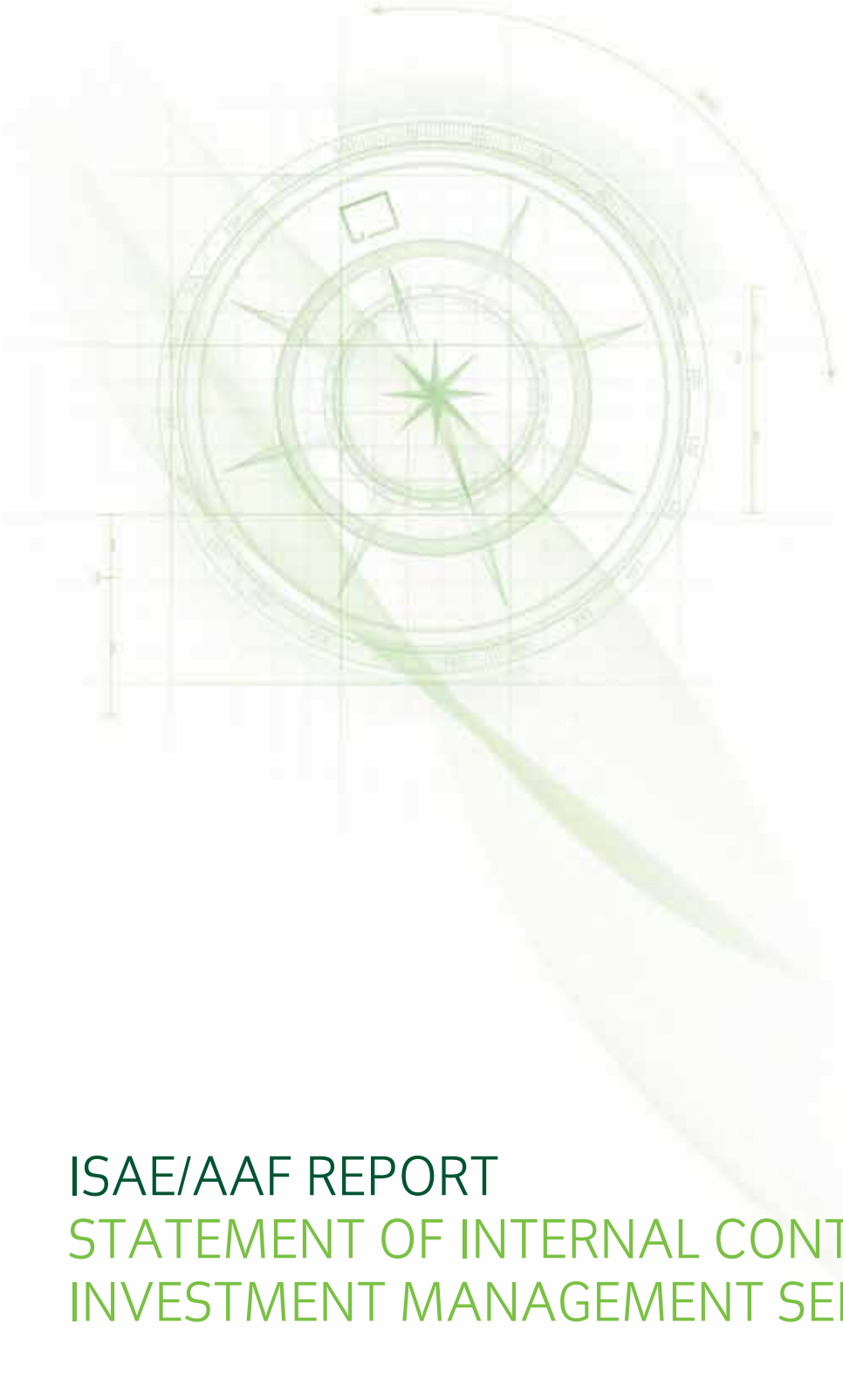
FOR PROFESSIONAL CLIENTS ONLY.
NOT TO BE DISTRIBUTED TO RETAIL CLIENTS.



ISAE/AAF REPORT
STATEMENT OF INTERNAL CONTROLS OVER INVESTMENT MANAGEMENT SERVICES

FOR THE YEAR ENDED 31 DECEMBER 2014

Insight INVESTMENT

A BNY MELLON COMPANY℠

Insight Investment is a leading asset manager focused on designing investment solutions to meet our clients' needs. Launched in 2002, Insight is responsible for assets under management of £362.5bn[1] across absolute return, fixed income, liability-driven investment, currency risk management, cash management, and multi-asset and specialist equity strategies.

[1] Data as at 31 December 2014. Insight's assets under management are represented by the value of cash securities and other economic exposure managed for clients.

CONTENTS

1. INTRODUCTION

1.1 SCOPE

This statement of internal controls over investment management services has been prepared in accordance with

- AAF 01/06 'Assurance reports on internal controls of service organisations made available to third parties', issued by the Institute of Chartered Accountants in England and Wales.
- ISAE 3402 "Assurance Reports on Controls at a Service Organisation" set out by the International Auditing and Assurance Standards Board.

Insight Investment Management Limited through its subsidiary Insight Investment Management (Global) Limited and Pareto Investment Management Limited (together referred to as 'Insight') act as discretionary investment manager and adviser for segregated and pooled fund clients typically sourced from pension funds, sovereign wealth funds, insurance groups and local authorities.

The Directors of Insight have prepared this statement of internal controls, setting out the controls and procedures adopted in the conduct of its investment management responsibilities. Other specific details regarding the scope and use of this report are found in the Report by the Directors and the Report by the Reporting Accountants.

This report comprises of the:

- Report by the Directors
- Overview of Insight's Control Environment
- Statement of internal controls together with the tests performed by the reporting accountants
- Report by the reporting accountants

1.2 COMPANY BACKGROUND

Insight is a specialist asset manager, advising and managing funds for institutional and retail clients across a range of asset types: principally equities; bonds; derivatives and cash. Insight's assets under management totalled £362.5bn[1].

1.3 SIGNIFICANT CORPORATE RESTRUCTURING

There was no significant corporate restructuring during the year under review.

[1] Data as at 31 December 2014. Insight's assets under management are represented by the value of cash securities and other economic exposure managed for clients.

2. REPORT BY THE DIRECTORS

As directors we are responsible for the identification of control objectives relating to customers' assets and related transactions in the provision of investment management and the design, implementation and operation of the control procedures of Insight Investment Management Limited 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.

The control criteria, as relevant to Investment Management activities and IT, as set out in Appendix 1(ii) and 1(vii) of AAF01/06 respectively, have been applied, with the exception of the following:

Section: ACCEPTING CLIENTS

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

Rationale: The Authorised Corporate Director has not appointed Insight to provide the services described in the control above. This function is performed by an externally appointed Administrator and therefore not a relevant control objective for Insight.

Section: MAINTAINING FINANCIAL AND OTHER RECORDS

Control Objective: Pooled funds are priced and administered accurately and in a timely manner

Rationale: The Authorised Corporate Director has not appointed Insight to provide the services described in the control above. This function is performed by an externally appointed Administrator and therefore not a relevant control objective for Insight.

Section: CASH MANAGEMENT AND SEGREGATION OF ASSETS

Control Objective: Investments are properly registered and client money is segregated

Rationale: Insight does not have regulatory permissions to hold client money and assets. Therefore this is not a relevant control objective for Insight.

Section: MONITORING COMPLIANCE (Information Technology)

Control Objective: Outsourced activities are properly managed and monitored

Rationale: Insight does not outsource any of its information technology activities. Therefore this is not a relevant control objective for Insight.

We have evaluated the effectiveness of Insight'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 01 January 2014 to 31 December 2014 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.

Charles Farquharson
Chief Risk Officer

2 June 2015
Signed on behalf of the Board of Directors

3. OVERVIEW OF INSIGHT'S CONTROL FRAMEWORK

3.1 CONTROL ENVIRONMENT

The governance and control framework adopted by Insight (as seen in Figure 1 below) serves as a structure for establishing strong internal controls that promote efficiency, minimise risks, help ensure the reliability of the financial statements and compliance with laws and regulations.

Figure 1: Control framework

3.1.1 Insight Board

The Board of Insight has overall responsibility for business and strategy. The members of the Board include four independent Non-Executive Directors. The Insight Board meets at least every quarter.

3.1.2 Executive Management Committee

The Executive Management Committee (EMC), the structure of which is set out in Figure 3, is the key business operating committee for Insight and its subsidiaries. It is responsible for the overall performance of all aspects of the business and the recommendation of strategy. The EMC comprises the Executive Directors of the Insight Board, as well as the HR Director and the Head of Fixed Income and Currency.

Figure 2: Insight governance structure

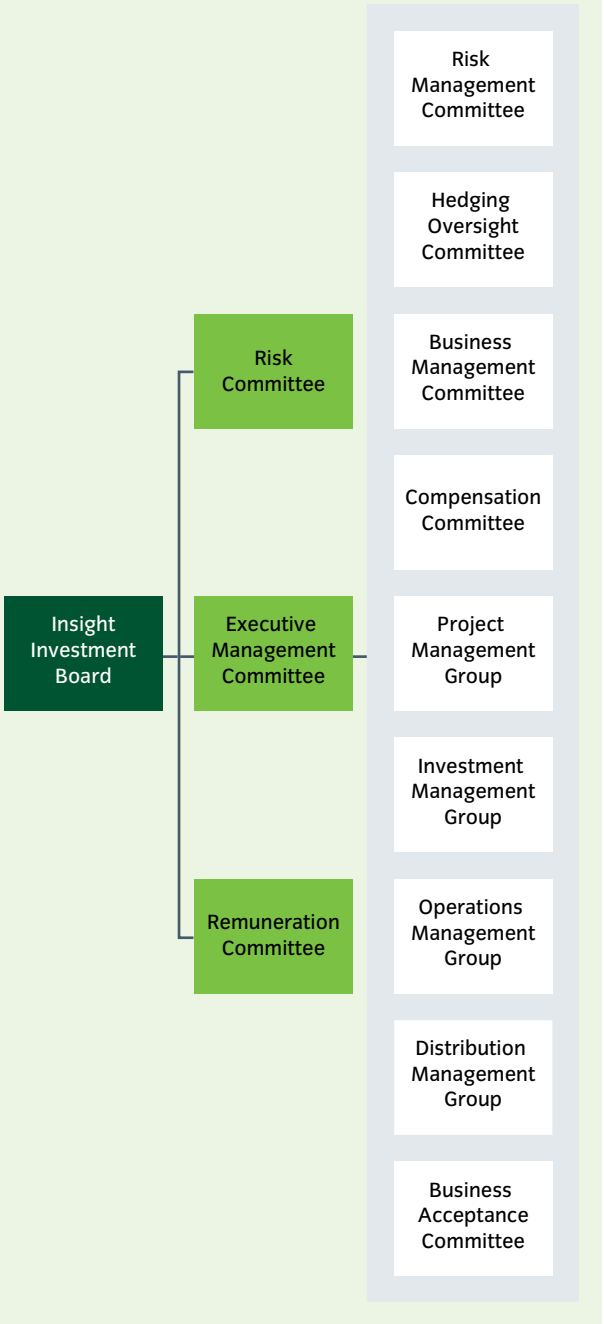
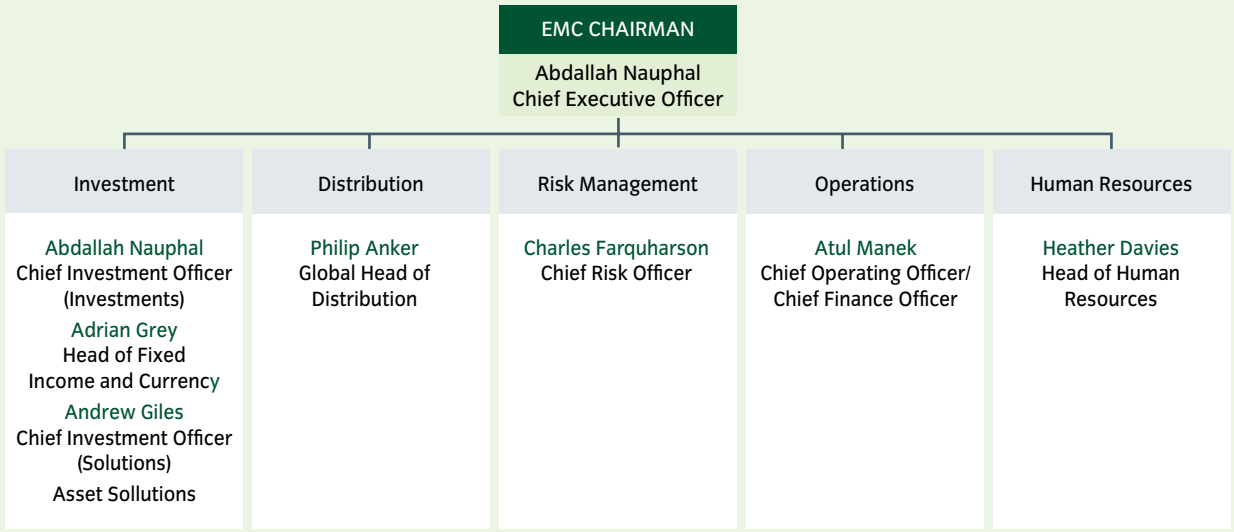


Figure 3: The Executive Management Committee



3.1.3 Risk Management Committee

The Risk Management Committee (RMC), chaired by the Chief Risk Officer, operates as a sub-committee of the EMC and has the same membership. The RMC is responsible for developing an appropriate risk strategy, agreeing policies and setting relevant standards. It monitors and reviews all areas of the business to provide internal assurance to the EMC and the Board of compliance with internal and external requirements. The RMC oversees actions required to address any actual or potentially adverse risk position.

3.1.4 Management accountability

The Compliance and HR Teams review all senior management positions to identify those that would be deemed by the FCA to be Significant Influence Approved Persons (SIAPs).

SIAPs are deemed by the FCA to have a higher degree of accountability than other 'Approved Person' positions and have the prime responsibility for ensuring that satisfactory systems and controls are in place and responsibilities in their areas are clearly defined.

All SIAPs are required to have a BNY Mellon Position Description in place that sets out the scope of each SIAP's responsibility.

The Position Descriptions are reviewed every six months, updated where necessary and signed off by each SIAP and their line manager. SIAPs must also ensure that:

- The operating structure and reporting lines for their areas are defined, documented and communicated to all staff;
- Direct reports are formally advised of their specific responsibilities and accountabilities, and are required to do likewise with their teams;
- Where new or additional responsibilities are transferred to a SIAP the scope of these are agreed between the parties and clearly documented to ensure a robust handover process;
- Where a SIAP becomes responsible for a new area of activity they take immediate steps to familiarise themselves with the area concerned, including any key risk areas. A plan of action is produced to address any longer-term knowledge gaps;

- Any specific delegations to direct reports or other team members are formally advised and recorded, and processes put in place to monitor the effective performance of the delegation.

