preparing the Description and the accompanying statement set out on page 4, including the completeness, accuracy, and method of presentation of the Description and the statement; providing the services covered by the Description; specifying the criteria including the control objectives and stating them in the Description; identifying the risks that threaten the achievement of the control objectives; and designed and operating effectively to achieve the related control objectives stated in the Description.

The control objectives stated in the Description include the internal control objectives developed for service organisations as set out in the Institute of Chartered Accountants in England and Wales Technical Release AAF 01/06 "*Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties*" ["ICAEW Technical Release AAF 01/06"].

Reporting accountants' responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in that Description.

Framework applied

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised) (ISAE 3000) "*Assurance Engagements Other than Audits or Reviews of Historical Financial Information*" and ICAEW Technical Release AAF 01/06 and having regard to International Standard on Assurance Engagements 3402 (ISAE 3402) "*Assurance Reports on Controls at a Service Organization*". Those standards require that we obtain sufficient, appropriate evidence on which to base our conclusion.

Our Independence and Quality Control

We comply with the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants and we apply International Standard on Quality Control (UK and Ireland) 1 "*Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services Engagements"*. Accordingly, we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements and professional standards (including independence, and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour) as well as applicable legal and regulatory requirements.

Scope of work

Our work involved planning and performing procedures to obtain evidence about the presentation of the Description of the Overall Control Environment and the design and operation of those controls. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organisation.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent limitations

LGIM(H)'s Description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the investment management activities that each individual customer may consider important in its own particular environment Also, because of their nature, controls at a service organisation may not prevent or detect and correct all errors or omissions in processing or reporting transactions.

Return to top

Our opinion is based on historical information and the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls would be inappropriate.

The relative effectiveness and significance of specific controls at LGIM(H), and their effect on assessments of control risk at customers' organisations are dependent on their interaction with the controls and other factors present at individual customer organisations. We have performed no procedures to evaluate the effectiveness of controls at individual customer organisations.

Opinion

In our opinion, in all material respects, based on the criteria including specified control objectives described in the directors' statement on page 4:

(a) the Description on pages 9 to 20 fairly presents the investment management activities or system that were designed and implemented throughout the period from 1 January 2019 to 31 December 2019;

(b) the controls related to the control objectives stated in the Description on pages 21 to 23 were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2019 to 31 December 2019; and

(c) the controls that we tested were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives stated in the Description were achieved throughout the period 1 January 2019 to 31 December 2019.

Description of test of controls

The specific controls tested and the nature, timing and results of those tests are listed on pages 24-61.

Sub-service organisations

LGIM(H) uses select trading services of Legal & General Investment Management Inc. (LGIMA). LGIM(H)'s management description includes the relevant LGIMA control system that was designed and implemented throughout the specified period and the aspects of the controls that may be relevant to a user organisation's internal control, as it relates to an audit of financial statements. The control objectives were specified by the management of LGIM(H).

The services performed by subservice organisations, other than LGIMA, are outlined on pages 9-10. LGIM(H) has applied the carve-out method to these subservice organisations. Therefore, the Description excludes the control objectives and related controls at the subservice organisations. Accordingly, our procedures do not extend to controls at the subservice organisations.

Yours faithfully

KPMG LLP

KPMG LLP
Chartered Accountants

Return to top

4. Control environment

4.1 Background

ISAE 3402 was established by the IAASB to provide a global framework for service auditors to provide a report for use by user entities and their auditors on the controls at a service organisation. AAF 01/06 refers to the Technical Release AAF 01/06 “Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties” issued by the ICAEW.

We have used the control objectives for investment management and information technology established by the Audit and Assurance Faculty (AAF) in AAF 01/06.

Processes and controls designed to meet the control objectives are identified and documented by us, the service organisation.

Our service auditors, KPMG LLP, carried out a detailed review of the control environment to consider the fairness of presentation, design suitability and operating effectiveness of the controls during the year.

4.1.1 Scope

This report only covers the controls, policies and procedures in relation to the unitised funds in the following areas of operation:

- Accepting clients
- Authorising and processing transactions
- Maintaining financial and other records
- Cash management and safeguarding assets
- Monitoring compliance
- Reporting to clients
- Restricting access to systems and data
- Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats
- Maintaining and developing systems hardware and software
- Recovering from processing interruptions
- Monitoring IT compliance

This ISAE 3402/AAF 01/06 Type II report has been performed using the “Carve-Out Method”. Under this method, the processes and controls carried out by third party service providers to LGIM(H) and its subsidiary companies have been excluded from the scope of the report. As a result, the controls carried out by third party service providers are not subject to independent testing by KPMG as part of the ISAE 3402 / AAF 01/06 examination of LGIM(H). However, LGIMA prepare their own report and for a limited number of key controls relevant for UK clients they are included within this report. The functions and nature of the processing performed by the third party service providers have been described at a high level so that the users of this report may understand the significance of the functions performed. In addition, the monitoring controls carried out by LGIM(H) have been included the report and have been independently tested by KPMG.

Return to top

The pooled funds have delegated the day-to-day investment management to Legal & General Investment Management Limited (LGIML), except where specific other third parties are described. The portfolios of securities and cash underlying each fund are held by independent corporate custodians. Management of the US fixed income portfolio is sub-delegated to Legal & General Investment Management America Incorporated (LGIMA). Management of the property fund is delegated to Legal & General Property Limited (LGP). Both LGIMA and LGP issue separate reports on internal controls for their respective operations. A separate report is also issued for clients who invest in segregated vehicles.

LGIML has outsourced some of its investment operations functions for some fund ranges. The outsourced activities are detailed below within the fund descriptions. High level oversight arrangements for their relationships are detailed within this report.

The pooled funds are described below:

Legal and General Assurance (Pensions Management) Limited (PMC)

In PMC funds, clients enter into a contract of insurance with PMC, the value of which is linked to the value of PMC unitised funds. PMC is a separate legal entity within the Legal & General Group. As a result of corporate structuring and the operation of company law, the assets contained in these companies are ring-fenced from the rest of the Legal & General Group. Custodian services are provided by HSBC Securities Services and Citibank, N.A.

UK Open Ended Investment Company (OEIC)

The UK OEIC has two sub-funds – the LGIM Euro Corporate Bond Fund and the LGIM Global Corporate Bond Fund. Legal & General (Unit Trust Managers) Limited is the Authorised Corporate Director for these pooled funds and LGIM Ltd is the investment manager and valuation and pricing agent. Northern Trust Global Services Limited is the transfer agent and custodian. The management company is Legal & General (Unit Trust Managers) Limited having moved from the LGIM Corporate Director Limited (CDL) in July 2019.

Legal & General Authorised Contractual Scheme (ACS)

The ACS is a UCITS compliant co-ownership scheme constituted in the United Kingdom. The investment manager and distributor is LGIM Ltd and the management company is Legal & General (Unit Trust Managers) Limited having moved from the LGIM Corporate Director Limited (CDL) in July 2019.

LGIM Liquidity Funds plc

This is a self-managed, Irish domiciled OEIC which invests in high quality, short term fixed income and money market securities. It has four sub funds – the Sterling, Euro and US Dollar Liquidity Funds and Sterling Liquidity Plus Fund. LGIM Ltd is the investment manager and the management company is LGIM Managers (Europe) Limited (LGIM Europe). Northern Trust International Fund Administration Services (Ireland) Limited is the administrator and Northern Trust Fiduciary Services (Ireland) Limited is the custodian.

Legal & General SICAV Funds

This is a Luxembourg based range of funds. The investment manager is LGIM Ltd and the management company is LGIM Europe. Northern Trust Global Services Limited, Luxembourg Branch is the administrator, depositary and paying agent.

Legal & General ICAV

This is an open-ended umbrella-type Irish Collective Asset-management Vehicle with limited liability. LGIM Ltd is the investment manager and distributor. Northern Trust International Fund Administration Services (Ireland) Limited is the administrator and Northern Trust Fiduciary Services (Ireland) Limited the custodian. The management company is LGIM Europe.

Return to top

Qualifying Investor Alternative Investment Fund (QIAIF)

This is a specialist fund range targeted at sophisticated and institutional investors. LGIM Europe is the management company and LGIM Ltd is the investment manager.

The pooled funds have delegated the day-to-day investment management to LGIM Ltd, except where specific other third parties are described. The portfolios of securities and cash underlying each unitised fund are held by independent corporate custodians. Custodians in the context of this report refer to HSBC Global Investor Services, Citibank N.A and Northern Trust.

Return to top

4.1.2 Corporate structure

Figure 1: Group Structure showing key subsidiaries of Legal & General Investment Management (Holdings) Limited

KEY

- In scope entity
- Out of scope entity

Return to top

LGIM(H) is a wholly owned subsidiary of Legal & General Group PLC. Where appropriate, individual companies within the group structure are regulated financial services firms. In the UK, they are regulated by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA), or, in the case of PMC, both. The Legal & General (L&G) Irish companies are regulated by the Central Bank of Ireland and in the USA, LGIM America and Global Index Advisors are regulated by the Securities Exchange Commission.

Regulators require, among other things, individual approval of key managers and staff and undertakings that they will abide by regulatory rules. They hold regular liaison meetings with us as part of their "close and continuous" supervisory relationship with regulated entities within the LGIM(H) group, at which business developments and any issues arising are discussed.

Legal & General (Unit Trust Managers) Limited, LGIM ETF Managers Limited, LGIM Real Assets Limited (LGRA), Legal & General Property Limited, LGIM Real Assets (Operator) Limited, LGIM Commercial Lending Limited, LGIM Asia Limited, LGIM Japan KK, Legal & General Investment Management United States (Holdings) Inc., Legal & General Investment Management America Inc. (LGIMA) and Global Index Advisors are out of scope for this report. However, LGIMA prepare their own report and for a limited number of key controls relevant for UK clients they are included within this report. Legal & General Property also prepare their own report for certain funds.

The company maintains a well-defined and appropriate apportionment of significant responsibilities among its directors and senior managers in such a way that it is clear who has which of those responsibilities and the business of the company can be adequately monitored and controlled.

4.2 Overall control environment

The directors of LGIM(H) are committed to a strong control environment. This commitment is reinforced through individual ownership of significant risk areas by the directors. This strong control environment is achieved through:

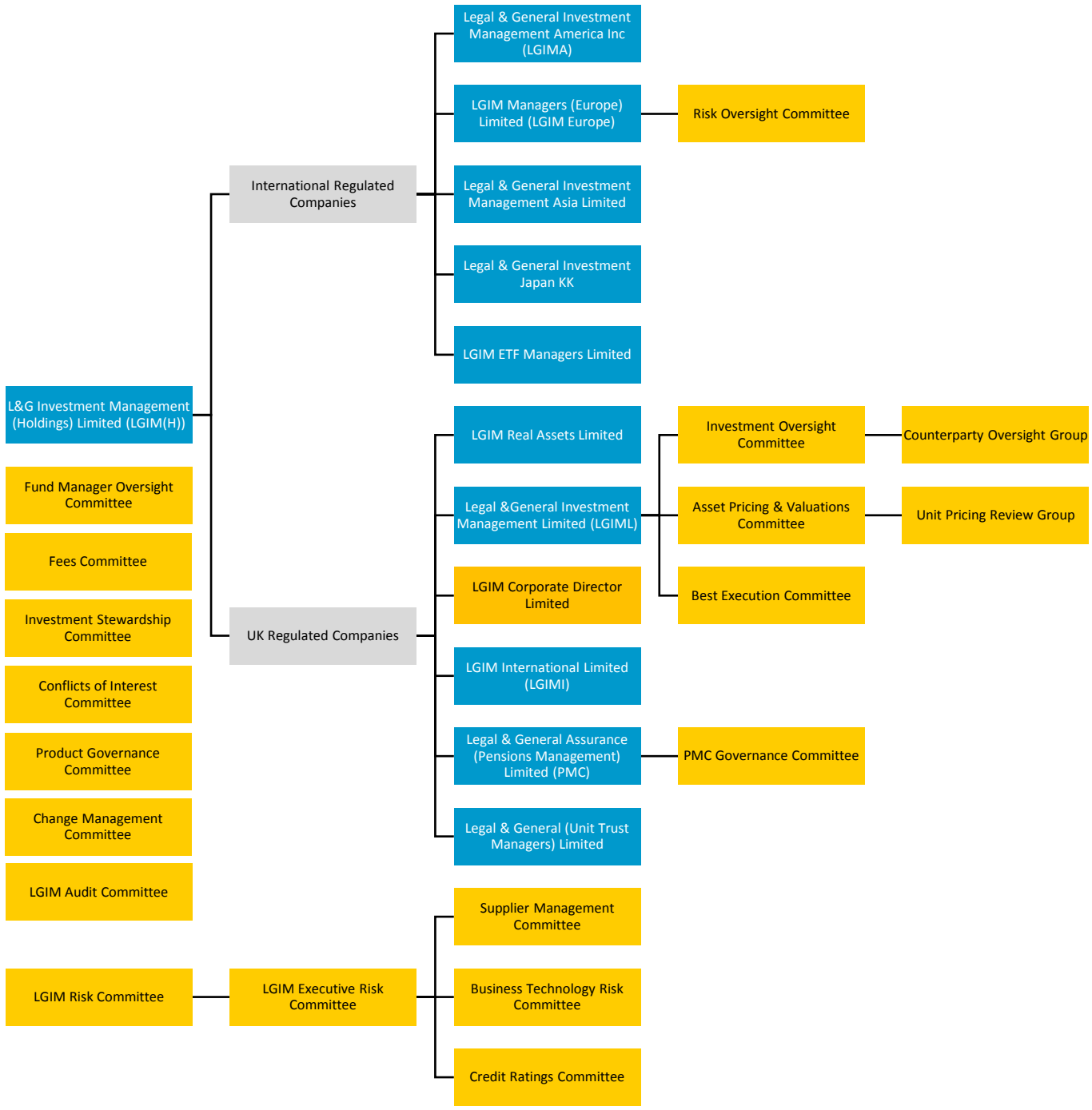
4.2.1 Management control

- A formal board structure (see Figure 2) and a schedule of specified matters which require review and approval by relevant board directors
- A formal control/risk self-assessment process consistent with the requirements of the FCA Systems and Controls rules, undertaken by management at regular intervals, including assessment of forward-looking and strategic risks, review of control processes and reporting on the effectiveness of the control environment
- A central database containing information on: risk assessments and key processes to manage those risks; the identification, escalation and monitoring of actions to resolve control issues or operational losses; and the recording and monitoring of actions to implement recommendations to address any control weaknesses identified during audits or compliance reviews
- Regular reporting on the effectiveness of key processes and controls that manage risk throughout the organisation
- Clear definition of management and staff responsibilities and reporting lines, including appropriate segregation of duties between investment, dealing and settlement activities

Return to top

Figure 2: Structure of Principal Regulated Company Boards and Formal Committees

KEY
- Legal Entity
- Legal Entity Governance Committee



Return to top

4.2.2 Risk management framework & policy

Overall responsibility for the management of risk is vested in the LGIM(H) board. To support it in this role, a risk framework is in place comprising individual company boards and formal committees responsible for overseeing risk review functions, risk management policies and risk assessment processes. These are underpinned by defined risk principles describing the behaviours, practices and culture to support effective risk governance. The framework provides assurance that risks are being appropriately identified, assessed and managed.

In order to design, implement and maintain suitable internal controls the directors of the company identify the key risks which could prevent the business from achieving its objectives. This includes all areas where failure could lead to major loss or impact on reputation. The directors review and assess risks in terms of impact and likelihood of crystallisation. This allows the directors to consider the relative importance of each risk and the degree of priority to be attached to the establishment of internal control objectives. The directors receive regular reports on the achievement of internal control objectives and review of these reports provides the basis for their assessment of the effectiveness of risk management measures.