All other staff members have role profiles that set out the purpose of their role and their designated responsibilities. The role profiles also indicate the required levels of knowledge, skill and experience, and the personal qualities that the job holder is expected to demonstrate.

3.1.5 Policies and procedures

A suite of policies and procedures are in place and communicated across the business to ensure that all colleagues recognise their responsibilities in their business activities and the control environment. All policies are published on Insight's intranet site for colleague reference. Compliance with these policies is regularly monitored and reviewed.

In addition, policies and procedures are in place for hiring, training, promoting and compensating colleagues. This results in the recruitment, development and retention of competent and trustworthy people necessary to support an effective internal control system.

3.2 RISK ASSESSMENT AND MONITORING

The Insight Corporate Risk Framework outlines the governance, processes and controls put in place by the Executive Management Committee ('EMC') to adequately manage the risks arising out of the activities undertaken by Insight.

3.2.1 Risk and Control Self Assessment

Management has primary responsibility for identifying and evaluating any significant risks to the business and for designing and operating suitable controls to mitigate risk. This is performed and documented through the Risk and Control Self Assessment (RCSA) programme and reported to the RMC and Board as appropriate.

The features of RCSA:

- All business areas maintain a RCSA profile
- RCSA profiles capture and assess the risks identified within each business area
- The mitigating controls for each risk are documented and assessed
- Any control weaknesses and respective action plans are documented and tracked to resolution
- All risks and controls have owners identified and are apportioned to a committee within Insight's Governance structure to ensure accountability
- RCSA profiles are maintained through regular review by the business and periodic challenges raised by the Corporate Risk team and monitoring reviews conducted by the Compliance team. Monthly reporting is provided by the Corporate Risk team to Insight's Governance committees
- Aggregated reporting is provided by the Corporate Risk team to the RMC monthly and the Board quarterly

3.2.2 Risk Management Division

The Risk Management Division is headed by the Chief Risk Officer ("CRO"), an Executive Director reporting to the CEO. The role of the team is to provide an independent oversight of all business activities and to ensure that the business fulfils and complies with all the necessary regulatory and Corporate Risk requirements. Risk Management activities are established as follows:

Compliance

The Compliance team is responsible for the identification and assessment of current and future changes in regulation, formulation of policy and provision of guidance to ensure that the Insight brand is properly protected and any competitive opportunities are fully explored. The team works closely with management to ensure Insight has appropriate arrangements for controlling regulatory risks.

Such arrangements include:

- Policies
- Regulatory development
- Training
- Anti-financial crime activity

The team is also responsible for the provision of ongoing advice on day-to-day business issues; monitoring and assurance of robustness of controls; compliance with regulation; and monitoring compliance with investment mandates.

The team maintains a Risk-Based Functional Monitoring Programme. The findings are linked into the relevant RCSA profiles as part of the challenge process.

Corporate Risk

The Corporate Risk Management team is responsible for the design and development of the risk management framework including procedures, controls, standards, systems, key indicators, management information, risk profiles and appetite statements. The team's objective is to promote industry best practice of risk management to ensure that Insight has a thorough understanding and appreciation of its risks so that appropriate management decisions can be made.

Corporate Risk is also responsible for ensuring that Insight has effective Business Continuity planning and Information Risk Management practices.

Investment Risk

The Investment Risk Team is primarily responsible for the oversight and governance of investment risks within Insight's range of funds (UCITS and QIAIFs). In addition, it ensures the business has adequate controls in place to manage the risks arising from the derivative risk exposures held on behalf of our clients. The team formulates and has oversight of our derivatives policies and carries out the model validation process. The team also provides advice regarding settlement and counterparty risk.

3.2.3 Group Internal Audit

Group Internal Audit carries out independent risk-based reviews of Insight's controls and procedures. Reports from these reviews are issued to senior management for action. The Risk Management Division monitors the implementation of these action points, and unresolved issues are referred to the RMC.

3.3 INFORMATION AND COMMUNICATION

3.3.1 Escalation and management reporting

Policy breaches and control failures are reported and escalated to management through the incident reporting system. The incidents recorded include details of the impacts, causes, and remedial actions taken. The incidents are reviewed by the Corporate Risk team for completeness and accuracy. Trends and individual significant issues are reported in a timely manner to the CRO, Risk Committees and the Board depending on the severity of the incident. For example, high risk / value incidents that significantly impact our clients, the profitability or operation of the business must be immediately escalated to the members of the EMC.

The Risk Management teams report on the status of risks identified and control issues across Insight to the Governance Committees on a monthly basis and the Insight Board on a quarterly basis.

All Business Heads report on the status of objectives and risks identified in their business areas in a monthly management information report to the EMC or other relevant Governance Committees. The management information includes a mix of performance and risk indicators. For example, from the Investment Management Division, information reported may span from investment performance and attribution to headcount within the investment teams. Financial reporting is sourced from Insight's Financial Reporting System. Actions are identified for any breaches in risk appetite or performance targets, and the Board and Executive Committees instruct further investigation as required.

3.3.2 Colleague communication

Management communicate to colleagues through a variety of different channels dependent on the message. These channels include: team meetings, business updates, profile lunches, training programmes, policies, newsletters, the Insight intranet and email circulations.

3.3.3 Client communication

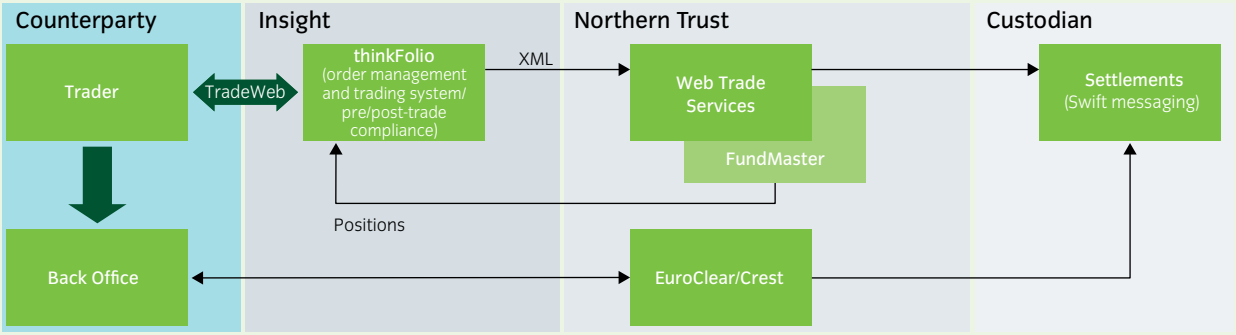
Insight communicates with its clients through a number of different channels. Typically, clients receive periodic reports on their portfolio or fund performance. These reports detail market commentary, portfolio performance and Insight's investment and economic outlook. Reports are supplemented by regular meetings with Client Directors, updated information on our website and Insight-organised seminars on topical financial industry issues.

3.3.4 Trade work Flow

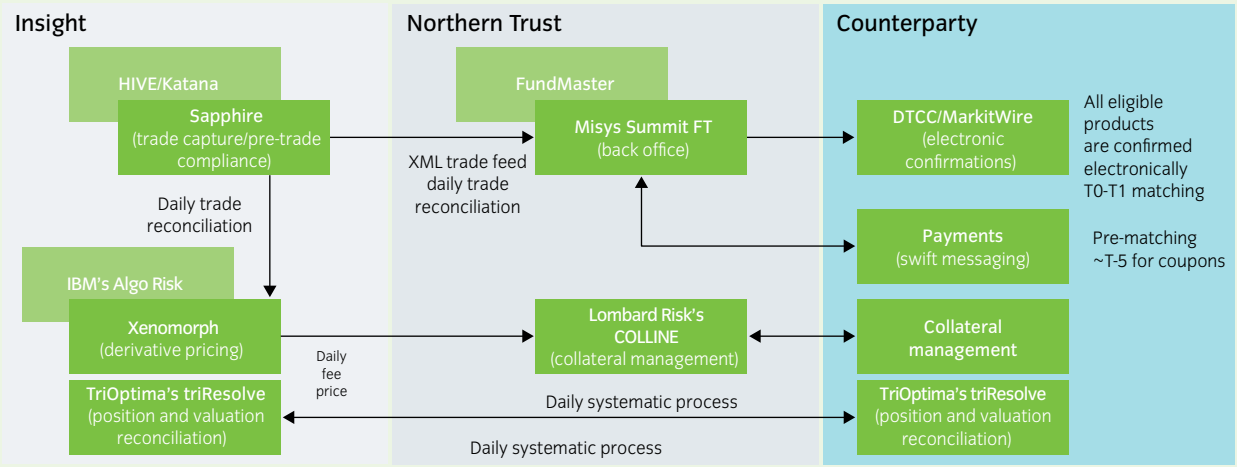
The systems used in the investment management process are presented in the Trade workflow chart (Figure 4).

Figure 4: Trade workflow

Fixed income flow is outlined below.



The OTC derivative trade flow is outlined below.



Xenomorph (third party): Xenomorph is an "intelligent" data warehouse for all instrument universes, positions, projected cash flow streams, curves and static data used by Insight in its derivative process. The system contains a range of valuation and pricing models and provides the official "close of business" valuation system for all OTC derivatives traded by Insight, including swaps.

IBM Algo Risk "ARA" (third party): ARA is the online risk management interface used by the portfolio and risk managers to monitor portfolio risk and factor sensitivities. ARA provides detailed and comprehensive portfolio risk analytics, scenario analysis, stress testing and what-if analysis.

thinkFolio (third party): thinkFolio is the fixed income modelling and decision support tool. It enables portfolio managers to review their portfolio relative to benchmark and model, and to raise orders. The system also enables portfolio managers to look at counterparty exposure as well as bucketed maturity and interest sensitivity of their fund. It is also used for guideline and compliance checking. It monitors a given fund's holding against the Investment Management Agreement ("IMA") and/or regulatory rules on a post-trade and, usually, pre-trade basis with any significant exceptions being recorded, investigated and, if necessary, escalated to the appropriate individuals/committees.

Sapphire (proprietary): Sapphire is the proprietary deal capture and execution system for OTC derivatives.

Summit (third party): Summit resides within Northern Trust's trade operations area and it is the OTC derivative processing system designed to manage post-execution settlement, cash flow management, and operational events.

TriOptima (third party): TriOptima is used to undertake trade-level OTC derivative pricing reconciliation with counterparties.

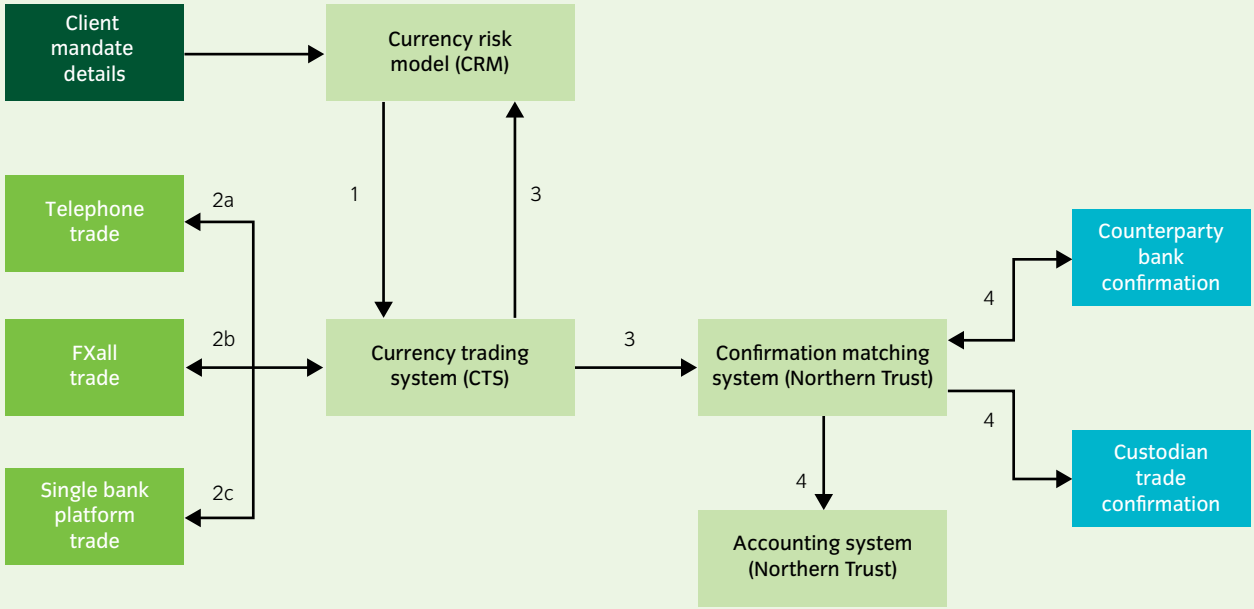
Fundmaster (third party): Fundmaster is Northern Trust's core accounting platform.

Colline (third party): Colline is used by Northern Trust to monitor and mitigate the counterparty credit risk associated with derivative exposures. It is a market-leading collateral management system, written by Lombard Risk, in use by a number of the world's leading banks. It handles all of the daily collateral workflow in a fully integrated and automated process for all of clients' OTC derivative positions.

MTM/Markitwire (third party): MTM/Markitwire is an electronic matching and confirmation system.

The order generation and execution for Currency Risk Management strategies is outlined below (Figure 5);

Figure 5: Currency Risk strategies trade flow



1. Currency risk model instructs Currency Trading System.
2. Trade with bank. More details on Single Bank Trading Platform and FXall are provided below.
3. Trade details disseminated.
4. Northern Trust (Insight's back office books the trade and sends an automatic Swift message to the bank and custodian).

Currency Model: Pareto's currency models signal to the Pareto foreign currency traders (via the CTS discussed below) the trades that they must execute to change the hedges in the client's currency programme. Both currency forward and option trades are signalled for Pareto's currency overlay (CRM). The CRM model contains all the data relevant to the client's mandate. This data includes foreign currency allocations, risk constraints and the benchmark.

Currency Trading System (CTS): A bespoke system developed in-house, the CTS is the key trader/ model interface. The details of the trade, which includes the amount, price and whether to buy or sell appears on the screen at the traders' desks. This is a vital part of the system as it allows the traders to monitor key trade details, including counterparty exposure levels, the progress of any particular trade through the system, the identity of the trader executing the trade and the counterparty bank involved. The CTS includes a trade aggregation component, which is responsible for (i) the aggregation of trades across common accounts, currency pairs and settlement dates prior to execution, and (ii) their corresponding disaggregation post-execution.

Telephone trade (2a): The process of buying and selling shares over the phone. Prices are quoted to investors over the phone and if the investor confirms to deal at the quoted price, then the deal is executed, at the quoted price, at that time. Confirmation of the deal is sent to the investor.