The primary responsibilities of the principal formal committees shown in Figure 2 are:

- **LGIM Risk Committee (LRC)** – This committee's primary role is to provide guidance to the LGIM(H) board with regard to the LGIM(H) Group's risk appetite, to provide advice on what constitutes acceptable risk taking and to provide oversight of the LGIM(H) Group's risk management policies and procedures.
- **Executive Risk Committee (ERC)** – The ERC exercises the responsibility of the LRC and the LGIM(H) Board for ensuring the management of risk and regulatory compliance throughout the LGIM(H) Group. Its primary role is to ensure that the critical risks and regulatory obligations within the LGIM(H) Group are identified, assessed and managed by appropriate control processes, ensuring that responsibility and accountability for risk and compliance management rests with the appropriate senior management.
- **Investment Oversight Committee (IOC)** – This committee's role is to ensure that the critical investment risks inherent in the business are identified, assessed and managed by the appropriate processes. The Committee will issue and maintain appropriate risk policies, including an expression of acceptable levels of risk appetite and exposure. The committee does not itself actively manage any specific risks.
- **Counterparty Oversight Group (COG)** – This is a sub-committee of the IOC. Its role is to determine, monitor and review LGIM(H)'s policies on the management of client exposure to counterparty credit risk, and to set, monitor and review the counterparty approval process and policies.
- **Asset Pricing and Valuation Committee (APVC)** – The role of this committee is to oversee and approve valuation and pricing policies and methodologies across all asset classes (including but not limited to securities, derivatives, property and private equity). The committee will also act as the final arbiter of any disagreements that arise within LGIM(H) on valuation and pricing matters. The committee has a responsibility for ensuring that there are appropriate procedures in place to resolve significant valuation and pricing issues as and when they arise.
- **Unit Pricing Review Group (UPRG)** – This is a sub-committee of the APVC. Its role is to advise the APVC in respect of relevant unit pricing policies and processes, for fund ranges for which LGIML is the investment manager and/or administrator.
- **PMC Governance Committee** – This is a sub-committee of the PMC board. The sub-committee's role is to review papers on behalf of the board on matters including but not limited to financial results, capital assessments, and the operation of PMC's business. Where the papers seek approval for a material change to PMC's business the papers will be presented subsequently to the board for approval. Where the papers do not present a material change the sub-committee can approve on behalf of the board.

Return to top

- **Business Technology Risk Committee** – This committee's role is to act as a controlling influence over the development and operation of business continuity management within LGIM(H). The committee will ensure that appropriate plans, technology and facilities are available and suitably tested, enabling the timely and safe recovery of critical business activities, following a crisis or major operational disruption. It also ensures that appropriate policies and procedures are in place and operated in LGIM in relation to information security.
- **Investment Stewardship Committee** – This committee is chaired by an LGIM non-executive director and provides oversight in relation to any potential conflicts of interest and contentious corporate governance issues.
- **Risk Oversight Committee** – This committee is chaired by the Chief Risk Officer of LGIM Europe and serves to exercise the LGIM Europe board's responsibility for overseeing the management of risk and regulatory compliance throughout LGIM Europe.
- **Supplier Management Committee** – This committee's primary objective is to oversee the management of supplier risk and to set the framework for its management within LGIM(H). It is responsible for ensuring outsourced and essential suppliers, as defined within the Group Outsourcer & Essential Supplier Services Policy and the Group Insourcing Policy, are being managed and overseen appropriately.
- **Best Execution Committee** – This committee exercises the responsibility of the LGIM(H) and LGIMI boards for demonstrating effective oversight and governance of best execution. Its primary role is to oversee the effectiveness of the Best Execution Policy and ensure that delivery of best execution is achieved, managed and monitored in line with client and regulatory obligations.
- **Product Governance Committee** – This committee has two purposes: product development and product governance. Product development involves overseeing the design, development and design of new products and new instruments, and managing new mandates and distribution arrangements. Product governance is about making sure that pooled fund products are appropriate, and that information provided to distributors is fit for purpose.
- **Fund Manager Oversight Committee** – This committee is responsible for ensuring that the investment management activities and associated services performed by LGIML, its delegates and other fund managers are conducted in accordance with all applicable regulations, the terms of the relevant governing IMA and the policies and procedures of LGIM(H).
- **Credit Ratings Committee** – The role of the Credit Ratings Committee is to independently maintain LGIM(H)'s rating methodology/approach and to assign ratings in accordance with this approach.
- **Conflicts of Interest Committee** – The committee's purpose is to provide independent oversight of LGIM(H) firms' identification, management and disclosure of conflicts of interest and potential conflicts of interest.
- **Fees Committee** – The committee's principal purpose is to monitor, review and approve all fee rate changes on behalf of LGIM(H) and its subsidiary undertakings. Under delegated authority from the board of each subsidiary undertaking, it will sign off all fee rate changes for existing business and set new and appropriate fee rates for new activities.
- **LGIM Audit Committee** - This committee has oversight of the LGIMH Group as a whole reporting on issues and conclusions on adequacy and effectiveness of the LGIM(H) Groups system of Internal Controls, as well as discharging duties around, Internal Auditors, External Auditors, Financial statements, Statutory and Regulatory Reporting.
- **Change Management Committee** - This Committee ensures that funding for Change is prioritised, managed and governed within a strong control framework. All LGIM Change is tracked centrally by this Committee.

Return to top

4.2.3 Audit, compliance and risk management

LGIM(H) uses the 'three lines of defence' model to manage its operational risk. This governance framework is shown below:

First Line	LGIM(H) board, subsidiary boards, and boards of subsidiary companies	
	Management	
Second Line	Risk Management	Compliance
Third Line	L&G Group Internal Audit / External Oversight	

Senior management within the key control functions of Internal Audit, Compliance and Risk Management teams liaise on a regular basis to ensure both that the monitoring activities of the functions are coordinated efficiently and that a common understanding of risks within the business is maintained.

A strong control environment is achieved through:

An active, professionally staffed Operational Risk Management department providing advice on the consistent assessment of operational risks and supporting the reporting process of critical risk management issues. This is achieved by:

- A formal risk management framework outlining risk management policies, appetite and culture including responsibilities and control processes
- Provision of support and guidance to management on the embedding of the risk management framework into business processes and activities
- Provision of support and guidance on the use of the Risk Management System (RMS). RMS is an online database which supports the risk and control monitoring processes across LGIM(H). RMS is designed to provide a formalised means by which business function heads manage their risks. It works on the principle of assigned responsibility whereby the staff member who actually performs the key controls that mitigate risk is assigned responsibility for reporting upon the operation of those controls to management. Assigned responsibility ensures that the person who is in the best position to report upon the operation of key controls does so
- Designated individuals updating RMS with confirmation that specific controls have been performed and control objectives have been achieved. The process is one of self-assessment overlaid with line supervisory oversight and is overseen by a series of validation checks by the Risk Management team and reports to management
- A monthly LGIM(H) Executive Risk Committee (ERC) which is chaired by the LGIM CRO and consists of senior directors. At the ERC, key risk issues, forward-looking and key strategic risks are identified and assessed along with the actions taken to address risk. This committee also has a key role in monitoring both the application of the risk framework and the actions taken to address risk events. A management information pack is provided for review by the committee that includes details of the key risk issues facing LGIM(H); Internal Audit, External Audit and LGIM Compliance reports as well as progress on addressing issues identified; key risk events and the actions taken to address them; and reports on the successful operation of the risk management framework
- A quarterly Legal & General Group Executive Risk Committee, which receives reports from the ERC and the risk committees of other firms within the Group on the effectiveness of risk management control processes embedded in the normal management procedures and provides oversight on the successful operation of the committee within the overall Group risk management framework

Return to top

An active, professionally staffed, Compliance department responsible for oversight of compliance with regulatory requirements and standards including the FCA rules and other relevant regulations by:

- Provision of training and support to all Approved Persons including coordinating an annual confirmation from all Approved Persons that they have complied with all requirements of the FCA's Approved Persons regime (expanded by the Senior Managers' and Certification (SMCR) regime in December 2019.)
- Provision of policy advice and guidance to the regulated firms including the provision of an online compliance manual to staff
- Arranging training for appropriate members of staff on the regulatory environment and any changes, including computer based training
- Carrying out regular monitoring to ensure regulated firms have appropriate systems, procedures and controls in place and ensuring appropriate remedial action is taken where significant regulatory issues have been identified

An active, professionally staffed Group Internal Audit department which is independent of all business functions, having a direct reporting line to the Legal & General Group Audit Committee. Group Internal Audit will carry out:

- Independent reviews and audits of the controls mitigating the key risks in all areas of the business, prioritised according to the relative risk of each assignment as determined by the Group Chief Internal Auditor in conjunction with senior business management
- Audit assignments aiming to provide assurance to management on the extent to which internal controls:
    - are adequate to manage risk
    - are being performed
    - safeguard the Group's resources and promote effective and efficient use
    - ensure the integrity of records of financial and other transactions
    - achieve adherence to legal and regulatory requirements

Return to top

4.2.4 Information technology

Key systems referred to in this report comprise the fund accounting system (the prime record system used for portfolio administration and valuations), and the order management systems (used by fund managers and dealers to instruct and record deal executions). A separate order management process is used for over-the-counter (OTC) derivative transactions to that used for exchange-traded securities and money market transactions. The systems and facilities incorporate controls designed to ensure that these facilities provide a base for efficient, secure and effective administration.

The table below details the systems included in the testing of control objectives within this report:

System	Application type	Function
Quasar	Bespoke	Supports the operation of Fund accounting and the valuation of funds. Multiple functionality including (Deal processing, Cash management, FX & Money Market, Corporate Actions, Income Processing, Asset Pricing, Regulatory Limit Checks)
OMS	Bespoke	Order management and trade booking for listed securities, FX and deposits
DOMS	Bespoke	Order management and trade booking for OTC derivatives
EMS	Bespoke	Fund exposure management for cash deposit placing
Scope (including ADM, STP-Gateway)	Bespoke	Administration and management of PMC pooled pension schemes and investments in LGIM funds by these schemes. Provision of reports detailing scheme activity, scheme valuation, scheme performance and LGIM fund performance
MIG 21	Third Party	Post trade compliance tool used to determine whether funds comply with defined investment guidelines relating to holdings and index tracking amongst others
TLM	Third Party	Reconciliation application used to perform cash reconciliations between Quasar and custodians
ROMPA	Bespoke	Order management system for repurchase agreements
Vermilion	Third Party	Client reporting tool
Swift	Third Party	Financial messaging network which exchanges messages between banks & other financial institutions. Swift Alliance is a messaging system used to communicate with custodians

Externally hosted and managed systems:

Externally hosted systems: Bloomberg AIM, TradeWeb and MarketAxess, are included in the scope of the control objectives and controls, other than where the controls are specific to locally hosted applications

IT Infrastructure supply chain organisations:

Infrastructure hosting and IT operations were outsourced to HCL Technologies Ltd. in 2018 and 2017. The data centre services control objectives and the respective controls noted in this report are addressed in the relevant SOC 1, SOC II reports provided by HCL Technologies Ltd and the SOC I, SOC II and ISO27001 reports provided by the sub-contracted data centre provider.

Return to top

In April, an interoperability issue between two vendor supplied products required executing a controlled fail-over to the alternative data centre. All systems were moved successfully and the regulator was kept informed during that process. While the event provided assurance that systems and data can be recovered to an alternative location, there were some deficiencies that prevented failover within expected parameters which have been addressed. LGIM proceeded with executing the planned H2 Disaster Recovery tests to support the controls described in this report and to assure that the identified control deficiencies had been mitigated.

4.2.5 Human resources policies

At the heart of the company's business strategy is a commitment to deliver high quality service to clients. In order to achieve this, the Human Resources (HR) department maintains policies and facilitates business procedures dealing with the recruitment, training and retention of high quality staff. By matching resources to business needs and strategy, a positive client experience can be delivered: meeting the administrative and investment needs of existing clients, attracting new business, and managing the various risks and processes involved in running a complex business to high standards. The company's approach to mitigating fraud and other dishonest acts is supported by promoting an open and honest culture in all dealings between employees, managers and those parties with which the company has contact. A formal Code of Ethics and an anti-bribery and corruption policy sets out the company's expectations in this respect. In addition, the company has defined whistle-blowing procedures to enable all employees to raise matters of concern in confidence.

4.2.6 Insurance

Insurance policies (for example professional indemnity insurance) are in place and cover is kept under regular review through the Group Risk Management team.

4.2.7 Capital adequacy and security of assets

In order to safeguard consumer and investor interests, calculations of the minimum capital required for LGIM(H) to withstand negative events are performed on an annual basis. The approach is set out in regulation; Solvency II for insurers and the Internal Capital Adequacy Assessment Process (ICAAP) for applicable financial services firms. The processes are supervised by the PRA and FCA respectively. The capital calculations take into account loss data from LGIM(H) and from across the industry to assess the likelihood and impact of potential negative events, and their outcome on the continued solvency of LGIM(H). The company maintains a level of capital in excess of the solvency requirements specified by the regulators. The capital levels are regularly monitored and reviewed by senior management.

4.2.8 Oversight of outsourced functions

Key suppliers such as custodians, trustees and transfer agencies to the pooled funds are managed by named relationship managers in accordance with the Group Outsourcer & Essential Supplier Services Policy. The relationship manager defines and agrees KPIs and SLAs, monitors these, and meets regularly with the third parties to review the quality of service that they provide. The Supplier Management Committee acts as an oversight body, under the authority delegated to it from the ERC, ensuring individuals appointed to relationship management roles act in accordance with Group Policies and Procedures and that issues and events are managed within the context of the Group risk management framework.

4.2.9 Corporate governance activity

LGIML is a major investor in the UK and holds approximately 3% of the shares in most companies listed in the FTSE All-Share Index. Corporate governance activity is led by the dedicated Corporate Governance and Responsible Investment team and overseen by the LGIM Corporate Governance Committee. This committee is chaired by an LGIM non-executive director and meets regularly to ensure that potential conflicts of interest are minimised and appropriately managed. We comply with the principles set out in the Financial Reporting Council's UK Stewardship Code as revised in October 2019 and we seek independent assurance over this compliance on a periodic basis. Further details as to how this is achieved and the reporting accountants' assessment of reporting on the Statement of application of Principles and related guidance of the UK Stewardship Code for institutional investors is available on the LGIM website (**www.lgim.com**).

Return to top

5. Control objectives

Summary of control objectives

1 Accepting clients

1.1 Accounts are set up and administered in accordance with client agreements and applicable regulations

1.2 Complete and authorised client agreements are operative prior to initiating investment activity

1.3 Client take-ons, including in-specie transfers, are monitored, documented and opening positions are accurately reported to clients

1.4 Investment limits and restrictions are established

1.5 In-house pooled fund unit-holder activity is recorded completely, accurately and in a timely manner

2 Authorising and processing transactions

2.1 Investment strategy is set and implemented in a timely manner

2.2 Investment transactions are properly authorised, executed and allocated in a timely and accurate manner

2.3 Transactions are undertaken only with approved counterparties

2.4 Commission levels and transaction costs are monitored

2.5 Investment and related cash transactions are completely and accurately recorded and communicated for settlement in a timely manner

2.6 Corporate actions are processed and recorded accurately and in a timely manner

2.7 Proxy voting instructions are generated and recorded and carried out accurately and in a timely manner

2.8 Client new monies and withdrawals are processed and recorded completely and accurately; withdrawals are appropriately authorised

3 Maintaining financial and other records

3.1 Investment income and related tax are accurately recorded in the proper period

3.2 Investments are valued using current prices obtained from independent external pricing sources or determined according to approved pricing policies and procedures for fair values in circumstances where independent sources are not available

3.3 Cash and investment positions are completely and accurately recorded and reconciled to third party data

3.4 Investment management fees and other account expenses are accurately calculated and recorded

3.5 Pooled funds are priced and administered accurately and in a timely manner

4 Cash management and safeguarding of assets

4.1 Uninvested cash is managed with regard to diversification of risk and security of funds

4.2 Investments are properly registered and client money segregated

5 Monitoring compliance

5.1 Client portfolios are managed in accordance with investment objectives, monitored for compliance with investment limits and restrictions and performance is measured

5.2 Outsourced activities are properly managed and monitored and conflicts of interest identified to clients

5.3 Transaction errors (including guideline breaches) are rectified promptly and clients treated fairly

5.4 Counterparty exposures are monitored

6 Reporting to clients

6.1 Client reporting in respect of portfolio transactions, holdings and performance, commission and voting is complete and accurate and provided within required timescales

7 Restricting access to systems and data

7.1 Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals

7.2 Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques

7.3 Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles

8 Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats

8.1 IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner

8.2 Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure

8.3 The physical IT equipment is maintained in a controlled environment

8.4 Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g. firewalls, anti-virus etc.)

9 Maintaining and developing systems hardware and software

9.1 Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented

9.2 Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

10 Recovering from processing interruptions

10.1 Data and systems are backed up regularly, retained offsite and regularly tested for recoverability

10.2 IT hardware and software issues are monitored and resolved in a timely manner

10.3 Business and information systems recovery plans are documented, approved, tested and maintained

11 Monitoring IT compliance

11.1 Outsourced activities are properly managed and monitored

Exclusions

This report excludes certain control objectives included for investment management and information technology in Technical Release AAF 01/06 as explained below:

AAF 01/06 Illustrative control	Reason for exclusion
Responsibility for generating proxy voting instructions is clearly established	When accepting new clients, the client documentation clearly states that LGIML retains responsibility for all proxy voting. Clients are allocated units in pooled investment funds, and do not own the underlying securities.

Return to top

6. Control objectives, control procedures and service auditor's tests

1	ACCEPTING CLIENTS	
1.1	**Accounts are set up and administered in accordance with client agreements and applicable regulations** Account set up is handled by a dedicated member of the Client Implementation team. Client take on checklists are used to monitor the client journey, for example, to make sure that Know Your Client and Anti-Money Laundering checks have been completed, that a valid client agreement has been signed and that Fund Operating Guidelines and benchmarks have been agreed. They also check that the fund set up team has correctly set up the new account in the various systems and that external relationships such as with custodians and brokers, have been established.	
	Control procedure	**Testing performed by KPMG LLP and Results**
1.1.1	On an ad-hoc basis whenever a new client is accepted, the Client Implementation team complete and approve a take on checklist and evidence the policy/fund has been set up in accordance with client agreements and applicable guidelines prior to initiating investment activity. This is independently reviewed by a senior implementation executive or team manager as evidenced by electronic signature on SalesForce within the Policy Document IMPDOC.	For a selection of new clients, KPMG obtained the SalesForce screenshot and inspected for evidence that the take on checklists were completed by the Client Implementation Team and reviewed by a senior implementation executive or team manager prior to initiating investment activity, as evidenced by their electronic sign off within the Policy Document IMPDOC in Salesforce. No exceptions noted.
1.1.2	On an ad-hoc basis for new or amended benchmarks, benchmark details are set up and amended by a member of the Allocation Strategy Management team onto the unit holding administration system (Scope) and reviewed by an independent member of the Allocation Strategy Management team as evidenced by an electronic sign-off in Scope. Client mandates, asset allocation benchmarks, ad-hoc instructions or any amendments must be instructed in writing by clients.	For a selection of new and amended benchmarks, KPMG obtained the Scope system sign-offs and inspected for evidence that they were input onto the unit holding administration system by a member of the Allocation Strategy Management team and were reviewed by an independent team member. No exceptions noted.
1.2	**Complete and authorised client agreements are operative prior to initiating investment activity** A pooled client account is not activated on the unit holding administration system (Scope) until complete and authorised agreements have been received, and until funds are made investable cash cannot be invested. The aide-memoire that is completed at client take-on includes a check that all such requirements have been fulfilled, and this must be completed before a the policy number document is issued to the client.	

	Control procedure	Testing performed by KPMG LLP and Results
1.2.1	On an ad-hoc basis whenever a new client is accepted, the Client Implementation team complete and approve a take on checklist and evidence the policy/fund has been set up in accordance with client agreements and applicable guidelines prior to initiating investment activity. This is independently reviewed by a senior implementation executive or team manager as evidenced by electronic signature on SalesForce within the Policy Document IMPDOC.	For a selection of new clients, KPMG obtained the SalesForce screenshot and inspected for evidence that they were completed by the Client Implementation Team and reviewed by a senior implementation executive or team manager prior to initiating investment activity, as evidenced by electronic sign off within the Policy Document IMPDOC in Salesforce. No exceptions noted.
1.3	**Client take-ons, including in-specie transfers, are monitored, documented and opening positions are accurately reported to clients** Once clients have been set up by the Client Implementation team and they have a client reference number, any existing assets can be transferred in by the Transfers team. They may be notified of impending transfers in or out through a variety of sources. These notices are put on a master spread sheet and every quarter the team checks this and chases up any cases about which they have not had a recent update. A transfer case is deemed live when they have a transfer date. At this point they receive a list of assets (for in-specie transfers) or a cash transfer amount from the ceding manager, or provide one to the new manager if LGIM is ceding the assets. The cash value or in-specie assets are uploaded into the fund accounting system (Quasar). Quasar automatically sends out SWIFT messages which are matched with the corresponding message from the ceding manager. Any unmatched items are followed up by the Failed Trades team.	
	Control procedure	**Testing performed by KPMG LLP and Results**
1.3.1	On an ad-hoc basis whenever a new client is accepted, the Client Implementation team complete and approve a take on checklist and evidence the policy/fund has been set up in accordance with client agreements and applicable guidelines prior to initiating investment activity. This is independently reviewed by a senior implementation executive or team manager as evidenced by electronic signature on SalesForce within the Policy Document IMPDOC.	For a selection of new clients, KPMG obtained the SalesForce screenshot and inspected for evidence that they were completed by the Client Implementation Team and reviewed by a senior implementation executive or team manager prior to initiating investment activity, as evidenced by their electronic sign off within the Policy Document IMPDOC in Salesforce. No exceptions noted.
1.3.2	On an ad-hoc basis for new or amended benchmarks, benchmark details are set up and amended by a member of the Allocation Strategy Management team onto the unit holding administration system (Scope) and reviewed by an independent member of the Allocation Strategy Management team as evidenced by an electronic sign-off in Scope. Client mandates, asset allocation benchmarks, ad-hoc instructions or any amendments must be instructed in writing by clients.	For a selection of new and amended benchmarks, KPMG obtained the Scope system sign-offs and inspected for evidence that they were input onto the unit holding administration system by a member of the Allocation Strategy Management team and were reviewed by an independent team member. No exceptions noted.

1.3.3	New clients and new transfers are allocated to dedicated case managers who track them to completion on a New Business spread sheet. Throughout the event, the case manager adheres to agreed procedures and transfer checklists to ensure the event is processed in line with client instruction and LGIM's risk framework, Completed transfers are peer reviewed by other team members or the managers to check that they have been correctly processed by the case manager as well as other departments. The Transfers team also confirms on RMS that they have done these reviews by electronic sign-off that is retained in the system.	For a selection of new clients and transfers KPMG obtained the RMS responses and inspected for evidence that the assigned team member or case manager reviewed transfers for completeness and accuracy as evidenced by electronic sign off retained on the system. No exceptions noted.
1.3.4	A transfer report is only prepared upon request from the Client or Client Relationship Team for PMC Funds only. This is then provided to the client once the event has been fully completed. The reports for in-specie transfers are reviewed for completeness and accuracy by management in the Transfer Team, which is evidenced by a sign off on the transfer checklist.	For a selection of requested PMC client transfers, KPMG obtained the transfer report and transfer checklist and inspected for evidence that the report was completed for all transfers, and reviewed by management in the Transfer Team for completeness and accuracy of the in-specie transfers as evidenced by their sign off on the transfer checklist. No exceptions noted.
1.3.5	Transfers are automatically matched via SWIFT messages to the ceding or receiving fund manager. Unmatched items are reported on a weekly basis on the failed trades report by the Transfers Team who then notify the relevant parties and investigate until the trades clear. This is evidenced by the sign-off of the failed trades report by the Transfers team.	For a selection of weeks, KPMG obtained the 'failed trades' report and inspected for evidence that unmatched items were investigated and cleared and that the report was reviewed as evidenced by sign-off on the failed trades report by the Transfers Team No exceptions noted.
1.4	**Investment limits and restrictions are established**. Investment guidelines and restrictions are documented in the fund documentation (IMA, prospectus, fact sheet etc.), which is completed as part of the fund set-up process. A Fund Objectives and Guidelines document (FOG) or Control Summary Report (CSR) is created for each fund which details all fund guidelines. The majority of guidelines are loaded into the guideline monitoring systems (MIG 21/Charles River (CRD)) whilst a very small number of rules that cannot be coded into MIG 21/CSR are manually monitored.	
	Control procedure	**Testing performed by KPMG LLP and Results**
1.4.1 a	MIG21/FOG: A Fund Objectives and Guidelines document (FOG) is created for each fund by the Guideline Management and Control (GMC) team which summarises all of the investment guidelines and restrictions as part of the IMA. Each new FOG is reviewed for completeness and accuracy by the Fund Manager and GMC team, which is evidenced by a sign-off on the FOG.	For a selection of new funds, KPMG obtained the FOGs and inspected for evidence that the FOG was reviewed for completeness and accuracy by the Fund Manager and GMC team as evidenced by the physical sign-off on the FOG. No exceptions noted.

1.4.1 b	CRD: From 29 January 2019, for index funds, a Control Summary Report (CSR) is created for each fund by the Guideline Management and Control (GMC) Coding team which summarises all of the investment guidelines and restrictions as part of the IMA. Each new CSR is reviewed for completeness and accuracy by the GMC Monitoring team, which is evidenced by email approval to the Portfolio Monitoring Team.	For a selection of new funds implemented in CRD, KPMG obtained the CSR and inspected for evidence that a GMC Ticket/E-mail request from GMC Monitoring was raised and the CSR was reviewed for completeness and accuracy by the GMC Monitoring Team as evidenced by approval email. No exceptions noted.
1.4.2 a	MIG21/FOG: On an ad-hoc basis, amendments to the IMAs are initiated upon request of the Implementation team and are independently reviewed by the GMC team. Where applicable the GMC team update the FOG, which is evidenced by the reviewer sign off, and/or changes applied in MIG21 as evidenced by the electronic reviewer sign-off on the release session which is retained in the system.	For a selection of amendments made to IMAs, KPMG obtained the FOGs and inspected for evidence that each change had been reviewed independently by the GMC team as evidenced by the electronic sign-off in MIG21 or the FOG had been signed-off by a reviewer. No exceptions noted.
1.4.2 b	CRD: From 29 January 2019, for live index funds, on an ad-hoc basis, amendments to the IMAs are initiated upon request of the Implementation team and are independently reviewed by the GMC team. Where applicable GMC Monitoring Team raises a GMC ticket to GMC Coding requesting amendment to CRD and CSR. The closure of ticket is retained as amendment completion.	For a selection of amendments made to IMAs, KPMG obtained the GMC Ticket request as evidence of amendment completion. No exceptions noted.
1.4.3 a	MIG21/FOG: The majority of investment restrictions and guidelines are monitored through MIG21. These are input by a member of the GMC team when a change is required on an ad-hoc basis and are reviewed and released by a second person in the team by a system enforced secondary check before the fund goes live. The review and release is evidenced by electronic sign-off within the system and is retained for MIG21.	For a selection of new funds, KPMG obtained the investment restrictions and guidelines and inspected for evidence that the guidelines were entered on to MIG21 and reviewed by another member of the GMC team prior to fund activity taking place as evidenced by electronic sign-off retained in the system. No exceptions noted. KPMG observed that MIG21 enforced a secondary check before new and amended investment restrictions and guidelines could be released. No exceptions noted.

1.4.3 b	CRD: From 29 January 2019, for live index funds, the majority of investment restrictions and guidelines are monitored through CRD. A GMC ticket is raised by GMC Monitoring and submitted to GMC Coding for coding within CRD. A CSR report is created and reviewed by GMC Monitoring team.	For a selection of new funds, KPMG observed that CRD tickets are raised CSR signed off by GMC Monitoring No exceptions noted.
1.5	**In-house pooled fund unit-holder activity is recorded completely, accurately and in a timely manner** Client instructions are received by email, post or fax. Emails and faxes are automatically uploaded into a workflow tool (SalesForce) where post is scanned and manually uploaded. Instructions are then processed into the unit-holder administration system (Scope) which are peer reviewed in the weekly cycle. Daily and midday cycles are automated and do not require manual judgement. They are also matched against money received into the six bank accounts that have been set up for this purpose (GBP, EUR and USD for the daily and weekly priced funds). Occasionally, money is received into the bank account without any accompanying instructions. These are investigated as far as possible but if no client instruction is received, and no standing instructions exist, then the money is returned to the payer	
	Control procedure	**Testing performed by KPMG LLP and Results**
1.5.1	On a weekly basis, PMC TA (Transfer Agents) check the policy dashboard in Scope to verify that all policy decisions are made and once the feeder decisions have been made, the cashflows are issued. In the weekly cycle, this is peer reviewed on the Fund Movement checklist within the team to confirm that any decisions outstanding are of acceptable tolerances. This review is evidenced by the sign-off on the Fund Movement checklist.	For a selection of weeks, KPMG obtained the Fund Movement Checklist and inspected for evidence that they were performed and reviewed by appropriate independent personnel on the PMC TA as evidenced by their sign-off on the Fund Movement checklist. No exceptions noted.
1.5.2.a	From 1 January to 30 June: For each daily, midday and weekly dealing cycle, a Policy and Feeder Reconciliation is completed by the Transfer Agent team over the cash module of the unit holding administration system, the Investment Summary Report and the Feeder Fund Report for creations, cancellations and switches between funds. This is evidenced by the signed-off reconciliation or daily/weekly checklist which is peer reviewed by another member of the Transfer Agent team	For a selection of days and weeks, KPMG obtained the Policy and Feeder Reconciliations and inspected for evidence that these were completed appropriately and independently peer reviewed as evidenced by physical sign-off on the reconciliation or daily/weekly checklist. No exceptions noted

1.5.2.b	From 30 June: For each daily, midday and weekly dealing cycle, a Policy and Feeder Reconciliation is completed by Scope over the cash module of the unit holding administration system, the Investment Summary Report and the Feeder Fund Report for creations, cancellations and switches between funds. If there are any reconciliation breaks, PMCTA receive an automated email warning of break so they are able to investigate before proceeding with Allocations as evidenced by a cleared reconciliation or annotation on the reconciliation if the break is not cleared.	For a selection of days and weeks, KPMG obtained the automated email warning of break and inspected for evidence that the reconciliation breaks were investigated before proceeding with Allocations as evidenced by a cleared reconciliation or annotation on the reconciliation if the break is not cleared. No exceptions noted
2	**AUTHORISING AND PROCESSING TRANSACTIONS**	
2.1	**Investment strategy is set and implemented in a timely manner** Investment strategy is set and documented in a Fund Objectives and Guidelines document (FOG) or Control Summary Report (CSR) which is completed as part of the fund set up process. The details are loaded into the guideline monitoring systems. Performance and risk benchmarks are also loaded into the relevant risk systems and implementation of the investment strategy is monitored by these teams	
	Control procedure	**Testing performed by KPMG LLP and Results**
2.1.1 a	MIG21/FOG: The majority of investment restrictions and guidelines are monitored through MIG21. These are input by a member of the GMC team when a change is required on an ad-hoc basis and are reviewed and released by a second person in the team by a system enforced secondary check before the fund goes live. The review and release is evidenced by electronic sign-off within the system and is retained for MIG21.	For a selection of new funds, KPMG obtained the investment restrictions and guidelines and inspected for evidence that the guidelines were entered on to MIG21 and reviewed by another member of the GMC team prior to fund activity taking place as evidenced by electronic sign-off retained in the system. No exceptions noted. KPMG observed that MIG21 enforced a secondary check before new and amended investment restrictions and guidelines could be released. No exceptions noted.
2.1.1 b	CRD: From 29 January 2019, for live index funds, the majority of investment restrictions and guidelines are monitored through CRD. A GMC ticket is raised by GMC Monitoring and submitted to GMC Coding for coding within CRD. A CSR report is created and reviewed by GMC Monitoring team.	For a selection of new funds, KPMG observed that CRD tickets are raised CSR signed off by GMC Monitoring No exceptions noted.