FXall (Third party trading platform) (2b): Smaller trades are normally electronically processed using a third party system called FXall. FXall is a multi-bank foreign exchange portal for institutional clients. API feeds from FXall are integrated into the CTS, so competitive quotes from multiple banks are provided simultaneously for the trader to review. This functionality is linked into the compliance module so that no quotes are requested from any institution that would result in a breach of an exposure.

Single Bank Trading Platform (2c): The traders have access to a number of Single Bank Trading Platforms that allow them to place bids or offers into the market and potentially avoid paying the market spread. This method is typically used for breaking down larger block transactions and reduces the impact on the market of such trades. The CTS receives automatic notification of executed trades from these platforms.

4. STATEMENT OF INTERNAL CONTROLS

This section contains the statement of internal controls for investment management for the year ended 31 December 2014. The objectives, controls and testing performed by KPMG is outlined below;

4.1 Accepting clients

- Accounts are set up and administered in accordance with client agreements and applicable regulations
- Complete and authorised client agreements are operative prior to initiating investment activity
- Client take-ons, including in-specie transfers, are monitored, documented and opening positions are accurately reported to clients
- Investment limits and restrictions are established
- Responsibility for generating proxy voting instructions is clearly established

4.2 Authorising and processing transactions

- Investment strategy is set and implemented in a timely manner
- Investment transactions are properly authorised, executed and allocated in a timely and accurate manner
- Transactions are undertaken only with approved counterparties
- Commission levels and transaction costs are monitored
- Investment and related cash transactions are completely and accurately recorded and communicated for settlement in a timely manner
- Corporate actions are processed and recorded accurately and in a timely manner
- Proxy voting instructions are generated and recorded and carried out accurately and in a timely manner
- Client new monies and withdrawals are processed and recorded completely and accurately; withdrawals are appropriately authorised

4.3 Maintaining financial and other records

- Investment income and related tax are accurately recorded in the proper period
- 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
- Cash and investment positions are completely and accurately recorded and reconciled to third party data
- Investment management fees and other account expenses are accurately calculated and recorded

4.4 Cash management and segregation of assets

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

4.5 Monitoring compliance

- Client portfolios are managed in accordance with investment objectives, monitored for compliance with investment limits and restrictions and performance is measured
- Outsourced activities are properly managed and monitored and conflicts of interest identified to clients
- Transaction errors (including guideline breaches) are rectified promptly and clients treated fairly
- Counterparty exposures are monitored.

4.6 Reporting to clients

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

4.7.1 Restricting access to systems and data

- Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals
- 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
- Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles

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

- IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner
- Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure
- Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g., firewalls, anti-virus etc.)
- The physical IT equipment is maintained in a controlled environment

4.7.3 Maintaining and developing systems hardware and software

- Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented
- Data migration or modification is authorised, tested and, once performed, reconciled back to the source data

4.7.4 Recovering from processing interruptions

- Data and systems are backed up regularly, retained offsite and regularly tested for recoverability
- IT hardware and software issues are monitored and resolved in a timely manner
- Business and information systems recovery plans are documented, approved, tested and maintained

4.1 ACCEPTING CLIENTS

The client take-on process follows an established procedure which involves various teams including a dedicated Client Director

and Service Administrator for each client, Northern Trust (NT) Transitions, Legal, Middle Office, Risk and Investment Management teams. A template Investment Management Agreement (IMA) is used as a basis for negotiating specific terms with each new client. All IMAs are subject to review by various departments before sign-off. A transition checklist is in place which specifies the required processes which need to be followed for all client take-ons.

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

Anti-Money Laundering ("AML") checks on new clients are performed and documented on our AML Verification Checklist by Insight's Client Service ("CS") team. The identification or 'Know Your Customer' (KYC) documentation is obtained for all new customers in accordance with both internal and group policies and UK regulation. Upon receipt of all supporting documentation, the Client Director and the Compliance Manager (Anti-Financial Crime) review and sign off the completed verification checklist. The CS team retain copies of all verification documents as required by policy and regulation. The original signed IMA goes into the safe and a copy is placed on file by the CS team.

NT set up and maintain accounts on their Investment Accounting system (Fundmaster) and instructions are sent to Insight IT by Insight Middle Office for static data updates and maintenance across Insight front office data applications. A client's final IMA is sent to the Mandate Control team to input the client's investment restrictions into thinkFolio (pre and post-trade compliance monitoring system). The coding is signed off by the Mandate Control team, Fund Manager(s) and the Client Director.

The controls ensuring that the clients' other key elements are set up accurately and in a timely manner in accordance with client agreements are covered within other sections of this document:

- Investment guidelines and restrictions – section 4.1.4
- Proxy voting – section 4.2.7
- Investment Management fees – section 4.3.4
- Client reporting – section 4.6.1

Detailed Controls	Testing Performed by KPMG LLP and Results
The Client Services (CS) team inspect all the KYC documentation for any evidence of risk factors and complete an AML verification checklist. The client services associate (CSA) signs off the AML verification checklist as evidence of the review of the documents. The Client Director and Compliance Manager (Anti-Financial Crime) review the checklist and supporting documents to verify the accuracy and completeness of the checklist, and sign off the completed AML verification checklist as evidence of the review.	For a selection of on boarded clients, inspected the completed AML verification checklists and supporting documents and noted that the checklist had been completed by the CSA and signed off by the Client Director and Compliance Manager. No exceptions noted.
The Investment Management Agreement is signed off by authorised signatories of Insight and the client. A listing of client authorised signatories is maintained for each client. Insight authorised signatories lists are reviewed and approved by the CEO. The list is signed as evidence of the review.	For a selection of new clients, inspected the signed IMAs and authorised signatory lists of both the client and Insight and noted that the agreement had been signed off by authorised signatories of both Insight and the client. KPMG also noted that Insight authorised signatory lists had been signed off by the CEO. No exceptions noted.

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

The coding workflow in thinkFolio places a systemic 'no trading' rule on new accounts until the coding is activated. The activation cannot take place until the new IMA has been authorised by Insight and the client.

For Currency Risk Management (CRM) accounts, the Pareto Client Portfolio Management (CPM) team coordinate the setup of the account, whilst Legal handles any contractual issues. The various parameters and constraints are coded into the model so that the model adheres to the client requirements. The CPM team sign the Account Setup Schedule to indicate that the account setup has been completed. An account opening report is distributed to the client.

Detailed Controls	Tests Performed by KPMG LLP and Results
Client accounts are coded into thinkFolio by Mandate Control. There is a systemic 'no trading' rule in thinkFolio to prevent trading activity prior to authorisation. Mandate Control do not remove the rule until the restrictions coding form has been signed off. Client Services notify Mandate Control when an IMA has been signed by authorised signatories of Insight and the client. Upon receipt of the email, a member of the Mandate Control team codes the investment guidelines and restrictions into thinkFolio ('Coder'). Prior to activation in the system, another member of the team reviews the coding ('Checker') for completeness and accuracy. Both individuals sign the thinkFolio restrictions coding form to evidence that the restrictions have been coded. Copies of the form are retained. Trading activity is retained in thinkFolio.	For a selection of new clients, inspected the signed and dated IMAs and observed the thinkFolio trading activity history, and noted that the IMAs had been authorised prior to Insight initiating investment activity. KPMG also inspected the thinkFolio restrictions coding form and noted that both the Coder and Checker had signed off the form to verify the accuracy and completeness of the restrictions prior to Insight initiating trading activity. No exceptions noted.
For Currency Risk Management accounts, investment guidelines and restrictions documented in the IMA are signed off by authorised signatories of Insight and the client. Guideline restrictions in the IMA are coded into the currency risk model by the Pareto Research team and the Currency Application Support team. The Client Account Setup Schedule is signed by a member of the Currency Application Support team as evidence that the model parameters are coded accurately. Models are deployed into the live environment by the Currency Application Support team. On the date the account is active, the model is run to generate FX Forward trades. Pareto Research review the coding for accuracy and sign the Client Account Setup Schedule as evidence that the model parameters are coded accurately. Copies of the schedule are retained. The client receives an Account Setup Report which includes trading activity.	For a selection of new currency risk management accounts, inspected copies of the signed and dated IMAs and account reports and noted that the IMA had been authorised prior to initiating investment activity. No exceptions noted. KPMG also inspected the account set-up schedule to determine whether the schedule had been signed off by Research and Currency Application Support team to verify the accuracy and completeness of the restrictions coded. **Exception noted:** For 1 out of the 2 clients selected, it was noted that the signed account set up schedule had not been retained. **Management response:** The missing Account Set-up Schedule above refers to an existing account transition. All investment management activities were handled correctly. However, the CPM team failed to follow the procedure of filing a paper based Account Set-up Schedule. The remedial action was to remind members of the CPM team to follow the established procedure.

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

During the transition liaison period, the NT Transition team receives stock lists and / or confirmation of cash values from the previous manager. On trade date, the previous manager confirms stocks and cash to be received. This is then loaded to Fundmaster via an IDX file. Confirmation of receipt is sent by the Custodian and retained in the transition file. A three-way manual reconciliation is performed by the NT Transition team of the stock and cash balances in Fundmaster to the custody records and the previous manager. Any exceptions are investigated and resolved. The reconciliation is signed off by a NT Transitions manager and retained in the transition file.

Take-on valuation is produced by the NT Client Reporting team and reviewed for accuracy by the NT Transitions team prior to it being issued to the client.

Weekly and monthly Management Information (MI) is sent to Insight by NT Operations to enable the monitoring of volume, timeliness and accuracy of transitions in accordance with the agreed Service Level Agreement. The MI is reviewed and escalated to senior management as appropriate.

Detailed Controls	Tests Performed by KPMG LLP and Results
MI and KPIs from NT Operation on volume, timeliness and accuracy of transitions is reviewed at the weekly Transitions Functional Service Meeting (FSM) and monthly Senior Management Committee (SMC) meetings in accordance with the agreed Service Level Agreement (SLA). Any issues or outstanding actions are escalated to senior management.	For a selection of weeks prior to July 2014, inspected the weekly transitions MI and Transitions FSM minutes and noted that the transitions data had been reviewed. KPMG also inspected the FSM Actions Log and noted that the issues identified in the Transitions FSM minutes had been recorded and escalated.
The minutes and MI packs for the weekly FSM and monthly SMC meetings are retained.	No exceptions noted.
A summary of the MI on transitions data is also reviewed at the monthly Operational Management Group (OMG) meeting. Meeting packs are retained.	For a selection of weeks after July 2014, inspected the central log of transitions maintained by the transitions team and the weekly status report emails with NT and noted that the transitions data had been reconciled.
In addition, from July 2014, the Client Service team maintain a log of current and planned transition events. The tracker is submitted to Northern Trust weekly via email prior to the next weekly status call. The status of the tracker is reviewed for accuracy and completeness with Northern Trust during the weekly status call. The review is evidenced via an email to Northern Trust with the updated tracker.	No exceptions noted. For a selection of months, inspected the SMC and OMG meeting packs and minutes and noted that transitions data had been reviewed. No exceptions noted.

4.1.4 Investment limits and restrictions are established

Investment guidelines and restrictions documented in the IMA are signed off by authorised signatories of Insight and the client. These are coded into thinkFolio by a coder and checker of the Mandate Control team, and then reviewed for accuracy by the Fund Manager and Client Director within 10 and 5 business days respectively of the IMA being coded. This review is evidenced by the signing of the restrictions control sheet. Any pending signatures are escalated to member(s) of the EMC for review.

Currency Risk Management strategies are quantitative. The various parameters and constraints are coded into the Currency Risk Model so that the model adheres to the client requirements. The model therefore does not generate trades that are in breach of these guidelines. Clients' permitted counterpartie constraints are coded into the Currency Trading System by the Currency Application Support team. The Currency Risk Management teams (Research and Client Portfolio Management) and the Currency Application Support team sign the Account Setup Schedule to indicate that the account setup has been completed. A client request for a mandate change on an existing account which requires the adjustment of model parameters (e.g. hedge range, benchmark) are performed by the Pareto Research team.

Detailed Controls	Testing Performed by KPMG LLP and Results of testing
Investment guidelines and restrictions documented in the IMA are signed off by authorised signatories of Insight and the client. The investment guidelines and restrictions are coded into thinkFolio by Mandate Control and then reviewed for accuracy by the Fund Manager and the Client Director. The Fund Manager and Client Director are required to review and sign off the thinkFolio restrictions control sheet within 10 days and 5 days respectively. Any overdue signatures are escalated to a member (or members) of the EMC by email. KPIs on timeliness of coding and sign-off are recorded and reported to the OMG monthly.	For a selection of new clients, inspected signed IMAs and authorised signatory lists for both Insight and the client, and noted that the IMAs had been signed by signatories of both Insight and the client. No exceptions noted. For a selection of new clients, inspected the restrictions control sheet and noted that the control sheet had been signed off by the fund manager and client director within 10 and 5 business days of the IMA being coded. KPMG also inspected the escalation emails for exceptions to the rule and noted that the exceptions had been escalated. No exceptions noted. For a selection of months, inspected the OMG meeting pack and noted that the coding sign off KPIs had been reported and monitored. No exceptions noted.
Any amendments to an IMA by the client are submitted to the Client Services team in a signed side letter. Client Services email the signed side letter to Mandate Control for processing. A member of the mandate control team codes the amendments into thinkFolio and prior to activation in the system, a second member of the team reviews the coding for accuracy and completeness. Both members of Mandate Control sign off the restrictions control sheet as evidence of the process. An audit trail is maintained within the thinkFolio system showing the completion and review of amendments by the coder and checker.	For a selection of IMA amendments, inspected copies of the thinkFolio restrictions control sheet and noted that the control sheet had been signed off by the checker and coder. KPMG also inspected the thinkFolio restrictions control sheet and signed side letter and noted that the amendments made to thinkFolio agreed to the signed side letter. No exceptions noted.
For Currency Risk Management accounts, investment guidelines and restrictions documented in the IMA are signed off by authorised signatories of Insight and the client. Guideline restrictions in the IMA are coded into the currency risk model by the Pareto Research team and Currency Application Support team. The Client Account Setup Schedule is signed by a member of the Currency Application Support team as evidence that the model parameters are coded accurately. Models are rolled out into the live environment by the Currency Application Support team. Pareto Research review the coding for accuracy and sign the Client Account Setup Schedule as evidence that the model parameters are coded accurately. Copies of the schedule are retained.	For a selection of new accounts, inspected the account set-up schedule to determine whether the schedule had been signed off by Research and Currency Application Support team to verify the accuracy and completeness of the restrictions coded. **Exception noted:** For 1 out of the 2 clients selected, it was noted that the signed account set up schedule had not been retained. **Management response:** The missing Account Set-up Schedule above refers to an existing account transition. All investment management activities were handled correctly. However, the CPM team failed to follow the procedure of filing a paper based Account Set-up Schedule. The remedial action was to remind members of the CPM team to follow the established procedure.
Following authorisation of amendments to a client IMA, the Client Portfolio Management (CPM) team communicates via email any change in model parameters to the Research team. Following completion of the amendment by the Pareto Research team, the Account Change form is signed by the Pareto Research team and Client Portfolio Management team to evidence the change has been implemented accurately.	For a selection of amendments, inspected the account change form and noted that the form had been reviewed and signed off by both Research and CPM. No exceptions noted.