2.1.2 a	MIG21/FOG: On an ad-hoc basis, amendments to the IMAs are initiated upon request of the Implementation team and are independently reviewed by the GMC team. Where applicable the GMC team update the FOG, which is evidenced by the reviewer sign off, and/or changes applied in MIG21 as evidenced by the electronic reviewer sign-off on the release session which is retained in the system.	For a selection of amendments made to IMAs, KPMG obtained the FOGs and inspected for evidence that each change had been reviewed independently by the GMC team as evidenced by the electronic sign-off in MIG21 or the FOG had been signed-off by a reviewer. No exceptions noted.
2.1.2 b	CRD: From 29 January 2019, for live index funds, on an ad-hoc basis, amendments to the IMAs are initiated upon request of the Implementation team and are independently reviewed by the GMC team. Where applicable GMC Monitoring Team raises a GMC ticket to GMC Coding requesting amendment to CRD and CSR. The closure of ticket is retained as amendment completion.	For a selection of amendments made to IMAs, KPMG obtained the GMC Ticket request as evidence of amendment completion No exceptions noted.
2.1.3	The Scope algorithms that calculate pooled fund performance are owned by the Performance Team, which is independent of the fund managers. Any changes to the algorithms are tested by the Performance team before they are made live. This is evidenced by the development team obtaining email sign off by the performance team prior to changes being made live.	KPMG enquired of management whether any instances of changes to the algorithms within Scope occurred during the period and were informed no instances had occurred. KPMG inspected the Scope system version control and confirmed that no changes to algorithms have been made in the year. Since there were no instances, the operating effectiveness of the control could not be tested.

2.2 Investment transactions are properly authorised, executed and allocated in a timely and accurate manner

Investment transactions are processed on a number of platforms, depending on the instrument type. Most transactions (equities, fixed income, cash instruments and listed derivatives) are effected on the core systems - OMS and EMS / EMSX. OTC derivatives transactions are carried out on Bloomberg AIM, DOMS, or using a series of Order Raising Spread sheets. Transactions are initiated and executed only by authorised persons. This segregation of duties is enforced in the OMS, EMS, and Bloomberg AIM systems. For all other systems, there are manual checks in place to ensure that only authorised persons initiate and raise orders. Trades are allocated independently of the fund managers by the Global Trading team. They follow default allocation rules (which are coded in OMS). Occasionally, these may be overridden, for example to take account of minimum lot sizes in fixed income instruments. These manual overrides are reviewed by the Compliance team. For fund managers (FMs) and dealers to become authorised they need to be deemed competent by their line manager and to be authorised by the FCA. Their names and authority limits are added to an authority schedule which is validated by the Operational Risk Team. Once signed off the Data Services, Reference Data team (RDT) codes the approvals and restrictions into OMS. On a six monthly basis, the RDT confirms that the access levels and limits in the order management systems agree with the latest authorised limits schedules. An exception report is produced every month by the Risk Management team which identifies any deals placed by an unauthorised party and this is reviewed by senior dealers. For all securities in OMS, a list of restricted securities is maintained by the respective senior FMs and reviewed by the Compliance team. The system generates an email notifying Compliance if the list has been amended. For some fixed income securities, a list of restricted securities is maintained on spread sheets.

	Control procedure	Testing performed by KPMG LLP and Results
2.2.1	On an ad-hoc basis, fund managers and dealers with order raising or dealing permissions are only given access to trade when they have been authorised by the FCA and deemed competent by their line manager. A ticket request for access in service now is raised and approved in system by line manager for access. These authorities are validated by the Operational Risk team before they are coded into the relevant system. This is evidenced by the email approval received from the respective line manager. LGIMA control: Transactions executed within TradeWeb, MarketAxess, Portware, FX ALL and Bloomberg must be initiated by authorized traders. Access to these applications is reviewed on an annual basis and requested modifications are appropriately updated by the System Owner.	For a selection of new users with order raising or dealing permissions, KPMG obtained the email approval and ticket request and inspected for evidence that it was obtained from the respective line manager and validated by the Operational Risk team. No exceptions noted. LGIMA control: KPMG inspected the TradeWeb, MarketAxess, Portware, FX ALL, and Bloomberg AIM annual user access reviews, to determine that the reviews were completed annually by the system owner and identified access issues were updated in the systems. No exceptions noted. KPMG assessed the lists of users with trading access in TradeWeb, MarketAxess, Portware, FX ALL, and Bloomberg AIM, to determine that access was appropriately restricted, as evidenced by each user's job title and responsibilities in the system. No exceptions noted.

2.2.2	On a bi-annual basis, the RDT confirms that the access list and limits on the order management systems agree with the latest authorised access list, which is evidenced by email confirmation to the Operational Risk Team.	KPMG obtained the half year management review of all users' access rights and inspected for evidence that the review of the system access lists on the order management system was performed as evidenced by the email confirmation to the Operational Risk Team. No exceptions noted.
2.2.3	RDT circulates a schedule of authorised traders to key brokers. This schedule is reviewed on a quarterly basis by head of departments for sign off; only then is circulation to counterparties permitted. The review is evidenced by the physical sign-off by the Chief Operating Officer/Finance Director and the Chief Executive Officer (LGIM) on the updated schedules.	For a selection of quarters, KPMG obtained the updated schedule of authorised dealers and inspected for evidence of the review by the Chief Operating Officer/Finance Director and the Chief Executive Officer (LGIM) prior to circulation to counterparties as evidenced by physical sign-off on the schedule No exceptions noted.
2.2.4	On a monthly basis, Operational Risk Management prepares a report of trades executed by dealers that were either under supervision or had not been authorised for a particular instrument. This report is distributed to and reviewed by the head of the Global Trading Team (GTT) for appropriateness. The review of the report is evidenced via email to the Head of Global Trading Team.	For a selection of months, KPMG obtained the report of trades executed by dealers that were either under supervision or had not been authorised for a particular instrument and inspected for evidence of review by the head of the Global Trading Team as evidenced by email. No exceptions noted.
2.2.5	On an ad-hoc basis when instrument restrictions are recorded, this is done by placing a block against the instrument in OMS, this prevents trading within OMS as evidenced by the automated system error message.	KPMG confirmed through observation of OMS that an instrument on the restricted security list could not be traded as the dealing systems prevented the trade from being processed as evidenced by the system error message. No exceptions noted.
2.2.6	For Active Fixed Income, restrictions against a relevant listed issuer are recorded in the relevant spread sheet. On a monthly basis, Compliance undertakes a review of all Active Fixed Income trades to check that restricted securities have not been traded. This is evidenced by annotations and comments on the spread sheet as part of the monthly compliance review and, where breaches are noted, a CEAL being raised in RMS.	For a selection of months, KPMG obtained the monthly compliance review of Active Fixed Income restrictions against trading activity and inspected for evidence that the review was performed as evidenced by the annotated spread sheet. In situations where an issue was noted, KPMG inspected that a CEAL was raised in RMS. No exceptions noted.

2.2.7	LGIMA control: Bloomberg AIM issues pre- trade warnings for purchases that do not comply with investment guidelines. The pre-trade warnings appear on the Bloomberg AIM “LGIMA Daily Compliance - End of Day Summary” report. The Risk & Trade Compliance Team reviews the report and documents the resolution or explanation of issues within one business day. On a daily basis, the Bloomberg AIM monitors trading activity and flags identified breaches of investment guidelines and sends them to the Risk & Trade Compliance Team. The breaches identified, including duration benchmarks appear on the Bloomberg AIM “LGIMA Daily Compliance - End of Day Summary” report. Operations management reviews the report and documents the resolution or explanation of issues within one business day.	LGIMA control: KPMG observed a trader attempt to execute a trade in Bloomberg AIM that was not in compliance with the account's compliance guidelines, to determine that the system issued a pre-trade warning and prohibited the trade from further processing and the failed trade appeared on the “LGIMA Daily Compliance – End of Day Summary” report. No exceptions noted. KPMG observed a trader attempt to execute a trade in Bloomberg AIM that was in compliance with the account's compliance guidelines, to determine that the system allowed the trade to process and the successful trade did not appear on the “LGIMA Daily Compliance – End of Day Summary” report. No exceptions noted. For a selection of days, KPMG obtained the "LGIMA Daily Compliance - End of Day Summary" reports and inspected for evidence that the reports and supporting documentation review was performed over each guideline breach and a resolution or explanation of the issue was provided by the Risk & Trade Compliance Team as evidenced by their sign-off on each entry within the report. No exceptions noted.

2.2.8	The dealing system automatically allocates executed trades according to pre-defined rules. This may be overridden by the GTT either for trading reasons or on instruction from the fund manager. Where a rule is overridden, the GTT are required to document justification for the manual allocation in the monitoring schedule. The Compliance department review dealer justification for manual allocations on a monthly basis in the monitoring schedule as evidenced by Compliance's annotation and resolution on the schedule. Where responses are deemed to be inadequate, a CEAL is raised to record the details of the transaction for follow up. LGIMA control: The Compliance Team reviews a sample of executed trades on a monthly basis to ensure the Allocations Policy is followed. If a trade is reallocated after execution, a Post Trade Re-Allocation form must be completed and signed off by the trader/Portfolio Manager and a member of Compliance.	For a selection of months, KPMG obtained the monitoring schedule and inspected for evidence that the Compliance team had reviewed dealer justifications for amended allocations as evidenced by annotation and resolution on the monitoring schedule. In situations where the compliance team did not deem the dealer response to be adequate, KPMG obtained the CEAL and inspected for evidence that it was raised and recorded. No exceptions noted. LGIMA control: For a selection of months, KPMG obtained the monthly reviews of trade allocations and inspected for evidence that the review and supporting documentation over the trade were analysed, to determine whether a review was performed by the Compliance Team and any allocation exceptions were investigated and resolved as evidenced by their sign-off on the monthly report and supporting documentation by the Compliance Team. No exceptions noted. For the one trade during the period where allocations were adjusted after trade execution, KPMG obtained the Post-Trade Re-Allocation Form and inspected for evidence that the allocation adjustment was reviewed and approved by both the Portfolio Manager and the Risk & Trade Compliance Team as evidenced by their sign-off on the form. No exceptions noted.
2.2.9	On a monthly basis, the Compliance department reviews all trades that were carried out using Order Raising Spread sheets for segregation of duties to confirm they were initiated by an authorised fund manager and executed by an authorised dealer as evidenced by annotated comments in the spread sheet which is retained.	For a selection of months, KPMG obtained the Order Raising Spread sheets and inspected for evidence that the Compliance department carried out a review of segregation of duties as evidenced by the Compliance annotation on the spread sheet. No exceptions noted.
2.2.10	On an ad-hoc basis, trade instructions are submitted to the Dealing Desk electronically once they have been authorised by the Fund Manager. The trade instructions are then executed as soon as practical by telephone or electronically. Only Dealers can execute trades as enforced by the system, whereby trades are electronically routed to the dealers.	For a selection of trade instructions, KPMG observed through the OMS that a deal was routed to the dealers' electronic blotter and that the system ensured that the fund manager could not execute their own trade on the system No exceptions noted.

2.2.11	On a bi-monthly basis, the Compliance Department reviews a sample of trades to obtain a rationalisation from the trading desk if 'best execution' had not been achieved. The review is evidenced by a spreadsheet which contains proof of investigation where applicable.	For a selection of months, KPMG obtained the investigation reports and inspected for evidence of the bi-monthly investigation reports that the Compliance team reviewed for best execution and any exceptions were followed up via email with the trader for explanation as evidenced by annotation on the spreadsheet. No exceptions noted.
2.3	**Transactions are undertaken only with approved counterparties** The requirement for a new counterparty is raised by a fund manager or dealer. They contact Trade Support which coordinates the set up process which covers Legal, Compliance, Risk Management, Credit and Operations sign off. Trade Support then instruct Investment Support to add the counterparty to the order management system (OMS).	
	Control procedure	**Testing performed by KPMG LLP and Results**
2.3.1 a	On an ad-hoc basis, when a counterparty is added to the dealing system, a New Counterparty Form is completed by Operations and submitted for approval via email. The counterparty is approved by Legal, Compliance, Risk, Credit, senior dealers and Operations as evidenced by email. Temporary counterparties require approval from only Compliance and senior dealers. Evidence of the review and approval is through email sign off of the approval form by the relevant teams.	For a selection of new counterparties, KPMG obtained the approval form and email evidence and inspected for evidence of required approval obtained from Legal, Compliance, Risk, Credit, senior dealers and Operation. For a selection of temporary counterparties, KPMG obtained the approval form and email evidence and inspected for required approval obtained from compliance and senior dealers only No exceptions noted.
2.3.1 b	The senior operations specialist maintains a system of standing data of approved brokers. Front office staff are prevented from making changes to the approved list of brokers by the system. System parameters restrict trades such that they cannot be entered into the system for unapproved brokers.	KPMG observed that the trades could only be entered into the system for the approved brokers, and the front office staff had no ability to make changes in the system to the approved list of brokers. No exceptions noted.
2.4	**Commission levels and transaction costs are monitored.** The Best Execution Committee, which is attended by the heads of asset classes and head of the Global Trading Team, discusses a monthly report which details commission levels and turnover rates prepared by GTT.	
	Control procedure	**Testing performed by KPMG LLP and Results**
2.4.1	A monthly Activity Report is generated by the Trading Research & Analysis team for all senior traders to review. In addition the best execution committee meets quarterly to review all trading activity for the previous period. In these meetings execution quality and outliers are reviewed, as well as counterparty activity levels. The meeting minutes are recorded and retained.	For a selection of months, KPMG obtained the minutes of the Best Execution Committee meeting and inspected for evidence of the reports being reviewed and discussed at the meeting as evidenced by the retained minutes. No exceptions noted.

2.5	**Investment and related cash transactions are completely and accurately recorded and communicated for settlement in a timely manner.** On a daily basis, trades are booked in the relevant order management systems. Trade details are matched to broker confirmations before being settled via automated SWIFT instructions. Failures and reconciliation breaks are investigated and resolved in a timely manner. Progress on investigations is monitored by management.	
	Control procedure	**Testing performed by KPMG LLP and Results**
2.5.1	On a daily basis, confirmed trade details are settled via standard automated SWIFT instructions. Any settlement failures are investigated and resolved by the settlements team. This is evidenced by a daily exception report showing outstanding trades and the cause is escalated to senior management for investigation via email.	For a selection of days, KPMG obtained the exception reports and escalation emails and inspected for evidence that settlement failures reports were run and failures were escalated to management via email. For the same selection, KPMG obtained a subsequent exception report and inspected for evidence that failures were resolved. No exceptions noted.
2.5.2	On a daily basis, an automated cash reconciliation is performed between the bank account statements received via SWIFT and the manager's records for each fund. Reconciling items are investigated and resolved in a timely manner by Operations as evidenced by annotation on the cash reconciliation.	For a selection of days, KPMG obtained the daily checklists, and inspected for evidence that trade queues were monitored by the Trade Processing team as evidenced by sign-off on the checklist. No exceptions noted.
2.5.3	On a daily basis, an automated cash reconciliation is performed between the bank account statements received via SWIFT and the manager's records for each fund. Reconciling items are investigated and resolved in a timely manner by Operations as evidenced by the cash reconciliation annotation	For a selection of days and funds, KPMG obtained the automated cash reconciliations and inspected for evidence that they were being performed and that unreconciled items were investigated and resolved in a timely manner by Operations as evidenced by annotation on the reconciliation No exceptions noted.
2.5.4	On a daily basis, trade details are automatically or manually matched to broker confirmations. Any discrepancies in details are highlighted and investigated by the Trade Processing team). Progress on investigations is monitored by management as evidenced by the daily checklist sign-off.	For a selection of days, KPMG obtained the daily checklists and inspected for evidence that trade queues were monitored by the Trade Processing team as evidenced by sign-off on the checklist. No exceptions noted.
2.5.5	On a daily basis, trade details recorded in OMS are automatically messaged to FCMs (Clearing Brokers) and are allocated on Exchange per fund. Broker confirmations are received and matched with the trades' recorded in OMS. Progress on investigations is monitored by Operations management. Trades are monitored on an intraday basis and the positions are checked T+1 as evidenced by the daily F&O checklists sign-off.	For a selection of days, KPMG obtained the daily F&O checklists and inspected for evidence that the trade queues were monitored by Operations and investigated in a timely manner as evidenced by sign-off of the checklist. No exceptions noted.

2.6	**Corporate actions are processed and recorded accurately and in a timely manner.** Corporate action events are received via a number of direct market feeds and independent sources and are subject to validation before entry in the live system. A sample of corporate actions are reviewed on a monthly basis to ensure they have been executed in line with the instructions received.	
	Control procedure	**Testing performed by KPMG LLP and Results**
2.6.1	On an ad-hoc basis, notification of corporate action events are received via a number of direct market feeds and independent custodian sources. All event information received is reviewed by Operations to ensure accuracy and validity prior to inclusion in the live system. All corporate action information is verified against a second independent source prior to being input to the live system as evidenced by the event pack sign-off by Operations.	For a selection of corporate action events, KPMG obtained the event pack and inspected for evidence that all event information received was reviewed by Operations for accuracy and validity and verified against a second independent source as evidenced by the sign-off. No exceptions noted.
2.6.2	On a monthly basis, a Corporate Actions supervisor performs a review of a selection of corporate actions to ensure that they are executed in line with the corporate action instructions. Evidence of the review is maintained through annotation on the corporate actions spread sheet which is retained.	For a selection of months, KPMG obtained the corporate action review spread sheet and inspected that a Corporate Actions supervisor performed a review to confirm that a selection of corporate actions were executed as instructed, has been processed on the correct execution, as evidenced by the annotation on the corporate actions spread sheet. No exceptions noted.
2.7	**Proxy voting instructions are generated and recorded and carried out accurately and in a timely manner** The Corporate Governance Team have 6 custom voting policies: UK, North America, France, Brazil, Japan and Global which are reviewed on an annual basis and updated if appropriate. The updated policies are then provided to ISS whose custom team apply the relevant policy to meetings in these markets. The Corporate Governance Team on a weekly basis monitors how these policies are being applied by ISS. Each governance analyst reviews a sample of the voting decisions applied for company meetings in each of the main regions: North America UK and Europe. The Team receives daily voting alerts from ISS on any meetings where the decision has been referred to the Team. All voting referrals are recorded on a spread sheet which evidences all changes and the reason for the change	

	Control procedure	Testing performed by KPMG LLP and Results
2.7.1	The Corporate Governance Team receives daily voting alerts from the proxy advisors (ISS) on any meetings where the decision has been referred to the Team. For all referred emails a team member reviews the voting research from ISS. If a team member has had an engagement with the company or knows the company well they may take voting action based on their sector/company knowledge. However, on contentious issues where there is any concern about how the vote should be applied a virtual team voting meeting will be held to agree resolution. These emails are retained for audit purposes.	For a selection of voting decisions, KPMG obtained email discussion on contentious issues and the vote confirmation report and inspected for evidence that the vote was discussed and resolution agreed upon as evidenced by the email sign off. No exceptions noted.
2.8	**Client new monies and withdrawals are processed and recorded completely and accurately; withdrawals are appropriately authorised** All funds received are paid into the PMC management account which is reconciled on a daily basis. A decision maker is notified and considers the best treatment for the cash, in line with the client's investment objectives, which are then reviewed for completeness by the PMC Transfer Agents. Redemptions and changes to payment details are verified against policy and client instructions before being progressed. Straight through processing instructions are automatically reviewed by the system against set parameters where exceptions are then investigated by the Client Order Management team.	
	Control procedure	**Testing performed by KPMG LLP and Results**
2.8.1	For new monies, all funds received are paid into the PMC management account. On a daily basis, bank reconciliations are prepared and reviewed by separate members of the Operations team as evidenced by sign-off on the bank reconciliation.	For a selection of days, KPMG obtained the bank reconciliations and inspected for evidence that they were prepared and reviewed by separate members of the Operations team such that all new monies were reconciled as evidenced by the review sign-off. No exceptions noted.
2.8.2	On an ad-hoc basis, new monies are received into the weekly / daily dealing account and referenced to the client number and name. On confirmation from the Client Data and Documentation Management (CDDM) that the client has been set up, the funds are moved to the client record and approved against the client name by the Cash team. The client instruction is then processed by the Client Order Management team (COM) team as evidenced by the client instruction set-up and electronic approval in SalesForce.	For a selection of new cash receipts in the weekly and dealing accounts, KPMG obtained the client instruction and inspected for evidence that this was set up on the system by the COM team as evidenced by the electronic approval in SalesForce. No exceptions noted.

2.8.3	On an ad-hoc basis, when cash has been allocated to a client account a member of the Client Order Management (COM) team with decision maker capabilities is alerted on screen by the Client Relationship Executive (CRE) team in Scope. The decision on how best to treat the cash in order to meet the client's investment objectives is made based on screen-based criteria or on automated data held on the system. This criteria/instruction is reviewed by COM or if clarification is required a confirmation is requested from the client via email and the decision is made as evidenced by the system criteria and electronic sign-off by the decision maker once complete.	For a selection of decisions, KPMG inspected the system and confirmed that the decision maker had applied the client's investment objectives accurately as per their instruction /email confirmation as evidenced by electronic sign-off by the COM decision maker retained in the Scope system. No exceptions noted.
2.8.4	Redemptions and/or amendments to payment details in pooled funds are received on an ad-hoc basis and are only made when received in accordance with the requirements of the managed fund policy and once client signatory has been both authorised and verified. The CDDM team review and verify instructions received for appropriate authority to those held on file. This is evidenced by sign-off of the client instructions by the Client Order Management team	For a selection of redemptions and amendments, KPMG obtained the client instructions and inspected for evidence that a review was performed as evidenced by sign-off from the CDDM team to verify that they were authorised and that the signatories had been authorised and verified to those held on file. No exceptions noted.
2.8.5	Instructions received via straight-through processing (STP) are compared automatically to SalesForce system parameters before being processed. Discrepancies are automatically moved to an exception queue and investigated by the Client Order Management team before being processed as evidenced by electronic sign-off on the system which is retained. Instructions that are not STP are processed on instructions received by the client. That are dual keyed into the system.	For a selection of straight-through processing discrepancies, KPMG obtained the system sign-off and inspected that discrepancies were investigated and resolved before being processed as evidenced by sign-off on the system by the Client Order Management team. No exceptions noted.
3	**MAINTAINING FINANCIAL AND OTHER RECORDS**	
3.1	**Investment income and related tax are accurately recorded in the proper period** Income events are received through a direct market feed and compared against the previous day's data where changes are investigated by Operations. Updates to event information are received by email from the custodian and automatically updated in Quasar. The process is reviewed by a supervisor. A quarterly report of tax reclaim data is also received from the custodian and is reconciled against the data in Quasar. All tax reclaim accruals are reconciled by Operations to payments received. Exceptions for both reconciliations are investigated to resolution by Operations.	

	Control procedure	Testing performed by KPMG LLP and Results
3.1.1	On a daily basis, notification of income events are received via a direct market feed from IDS. All feed data is uploaded into a report automatically and any changes from the previous day are identified and investigated by the Operations team as evidenced by the primary generation checklist which is signed-off by Operations.	For a selection of days, KPMG obtained the primary generation checklist and inspected for evidence that income event changes identified were investigated, reviewed, and where necessary, adjustments made by Operations as evidenced by the review and sign-off on the checklist. **Exception noted:** For 1 out of 25 days selected, KPMG noted that the there was no evidence that the checklist was reviewed.
3.1.2	On a daily basis, updates to event information such as unit trusts (estimated and confirmed rates) are received by e-mail from the custodian and automatically sent to Quasar to be updated. This process is then reviewed by a supervisor as evidenced by the primary generation checklist which is signed-off.	For a selection of days, KPMG obtained the primary generation checklist and inspected for evidence that the Quasar capture of the changes to event information was reviewed by a supervisor as evidenced by sign-off on the checklist. No exceptions noted.
3.1.3	Tax reclaim data is received from the custodian on a quarterly basis and this information is compared to the data in Quasar (the fund accounting system). A macro enabled spread sheet is used to compare the two sources of data and an exception report is generated. Exceptions are investigated and resolved in a timely manner by Operations. This is evidenced by the annotated reconciliation which is retained.	For selection of quarters, KPMG obtained the reconciliations and selected exceptions resolved, and inspected for evidence that they were investigated and then removed from the fund accounting system as evidenced by the annotation on the reconciliation by the Operations team. No exceptions noted.
3.1.4	On an ad-hoc basis, market changes relating to dividend withholding tax around the world are reviewed to ensure that any developments on taxation agreements involving the UK are amended where necessary to recalculate entitlements from the date of the law change as evidenced by the changes in Quasar being time stamped and retained in the system by the Operations team.	For a selection of changes relating to dividend withholding tax rates, KPMG obtained the Quasar screenshots and inspected for evidence that the change was made accurately on the system and agreed to the independent source of information as evidenced by the electronic sign-off by the operations team which is retained in the system. No exceptions noted.
3.1.5	On a daily basis, tax reclaim accruals are reconciled by the Operations team to payments received. Un-reconciled items are investigated by the team and resolved on a timely basis as evidenced by sign off on the primary generation checklist and annotation on the reconciliation.	For a selection of days, KPMG obtained the primary generation checklist and the actual reconciliation and inspected for evidence that tax reclaim accruals and payments were reconciled and that un-reconciled items were resolved on a timely basis as evidenced by annotation on the reconciliation and sign off on the primary generation checklist. No exceptions noted.

3.2	**Investments are valued using current prices obtained from independent external pricing sources or determined according to approved pricing policies and procedures for fair values in circumstances where independent sources are not available** A documented pricing hierarchy is used to determine pricing sources for each type of exchange traded security, received via automated feed. A standard template is used to set up or amend securities in LGIM systems, which is then reviewed by a second team member. Prices received for OTC instruments and vanilla fixed income and equity instruments are reviewed against pre-determined tolerances and discrepancies outside of tolerance are investigated by the Derivative pricing team and Asset pricing team respectively. Static prices are reviewed by the fund managers for appropriateness with amendments approved by a Investments Director, Head of Department, or the Head of Global trading Team and 2 voting members of the Asset Pricing and Valuations Committee. The price change process is operated across two independent teams to ensure segregation of duties. Pricing decisions are reported to the Asset Pricing and Valuations committee on a quarterly basis for a review independent from the fund managers.	
	Control procedure	**Testing performed by KPMG LLP and Results**
3.2.1	Automated price feeds for exchange-traded, fixed income securities and externally managed funds are received from independent external sources on a daily basis. A documented pricing hierarchy, which is approved annually by the Asset Pricing and Valuations Committee (APVC), as evidenced by meeting minutes, is used to determine primary and alternative pricing sources for each type of exchange-traded security. In exceptional circumstances the pricing ladder for a specific fund or asset class may need to be amended. This is evidenced by a system sign off by the CRM and the Investments Director.	KPMG obtained and inspected the minutes of the relevant APVC meeting and confirmed that the pricing hierarchy was approved annually for the automated price feeds within the period as evidenced by discussion within and approval of the minutes. No exceptions noted. For a selection of securities, KPMG inspected Quasar and noted that securities had been priced according to the pricing hierarchy. No exceptions noted. KPMG enquired of management whether any instances of amendments to the pricing ladder occurred during the period and were informed no instances had occurred. Since there were no instances, the operating effectiveness of this part of the control could not be tested.
3.2.2	Securities are set up and amended accurately in LGIM systems by using a standard template from the Data Management Office. Every security set up and amendment must be approved by someone other than the originator in the Data Management Office as evidenced by the “input and authorise” sign-off process enforced by the system. Audit trail of sign offs are maintained on the system	For a selection of security set ups and amendments, KPMG inspected the systems and confirmed that the two stage input and authorise process was enforced by the system for asset set-up as evidenced by electronic sign off. KPMG also inspected that list of users have the correct access to securities on the system. No exceptions noted.

3.2.3	On a daily basis, for OTC instruments, prices and positions received from independent external counterparties are compared against LGIM valuations/external price sources as per the Asset Pricing Framework, by the Collateral Utilities team utilising Tri Resolve data and VBA tools. The DTS pricing team undertake validation/tolerance checks as evidenced by the Master spread sheets files sent to them by the Collateral Utilities team or completion of the OTC daily checklist. In addition, any discrepancies over £5 million are sent to the DTS pricing team by email from the Collateral Utilities team to be investigated and a response is provided back to the Collateral Utilities team with commentary/resolution as evidenced by retained emails.	For a selection of days, KPMG obtained the Master spread sheets and inspected for evidence that the prices and positions of OTC instruments received from independent external counterparties were compared to LGIM valuations/external price sources by the Collateral Utilities team or the OTC daily checklist was completed. KPMG inspected for evidence that the discrepancies over £5 million were sent to the DTS pricing team to be investigated via email and a response is provided with resolution as evidenced by emails. No exceptions noted.
3.2.4	On a daily basis, exception report checklists are created for any price movements on vanilla Fixed Income and Equity instruments monitored by the Asset Pricing team outside set tolerances (5% for equity and 2% for bonds), where prices received have not changed within a set period or where no price has been received. Each item on the exception report is investigated when they occur and an appropriate pricing decision is made which is reviewed and signed off by a senior member of the Asset Pricing team, as evidenced by the annotation on the exception report checklist.	For a selection of days, KPMG obtained the exception report checklists and inspected that exceptions were created for any price movements outside set tolerances, where prices received have not changed within a set period or where no price has been received. No exceptions noted. For a selection of days, KPMG obtained the checklists and inspected that daily exceptions were reviewed by a senior member of the Asset Pricing team and that any exceptions were investigated and resolved as annotated on the checklists No exceptions noted.
3.2.5	Where prices are static, the Asset Pricing team extracts the Quasar data on a monthly basis for review by the Fund Managers to confirm continued appropriateness of the prices as evidenced by sign-off by the fund manager on the report. Any amendments to prices requested by the Fund manager where supporting documentation is not available through standard market sources are reviewed for appropriateness and signed off by Investments Director and two members of the Asset Pricing and Valuations Committee. This is evidenced by static price reports and email approval.	For a selection of months, KPMG obtained the static price reports and inspected for evidence that they were independently reviewed and signed off by a fund manager. No exceptions noted. For a selection of amendments where supporting documentation is not available through standard market sources, KPMG inspected for evidence that changes were independently reviewed and signed off by an Investments Director and two members of the Asset Pricing and Valuations Committee as evidenced by an email sign-off. No exceptions noted.