4.1.5 Responsibility for generating proxy voting Instructions is clearly established

The delegation of responsibility for executing proxy votes to Insight is outlined within the Investment Management Agreement. The IMA is signed off by authorised signatories of Insight and the client.

Detailed Controls	Tests Performed by KPMG LLP and Results
The delegation of responsibility for executing proxy votes to Insight is defined in the Investment Management Agreement (IMA). The IMA is signed off by authorised signatories of Insight and the client. A listing of client authorised signatories is maintained for each client. Insight authorised signatories lists are reviewed and approved by the CEO on an annual basis. The list is signed as evidence of the review.	For a selection of new clients, inspected the signed IMAs and noted that the IMAs contained a clause for the procurement of the exercise of voting rights by Insight. KPMG also inspected the signed IMAs and authorised signatory lists for the selected clients and noted that the IMA had been signed off by authorised signatories of both Insight and the client. No exceptions noted.

4.2 AUTHORISING AND PROCESSING TRANSACTIONS

4.2.1 Investment strategy is set and implemented in a timely manner

Regular investment meetings are held, per asset class and region, with input from Analyst, Research and Strategy teams, at which investment policy is set. Accounts are grouped with others that run against the same benchmark and managed to a model portfolio, where applicable.

Detailed Controls	Tests Performed by KPMG LLP and Results
Investment Management Teams meet weekly to discuss strategy and portfolio construction. The results of the discussion are recorded in meeting minutes, which are retained.	For a selection of weeks, inspected meeting minutes for the Investment Management Team meetings to determine whether the minutes included discussion of strategy and portfolio construction. **Exception noted:** For 1 out of the 5 weeks selected, it was noted that the meeting minutes had not been retained. **Management Response:** The meeting referred to above is the Global Government meeting. The meeting was held as scheduled, however due to an administrative error, a copy of the minutes could not be located on file. The remedial action was to remind the meeting Secretary of the established procedure to retain meeting minutes.
The Investment Management Group (IMG) meet monthly to review and discuss allocation, portfolio summary, performance, risk & sensitivity, market fundamentals, valuations and credit strategy. The meeting packs and minutes are retained as evidence of discussion.	For a selection of months, inspected the IMG meeting packs and minutes and noted that the pack and minutes included evidence of review of allocation, portfolio summary, performance, risk & sensitivity, market fundamentals, valuations and credit strategy. No exceptions noted.

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

Evidence of the authorised individual responsible for each investment decision is recorded on the order management systems. Electronic order transmission is used where available as this ensures speed and accuracy of order placing. The systems capture time-stamps and retain a full audit trail. ThinkFolio and Sapphire identify any unexecuted orders to the Fund Managers and Traders.

'Hard' and 'Soft' restrictions are coded into thinkFolio. 'Soft' coded restrictions can be overridden by the Fund Manager with an appropriate rationale.

'Hard' restrictions cannot be overridden and therefore the trade cannot be processed. Electronic pre-trade compliance checking ensures orders are compliant with client IMAs prior to being passed to dealers for execution. Pre-trade overrides are captured within the system audit trail. A post-trade report from thinkFolio is also run and reviewed daily by a member of the Mandate Control team. Active breaches are reported in the incident reporting system, Resolve.

When placing orders through a broker, the execution prices are monitored to ensure the brokers obtain best execution. When dealing 'Over the Counter', evidence of best execution is retained by the trading desk. Competing prices (price yield or spread) are obtained by the Fixed Income dealing desk prior to placing an order. A log of competing prices for each transaction is retained by the desk with the executed price. A sample of transactions is reviewed on a quarterly basis by the Compliance team to ensure best execution is being obtained. Any exceptions are investigated by the Compliance team and recorded. The Compliance team also checks all equity deals for best execution on a daily basis. A report of executed trades from thinkFolio is compared with VWAPs (Volume-Weighted Average Prices) from Bloomberg. Differences greater than 0.5% are investigated and documented. The Compliance team maintain a spreadsheet of all variance checks, and include explanatory narrative for all investigated discrepancies. Records of these checks are retained by the Compliance team. The occurrences of the checks are also reviewed as part of periodic functional reviews undertaken by Compliance as part of the risk-based monitoring plan.

In accordance with FCA regulations, and to ensure accuracy of executed transactions, Fund Managers and Traders telephone instructions are recorded and backed up on a daily basis. Records are stored off-site.

ThinkFolio, the electronic order management system, allocates trades to underlying accounts on a pro-rata basis and enables a clear audit trail of allocation (and any subsequent reallocation). In the event that this approach is not appropriate, for example, the resultant holding may be so small that it is unsuitable for the client – the allocations can be adjusted. In these circumstances, the reason for the departure from the standard procedures is fully documented. The Compliance team, as part of monthly desk-based monitoring, undertakes independent reviews which include testing fair and timely allocation and adherence with Insight's Order Execution policy. The report is published and sent to senior management, including the CEO for information.

For Currency Risk Management accounts, the investment strategy is quantitative, model-driven. Client's guidelines are encoded in the model. This ensures the generated trades are guideline compliant.

Detailed Controls	Tests Performed by KPMG LLP and Results
Competing prices (price yield or spread) are obtained by the Fixed Income dealing and Currency Risk Management desks prior to placing an order. Where competing prices cannot be obtained, the desk documents the reason for the non-competitive order in the dealer's log. A log of competing prices for each transaction is retained by the desk with the executed price. Compliance conduct a quarterly review of a selection of random samples from the records kept by the Fixed Income dealing desk. The quarterly reviews are documented within a pack. Any exceptions (i.e. where the best price is not executed) lead to an investigation by Compliance. The investigation is conducted with the dealer. If Compliance need additional information, the exception is escalated to the Head of FI dealing desk. The records of the investigation and resolution are included in the documentation pack.	For a selection of fixed income trades, inspected copies of the dealers' blotter and noted that competing prices were obtained for trades. No exceptions noted. For a selection of quarters, inspected the compliance quarterly review packs and noted that a selection of trades had been investigated by Compliance. No exceptions noted.
Investment Guidelines specified in the IMAs are 'hard' coded into thinkFolio (no override possible), or 'soft' coded (warning can be overridden by the Fund Manager). Overridden warnings and rationale are reported on the pre-trade breach report. The pre-trade overrides are reviewed daily using the pre-trade functionality on thinkFolio by a member of Mandate Control to review Fund Manager rationale and also to identify any coding errors. Incidents are reviewed on a T+1 basis by a member of the Mandate Control Team. The audit trail of post-trade review is maintained within the thinkFolio system. Any active breaches, and proposed actions, are logged in the incident reporting system (IRS) and tracked by Compliance. Outstanding actions are reported to the monthly Risk Management Committee. Meeting minutes are retained.	For a selection of dates, inspected the pre-trade override report and noted that the report had been reviewed by Mandate Control. No exceptions noted. For a selection of dates, inspected the post-trade breach reports and noted that the report had been reviewed by Mandate Control. No exceptions noted. For any breaches identified in the selection of dates, inspected the Incident Reporting System register and noted that the incident had been raised and monitored in the system. No exceptions noted. For a selection of months, inspected the RMC minutes and noted that outstanding actions had been reported and discussed. No exceptions noted.
Compliance checks a selection of equity deals for best execution on a quarterly basis. A report of executed trades from thinkFolio is compared with the volume-weighted average price (VWAP) from Bloomberg. Any differences between the two prices that is greater than 0.5% are investigated by Compliance. Compliance maintains a spreadsheet of all variance checks and includes explanatory narrative for the differences investigated.	For a selection of quarters, inspected copies of the compliance best execution checklist and noted that the best execution testing had been performed and investigation of any variances had been performed. No exceptions noted.

The Compliance team maintain a risk-based functional monitoring plan which details a programme of functional reviews to be undertaken over the next eighteen months. The plan is reviewed and updated once every 6 months and presented to Insight's Board for approval. The Compliance team undertake functional reviews in accordance with Insight's risk-based monitoring plan. The results of the fieldwork undertaken, findings and any agreed actions are published in a formal report and sent to senior management including the CEO for information. Agreed actions identified on the report are tracked to closure by the Compliance team. The actions are recorded and monitored in the Outstanding Actions Database.	For a selection of monitoring plans within the year, inspected the board approval and noted that the monitoring plan had been reviewed and authorised by the board. No exceptions noted. For a selection of functional reviews, inspected the final reports provided to senior management and noted that compliance had performed an independent monitoring process for the function. No exceptions noted. For a selection of the reports, inspected the final reports and the outstanding actions database and noted that the actions points had been recorded, monitored and resolved by compliance. No exceptions noted.
The Compliance team check adherence with the Order Execution policy for the exchange-traded and OTC instruments. Compliance reviews are performed on a quarterly basis across a sample of deals. The prices obtained are compared to the VWAP for the underlying security for that day and/or the daily high/low price for the asset/index on the day and/or the best quote received. Any exceptions are investigated with the dealing desks and the results of the investigation are recorded in the documentation pack.	For a selection of quarters, inspected the compliance OTC review pack and noted that testing over the adherence to the order execution policy had been performed and all exceptions had been investigated and resolved. No exceptions noted.
The Compliance team perform quarterly desk-based monitoring to test for timely and fair allocation and adherence with Insight's Order Execution policy. Any items which do not satisfy the timely or fair allocation criteria are investigated with the dealing desk and the results of the investigation are recorded in the documentation pack.	For a selection of quarters, inspected the compliance review pack and noted that testing over the timely and fair allocation of trades had been performed and any exceptions had been investigated and resolved. No exceptions noted.

4.2.3 Transactions are undertaken only with approved counterparties

Trades can only be placed with brokers who have been approved by the Counterparty Credit Committee (CCC) using the documented broker approval process. Only approved brokers are set up on the trade processing systems and trades with 'unapproved' brokers cannot be processed. The approved broker / counterparties list is maintained by the Legal team and Corporate Risk.

The application forms for a new broker or counterparty must be signed by the sponsoring Dealer/Fund Manager and Department Head, prior to presentation to the CCC for approval. The CCC checks that the application form is complete, internal classification and categorisation has been applied by Insight's credit team and any required due diligence documentation has been supplied and reviewed by the Legal and Compliance teams. The CCC also assesses any credit degradation of existing counterparties.

In addition, for liquidity purposes, there is a fast-track broker approval process. The approval is requested only where there is a legitimate business need to seek urgent temporary approval of a broker for a one-off trade. A list of all completed fast-track broker applications is provided to both the CCC and Insight's Dealing Oversight Committee.

The Legal team co-ordinates and monitors the completion of each stage of the process. A checklist accompanying the Broker Application & Approval Form is signed off by the sponsor, the department head, the Legal and Risk Management teams, and the credit analyst should a credit review be required. Those counterparties with no ratings or a rating below A- require a credit review.

Once completed, Middle Office arrange for the broker to be added to the approved broker / counterparties list and for the broker / counterparty to be set up in CADIS. To ensure segregation of duties, access controls are in place to restrict who can set up new brokers / counterparties on the trade processing systems. An audit trail is available to identify the individuals who set up the accounts (see Information Technology section).

For Currency Risk Management Accounts, client specified constraints on available counterparty banks and exposure limits are embedded within the Currency Trading System. Currency Application Support encodes the parameters on account setup and at times of amendments. Currency Application Support sign the electronic sign-off system or the CTS Configuration Amendment Form as evidence of review.

Detailed Controls	Tests Performed by KPMG LLP and Results
An approved counterparty list is maintained by the Counterparty Credit Committee (CCC). The approved counterparties are maintained in CADIS (which feeds into thinkFolio, Sapphire and CTS). As a system control, trades with unapproved counterparties cannot be processed.	For a selection of trades, inspected the approved counterparties list and the CADIS counterparty records and noted that the counterparties for the selected trades were present on the approved counterparties list that had been approved by the CCC. No exceptions noted.
The monthly Counterparty Credit Committee (CCC) formally approves requests for new brokers or counterparties. Any changes to approved counterparties are discussed at meetings of the CCC. The authorisation for Middle office to add an approved broker or counterparty is provided by the CCC in the CCC meeting minutes, which are retained.	For a selection of months, inspected the CCC minutes and noted that new counterparties had been approved and counterparty amendments had been discussed and approved. No exceptions noted.
For one-off trades with a non-approved broker, the Fund Manager or Dealer completes an online application form to request temporary approval. The application is reviewed and approved by an authorised individual in the system. The approval is performed electronically within the system. Completed and approved applications are forwarded to Insight Middle Office who activate the broker in CADIS to facilitate the one-off trade and then deactivate the broker once the trade has been processed. An audit trail is retained in CADIS to evidence approval and deactivation.	For a selection of one-off trades with a non-approved broker, inspected the fast-track approval form and CADIS email trail and noted that the form had been approved and the broker had been deactivated after the trade. No exceptions noted.
For Currency Risk Management accounts, client counterparty account rules are encoded within the CTS by Currency Application Support. The Currency Application Support team members responsible for the coding and review sign the Account Setup Schedule as evidence that the rules have been coded completely and accurately. Amendments to client account rules are evidenced by sign-off by the coder and reviewer on the CTS Configuration Amendment Form by Currency Application Support team.	For a selection of new accounts, inspected the account setup checklist and noted that the checklist had been signed off by a second member of the Currency Application Support team. No exceptions noted. For a selection of CTS amendments, inspected the CTS Configuration Amendment form and noted that the form had been signed off by a second member of the Currency Application Support team. No exceptions noted.

4.2.4 Commission levels and transaction costs are monitored

Commission sharing agreements (CSAs) are in place for commissions generated from physical equity trades. Transaction files are generated and reconciled to CSA broker research commission pools by Insight's Middle Office who instructs payment on the basis of the Insight Specialist Equity team's target commissions.

No commission is paid on fixed income trades as transaction costs are included in the price spreads. Exchange-Traded Derivatives are subject to an execution fee and a standard clearing fee. All Executing Brokers must comply with Insight's Exchange-Traded Derivative Execution Fee policy. Over-the-Counter derivatives transaction costs are included in the bid/offer spread. Monthly fee reports are produced by the fund administrators and reconciled to dealer reports for analysis. Fund of fund deals are exempt from execution costs as the deal is executed directly with an Authorised Fund Manager. The annual management charge is included in the price of the fund.

For transaction costs, monthly reports of turnover and commission per broker / counterparty is reviewed by the Investment Management Group (IMG).

Detailed Controls	Tests Performed by KPMG LLP and Results
A monthly report of commission or turnover per counterparty is reported to the Investment Management Group (IMG) for review of unusual items. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of months, inspected the IMG meeting packs and minutes and noted that turnover and commission per counterparty had been discussed. No exceptions noted.

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

Equity and fixed income trades

All equity, gilt and other fixed income trades are recorded in Fundmaster, NT's investment accounting system. Transactions interface electronically with Web Trade Service (WTS) from thinkFolio, Insight's order management system, and from there to Fundmaster. WTS is the trade matching engine on the NT platform that manages the flow of information across SWIFT, Central Trade Matching (CTM) and CrossMar Matching Services (CMS) for the post-execution processing of trades. CTM is the matching engine for Fixed Income and Equity trade confirmations. CMS is the matching engine for FX trade confirmations.

The WTS system electronically matches each trade with the brokers' / counterparties' records extracted from CTM. The matching process ensures that the ISIN, nominal, price, commission and charges are the same on both Insight's and the brokers' / counterparties' records. WTS generates a trade history report to provide evidence of matched trades.

Small tolerance levels are permitted on the commission and charges. The tolerance levels are designed to ensure that timely settlement of trades is not delayed by the investigation of non-material differences between Insight and broker / counterparty records. The tolerances vary by market and instrument. Where non-material differences arise, the WTS system automatically adjusts the Insight record to agree with the broker / counterparty. An audit trail recording the resolution of non-material differences is retained electronically in the WTS system.

If differences arise that exceed the pre-set tolerance levels, workflow software within the WTS system electronically flags and routes the item to a member of the Trade Processing team. The member of this team investigates and resolves the difference through the liaison with the broker / counterparty and the investment management staff who placed the trade. Once resolved, either Insight amend the details of the trade in their records to match the broker / counterparty, or the broker / counterparty amend and resubmit their record via CTM for re-matching in WTS at Insight.

FX trades

FX trades are sent to Fundmaster by thinkFolio via Misys. In Fundmaster, trades are created, which then create unmatched trades in Misys. Once an identical counterparty confirmation MT300 is received, the trade is matched in Misys and instructed to the custodian for settlement via the interface to SWIFT. When the trade has been instructed to the custodian via SWIFT, the trade is flagged as instructed in Misys. Any trades that are unmatched after a certain time period result in the Misys workflow function producing a warning message for investigation by the team. SWIFT automated trade instructions can only take place for trades that have been matched by Misys (or where tight deadlines are in place, accelerated and authorised by the NT Trade Processing team). Trades can only be instructed to the custodian with whom a 'key exchange' has been performed.

A 'key exchange' involves the swapping of an 'electronic signature' between two organisations that use the SWIFT system. It is only after a key exchange has been performed that SWIFT messages can be sent or received between them. A key exchange can only be performed by one individual in the NT Operations team, which ensures that there is control over the custodian to which messages and instructions can be exchanged. Each time a message is sent over the SWIFT network, there is a system check performed to ensure that a key exchange has been performed between the sender of the message and the recipient.

Misys flags 'unmatched trades', i.e. those that are approaching the settlement date but which have not been matched in Misys or instructed to the custodian. A senior member of the NT Trade Processing team reviews these system-generated warning flags throughout the day and ensures that they are investigated and resolved. An audit trail of the status of trades and actions taken to progress them is retained electronically in the Misys system.

Money Market trades

Money Market trades (cash deposits, certificates of deposit and commercial paper) are placed and then recorded on thinkFolio by the investment management Treasury team. The Cash team in Trade Processing monitors thinkFolio reports throughout the day for money market trades. ThinkFolio sends money market trades to WTS. They are then loaded into Fundmaster. The trade details are confirmed with the broker / counterparty by the Cash team either by telephone, by fax or by the receipt of SWIFT messages from the broker / counterparty. A log of the telephone call is written on the deal ticket, the hard copy SWIFT message or the fax is retained as evidence of the confirmation and subsequent postal confirmation is also retained.

Money market trade mismatches and exceptions are investigated immediately and resolved by the Cash team. Once matched the money market trades are manually authorised and instructed for settlement to the custodian via Custody Passport for NT custody or SWIFT.

The manual authorisation process is initiated by manual input of the instruction into Custody Passport or SWIFT. A second person authorises the instruction. Access to Custody Passport and the SWIFT system for the input and release of payments and instructions is restricted to designated members of staff.

Derivative trades

Exchange-Traded Derivative (ETD) orders are placed and executed by Insight dealers through thinkFolio. The trades feed into Fundmaster. A daily 3-way reconciliation is performed between Fundmaster, SunGard GMI (NT's ETD derivative processing system designed to manage post-execution settlement, margin management and operational events), and the Clearing Broker (part manual). Any differences are investigated and resolved. The details of the reconciliation are kept within a daily pack and archived. The reconciliation process is included in the daily checklist of tasks that are signed at the end of each day by the ETD team leader.

Over-the-Counter (OTC) transactions undertaken by investment management are raised within thinkFolio or Sapphire and executed through the order management system Sapphire. The details of the transactions are automatically processed to Fundmaster and Summit, the key processing platform for derivatives, verified, and then checked against the broker / counterparty confirmation. This process is included in the end of day check list of tasks and is signed each day by a senior manager in the Derivatives team.

The life cycle of the transaction is monitored by the Derivatives team. If collateral is required for a client undertaking derivative trades, a Credit Support Annex is implemented with the relevant broker / counterparty as signed off by the Insight authorised signatory as agent of the client and the counterparty. Derivatives exposure is monitored daily by the Derivatives team and checked against the broker / counterparty exposure in order to determine any need for collateral movements. Any movements in collateral are within the set parameters of the Credit Support Annex. All exposures and movements are recorded and monitored within Colline.

Failed trades

Failed trades, i.e. those that have not successfully settled on the agreed settlement date, may be notified to Insight by the broker / counterparty and/ or custodian. Notification can be received by fax, email, phone, or report from the custodian's proprietary system. The failed trades are recorded on the Failed Trade spreadsheet by a member of the Trade Processing team. The failed trade report is manually generated from this spreadsheet. In addition, the Quality Assurance team proactively monitors actual cash payments and receipts for trade settlement against transactions generated by Fundmaster using TLM, the stock and cash reconciliation system. Any discrepancies are recorded on TLM. A member of the Trade Processing team investigates failed trades through a review of Insight's records and discussion with the broker / counterparty and custodian in order to facilitate settlement as soon as possible. The Trade Processing team retains hard copy records of the actions taken to resolve the failed trade.

Monitoring

A robust suite of Management Information and reports are produced on a daily, weekly and monthly basis by NT Operations for Insight to monitor the timely and accurate processing of all transactions. Issue logs are maintained and regular service review meetings are held to ensure all issues that impact investment and related cash transactions are completely and accurately recorded, and settled in a timely manner.

Currency Risk Management Accounts

For Currency Risk Management Accounts, all deals are executed through recorded mechanisms, including FXall, CTS and single bank platforms. The vast majority of forward trades are processed on a straight through basis from the models to the CTS to the accounting and SWIFT messaging systems to the counterparty bank and custodian for each account. The remaining trades involve manual processes to communicate with the client and/or custodian.

A Cash flow Warning System is used to monitor forward contracts that are close to maturity and identify the probable profit / loss position on the account. Forward Estimate Letters are distributed to clients stating estimated profit/loss position. Once the Forward contract has matured, a Settlement Letter is prepared confirming the profit/loss position. The position stated in the letter is verified by the Client Services team against the Cash flow Warning System notification and closure of position email notification from Pareto's Trading team.

European Market Infrastructure Regulation ('EMIR')

Insight is working to ensure its clients comply with EMIR rules for the mandates Insight manage. The formal responsibility for complying with the EMIR rules resides with the counterparty to a derivative transaction (i.e. the client itself for segregated mandates). Since 15 March 2013, most counterparties have been required to have procedures in place to report to national regulators on a monthly basis the number of non-cleared OTC derivative contracts that are not confirmed within five business days.

Detailed Controls	Tests Performed by KPMG LLP and Results
NT provide weekly MI detailing cash (non-derivatives) volumes, timeliness of confirmations, number of failed trades over ten days and number of cancelled trades. The MI is reviewed by Market Operations at the weekly Functional Service Meeting (FSM). The MI and minutes of the meetings are retained by Insight Middle Office.	For a selection of weeks, inspected the Market Operations FSM minutes and noted that the MI had been discussed. No exceptions noted.
Daily and weekly issues logs are maintained by NT. The issues logs are reviewed by Market Operations at the weekly FSM. Any significant issues are escalated to the SMC on a monthly basis. The issues logs and the minutes of both meetings are retained by Insight Middle Office.	For a selection of weeks, inspected the weekly issues log and the Market Operations FSM minutes and noted that the weekly issues logs had been discussed. No exceptions noted. For a selection of months, inspected the SMC minutes and noted that significant issues had been escalated to the SMC. No exceptions noted.
Monthly KPIs on contracted outsourced operational services are sent to Insight Middle Office. The monthly KPIs are discussed at the Market Operations and Derivative Operations FSMs, as well as at the monthly SMC. The MI and minutes of the meetings are retained by the Insight Middle Office. A summary on NT's performance is also provided as part of the OMG reporting packs, which are reviewed and retained.	For a selection of weeks, inspected weekly Market Operations and Derivative Operations FSM minutes and noted that KPIs had been discussed. No exceptions noted. For a selection of months, inspected the SMC minutes and meeting pack and noted that the KPIs had been reviewed. KPMG also inspected the OMG minutes and the OMG reporting pack and noted that a summary had been reviewed. No exceptions noted.
NT provides weekly MI detailing the processing of Derivatives trades. The MI is reviewed at the weekly Derivative Operations FSM. The MI and minutes of the meetings are retained by Insight Middle Office. Any issues are escalated to the quarterly Derivatives Risk Committee (DRC) and SMC meetings. The minutes of the meetings are retained by Insight Middle Office. NT also provides monthly MI on confirmations that are aged over 5 days and therefore EMIR recordable. The MI is reported to the Operational Management Group (OMG) for discussion. The MI and OMG meeting packs are retained.	For a selection of weeks, inspected minutes of the Derivative Operations FSM and noted that the MI had been discussed. No exceptions noted. For a selection of months, inspected the meeting minutes of the DRC and SMC and noted that any significant issues had been escalated. No exceptions noted. For a selection of months, inspected the OMG minutes and the OMG meeting packs and noted that the MI had been reviewed. No exceptions noted.
For Currency Risk Management accounts, forward Estimate and Settlement letters are verified by the CSA Team by comparing the profit/loss position stated in the letter against the Cash Flow Warning System notification and closure of position email notification from Pareto's Trading team (settlement letter only). Once verified, the letter is signed by the Client Service Manager.	For a selection of Currency Risk Management accounts, inspected the settlement letter and email trail and noted that the letters had been verified by the CSA team, and that the letter had been approved by the Client Services Manager. No exceptions noted.

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

Corporate action entitlement data is supplied by the custodian and an independent data vendor. The NT Corporate Actions team reconciles the two data sources and any discrepancies are checked against a third independent data source.

For each corporate action event, a file is established containing all records and information relating to the corporate action. Each file has a pro forma cover sheet that sets out a checklist of the tasks that must be completed for the corporate action. Each task on the checklist is signed on completion by the member of the NT Corporate Actions team who completes the task. The file also contains copies of all correspondence related to the corporate action.

Once independent sources have been verified and any discrepancies have been resolved with the custodian, entitlement information is input into Fundmaster and the Corporate Actions Delivery and Response System (CDR), which is an automated corporate event system at NT, by the NT Corporate Actions team. The entitlement information is reviewed by a senior member of the NT Corporate Actions team who signs the checklist to evidence the check. The checklists are retained by NT in the corporate actions file.

For those corporate actions which require actions or decisions to be taken at a future date, an electronic diary system is used to record the dates and actions required. Access to the system is restricted to Corporate Action team members and data changes are authorised by a senior team member.

For voluntary corporate action events that require a decision on the options to be selected, the NT Corporate Actions team completes a standard form on CDR setting out the details of the corporate action, the options available and any relevant deadlines for decision. The form is given to the relevant Fund Manager, who completes the form on CDR with the preferred option, authorises and returns it to the NT Corporate Actions team. The relevant option is actioned by the NT Corporate Actions team and the decision form is retained in the corporate actions file.

The NT Corporate Actions team sends the election either by custodian proprietary link, or fax. A NT Corporate Action analyst inputs the instruction and a senior team member authorises it to be sent. For proprietary link instructions, evidence is available from the custodian website. For fax instructions, the copy of the fax is retained in the corporate actions file.

As part of the cash and stock reconciliation process, the NT Quality Assurance team identifies any differences between stocks and/or cash actually received in respect of NT Corporate Actions compared to the entitlement expected using the TLM system. The cash and stock transactions are fed into TLM from Fundmaster through an automated interface. Any differences are investigated and resolved by the NT Corporate Actions team and evidence of this is retained electronically in TLM. Outstanding issues relating to corporate actions are reviewed at regular service review meetings with the custodians.

A robust suite of Management Information and reports are produced on a weekly and monthly basis by NT Operations for Insight to monitor the timely and accurate processing of all Corporate Actions. Issue logs are maintained and regular service review meetings are held to ensure that all issues that impact Corporate Action related activity are discussed, escalated and resolved appropriately.

Detailed Controls	Tests Performed by KPMG LLP and Results
NT provides weekly MI detailing the processing of Corporate Actions. The MI is reviewed at the weekly Market Operations FSM. The MI and minutes of the FSM are retained by Insight Middle Office.	For a selection of weeks, inspected the Market Operations FSM minutes and noted that the MI on Corporate Actions had been discussed. No exceptions noted.
Monthly KPIs on timeliness and accuracy of Corporate Actions processing are sent to Insight Middle Office. The monthly KPIs are discussed at the next weekly Market Operations FSM and at the monthly SMC meeting. The MI and minutes of the meetings are retained by Insight Middle Office.	For a selection of weeks, inspected the minutes of the Market Operations FSM and noted that the KPIs had been discussed. No exceptions noted. For a selection of months, inspected the minutes of the SMC for evidence that the KPIs had been reviewed by the committee. No exceptions noted.

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

Proxy votes are cast on behalf of Insight by our voting agency Manifest, an external data source, voting service and research provider. Manifest identifies all resolutions where Insight's clients have a right to vote. The Middle Office team electronically connect to the voting agency using their custom designed web-based software. Middle Office monitors the system on a twice weekly basis to identify any forthcoming company events. Middle Office email all the forthcoming company events and company information listed in Manifest to the Fund Manager. The Fund Manager independently reviews the reports for each company event for any unusual items and provides voting instructions to Middle Office. Middle Office then record the votes in Manifest and the system updates the vote status to 'confirmed'. Where an event vote status has not been confirmed, Manifest notifies Middle Office via email before the date when voting is due in Manifest. Middle Office escalates the upcoming events to the Fund Manager for action.