3.2.6	On a quarterly basis, pricing decisions are reported to the Asset Pricing & Valuations Committee (APVC), which is comprised of senior management from the Operations and Finance areas and the Head of Global Trading, Head of Global Analytics, and ASM, and is independent of the Fund Managers (as per the Terms of Reference), to review the approach to security pricing. This review is evidenced by actions being noted in the minutes of each meeting.	For a selection of quarters, KPMG obtained the APVC meeting reports and minutes and inspected for evidence that issues/pricing decisions were escalated to the Asset Pricing & Valuations Committee for a decision on the price to be used. KPMG inspected the attendees as per the meeting minutes and the Terms of Reference to confirm that the Asset Pricing Sub-Committee was independent of the Fund Managers. No exceptions noted.
3.2.7	Segregation of duties exists over any subsequent price changes with any adjustments requiring the Valuations team to 'unlock' the price and the Pricing team to update the price on the system.	For a manual price changes, KPMG observed the system audit trail and inspected that the Valuation team had to 'unlock' prices in order for the Pricing team to make a manual price change. No exceptions noted.
3.3	**Cash and investment positions are completely and accurately recorded and reconciled to third party data** A daily cash reconciliation is automatically initiated and generates exception reports for investigation by Operations. Holdings are reconciled with custodian positions on a daily basis with a further monthly reconciliation performed at the custodian and fund level by the Custody Reconciliation team.	
	Control procedure	**Testing performed by KPMG LLP and Results**
3.3.1	On a daily basis, an automated cash reconciliation is performed between the bank account statements received via SWIFT and the manager's records for each fund. Reconciling items are investigated and resolved in a timely manner by Operations as evidenced by annotation on the cash reconciliation.	For a selection of days and funds, KPMG obtained the automated cash reconciliations and inspected for evidence that they were being performed and that un-reconciled items were investigated and resolved in a timely manner by Operations as evidenced by annotations on the reconciliation No exceptions noted.
3.3.2	Holdings are reconciled with custodian positions on a daily basis at a security transaction level by the Custody Reconciliation team and a monthly security reconciliation is carried out at both custodian and fund levels by each team, with any issues identified and resolved as evidenced by the annotated security reconciliations for stocks that have aged over 10 days.	For a selection of days and securities, KPMG obtained the daily custodian positions reconciliations and inspected for evidence that they were being carried out and that any issues identified were resolved by the Custody Reconciliation team as evidenced by the reconciliation annotation. No exceptions noted. For a selection of months and funds, KPMG obtained the monthly security reconciliations and inspected for evidence that they were being carried out and that any issues identified were resolved by the Custody Reconciliation team as evidenced by the reconciliation annotation for stocks that have aged over 10 days No exceptions noted.

3.4 Investment management fees and other account expenses are accurately calculated and recorded.

All initial investment management fee set-ups and changes to fee information are independently checked and authorised. Fee rates are input to the fund accounting system as part of the fund set-up as outlined in section 1.1. An estimated amount for quarterly custody fees is accrued in Quasar for each active fund. On a monthly basis, custodian custody fees are compared to the Quasar figure by fund accounting and any fees outside of tolerances are queried with the custodian.

Client specific unitised fund (CSUF) and Qualifying Investor Alternative Investment Fund (QIAIF or QIF) fund charges are calculated manually by the Senior Finance Analyst in the Investment Finance team. Complex invoices are reviewed by a Finance Manager for accuracy and completeness and subsequently reviewed by the Client Relationship manager (CRM).

	Control procedure	Testing performed by KPMG LLP and Results
3.4.1	On a quarterly basis, client specific unitised fund (CSUF) and QIF charges are calculated manually by the Investment Finance team. These complex invoices are reviewed by a second member of the team for completeness and accuracy and subsequently reviewed by the CRM as evidenced by the invoice sign-off.	For a selection of quarters and CSUF and QIF funds, KPMG obtained the complex invoices and inspected for evidence that they were prepared and reviewed by a second member of the Investment Finance team and subsequently reviewed by the CRM as evidenced by invoice sign-off. No exceptions noted.
3.4.2	All initial investment management fee set-ups and changes to fee information are independently checked and authorised by members of the invoice processing team as evidenced by electronic sign-off in thinkFolio.	For a selection of initial investment management fee set-ups and amendments, KPMG inspected the system and confirmed that these were subject to an independent check and authorisation by members of the invoice processing team as evidenced by electronic sign-off on the system. No exceptions noted.
3.4.3	Fee rates are input to the fund accounting system (Scope) as part of the fund set- up. Charges are then calculated automatically by the system during the weekly valuation process conducted by the Finance team.	KPMG observed the input of fee rates Scope and confirmed through reperformance that the system had calculated management fees automatically. No exceptions noted.
3.4.4	On a monthly basis, an estimated amount for monthly custody fees is calculated automatically in Quasar for each active fund. Custodian fees are compared to the Quasar figure by Fund Accounting and any fees outside of tolerances (the greater of +10% or £100) are investigated and resolved with the custodian. Investigation and resolution is evidenced by annotation on the Excel reconciliation and sign-off of the custody fee checklist by Operations.	For a selection of months, KPMG obtained the custody fee reconciliation and inspected for evidence that the tolerance checks on custody fees were carried out and discrepancies investigated/escalated as evidenced by the sign-off of the custody fee checklist by Operations. No exceptions noted.

3.5	**Pooled funds are priced and administered accurately and in a timely manner** Security prices are independently maintained by the Data Management Office team through automated security prices feeds. Movements outside of tolerance are reviewed annually by the Asset Pricing Committee. Price changes are subject to segregation of duties where one team 'unlocks' the price and a second team performs the update. Independent reviews of unit holding information, fund valuations and unit prices are performed by Investment Operations, before being validated and upload into the fund administration system.	
	Control procedure	**Testing performed by KPMG LLP and Results**
3.5.1a	The current security prices are maintained by the Asset Pricing Team which is independent of the Fund Managers. Automated security price feeds are received from external sources on a daily basis. Exception reports are created for any price movements outside the set tolerances (tolerances are reviewed on an annual basis by the Asset Pricing Committee) prescribed in Quasar, where prices received have not changed within a set period or where no price has been received. Each item on the exception reports is investigated and resolved by a member of the Asset Pricing team and evidenced by annotation on the exception packs and sign-off on the daily checklist.	For a selection of days, KPMG obtained the daily exception packs and inspected for evidence that the security pricing was administered by the Asset Pricing team and that any exceptions were investigated and resolved as evidenced by annotation on the daily exception packs or sign-off on the checklist. No exceptions noted.
3.5.1b	The exception reports highlighting security price movements outside the set tolerances (5% for equity and 2% for bonds) and their investigation and resolution are reviewed by a Pricing Senior. The review and approval of resolution is evidenced by annotation on the daily exception packs and sign-off on the daily checklist by the Pricing senior.	For a selection of days, KPMG obtained the daily checklist reviewed by a Pricing Senior and inspected for evidence that a review of the exceptions investigation and resolution by the Pricing team was undertaken as evidenced by sign-off by the Pricing senior on the checklist No exceptions noted.
3.5.2	Segregation of duties exists over any subsequent price changes with any adjustments requiring the Valuations team to ‘unlock’ the price and the Pricing team to update the price on the system.	KPMG observed the system audit trail and inspected that the Valuation team had to 'unlock' prices in order for the Pricing team to make a manual price change. No exceptions noted.
3.5.3	Fund valuations and unit prices are automatically generated at each valuation date, based on the valuations of the underlying securities, indices, accruals and cash. Independent reviews of the valuations control reports are carried out and evidenced on the valuation checklist for all fund valuations generated based on the fund valuation frequency as evidenced by sign-off by the Investment Operations team and these fund valuations are compared to benchmark indices. Once agreed, prices are automatically uploaded into the fund administration system.	For a selection of funds, KPMG obtained the weekly valuation control reports and inspected for evidence that the fund valuations and unit prices were subject to independent reviews by the relevant individuals as evidenced by sign-off by the Investment Operations team on the valuation checklists. No exceptions noted.

3.5.4	On a weekly basis, a reconciliation of unit holding information is undertaken between records held on the administration systems and imported units by the Investment Operations team. Any exceptions are investigated and resolved by the PMC Valuations team, with assistance from the PMC TA team as evidenced by the annotated reconciliation.	For a selection of weeks, KPMG obtained the weekly unit holder reconciliations and inspected for evidence that they were performed and exceptions investigated and resolved as evidenced by the annotated reconciliation performed by the PMC TA team. No exceptions noted.

4	**CASH MANAGEMENT AND SAFEGUARDING OF ASSETS**
	LGIM ensures that market standard custody agreements and segregated custody accounts are in place with their appointed custodians. Regular monitoring of the on-going credit worthiness of appointed custodians is carried out and regular business relationship and service level agreement review meetings are held with custodians. LGIM maintains contingency plans to move assets to another custodian were an existing custodian to begin to appear in danger of default. Investment Operations check on a monthly basis that each portfolio has a unique safekeeping number at the custodian to aid segregation of assets. System constraints ensure that un-invested cash is only placed with a select list of approved counterparties and that suitable diversification takes place to minimise counterparty credit risk. The counterparty list is regularly monitored and is amended to reflect credit rating downgrades or difficult market conditions.
4.1	**Un-invested cash is managed with regard to diversification of risk and security of** funds System constraints ensure that cash can only be deposited with approved money market counterparties. All money market counterparties must maintain a minimum credit standard. Compliance with this standard is monitored on an on-going basis by the Guideline Management and Control team Portfolio Monitoring team with output being provided to the Counterparty Oversight Group (COG) Any deposits over a minimum size must be placed with a number of approved counterparties to diversify risk. The number of counterparties is approved by the COG and details are loaded onto the exposure management system. Dealers trigger on-screen warnings if a trade breaches these limits.

	Control procedure	**Testing performed by KPMG LLP and Results**
4.1.1	System constraints on the Exposure Management System (EMS) ensure that cash can only be deposited with approved money market counterparties and that counterparty limits are held. Counterparties are approved through the process described in section 2.3.	KPMG confirmed through observation of a member of the GTT team placing a trade that the exposure management system details the counterparty limits and that cash deposits could only be placed with a counterparty that had been set up on the order management system and were within the counterparty limits. No exceptions noted. Testing on counterparty approval is described in section 2.3. No exceptions noted.

4.1.2	Credit ratings for money market counterparties are monitored electronically by the Portfolio Monitoring system. When a counterparty's credit rating drops below a specified threshold, it is removed from the approved counterparty list in line with LGIM's Counterparty Credit Risk Policy	KPMG enquired of management whether any instances of Money Market counterparties falling below the credit limit occurred during the period and were informed no instances had occurred. Since there were no instances, the operating effectiveness of the control could not be tested.
4.1.3	Counterparty concentration limits are held on the exposure management system and Dealers are alerted by on-screen warnings if a trade breaches these limits and are prevented when attempting to place a trade. Special approval must be obtained in order for the deal to be made by the Fund Manager via email.	KPMG confirmed through observation of the exposure management system that dealers were alerted and prevented when attempting to place trades that would breach counterparty concentration limits. No exceptions noted. KPMG enquired of management whether any instances of concentration limits requiring special approval occurred during the period and were informed no instances had occurred Since there were no instances, the operating effectiveness of this part of the control could not be tested.

4.2	**Investments are properly registered and client money segregated** Daily reconciliations are performed against bank account statements and manager's records as well as holdings and custodian positions. Reconciling items are investigated and resolved on a timely basis.	
	Control procedure	**Testing performed by KPMG LLP and Results**
4.2.1	On a daily basis, an automated cash reconciliation is performed between the bank account statements received via SWIFT and the manager's records for each fund. Reconciling items are investigated and resolved in a timely manner as evidenced by the cash reconciliation annotation.	For a selection of days and funds, KPMG obtained the automated cash reconciliations and inspected for evidence that they were being performed and that unreconciled items were investigated and resolved in a timely manner as evidenced by annotation on the reconciliation No exceptions noted.
4.2.2	Holdings are reconciled with custodian positions on a daily basis at a security transaction level by the Custody Reconciliation team and a monthly security reconciliation is carried out at both custodian and fund levels by each team, with any issues identified and resolved as evidenced by the annotated security reconciliations for stocks that have aged over 10 days.	For a selection of months and funds, KPMG obtained the monthly security reconciliations and inspected for evidence that they were being carried out with any issues identified and resolved by the Custody Reconciliation team as evidenced by the reconciliation annotation. No exceptions noted. For a selection of days, KPMG obtained the daily custodian positions and inspected for evidence that they were being carried out with any issues identified and resolved by the Custody Reconciliation team as evidenced by the reconciliation annotation for stocks that have aged over 10 days. No exceptions noted.

5	MONITORING COMPLIANCE	
5.1	**Client portfolios are managed in accordance with investment objectives, monitored for compliance with investment limits and restrictions and performance is measured** Formal fund investment guidelines are established for each fund and are loaded into the guideline monitoring systems (MIG 21/CRD) and the pre-trade compliance tool, Bloomberg AIM. Each Both systems monitor trading activity and flag identified breaches potential breaches of investment guidelines to the Portfolio Monitoring GMC team (for MIG 21 this is done via the internal system BTFS). The Guideline Monitoring and Control Portfolio Monitoring team then investigates the breach and raises a breach report if necessary. This is circulated to the fund manager, the client relationship manager and Operational Risk. Complex investment guidelines that cannot be programmed in the guideline monitoring systems are manually monitored on a periodic basis. A sample of manual monitoring tasks is reviewed on an annual basis by the GMC team. For PMC pooled funds, performance figures are calculated automatically by the pooled fund administration system (Scope). For the SICAV, OEIC and QIAIF funds, valuations are calculated by their respective administrators. Where these funds are wrapped in PMC units, the Net Asset Values feed into Scope for the PMC performance calculation. Otherwise, performance is calculated and published by an external provider (Lipper).	
	Control procedure	**Testing performed by KPMG LLP and Results**
5.1.1	A breaches log is maintained by the Guideline Management and Control (GMC) team for manual and automated guideline breaches. All guideline breaches are investigated and escalated on a timely basis by the GMC team and this is evidenced by an annotated breach report being issued upon resolution with annotation on delays if required.	For a selection of automatically and manually monitored guideline breaches, KPMG obtained the breach report and inspected for evidence that breaches were investigated on a timely basis, escalated and monitored by the GMC team. Where breach reports were delayed, KPMG inspected the report to confirm that a valid reason was noted as evidenced by the annotation on the breaches report No exceptions noted.
5.1.2	The Scope algorithms that calculate pooled fund performance are owned by the Performance Team, which is independent of the fund managers. Any changes to the algorithms are tested by the Performance team before they are made live. This is evidenced by the development team obtaining email sign off by the performance team prior to changes being made live.	KPMG enquired of management whether any instances of changes to the algorithms within Scope occurred during the period and were informed no instances had occurred. KPMG inspected the Scope system version control and confirmed that no changes to algorithms have been made in the year. Since there were no instances, the operating effectiveness of the control could not be tested.
5.1.3	On an annual basis for all rules not coded into MIG 21/CRD a random sample is selected for testing to ensure the monitoring has been performed, evidenced and any breaches escalated to the Guideline Management and Control team as evidenced by the annotation on the investigation spread sheet.	KPMG obtained the annual review and inspected the evidence of underlying checks to confirm that rules not coded in MIG21/CRD were monitored and breaches, where identified, were escalated to the Guideline Management and Control team as evidenced by the annotation on the investigation spread sheet. No exceptions noted.