Detailed Controls	Tests Performed by KPMG LLP and Results
Manifest identifies all resolutions where Insight's clients have a right to vote. All resolutions are flagged to Insight in Manifest. Middle Office monitor the system on a twice weekly basis to identify any forthcoming company events. Middle Office email all the forthcoming company events and company information listed in Manifest to the Fund Manager. The company information is detailed in a research report which includes the company background, financials and all the resolutions due for vote. The Fund Manager independently reviews the reports for each company event for any unusual items and provides voting instructions to Middle Office via email as evidence of the review. Middle Office then record the votes in Manifest and the system updates the vote status to 'confirmed'. The audit trail is retained by Middle Office. Where an event vote status has not been confirmed, Manifest notifies Middle Office via email before the date when voting is due in Manifest. Middle Office escalate the upcoming events to the Fund Manager for action.	KPMG observed the Manifest system and noted that forthcoming events were recorded and vote status was tracked in the system. For a selection of resolutions, inspected the email trail between Middle Office and the Fund Manager and noted that the Fund Manager provided voting instructions for the resolutions. KPMG also inspected the Manifest report and noted that the votes had been recorded in the system. No exceptions noted For a selection of resolutions, inspected the 'votes due' reminder email and noted that the automated email had been generated by Manifest. KPMG also inspected the email trail with the Fund Manager and noted that voting instructions had been provided. No exceptions noted

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

Client withdrawal requests are only accepted in writing and signed by designated signatories in accordance with the terms of the agreement between the client and Insight. Individual client instructed cash flows are accepted in writing or via email to specified Insight cash posting email address. Cash instructions are processed and validated by the CSA team prior to forwarding to Insight's cash posting team.

For Currency Risk Management accounts, the Pareto Client Portfolio Management (CPM) team perform a periodic revaluation process as mandated by the client. The Revaluation process takes into account changes in the underlying assets and currencies for updating portfolio data within the model. The data is uploaded via the Revaluation tool which electronically maintains an audit trail of sign-off. The application Matador can be used for a process overview to track the progress of revaluations and provides details of the process history.

Detailed Controls	Tests Performed by KPMG LLP and Results
Individual client instructed cash flows are accepted in writing, or via email to a specified Insight cash postings email address. Cash instructions are processed and validated by the CS team prior to forwarding to Insight's cash posting team. Written instructions are signed by authorised signatories in accordance with the terms of the agreement and validated against the approved signatory list within the IMA. The cash flow is processed by the Insight cash postings team. One member of the team will input the cash flow instruction data, and another member of the team will review the date for completeness and accuracy prior to posting. Any exceptions are highlighted by the Insight cash postings team and escalated to the relevant Client Service Associate for review. A record of the authorised instruction, authorised signatory list and e-mail notification is retained.	For a selection of client payment instructions, inspected the signed client instructions and relevant authorised signatory list to determine whether the client instructions had been validated by the CS team. KPMG also inspected the cash flow posting to determine whether the instruction had been input completely and accurately, and it had been input and authorised by two members of the payments team. **Exception noted:** For 10 out of 40 client instructed payments selected, Insight were unable to produce the original signed client instruction. **Management Response:** The cash payments process was insourced from Northern Trust in August 2012. This resulted in a number of legacy regular payments moving from NT to Insight. A subsequent review of the process highlighted the fact that the original client instructions when each payment was established had not been retained by NT. This is in not in line with Insight's current procedures. At this point Insight assessed the risk profile of each client (and payment) for which there was no original authorisation on file. This was performed using the criteria for simplified due diligence. Each client and payment was concluded to be low risk and therefore a decision was made to re-seek the client instructions for filing at the next client review date. Low risk clients are on a 3 year cycle and therefore these original client instructions will not be on file until late 2015.

For Currency Risk Management accounts, clients' underlying portfolio data is loaded into the Currency Risk Model via the Revaluation tool. A member of the CPM team reviews the revaluation data received from the client for accuracy and then signs-off within the revaluation tool. A secondary review for completeness and accuracy is performed by another member of the CPM team, who also-signs off in the Revaluation tool as evidence of the review. Once the data has been input into the Revaluation tool, the system checks the live model trading percentage change for the total portfolio value against a set of tolerance levels. Any exceptions above tolerance levels are escalated by CPM to the client to verify the change. From August 2014, the application Matador is used to monitor the revaluation process (except for legacy CRM accounts). Matador maintains a complete process history in an online portal, which identifies the preparer and reviewer(s) of the revaluation data. After the model is run, a member of the CPM team reviews the Minimum Tracking Basket Output data for accuracy and signs off in the Matador tool. Any exceptions are escalated to Pareto Research for investigation. A member of the Research team reviews the Tracking Basket for any exceptions and signs off in the Matador tool as evidence of the review.	For a selection of clients (prior to August 2014), inspected the revaluation proof sheet and noted that revaluation data had been signed off by two members of the CPM team, and that the model had been signed off by CPM. KPMG also inspected the tracking basket and noted that the tracking basket data had been signed off by Research. No exceptions noted For a selection of clients (post August 2014), inspected the revaluation proof sheet and noted that revaluation data had been signed off in Matador by two members of the CPM team, and that the model had been signed off by CPM in Matador. KPMG also inspected the tracking basket and noted that the tracking basket data had been signed off by Research. No exceptions noted

4.3 MAINTAINING FINANCIAL AND OTHER RECORDS

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

Income entitlement data is supplied by custodians and an independent data vendor. The data is scrubbed by comparison of at least two data sources. Any discrepancies are highlighted on a hard copy exception report. The NT Income team reviews the exception report and investigates and resolves any differences through the use of further independent data sources and discussion with the custodians. Copies of the exception reports and actions taken to resolve discrepancies are retained.

Once verified, the income entitlement data is input directly to Fundmaster by NT Custody. Any amendments to the data are checked by a senior member of the NT Income team.

As part of the cash reconciliation process, the Quality Assurance team identifies any differences between cash actually received in respect of income actions compared to the entitlement expected using the TLM system. The cash transactions are fed into TLM from Fundmaster through an automated interface. The NT Income team investigates and resolves any identified differences and a TLM report is retained electronically to evidence resolution. Outstanding issues relating to income are reviewed at regular service review meetings between NT Operations and the custodians.

A robust suite of Management Information and reports are produced on a weekly and monthly basis by NT Operations for Insight to monitor the timely and accurate processing of Investment Income and any relevant tax implications. The MI includes Income entitlement and accruals, accuracy and timeliness of processing. Issue logs are maintained and regular service review meetings are held to ensure that all issues that impact Investment Income related activity are discussed, escalated and resolved appropriately (see Monitoring Compliance section 4.5.2).

Detailed Controls	Tests Performed by KPMG LLP and Results
The timely and accurate processing of income and related tax is completed by NT in line with the SLA. MI and KPIs on income processing, including income accrued but not received, are reported to Insight's Middle Office at the weekly Market Operations FSM. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of weeks, inspected minutes of the Market Operations FSM and noted that the weekly MI on income processing had been discussed. No exceptions noted.

4.3.2 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

Listed securities prices and foreign exchange rates are checked and validated on a daily basis by the NT Pricing and Data Management team.

Prices are sourced from Northern Trust's internal pricing system, which sources its data from a wide range of vendors. The prices are scrubbed by cross vendor validation and price movement outside of tolerance for a specific market or instrument is flagged for investigation prior to feeding through to downstream systems.

Prices from the primary data vendor / Northern Trust are loaded into Fundmaster electronically. If any differences are found during the validation process, the Pricing and Data Management team conducts validation checks and manually corrects Fundmaster.

A pro forma checklist of tasks required to manually amend the security price is followed and signed off by the member of the Pricing and Data Management team making the price change. The manual input to Fundmaster is printed and reviewed by a second member of the team who signs off the checklist to evidence the review.

The Pricing and Data Management team maintains a list of security prices for securities not priced on a listed exchange or any other official price source, and updates it monthly by sending written requests to companies or brokers by fax, email or the Bloomberg message facility. Once obtained, the prices are manually input to Fundmaster and the relevant records kept on file.

For OTC derivatives, prices are generated by Insight through Xenomorph using independent external feeds of underlying market data from reputable pricing vendors and selecting the most appropriate inputs available for each of the assets held. Pricing models are developed by the IT Quantitative Development team in conjunction with Investment Risk and Fund Management. The models are independently validated and their output tested for accuracy before being released into production. The Derivative Risk Committee ensures that no OTC instrument is used until the accuracy of pricing capability has been evidenced. There is continuous review of market data, daily tolerance checks, validation of external pricing sources and active participation in the market to resolve pricing disputes.

A daily price review report from NT Operations detailing any unusual impacts to Pricing and Positions is sent to Insight IT. An email notification is then sent to the respective Insight Fund Manager(s). For any issues identified, root cause analysis and resolution is undertaken by NT Operations and findings are communicated to Insight IT throughout the day. Middle Office inform Fund Manager(s) of these findings.

Detailed Controls	Tests Performed by KPMG LLP and Results
A daily price review report from NT Operations is sent to Insight IT with any unusual impacts to pricing and positions. The report is reviewed by Insight Middle Office and any issues are escalated to Fund Managers via email. Insight Middle Office retain copies of the daily reports evidencing the resolution, including the notification to the Fund Manager. A summary of each week's daily review statistics is included within the Data Management & Pricing MI at the weekly Data Management FSM with commentary detailing why any prices have been amended as part of the daily review process. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of dates, inspected the daily review reports and noted that the report had been reviewed by Middle Office. KPMG also inspected the email notifications to the fund managers and noted that exceptions had been monitored to resolution. No exceptions noted. For a selection of weeks, inspected the weekly Data Management FSM minutes and noted that the pricing statistics had been discussed. No exceptions noted.
Prior to data being loaded into Xenomorph for curve construction and OTC pricing, there is a rule-based pre-validation data exception process performed within CADIS. A pre-pricing rule-based review and correction of Bloomberg/ Markit and Counterparty market data occurs automatically as part of the overnight OTC pricing batch. An email alerts Middle Office that a report is available on the application portal within the Intranet. Middle Office reviews the report for issues and escalates to Quantitative Operations via email. The email trail is retained.	For a selection of dates, inspected the morning OTC pricing report and email trail and noted that any exceptions within the report had been escalated to Quantitative Operations. No exceptions noted. For a selection of dates, inspected the evening OTC pricing report and email trail and noted that any exceptions within the report had been escalated to Quantitative Operations. No exceptions noted.
A daily report is generated within the Application portal on the Intranet after the pricing batch has finished identifying (a) any exceptions, spikes, stale or missing market data items market inputs to the overnight pricing (b) any exceptions, spikes, null or missing items in the set of prices generated by the overnight pricing batch. Middle Office reviews the report for issues and escalates to Quantitative Operations via email. On a weekly basis, Middle Office review TriOptima reports to identify any un-matched or mismatched trades, and trades with MTM valuation differences above specified tolerances. Exceptions with a persistent theme are logged on the OPC issues log. Any unresolved exceptions are escalated to the monthly OTC Pricing Committee and the quarterly DRC for review. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of months, inspected the OTC actions log and noted that exceptions had been monitored and actioned. No exceptions noted. For a selection of weeks, inspected the TriOptima reports and noted that the data had been reviewed by Middle Office. No exceptions noted. For a selection of months, inspected the OTC Pricing Committee minutes and DRC minutes and noted that exceptions had been discussed and followed up. No exceptions noted.

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

Cash records are maintained in Fundmaster for each client and reconciled to custodian records on a daily basis using TLM, an automated reconciliation system, by the NT Quality Assurance team.

Electronic SWIFT messages are received from the relevant custodians detailing all cash transactions for the previous day.

The messages interface directly into TLM, together with a file of all cash transactions recorded on Fundmaster. TLM electronically matches the custodian and Fundmaster transactions and identifies transactions that do not match. The Quality Assurance team is responsible for completion of reconciliations and ensuring that all outstanding items are resolved.

The Quality Assurance team investigates exceptions through a review of Insight's and the custodian's records and correspondence with the custodians. Exceptions may also be referred to the other operations teams for investigation, resolution and correction.

To maintain adequate segregation of duties, reconciliation and processing functions are separated within the Investment Operations department.

On a weekly basis the Quality Assurance team leader reviews a TLM report showing the number, value and age of all unresolved reconciling items and checks any items more than 30 days old to ensure that the actions being taken to resolve them are adequate. Each week that team leader issues an email setting out the results of the review to all senior managers in Investment Operations.

Where the client has appointed the custodian and the custodian is not able to provide electronic SWIFT messages, transactions are manually loaded on to TLM using information provided by fax by the custodian. The transactions are manually matched against the transactions downloaded from Fundmaster. A TLM reconciliation report evidences manually loaded trades.

Stock reconciliation is conducted using TLM to reconcile securities recorded on Fundmaster to those held at custodian. Electronic SWIFT messages are received from relevant custodian's detailing all stock positions at the month end. These are interfaced directly into TLM, together with a file of all stock positions recorded on Fundmaster. TLM electronically matches the custodian and Fundmaster positions and identifies positions that do not match. The Quality Assurance team has responsibility for completion of reconciliations and ensuring that all outstanding items are resolved. The Quality Assurance team investigates reconciling items, raises queries with the custodian or other Investment Operations teams, and ensures that issues are resolved.

TLM retains a full audit history of reconciling items and actions taken to resolve exceptions.

A robust suite of Management Information and reports are produced on a daily, weekly and monthly basis by NT Operations for Insight to monitor the completeness and accuracy of cash and security positions. Issue logs are maintained and regular functional service review meetings are held to ensure that all issues that impact the completeness and accuracy of cash and security positions are discussed, escalated and resolved appropriately.

For OTC Derivatives, a third-party tool (TriOptima) is used to reconcile Insight and counterparty terms & conditions (T&Cs) and MTM valuations for all OTC positions. Insights T&Cs and MTM valuations are loaded automatically after the overnight OTC pricing batch. On a weekly basis, Middle Office review TriOptima reports to identify un-matched/mis-matched trades and trades with MTM valuation differences above specified tolerances.

Detailed Controls	Tests Performed by KPMG LLP and Results
Daily MI and KPIs on cash and stock reconciliation breaks are reported to Insight Middle Office by NT. The MI and KPIs are reviewed at the weekly Market Operations FSM. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of weeks, inspected minutes of the Market Operations FSM and noted that the MI on cash and stock reconciliations breaks had been discussed. No exceptions noted.
Weekly MI on OTC trade volumes, ETD trade volumes, trade amendments and collateral disputes is monitored by Insight Middle Office at the weekly Derivative Operations FSM. Meeting minutes are retained.	For a selection of weeks, inspected the minutes of the Derivative Operations FSM and noted that the weekly MI on OTC trade volumes, ETD trade volumes, trade amendments and collateral dispute had been monitored. No exceptions noted.

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

Investment Management fees are typically calculated on a quarterly basis, or an agreed time period with the client. A calculation template is set up for each client containing the client specific fee rates and methodology as specified in the Investment Management Agreement. A member of the NT Client Administration team populates this template with the relevant data for the calculation period after the market values have been checked and reported to the client. A check sheet is completed during the process to ensure that all the relevant steps have been completed.