5.2	**Outsourced activities are properly managed and monitored and conflicts of interest identified to clients** LGIM adheres to a supplier governance plan that includes requirements such as each essential supplier should have a named relationship manager, SLAs must be set up and monitored, regular meetings must be held, and contingency plans should be made in case the supplier fails to fulfil the contracted requirement.	
	Control procedure	**Testing performed by KPMG LLP and Results**
5.2.1	On a monthly basis, performance of outsourced service providers is monitored by a review of management information reports together with monthly teleconference communication, as evidenced by review of the monthly management information reports and meeting minutes from the teleconference.	For a selection of months and outsourced service providers, KPMG obtained the monthly management information reports and minutes of meetings with the outsourced service provider and inspected for evidence that performance was monitored as evidenced by discussion of actions from meetings with outsourced service providers within meeting minutes. No exceptions noted.
5.2.2	On an annual basis, reports covering the adequacy of internal controls are received from all appointed custodians by Operations. These are reviewed for exceptions by the Operations team for any impact on the business as evidenced by any relevant material concerns being discussed/investigated with the custodian for appropriate action as per the annotation on the relevant report, copies of which are retained.	For a selection of custodian reports, KPMG obtained the custodians' most recent internal controls reports and inspected for evidence that they were obtained, reviewed and all significant issues investigated on an annual basis as evidenced by the annotated report which is retained. No exceptions noted.
5.2.3	A key supplier list is maintained by supplier managers to record the details of all key suppliers and track completion of the required activities as laid out in the Group Outsourcing and Essential Supplier Services Policy. This is overseen by the Supplier Management Committee that has overall responsibility for ensuring the Key Supplier List is an up to date accurate reflection of the current key suppliers providing services to the companies within the LGIM Group. On an annual basis the Chairperson of the Supplier Management Committee provides an update to the LGIM Executive Risk Committee on the completeness of the key supplier list and the progress of activities demonstrating adherence to the Group Outsourcing and Essential Supplier Services Policy including if any conflict of interests identified have been disclosed to clients. Discussion and any required actions are documented in the LGIM Risk and Compliance Committee minutes, copies of which are retained.	KPMG obtained the report detailing the annual review of key suppliers and the corresponding Executive Risk Committee minutes and inspected for evidence that the update to the key supplier list was discussed (including if there are any conflicts of interest) as evidenced by the meeting minutes. No exceptions noted.

5.3 Transaction errors (including guideline breaches) are rectified promptly and clients treated fairly

Errors are reported through the operational risk errors process and recorded on the risk management system as a Control Environment Action Log CEAL. On a monthly basis the operational risk team reconciles the CEAL log against financial loss data provided by Finance to ensure that all loss data has an accompanying CEAL. All CEALs reported over the course of each month are presented to the Risk and Compliance Committee with the higher severity CEALs reviewed in detail. Regulatory issues and breaches are reported to Compliance and evidenced through the breach reports.

	Control procedure	Testing performed by KPMG LLP and Results
5.3.1	On a monthly basis, the Finance team produces a report of all amounts paid in respect of transaction errors or compensation payments; the Operational Risk Management team performs a reconciliation between the Finance report and the RMS errors log to ensure that all entries on the Finance report correspond to an entry in RMS and that any outstanding error logs (CEALs) have been raised. This is evidenced using the reconciliation and form annotation.	For a selection of months, KPMG obtained the Operational Risk Management reconciliation and inspected for evidence that any outstanding CEALs had been raised promptly and discrepancies were investigated via the form as per the reconciliation annotation. No exceptions noted.
5.3.2	On a monthly basis, errors are collated into a CEAL report by Operational Risk team and included in the pack and sent to the ERC. The pack and all CEAL reports are reviewed at the meeting and any actions to be taken are noted as evidenced by meeting minutes of the review which are retained.	For a selection of months, KPMG obtained the ERC meeting minutes and inspected for evidence that error reports raised were reviewed by the ERC as per the minutes. No exceptions noted.
5.3.3	On a monthly basis, the Compliance team reviews details of breaches and where applicable assigns a regulatory rule reference to ensure that all regulatory issues are recorded and an email is sent from the Compliance to the Operational Risk Management team.	For a selection of months, KPMG obtained the error reports and related email support and inspected for evidence that the reports were reviewed by the Compliance team as evidenced by the email sent to the Operational Risk Management team. No exceptions noted.

5.4 Counterparty exposures are monitored

All money market counterparties must maintain a minimum credit standard. Compliance with this standard is monitored on an on-going basis by the Guidelines Management and Control team with output being provided to the Counterparty Oversight Group (COG). When a counterparty's credit rating drops below a specified threshold, it is removed from the approved counterparty list in line with LGIM's Counterparty Credit Risk Policy.
Details of money market counterparty concentration limits are held on an Exposure Management System which displays details of remaining balances available to be placed with counterparties. Dealers trigger on screen warnings if a trade breaches these limits. Deposits are then monitored by the Portfolio Monitoring team to ensure they are in accordance with these limits.

	Control procedure	Testing performed by KPMG LLP and Results
5.4.1	System constraints on the Exposure Management System (EMS) ensure that cash can only be deposited with approved money market counterparties and that counterparty limits are held. Counterparties are approved through the process described in section 2.3	KPMG confirmed through observation that the exposure management system details of counterparty limits were held and that trades could only be placed with a counterparty that had been set up on the order management system. Testing on counterparty approval is described in section 2.3. No exceptions noted.
5.4.2	On a bi-monthly basis, the COG reviews the list of existing counterparties and exposures to assess if they should still be maintained as counterparties based on policy criteria. Based on the review, the COG confirms they are still eligible and distributes results to relevant departments when changes have arisen. The COG notifies any changes to the Investment Oversight Committee (IOC) where relevant as evidenced by the meeting minutes.	For a selection of months, KPMG obtained the COG meeting minutes and inspected for evidence that a review of counterparties took place, and if counterparties were identified as no longer meeting the minimum credit criteria, they were subsequently removed from the system and noted in the meeting minutes as necessary. No exceptions noted.
5.4.3	Counterparty concentration limits are held on the exposure management system and Dealers are alerted by automatic on-screen warnings if a trade breaches these limits. Special approval must be obtained in order for the deal to be made by the Fund Manager via email.	KPMG confirmed through observation of the exposure management system that dealers were alerted and prevented when attempting to place trades that would breach counterparty concentration limits. There were no instances in the year of concentration limits requiring special approval. No exceptions noted.
5.4.4	A breaches log is maintained by the Guideline Management and Control team for manual and automated guideline breaches. All guideline breaches are investigated and escalated on a timely basis by the GMC team and this is evidenced by an annotated breach report being issued upon resolution.	For a selection of automatically and manually monitored guideline breaches, KPMG obtained the breach report and inspected for evidence that breaches were investigated on a timely basis, escalated and monitored by the GMC team. Where breach reports were delayed, KPMG inspected the report to confirm that a valid reason was noted as evidenced by the annotation on the breaches report. No exceptions noted.

6	REPORTING TO CLIENTS
6.1	**Client reporting in respect of portfolio transactions, holdings and performance, commission and voting is complete and accurate and provided within required timescales** LGIM provides monthly valuations and quarterly investment reports to meet client reporting requirements. These are largely system generated, but where manual input is required the information input to the system is checked independently by a separate individual. Reports usually include details of investment holdings, transactions during the period, performance, dealing costs, investment commentary and market background.

	Control procedure	Testing performed by KPMG LLP and Results
6.1.1	On a quarterly basis, client reports are generated automatically in Vermillion. Where manual input is required, information input to the system is reconciled against the client mandate by a separate individual of the Client Reporting team. Reports contain details of holdings, transactions, performance, dealing costs, and fund commentary and market background. The peer review is evidenced by the electronic checklist which is retained in the system for manually updated reports.	For a selection of quarters and funds, KPMG obtained the quarterly reports and inspected the electronic checklist and the document image processing system for evidence that they had been generated and reviewed. For a selection of funds in the quarter, if manual input was required, KPMG inspected for evidence that the report was reviewed by a separate individual of the Client Reporting team before it was issued. No exceptions noted.
6.1.2	On a quarterly basis, a client deadline report, comparing dates of report delivery against client deadlines, is maintained and reviewed by management Client Reporting Team as evidenced by the RMS responses/Vermilion system reports which are retained in the system.	For a selection of quarters, KPMG obtained the RMS responses and inspected for evidence that management maintained and reviewed the client deadline report for timely delivery as evidenced by the system retained report. No exceptions noted.

7	RESTRICTING ACCESS TO SYSTEMS AND DATA
7.1	**Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals** LGIM uses electronic ID card technology to restrict physical access into and within its offices. The Security team, upon notification from HR or line managers of leavers, removes access such that the access card is removed and destroyed or access is set to expire on the leaving date. Computer equipment and storage media are hosted in secure data centres to which only authorised persons are granted access. The data centre provider issues SOC I and SOC II reports annually covering the period November to October.

	Control procedure	Testing performed by KPMG LLP and Results
7.1.1	Physical access control systems, including badge access, mantraps at the entrance, visitor logs and mandatory escort for visitors are in place at each data centre used by LGIM.	KPMG reviewed the data centre SOC reports and noted that there are physical access controls, including badge access, mantraps at the entrance, visitor logs and mandatory escort for visitors in place at each data centre used by LGIM. No exceptions noted.

7.1.2	Physical access to LGIM premises is removed from employees upon receipt of a leavers email alert from ServiceNow, within one working day of the leaver's last day.	For a selection of leavers who had access to the LGIM premises, KPMG inspected the access card system disable dates and noted that physical access was removed within one working day of the leaver's last day. **Exception noted:** For 2 out of 25 leavers selected, KPMG noted that the user access cards were disabled after more than one working day of the leaver's last day. KPMG inspected the access card logs for these users and noted that the access cards had not been used after the last working day.
7.2	**Logical access to computer systems programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques.** Logical access to the LGIM network, applications and infrastructure is controlled through password protection. Password length and complexity is set by the IT department and is system-enforced. Access to applications and systems is managed through formalised Access Control Standards. Access to applications and systems is granted to users in line with appropriately authorised requests. Upon notification of a leaver or required access removal, access is removed within one working day of the required removal date. User access and entitlements to applications and infrastructure are recertified on a periodic basis, as per the scheduled frequency in the Access Control Standards.	
	Control procedure	**Testing performed by KPMG LLP and Results**
7.2.1	Access to applications and systems is granted to employees upon line manager approval.	For a selection of access creations and modifications, KPMG inspected the access request forms and ServiceNow tickets to determine whether approval was provided by line management and access to applications and systems had been granted according to the request. No exceptions noted.
7.2.2	Logical access to the LGIM network, applications and infrastructure is controlled through password protection.	KPMG inspected the password configuration for the network and in-scope applications to determine whether appropriate password complexity was enabled. No exceptions noted.
7.2.3	User access recertification for applications is performed as per the agreed recertification schedule in line with the LGIM Access Control Standards. Subsequent actions such as access modification or de-provisioning are initiated and tracked on Service-Now to completion.	KPMG inspected the bi-annual user access recertification and noted that LGIM applications users had been reviewed in line with the recertification schedule defined in the LGIM Access Control Standards. KPMG inspected the recertification review actions and system access and noted that subsequent access modifications and de-provisioning had been performed and logged in Service-Now. No exceptions noted.

7.2.4	User access to IT network, infrastructure and applications is disabled within one working day of the staff departure date.	For a selection of leavers, KPMG inspected Service-Now tickets and system disable dates to determine whether access to the IT network, infrastructure and applications had been disabled within one working day of the staff departure date. **Exception noted:** For 3 out of 25 leaver accounts selected KPMG noted that the users access had been disabled after one working day of their departure date. We noted that no Active Directory accounts out of the full population of leavers were accessed after the HR termination date.
7.2.5	There is a formal annual recertification process to review accounts with privileged access to the databases and operating systems supporting the in scope applications and where inappropriate access is identified a ServiceNow ticket is logged for resolution.	KPMG inspected the annual recertification of databases and operating systems supporting the in scope applications and noted that privileged infrastructure accounts had been reviewed. KPMG inspected the recertification review actions and system access and noted that subsequent access modifications and de-provisioning had been performed and logged in Service-Now. No exceptions noted.
7.3	**Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles** Access rights to Quasar, the core fund accounting and valuation system, have been defined to enforce a segregation of duties over maker-checker controls within the trade life cycle. An individual is prevented from initiating and authorising trades.	
	Control procedure	**Testing performed by KPMG LLP and Results**
7.3.1	LGIM Risk Management has defined toxic combinations for Quasar access rights. Quasar enforces maker-checker controls within the trade life cycle, so that one individual cannot initiate and authorise a trade.	KPMG inspected the initiation and authorisation of a trade within Quasar and noted that the system prevented the same individual from initiating and authorising the trade. No exceptions noted.
8	**PROVIDING INTEGRITY AND RESILIENCE TO THE INFORMATION PROCESSING ENVIRONMENT, COMMENSURATE WITH THE VALUE OF THE INFORMATION HELD, INFORMATION PROCESSING PERFORMED AND EXTERNAL THREATS**	
8.1	**IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner** IT Operations perform daily monitoring of business critical scheduled processes over applications and systems. Errors or failures in processing are logged and investigated by the IT operators and documented in the IT Operations Checklists. The details recorded includes run times, errors/failures and how these were resolved (re-runs or incidents), and the status of services. Changes to the scheduled jobs are made via the existing change management process.	

	Control procedure	Testing performed by KPMG LLP and Results
8.1.1	IT operators monitor scheduled processes and record these on a checklist every morning. They promptly investigate and resolve or escalate any errors in processing.	For a selection of dates, KPMG inspected the IT Operations Checklists and noted that monitoring was performed by the IT operators and exceptions were recorded on Service-Now as incidents. For a selection of incidents, KPMG inspected the resolution details and noted that exceptions were investigated and resolved in line with Service-Now SLAs according to incident priority. No exceptions noted.
8.1.2	Monitoring of network, database and application services is performed and events and disk usage space statistics reported to IT Management on a monthly basis.	For a selection of months, KPMG inspected the reports on network, database and application services events and disk usage and noted that the reports were reviewed by the Head of Infrastructure on a monthly basis. No exceptions noted.
8.1.3	Changes to job schedules are made via the existing change management process. For changes that alter user input/output or functionality, nominated business system users conduct user acceptance testing (UAT) and approve the migration of changes to the production environment on completion of UAT. In case of a technical change, i.e. a change that does not affect user input/output or functionality, nominated IT team members test the change and IT managers provide formal approval to go live.	For a selection of changes, including changes to job schedules for the in scope systems, KPMG inspected the change documentation and noted that testing had been signed off by appropriate users prior to migration to the production environment. No exceptions noted.
8.2	**Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure** LGIM receives and sends data transmissions to counterparties via OMGEO and SWIFT messages, which are industry standard information exchange services and LGIM uses industry standard SFTP solutions to provide controlled, secure communications to/from counterparties. The transmission protocols include alerts for files which have not been received or where transmission failures are noted. Trade confirmation and settlements are automatically matched in Quasar to messages from counterparties and exceptions are investigated and resolved.	

	Control procedure	Testing performed by KPMG LLP and Results
8.2.1	Trade confirmation and settlement instructions transmitted between the organisation and its counterparties are sent and received via OMGEO & SWIFT. Messages are automatically matched with those from counterparties and any exceptions are investigated and resolved promptly.	For a selection of trade confirmation and settlement instructions on Quasar received via OMGEO and SWIFT, KPMG inspected the message details and status and noted that the messages were automatically matched with the counterparty. For a selection of trade confirmations and settlement instructions which were not successfully matched, KPMG inspected the message details and evidence of investigation and noted that the exceptions were investigated and resolved. No exceptions noted.
8.2.2	Index price movements and fund prices are authorised and reviewed by separate members of the LGIM Investment Operations team and signed-off electronically, through online authorisation and review of the daily indices exception report. In the event an expected file is not received on time this is investigated and noted in the daily indices electronic report	For a selection of dates, KPMG inspected the index price movements and fund prices and noted that each movement was reviewed and signed-off electronically by separate members of the LGIM Investment Operations team. For a selection of dates, KPMG inspected the index price movements and fund prices and noted that in the event an expected file was not received on time, it was investigated and noted in the daily indices electronic report. No exceptions noted.
8.3	**The physical IT equipment is maintained in a controlled environment** LGIM's IT equipment is maintained in a secure environment which is controlled and monitored by the hosting provider through a dedicated Building Management System (BMS). The BMS is used to monitor environmental controls and alert data centre personnel to potential issues within the data centre, including critical electrical components, power management equipment, heating, ventilation, and air-conditioning (HVAC) equipment, and fire detection and suppression equipment. The hosting provider issues SOC I and SOC II reports annually covering the period November to October.	
	Control procedure	**Testing performed by KPMG LLP and Results**
8.3.1	Environmental controls, including fire detection, fire suppression, temperature and humidity monitoring equipment are installed at each centre used by LGIM. Scheduled maintenance procedures are performed to ensure that equipment is working properly.	KPMG reviewed the data centre SOC reports and noted that there are environmental controls, including fire detection, fire suppression, temperature and humidity monitoring equipment in place at each data centre used by LGIM. No exceptions noted.
8.3.2	The data centre facilities used by LGIM are monitored 24x7 by facilities engineers. On-site or on call staff are alerted by the Business Management System (BMS) for system exceptions.	KPMG reviewed the data centre SOC reports and noted that there are 24x7 facility monitoring controls in place. BMS alerts staff for any system exceptions. No exceptions noted.

8.4	**Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g., firewalls, anti-virus etc.)** LGIM IT has a dedicated Security Team that provides oversight over information security areas including network security such as firewalls and intrusion detection, application security, server and desktop security, and data security. Anti-virus software is installed on all desktops and servers, and additional layers of security are provided by content and packet intrusion detection systems, and centralised firewall infrastructure.	
8.4.1	Network monitoring is performed and reports on network security incidents are reviewed on a monthly basis by the Governance, Risk and Compliance Committee.	KPMG inspected the security tool used to perform network monitoring and noted that monitoring of the network was configured. For a selection of months, KPMG inspected the packs and minutes for the Governance, Risk and Compliance Committee and noted that network security incidents were reviewed. No exceptions noted.
8.4.2	Anti-Malware prevention measures are in place for desktops and servers as per the documented Anti-Malware standards. Incidents and statistics are recorded, fully investigated and reviewed on a monthly basis by the Governance, Risk and Compliance Committee.	KPMG inspected the Anti-Malware tools in place for desktops and servers and noted that measures were in place in line with the documented Anti-Malware standards. For a selection of months, KPMG inspected the packs and minutes for the Governance, Risk and Compliance Committee and noted that malware statistics and incidents were reviewed. No exceptions noted.
9	**MAINTAINING AND DEVELOPING SYSTEMS HARDWARE AND SOFTWARE**	
9.1	**Development and implementation of new systems, applications and software and changes to existing systems, applications and software, are authorised, tested, approved and implemented** Business cases for new system developments are submitted to the appropriate Change Boards for evaluation and authorisation. Version control processes are adhered to for all systems and electronic records of all changes are retained. Development and Production services are segregated or adhere to a formalised emergency access process which is monitored by IT Operations and the respective Platform Lead. All new systems (in-house and third-party) are independently tested by an in-house Quality Assurance function and all functional releases are also subject to a further user acceptance testing phase before being released into the live environment.	
	Control procedure	**Testing performed by KPMG LLP and Results**
9.1.1	Development personnel only have access to development code and are unable to update live production code. “Write/Change” and “Delete” access rights over live production code are restricted to authorised individuals only through the use of group memberships, to restrict migration of programs to production.	KPMG inspected the users with access to development environments, source code and the ability to perform changes to live production code to determine whether any individuals had the ability to develop and perform changes to production. No exceptions noted.

9.1.2	Quasar support accounts are used by Production Services to fix issues in production. The usage of the support accounts is produced daily by IT Operations and reviewed by the IT Quasar Platform lead on a daily basis.	For a selection of dates, KPMG inspected the Quasar Morning Checklists and noted that Quasar production support account usage was logged, linked to a corresponding Service-Now record and reviewed by the IT Quasar Platform lead. No exceptions noted.
9.1.3	Business cases for new system developments & projects are submitted to one of the three Sub Change Board's for approval (Investments, Distribution or COO / CRO). Project's requiring funding in excess of £500k are submitted to the main Change Board for approval.	For a selection of new system developments and projects, KPMG inspected the business case documentation and noted that it had been approved by one of the three Sub Change Boards or the main Change Board for projects over £500k. No exceptions noted.
9.1.4	The version control process is documented as part of the build procedure. Versioning tools are used to store and transfer code. A common development process is adhered to for all systems and electronic records retained of all version changes retained within the versioning tool.	KPMG inspected the version control tools and build procedures for LGIM developed systems and noted that versioning tools were used to store and transfer code and electronic records of version changes. No exceptions noted.
9.1.5	Changes to systems have to be submitted for approval by IT. The exception to this is standard changes which are pre-approved. The Change Advisory Board (CAB) prioritises, approves major/significant changes. Approvals are documented in CAB minutes and changes are tracked to completion through the CMS.	For a selection of changes, KPMG inspected the CMS records and CAB minutes and noted that the changes had been approved by appropriate management and by the Change Advisory Board (CAB) for major/significant changes. No exceptions noted.
9.1.6	For changes that alter user input/output or functionality, nominated business system users conduct user acceptance testing (UAT) and approve the migration of changes to the production environment on completion of UAT. In case of a technical change, i.e. a change that does not affect user input/output or functionality, nominated IT team members test the change and IT managers provide formal approval to go live.	For a selection of changes, KPMG inspected the CMS records and testing sign-offs and noted that changes to user input/output or application functionality were acceptance tested by appropriate end users prior to migration into the production environment. For a selection of technical changes, KPMG inspected the CMS records and testing sign-offs and noted that changes were tested by appropriate IT management prior to migration into the production environment. No exceptions noted.
9.1.7	Emergency changes follow the overall Change Management Policy. Emergency change requests are documented and subject to formal change management procedures including supporting documentation, back-out procedures and emergency approval by authorised IT and business personnel.	For a selection of emergency changes, KPMG inspected the CMS records and noted that the changes were approved by authorised IT and business personnel and had documented back-out procedures. No exceptions noted.

9.2	**Data migration or modification is authorised, tested and once performed, reconciled back to the source data** Data migrations or modifications are subject to the relevant authorisation and testing steps within the Development and Release process (refer to 9.1). The relevant business areas, supported by IT, are responsible for identifying appropriate additional checks over the migration.	
	Control procedure	**Testing performed by KPMG LLP and Results**
9.2.1	Data migration and modification is subject to checks over whether the data has been migrated from source to target completely and accurately. Evidence of the checks is retained as part of the migration.	KPMG enquired of management whether any instances of data migration on in scope applications occurred during the period and were informed no instances had occurred. Since there were no instances, the operating effectiveness of the control could not be tested.
9.2.2	Changes to underlying data are made following authorisation by an appropriate user or data owner. Authorisation is documented and retained.	KPMG enquired of management whether any instances of changes to underlying data occurred during the period and were informed no instances had occurred. Since there were no instances, the operating effectiveness of the control could not be tested.
10	**RECOVERING FROM PROCESSING INTERRUPTIONS**	
10.1	**Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.** Data and systems are replicated to an off-site recovery centre multiple times per day, depending on the criticality of the system or data as defined by policy. Recoverability of LGIM data and systems is tested annually by the business during scheduled business continuity tests.	
	Control procedure	**Testing performed by KPMG LLP and Results**
10.1.1	Data and systems are replicated at least daily to an off-site recovery centre.	KPMG inspected the back-up scheduler configuration and noted that data and systems were replicated to an off-site recovery centre multiple times per day, depending on the criticality of the system or data. For a selection of dates, KPMG inspected the IT Operations checklists and noted that data and software replication was monitored and errors had been logged and resolved as per control 8.1.1. No exceptions noted.

10.1.2	Recoverability of LGIM data and systems is tested annually by the business during scheduled business continuity tests.	KPMG inspected the annual recovery documentation for LGIM in scope systems and noted that the recoverability of LGIM data and systems was tested during scheduled business continuity tests. No exceptions noted.

10.2	**IT Hardware and software issues are monitored and resolved in a timely manner** Issues such as user reported events, hardware or software incidents are raised on the LGIM Service Management tool, as per the Incident Management policy. The tool is used to record all incidents, which are assigned an incident priority and investigated and resolved by specialist IT staff. The tool is monitored by the Service Desk team to prioritise incidents according to business impact and urgency.	
	Control procedure	**Testing performed by KPMG LLP and Results**
10.2.1	The LGIM Service Management tool is used to record all incidents reported by users and these are then followed up, investigated and resolved by specialist IT staff. Incidents are prioritised according to business impact and urgency.	For a selection of incidents, KPMG inspected the LGIM Service Management tool records and noted that the incidents were logged, investigated and resolved in a timely manner, in line with their prioritisation. No exceptions noted.
10.2.2	Reports are produced by the LGIM Service Management tool for IT management to review. Monthly analysis reports of incidents are included within the IT Management Committee. Root cause analyses are conducted of major incidents, identifying mitigating actions which are tracked to resolution within the Problem Management process.	For a selection of months, KPMG inspected the IT Management Reports and minutes noted that the monthly analysis of incidents, including root cause analysis and resolution of major incidents were reviewed by IT management. No exceptions noted.

10.3	**Business and information systems recovery plans are documented, approved, tested and maintained** The Business Continuity Management team is responsible for co-ordinating business continuity planning activity and this is overseen by the Business Technology Risk Committee (BTRC), which is chaired by senior management. The BTRC determines the strategy and has oversight of the Business Continuity Plans and recovery.	
	Control procedure	**Testing performed by KPMG LLP and Results**
10.3.1	The Business Technology Risk Committee (BTRC) comprising senior management receives reports from Business Continuity Plan (BCP) owners on a quarterly basis documenting testing results and actions, and provides direction and oversight in the development of existing BCPs.	For a selection of BCP reports, KPMG inspected the BTRC reports and minutes and noted that the committee had reviewed the BCP testing results and actions. Inspected the BTRC minutes and noted that the committee had reviewed and provided direction over the existing BCPs. No exceptions noted.

10.3.2	The business continuity teams have documented recovery plans that include: plan owner, review date, approver roles and responsibilities, and are reviewed on an annual basis.	For a selection of Business Continuity Plans (BCPs), KPMG inspected the plans and noted that each included the plan owner, date of review, approver, roles and responsibilities, and that it had been reviewed on an annual basis. No exceptions noted.

11	**MONITORING IT COMPLIANCE**	
11.1	**Outsourced activities are properly managed and monitored** All outsourcing relationships are monitored and controlled under the terms of the Group Outsourcing and Key Supplier Policy. The policy covers all stages of the relationship, from initiation of the arrangement, documentation of the relationship and on-going relationship management and oversight. Critical essential IT suppliers should have a named relationship manager, regular meetings must be held, and contingency plans should be made in case the supplier fails to provide the contracted requirement.	
	Control procedure	Testing performed by KPMG LLP and Results
11.1.1	LGIM adheres to a supplier governance plan that includes requirements such as critical essential suppliers should have a named relationship manager, regular meetings must be held, and contingency plans should be made in case the supplier fails to provide the contracted requirement.	KPMG inspected the governance plan over critical IT suppliers and noted that the accounts had a named relationship manager and contingency plan. For a selection of months, KPMG inspected the minutes for the Risk and Compliance committee and noted that the key vendor relationships were reviewed by the committee. No exceptions noted.

7. Complementary user entity controls

LGIM's processing of investment transactions for clients and its controls cover only a portion of the overall internal control environment for each client. LGIM alone cannot achieve a client's control objectives for processing transactions. Therefore, each client should evaluate its own internal controls in conjunction with the controls summarised in sections 5 and 6 of this report.

This section highlights other internal control considerations. Clients should evaluate their own internal controls to determine if appropriate procedures are in place to ensure a reliable communications system between themselves and LGIM:

- Clients should review account information in client confirmations, account statements and on the website to determine compliance with their investment instructions. Discrepancies should be reported to LGIM on a timely basis.

- Clients should promptly and carefully review their account balance and related activity statements. Discrepancies should be reported to LGIM on a timely basis.

- Instructions and information communicated to LGIM should be in accordance with the provisions in the investment management agreement (IMA) or other governing agreement.

- Clients should periodically update their investment guidelines or restrictions, and proposed changes to investment guidelines should be communicated promptly in writing to LGIM.

- To the extent that a client has online access to LGIM data, the client is responsible for establishing controls to properly administer user identifications and passwords, and to monitor user activity.

- Regular review and timely notification of changes in personnel from whom LGIM is authorised to take instruction.

The list above does not purport to be, and is not, a complete listing of controls that provide a basis for the assertions underlying clients' financial statements, nor does it extend to controls at other service organisation locations.

8. Management's response to exceptions noted

Control objective	Control procedure	Exception noted	Management response
3.1.1	On a daily basis, notification of income events are received via a direct market feed from IDS. All feed data is uploaded into a report automatically and any changes from the previous day are identified and investigated by the Operations team as evidenced by the primary generation checklist which is signed-off by Operations.	For 1 out of 25 days selected, KPMG noted that the there was no evidence that the checklist was reviewed.	In addition to a physical sign off on this daily checklist the manager electronically signs off this control daily on the Risk Management System (RMS). This electronic sign off was performed for this exception and reviewed by KPMG evidencing that this control was performed on the day so there was no control breakdown just a lack of a physical sign off.
7.1.2	Physical access to LGIM premises is removed from employees upon receipt of a leavers email alert from ServiceNow, within one working day of the leaver's last day.	For 2 out of 25 leavers selected, KPMG noted that the user access cards were disabled after more than one working day of the leaver's last day. KPMG inspected the access card logs for these users and noted that the access cards had not been used after the last working day.	The LGIM premises were not accessed after the leaving date for the noted individuals. In addition to revoking physical access in the building management system as part of this control, on the last day of employment all employees are exited from the premises and access cards returned to building security for formal destruction.
7.2.4	User access to IT network, infrastructure and applications is disabled within one working day of the staff departure date.	For 3 out of 25 leaver accounts selected KPMG noted that the users access had been disabled after one working day of their departure date. We noted that no Active Directory accounts out of the full population of leavers were accessed after the HR termination date.	The identified exceptions relate to isolated cases and there was no inappropriate access to systems and data after the termination dates. Detective controls are in place and regularly tested to monitor compliance with the leavers process.

Appendix 1 - terms of release of the 2018 AAF 01/06 / ISAE 3402 Report to prospective clients

Legal & General Investment Management (Holdings) Limited
One Coleman Street
London
EC2R 5AA
Tel: +44 (0)20 3124 3000

PRIVATE AND CONFIDENTIAL

Dear Prospective Customer

ISAE 3402 / AAF 01/06 Type II Reporting Accountants' Assurance Report

We attach a copy of a confidential Independent Reporting Accountants' Report (the "**Report**") on certain aspects of our internal controls environment and processes which has been prepared by KPMG LLP ("**KPMG**").

KPMG has agreed that we may disclose the attached Report to you, on the basis set out in this letter, to enable you to verify that a report has been commissioned by us and issued by KPMG in connection with our internal controls, subject to the remaining paragraphs of this letter, to which your attention is drawn.

KPMG's work was designed to meet our agreed requirements and the engagement activities were determined by our needs at the time. The Report should not be regarded as suitable to be used or relied on by any party other than us for any purpose or in any context.

In consenting to the disclosure of the Report to you KPMG does not assume any responsibility to you in respect of its work for us, the Report or any findings, conclusions, recommendations or opinions that KPMG has made in or connected with the Report and, to the fullest extent permitted by law, KPMG accepts no liability in respect of any such matters to you. If you rely on the Report, you do so at your own risk.

Except as required by law, the Report may not be copied, referred to or disclosed, in whole or in part, without KPMG's prior written consent. The Report and this letter are both confidential. Any disclosure of the Report beyond you and us, and any disclosure of this letter beyond you and us, may substantially prejudice our and/or KPMG's commercial interests. If applicable and you receive a request for disclosure of the Report or this letter under the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002 we would ask that in accordance with recommended practice, you let us and KPMG know and not make a disclosure in response to any such request without consulting both of us in advance and taking into account any representations made.

Yours faithfully

Legal & General Investment Management (Holdings) Limited