A Client Administration team manager verifies the calculations and signs off the check sheet evidencing their review. An invoice is then prepared and the details of the invoice are recorded on the fee invoice register.

Client investment fees are produced and checked by NT Client Administration. In line with the agreed Service Level Agreement, Insight receives monthly status reports detailing the accuracy and timeliness of client invoicing. A gatekeeper list of invoices is maintained by Insight Finance. The list contains any invoice requested by Finance or the Client Director. The Finance team reviews the invoices and confirms the accuracy of calculations to Northern Trust.

Detailed Controls	Tests Performed by KPMG LLP and Results
NT produce weekly invoice status reports for Insight Finance. On the second and third months of each quarter, Insight Finance and NT have a formal meeting to discuss status and review any invoice issues.	For a selection of months, inspected the minutes of the monthly meetings and noted that the status reports had been discussed. No exceptions noted.
A gatekeeper list of invoices requiring additional review is maintained by Insight Finance each quarter. Insight Finance review these invoices for accuracy and evidence review by sign off via email prior to issue.	For a selection of quarters, inspected the gatekeeper list of invoices, and the email trail between NT and Insight, and noted that the gatekeeper list had been approved by Insight. No exceptions noted.

4.4 SAFEGUARDING ASSETS

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

Uninvested cash is managed with regard to diversification of risk and security of funds. Cash is managed in line with the restrictions recorded in a fund's IMA, prospectus or guidelines. Where Insight's Liquidity Fund ('ILF') is a permitted asset, and subject to any regulatory or fund specific client restrictions, uninvested cash is swept into the ILF subject to any cash buffer required to be retained by the Fund Manager. Cash buffers retained are held on account with the Fund's appointed Custodian. Where ILF is not a permitted asset, uninvested cash is held on account with the fund's appointed custodian or placed on term deposit. Compliance with fund guidelines is monitored by Insight's automated compliance engine within thinkFolio. The ILF is an AAA rated Irish authorised collective investment vehicle, which is administered by Northern Trust (Dublin).

Detailed Controls	Tests Performed by KPMG LLP and Results
Investment guidelines and restrictions documented in the IMA are signed off by authorised signatories of Insight and the client. Where permitted by the IMA, diversification of risk is achieved by sweeping uninvested cash into the ILF, a triple A rated money market fund. Investment Guidelines specified in the IMAs are 'hard' coded into thinkFolio (no override possible), or 'soft' coded (warning can be overridden by the Fund Manager). Overridden warnings and rationale are reported on the pre-trade breach report. The pre-trade overrides are reviewed daily using the pre-trade functionality on thinkFolio by a member of Mandate Control to review Fund Manager rationale and also to identify any coding errors. Incidents are reviewed on a T+1 by a member of the Mandate Control Team. The audit trail of post-trade review is maintained within the thinkFolio system. Any active breaches, and proposed actions, are logged in the incident reporting system (IRS) and tracked by Compliance. Outstanding actions are reported to the monthly Risk Management Committee. Meeting minutes are retained.	For a selection of clients, inspected the signed IMA and noted that the investment guidelines stated that uninvested cash can be invested in in-house funds. KPMG also inspected the units holding report for the ILF and noted that uninvested cash had been invested in the ILF during the period. KPMG inspected the incidents register and noted that no incidents related to uninvested cash. No exceptions noted.

4.5 MONITORING COMPLIANCE

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

Client restrictions are coded into thinkFolio by the Mandate Control team (see 'Accepting Clients' section) and compliance with the investment guidelines is monitored by the Risk Management team on a daily basis.

'Hard' and 'Soft' restrictions are coded into thinkFolio. 'Soft' coded restrictions can be overridden by the Fund Manager with an appropriate rationale. The pre-trade report is reviewed daily using the pre-trade functionality on thinkFolio by a member of the Mandate Control team to identify coding errors. A post-trade report from thinkFolio is also run and reviewed daily by a member of the Mandate Control. The audit trail of post-trade review is maintained within the thinkFolio system. Where a breach is confirmed, an incident report is recorded on the Incident Reporting System in accordance with the breaches policy and reporting procedure. 'Hard' restrictions cannot be overridden and the trade cannot, therefore be processed.

Algo Risk is the on-line risk management interface used by Insight's portfolio managers to monitor portfolio risk and factor sensitivities in real time. Algo Risk provides detailed and comprehensive portfolio risk analytics, scenario analysis and stress testing as well as risk-based limit monitoring and what-if analysis.

The performance data underlying the various Insight board and committee reports is produced by the Northern Trust Performance team. The numbers in these reports are all subject to Northern Trust's standard checking procedures. The Insight Performance team conducts its own review on all of the reports before they are used in any of the board or committee papers. Any issues identified in these checks are referred to Northern Trust for resolution. An issues log is maintained by Northern Trust and discussed daily with the Insight Performance team.

For Financial Solutions Group (FSG) clients, Insight's Performance team generate account performance reports using internal Insight systems. Performance reports are summarised and sent to the Investment Management Group for review.

For Currency Risk Management accounts, Pareto's Client Portfolio Management team generate performance reports using internal Insight systems. Performance reports are summarised and sent to the Pareto Investment Management Group for review.

Detailed Controls	Tests Performed by KPMG LLP and Results
Investment Guidelines specified in the IMAs are 'hard' coded into thinkFolio (no override possible), or 'soft' coded (warning can be overridden by the Fund Manager). Overridden warnings and rationale are reported on the pre-trade breach report. The pre-trade overrides are reviewed daily using the pre-trade functionality on thinkFolio by a member of Mandate Control to review Fund Manager rationale and also to identify any coding errors. Incidents are reviewed on a T+1 basis by a member of the Mandate Control Team. The audit trail of post-trade review is maintained within the thinkFolio system. Any active breaches, and proposed actions, are logged in the incident reporting system (IRS) and tracked by Compliance. Outstanding actions are reported to the monthly Risk Management Committee. Meeting minutes are retained.	For a selection of dates, inspected the pre-trade override report and noted that the report had been reviewed by Mandate Control. No exceptions noted. For a selection of dates, inspected the post-trade breach reports and noted that the report had been reviewed by Mandate Control. No exceptions noted. For any breaches identified in the selection of dates, inspected the Incident Reporting System register and noted that the incident had been raised and monitored in the system. No exceptions noted. For a selection of months, inspected the RMC minutes and noted that outstanding actions had been reported and discussed. No exceptions noted.
For FSG clients, Insight's Performance team generate account performance reports using internal Insight systems. The performance reports are approved by the Fund Manager and then summarised performance reports are sent to the Investment Management Group for review. Minutes of the meetings evidence the review of account performance.	For a selection of FSG clients, inspected the monthly performance reports and fund manager approval email, and noted that the performance report had been generated and approved. No exceptions noted. For a selection of months, inspected the IMG meeting packs and noted that the account performance reports had been monitored. No exceptions noted.
For all other clients, Insight's Performance team receive monthly account performance reports from NT. MI on performance reporting is summarised and sent to the Investment Management Group for review. Minutes from these meetings evidence the review of account performance.	For a selection of months, inspected the IMG minutes and the IMG meeting packs and noted that the MI on performance reporting had been monitored. No exceptions noted.

For Currency Risk Management accounts, Investment guidelines and restrictions documented in the IMA are signed off by authorised signatories of Insight and the client. These are coded into the currency risk model by Pareto's Research team and Currency Application Support team. Models are rolled out into the live environment by the Currency Application Support team. The Client Account Setup Schedule is signed by Pareto Research and Currency application Support team as evidence that the model parameters are coded accurately. Following authorisation of Amendments to a client IMA, the Client Portfolio Management team communicates via email any change in model parameters to the Research team. Following completion of the amendment by the Pareto Research team, the Account Change Form is signed by the Pareto Research team and Client Portfolio Management team to evidence the change has been implemented accurately. Account Change Form is retained as evidence of the amendment.	For a selection of new accounts, inspected the account set-up schedule to determine whether the schedule had been signed off by Research and CAS to verify the accuracy and completeness of the restrictions coded. **Exception noted:** For 1 out of the 2 clients selected, it was noted that the signed account set up schedule had not been retained. **Management Response:** The missing Account Set-up Schedule above refers to an existing account transition. All investment management activities were handled correctly. However, the CPM team failed to follow the procedure of filing a paper based Account Set-up Schedule. The remedial action was to remind members of the CPM team to follow the established procedure. For a selection of amendments, inspected the account change form and noted that the form had been reviewed and signed off by both Research and CPM. No exceptions noted.
For Currency Risk Management clients, client performance data is generated monthly and sent to the Pareto Investment Management Group for review. Minutes from these meetings evidence the review of account performance.	For a selection of months, inspected the Pareto IMG meeting packs and noted that account performance had been reviewed. No exceptions noted.

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

The selection and appointment of outsource partners follows a disciplined process compliant with the outsourcing policy and regulatory requirements. Where necessary, specialist consultants are appointed to assist in the process which includes identification of possible suppliers, shortlisting, RFP assessment, due diligence and detailed contract review utilising appropriate legal support.

Insight's Chief Operating Officer has overall responsibility for Insight's outsourced arrangements. This is clearly articulated in his Senior Management Job Description. Senior management governance for the arrangements is provided through Insight's Executive Management Committee and Board as appropriate. Business as usual monitoring is in place through the Operations Management Group, dedicated Middle Office teams and a range of regular service review meetings at various appropriate levels. Appropriate policies and procedures are in place to govern day to day operations.

Legally binding contracts and detailed service level agreements are in place with suppliers. The contracts contain all the key 'control' elements required including contingency and Disaster Recovery arrangements (and regular testing thereof), protection of confidential information and appropriate access to premises and information for auditors and regulators.

The contracts also contain 'service credit' arrangements to create additional financial motivation for the provision of acceptable/desired service levels by suppliers. These are based on performance against a range of clearly articulated and reported benchmarks, measured in the form of Key Performance Indicators (KPIs), across the entire range of services provided.

Outsourcer performance is monitored by experienced dedicated teams within Insight who manage the day to day outsource relationships and act as interface between the outsourcer and Insight teams where appropriate. Relevant KPI reporting is received at various appropriate frequencies. Issues, and any required actions, are discussed at a range of regular service management meetings. Robust incident/breach reporting and escalation processes are in place between outsource suppliers and Insight.

Any significant issues emerging are escalated within Insight in accordance with the internal governance structure. This consists of the Risk Management Committee, comprising of Insight's executive directors, Group Risk and Audit divisions and ultimately, the Insight Board. Any issues for the attention of the Regulator are communicated by Insight Risk Management at the appropriate time.

For NT, in addition to the general service management meetings, a senior management Joint Oversight Committee (JOC) meets quarterly. The meeting is attended by the NT & Insight Heads of Operations and any significant issues and trends escalated from the weekly MI or monthly KPIs are discussed.

Conflicts of interest are recorded and managed under the Conflicts of Interest requirements set out in Insight's Compliance Manual. Conflicts of interest are also monitored in the functional reviews undertaken by Compliance. Where Insight has, or may have, a conflict of interest between itself and its customer, or between one customer and another customer, Insight pays due regard to the interests of each customer and manage the conflict of interest fairly. Also, under FCA SYSC (Systems and Controls) Rules, Insight is required to maintain and operate effective arrangements to take all reasonable steps to prevent conflicts from giving rise to a material risk of damage to the interest of clients. If arrangements cannot be made to manage the conflicts then, as a last resort, disclosure is made to the client before undertaking business.

Detailed Controls	Tests Performed by KPMG LLP and Results
The Service Level Agreement with NT Operations defines the operational service standards for the activities that are outsourced to NT Operations. The SLA is formally reviewed by Insight and NT Operations at least every 3 years to check that the SLA is appropriate and to reflect relevant changes. Final versions are jointly signed off by the relevant personnel at Insight and NT.	Limitation of Scope: KPMG was unable to ascertain the operating effectiveness of this control as there were no formal review during the period under review.
Conflicts of interest are managed by Compliance, a record of which is maintained in the Conflict of Interest Register. Newly identified conflicts are recorded on the register by Compliance. Any action points are followed up to resolution by Compliance with colleagues who are in conflict and recorded in the Conflict of Interest Register. A copy of the register is retained as evidence of resolution of conflicts of interest. Conflicts of interest are reported to the RMC for review. The RMC meets on a monthly basis. On a quarterly basis, the Executive Management Committee complete a conflicts of interest attestation to state that, to their knowledge, there have been no other conflicts of interest.	KPMG enquired of the Compliance Manager, as to whether there had been any new conflicts during the year and were informed that there had been 3 new conflicts. KPMG inspected the Conflicts of Interest register and noted that new conflicts during the year had been recorded, and that all actions taken in the resolution of conflicts had been recorded. No exceptions noted. For a selection of months, KPMG inspected the RMC minutes and noted that conflicts of interest had been discussed. No exceptions noted. For a selection of quarters, KPMG inspected the EMC confirmations and noted that the confirmation had been signed off by the EMC member. No exceptions noted.
Daily issues logs are maintained by NT. The issues logs are reviewed at the weekly Market Operations FSM. Any outstanding issues or actions are escalated to the monthly SMC. The minutes of the meetings are retained by Insight Middle Office.	For a selection of weeks, inspected the minutes of the Market Operations FSM and noted that issues had been monitored. No exceptions noted. For a selection of months, inspected the minutes of the monthly SMC and noted that any outstanding issues had been escalated and discussed by the committee. No exceptions noted.

Any significant performance issues or trends highlighted in the MI or KPIs reported by NT, in line with the SLA, are escalated to the Joint Oversight Committee (JOC) for oversight and resolution. The JOC is attended by NT & Insight Heads of Operations. The meetings are held on a quarterly basis. Meeting minutes are retained.	For a selection of quarters, inspected the JOC meeting minutes and noted that significant issues or trends within the MI and KPIs had been reviewed. No exceptions noted.

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

The incident reporting policy documents the process for identifying, reporting and escalating errors, losses, complaints or breaches. Incidents are recorded on the Insight Incident Reporting System (IRS) by the business areas that identify the incident and systemically escalated for senior management and compliance sign off depending on the severity and / or type of the incident. Actions to prevent re-occurrence are recorded in IRS. The Risk Management team actively manages the process to ensure the completeness of information and timely closure. Losses over £5,000, critical systems failure and all regulatory breaches are defined as significant incidents, which are independently reported to the Risk Management Committee by the Risk Management team.

A process is in place to ensure the Risk Management team are immediately notified of the complaint if it is from or on behalf of an 'eligible complainant', the complaint has come via the Financial Ombudsman Service, or the complainant is taking legal action (the Legal department is also advised). The complaints handling process is reviewed every 18 months as part of the Institutional Client Service review. A review report with any agreed actions is written and distributed to the appropriate areas. Any outstanding actions are monitored to completion by the Risk Management team.

Compensation offers are fair in relation to the acts or omissions for which Insight is deemed responsible. The Incident Reporting System integrates the incident reporting and payment authorisation processes into a bespoke workflow application administered by Risk Management. The authorised payment request is part of the workflow and sent to NT or the Finance department for payment.

Detailed Controls	Tests Performed by KPMG LLP and Results
The incident reporting system (IRS) documents identified complaints, breaches and errors. For any breaches logged, senior management monitor the incident reported in IRS and sign off electronically as evidence of review. An audit trail is retained in IRS.	For a selection of incidents reported during the year, inspected IRS records and noted that the incidents had been investigated and signed off by senior management. No exceptions noted.
Any incident causing a loss in excess of £5,000 is reported to the RMC for review. The minutes of the meetings are retained.	For a selection of months, inspected the RMC meeting packs and minutes and noted that significant incidents had been discussed. No exceptions noted.
Significant incidents are reported to the Operational Governance Committees (IMG and OMG) for review on a monthly basis. Minutes of the meetings are retained. The actions taken to resolve incidents are documented in IRS. An audit trail is retained in IRS, which shows the history of actions taken to resolve the incident.	For a selection of months, inspected the IMG and OMG meeting packs and noted that significant incidents had been reported to the committees. No exceptions noted.

Front Office review and document transaction errors in IRS and Department Heads authorise any compensation through sign-off in IRS. For compensation payable to Insight's clients, a request is sent to NT by Corporate Risk. Corporate Risk and Investment Operations sign-off the payment form to evidence authorisation. Copies of the payment requests are retained.	For a selection of incidents reported during the year, inspected the IRS audit trail and noted that the incident had been signed off by the relevant department head and business head. No exceptions noted. For a selection of incidents reported during the year, inspected the payment request forms sent to NT and noted that the payment form had been signed off by Corporate Risk and Investment Operations. No exceptions noted.

4.5.4 Counterparty exposures are monitored

Insight's Credit and Counterparty Committee has the overall responsibility for oversight of counterparties, counterparty exposures and collateral policy. The CCC is chaired by Insight's CRO and membership includes Heads of Division across the business.

Insight's Money Market Counterparty Committee (MMCC) has responsibility for oversight of counterparty and counterparty exposures for cash and near cash investments with whom Insight deals as an agent on behalf of its clients. Membership of MMCC includes the Head of Credit Analysis and the Head of Money Markets. The MMCC is a sub-committee of Insight's Credit and Counterparty Committee.

European Market Infrastructure Regulation ('EMIR')

Counterparties are required to have agreed detailed procedures and processes to deal with disputes over valuation or collateral relating to non-cleared OTC derivatives positions. The disputes must be resolved in a timely manner and specific processes must be in place for any disputes that are not resolved within five business days. Any disputes for an amount greater than €15m that are outstanding for over 15 business days needs to be reported to the national regulator.

Detailed Controls	Tests Performed by KPMG LLP and Results
Insight's Money Market Counterparty Committee (MMCC) meets at least ten times within a calendar year to monitor and review counterparties and counterparty exposures for cash and near cash investments with whom Insight deals as agent on behalf of clients. This information is monitored against quantitate risk indicators. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of months, inspected the MMCC meeting minutes and noted that counterparties and counterparty exposures had been discussed. No exceptions noted.
Insight's Credit and Counterparty Committee (CCC) meets at least ten times within a calendar year to monitor and review counterparties, counterparty exposures and collateral policy. This information is monitored against the requirements outlined in the OTC Counterparty Credit Policy. The results of the discussion are documented in meeting minutes, which are retained.	For a selection of months, inspected the CCC meeting minutes and noted that counterparties, counterparty exposures and collateral policy had been discussed. No exceptions noted.

Weekly MI on collateral movements, collateral disputes and collateral cash and stock reconciliations is monitored by Insight Middle Office at the weekly Derivative Operations FSM. Meeting minutes are retained as evidence of the discussion. In addition, Middle Office reviews Daily Collateral Disputes and takes appropriate action. The review is evidenced within the Daily Collateral Disputes File. Middle Office review collateral disputes for any that are EMIR reportable. A summary is provided to the DRC on a quarterly basis.	For a selection of dates, inspected the daily collateral disputes file and noted that the data had been investigated by Insight Middle Office. No exceptions noted. For a selection of weeks, inspected the minutes of the Derivative Operations FSM and noted that the weekly MI on collateral movements, collateral disputes and collateral cash and stock reconciliations had been monitored. No exceptions noted. For a selection of months, inspected the DRC minutes and noted that an EMIR report for collateral disputes had been reported and monitored at the committee meeting. No exceptions noted.

4.6 REPORTING TO CLIENTS

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

The completeness and accuracy of transactions and holdings is covered by the stock and cash reconciliation process in section 4.3. Commissions and Voting are covered in section 4.2, and the Monitoring Compliance in section 4.5. Performance calculations are part of the outsourced operation to NT (refer to monitoring of outsourced functions in the Monitoring Compliance section 4.5.2).

Regular reports, including valuations and performance data, are issued in accordance with regulatory requirements and the customer's own needs. Client valuations are generated by the NT Management Reporting system and are sent to clients in accordance with deadlines in the client agreement or within 25 business days after the end of the period to which they relate, whichever is earlier.

Performance is calculated in the PACE performance reporting system and sent to the Client Administration team daily.

Each client is assigned a client administrator who produces the reports and is familiar with the client's portfolio. A checklist of tasks required to ensure that valuations are accurate and issued in a timely manner is used when preparing client valuations and reports. Each task on the checklist is signed as it is completed. A team leader or senior colleague reviews the reports and the checklist before the reports are issued, and signs the checklist as evidence to that review.

The checks performed to ensure the accuracy of client reports vary depending on the nature of the contract the client has with Insight and the type of reporting provided to the client. Checks are included to ensure that:

- Cash and stock reconciliations have been completed and that no material reconciling items remain unresolved
- All income due to the client in the period has been received
- The performance return recorded in the valuation is accurate
- The dates of the reports are correct and in accordance with the client's requirements and regulatory requirements
- All reports in the client pack are consistent with one another and that the information appears reasonable in the context of the client's portfolio

In order to monitor progress and achievement of reporting deadlines against client and regulatory requirements, the Client Administration team maintains a 'performance log'; a record of target dates that must be achieved for the key tasks required to deliver the reports in a timely manner.

The actual date on which each task is completed is recorded against the target date. The team leader reviews the performance log to monitor progress and identify any potential delays. The performance log is electronically archived every month and used to provide monthly statistics to senior management on the timeliness of client reporting.

A robust suite of Management Information and reports are produced on a daily, weekly and monthly basis by NT Operations for Insight to monitor the timeliness and accuracy of client reporting. Issue logs are maintained and regular service review meetings are held to ensure that all issues that impact the timeliness and accuracy of client reporting are discussed, escalated and resolved appropriately.

For Currency Risk Management accounts, Pareto's Client Portfolio Management team is responsible for performance reporting. The performance calculations and other portfolio data shown in the reports are sourced from the Porpoise performance calculation system. Monthly reports are reviewed by a member of the Pareto Client Portfolio Management team prior to distribution.

Detailed Controls	Tests Performed by KPMG LLP and Results
In line with the agreed SLA, Insight receives weekly status reports on the timeliness of Client Reporting, and monthly MI on the accuracy and timeliness of Client Reporting, from NT Operations. The weekly status reports are monitored in the weekly Client Administration FSM and all action points are logged in the Client Administration FSM actions log. Any issues are logged in an issues log and tracked to closure by Client Administration. The monthly MI from NT Operations is reviewed at the next Client Administration FSM.	For a selection of weeks, inspected the weekly Client Administration FSM actions log and noted that issues highlighted in the weekly status reports had been logged and followed up. For a selection of months, inspected the minutes of the Client Administration FSM and noted that the Monthly MI has been reviewed. No exceptions noted.
For Currency Risk Management accounts, monthly client reports from the Client Reporting System are reviewed by a member of the CPM team. Once the client report is confirmed as accurate and complete, the member of CPM signs off on the monthly review spreadsheet, prior to dispatch. A monthly review spreadsheet is kept by CPM indicating the individual responsible and date of review of the client report as evidence of their review.	For a selection of months, inspected the monthly review spreadsheet and noted that the client performance reports had been signed off by CPM. No exceptions noted.

4.7 INFORMATION TECHNOLOGY

4.7.1 Restricting Access to Systems and Data

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

Physical access to Insight's premises is restricted by turnstiles and building security staff at the entrance of the building. Insight office space is restricted to authorised individuals by swipe card access.

All servers including media servers, application servers and network fileservers are installed in the communications rooms which are located within the Insight office space. In addition to the general office space restrictions, physical access to communications rooms requires a swipe card. Access to these rooms is restricted to Insight IT colleagues who have been approved by the Head of IT Operations (or their direct report). The physical access capabilities of building security and maintenance staff are controlled by building management. Reports of all access into the communications rooms are generated and reviewed weekly by the building landlord. Any unauthorised or suspicious entries identified are escalated to the Core Infrastructure Services manager or the Head of IT Operations for further investigation. Reports showing IT colleagues with access to the communication rooms are produced biannually, verified and signed off by the Head of IT Operations (or a direct report) manager. CCTV Cameras record the entrance to all of the communication rooms.

There is a dedicated Insight IT security manager responsible for all Insight IT security matters. All program documentation is stored electronically on the central file servers which are installed in the communications rooms.

Detailed Controls	Tests Performed by KPMG LLP and Results
Building security, passes and turnstiles are in place to prevent unauthorised access to building.	Observed the building entrances and noted the presence of building security staff, turnstiles in the ground floor entrance and swipe card readers to access the building. No exceptions noted.
Reports showing permitted access to communications rooms are produced biannually and signed off by the Head of IT Operations and Facilities (or his delegate). Visitors and contractors are escorted by a pass-holder.	Inspected communication for a selection of two access reports to evidence management review and approval by the Head of IT Operations and Facilities. Also noted that exceptions identified during the review were actioned upon by the building security team of Bank of New York Mellon. Observed contractors and visitor access to the communications room and noted that they were required to sign in with building security, and were escorted by an authorised pass holder. No exceptions noted.
All servers including media servers, application servers and network fileservers are installed within the physically secure communications rooms	Observed the communication rooms and noted that the media servers, application servers and network fileservers were physically present in the communications room. Inspected the server list maintained by the Infrastructure Support Team to determine the location of the servers. Observed that entry to the communications room was restricted to authorised personnel by means of a proximity access reader. No exceptions noted.
Communication rooms have restricted access with proximity access cards. Access to communication rooms is restricted to personnel who have been approved by the Head of IT Operations (or a direct report).	Observed entry to the communication rooms and noted that proximity access cards are required to gain access to the communication room. For a selection of users, inspected email evidence and noted the authorization by the Head of IT Operations of physical access to the communications room. No exceptions noted.

All equipment and backups stored in the DR site communications room are in a physically separated area with restricted access. Access is restricted to individuals approved by the Head of IT Operations (or a direct report).	Observed and noted that server backups are located in a physically separated area with restricted access. For a selection of users with access to the communications room at the DR site, noted evidence of approval from the Head of IT Operations. No exceptions noted.
Responsibility for approving security staff and maintenance staff access is delegated to the Head of Security and Head of Office Management on site at Insight's office respectively.	For a selection of security and maintenance staff provided access to the Insight Offices, inspected the access request forms and noted that the access had been approved by the Head of Security or the Head of Facilities. No exceptions noted.

4.7.1.2 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

Unauthorised network access is prevented through the use of user log-on IDs and passwords. Colleagues can only access applications appropriate to their function.

System log-on IDs and passwords are assigned to individual users by means of user accounts.

These accounts are authorised by the relevant line manager or department PA as part of the joiner's process and set-up by the IT Business Support team. Hard copies of joiner's forms are archived and on-line forms retained on the system.

At least twice a year IT Administration reconciles the list of personal network access accounts (Windows accounts) against legitimate reasons for an account to exist since the account owner may be a payroll employee, temporary staff or working for the Group. The reconciliation is approved by IT Security.

Colleagues leaving Insight have their system access accounts cancelled upon receipt of the leaver's form. For the majority of cases, the leaver's form is sent prior to the actual departure of the individual. In order to ensure that leaver's forms are generated for all staff that have left the company HR provide IT Admin with a report of all leavers each month to perform a check. The IT Helpdesk also receive a report showing all users that have not logged on for 30 and 90 days or more and monthly and quarterly checks on this are carried out which is then reviewed by IT Security. This report is also used to ensure contractor access is removed in a timely manner.

System controls force password change every month. Three incorrect log-on attempts result in the user's account being suspended. Accounts can only be unlocked when the user can confirm their identification.

Access to Insight's network from Insight laptops is enabled through a Virtual Private Network (VPN). This is secured with RAS tokens and PIN numbers, maintained and controlled by the IT Helpdesk.

System administrator access to business applications and databases can only be granted if approved by the system owner. Any changes to this access are reported daily to IT Administrator team through the daily security check reports. A Remedy ticket is raised for each day's reports. Remedy is the helpdesk workflow and record management application. The IT Administrator team resolve any unexpected content by inquiry or escalation to appropriate team members.

Members of server access rights groups are reported to the IT Administrator team every ninety days and are then sent to the system owners for their sign off/approval.

Detailed Controls	Tests Performed by KPMG LLP and Results
All users are issued with specific, personal user identities for access to, and control, within required systems. This enables controlled access to systems and information and allows segregation of duties, including across logical separation of production, UAT and development environments. Access to all systems requires a completed Windows authentication.	Inspected the list of active users for the network and applications and noted that the users were identified with unique user profiles which allow for access to systems and information and segregation of duties across production, UAT and development environments. No exceptions noted.
Access to user identities is controlled by personal passwords. User policy directs users not to share identities or credentials. Xenomorph, thinkFolio CTS and Sapphire use Windows authentication. Windows requires that users change network passwords every 30 days and enforces a minimum length of 8 characters, and compliance with complexity rules. Three incorrect log-on attempts lock the account. All Windows password activity is recorded. ARA access is controlled by Solaris logon: passwords have a minimum of 8 characters and must be changed every 30 days. EPM passwords are managed by super users within the business area.	Inspected the password configuration settings for the in-scope applications and the Windows Domain and noted that the password settings included the settings prescribed in the control. Inspected the IT Account Management Standard and noted that the document outlines the requirements for users to keep identities or credentials private. Inspected the system generated Windows AD password log and noted that all password activity (reset/change) is recorded. Observed the onscreen logon process and settings for CTS, thinkFolio, Xenomorph and Sapphire and noted that Windows authentication was used in the logon. Inspected the list of individuals who had access to make changes to the EPM passwords and noted that they were authorised to privileged users within the business area. No exceptions noted.
New users are issued with network accounts and application access on submission of an online Joiner form approved by HR.	For a selection of new joiners, inspected the 'joiners form' and noted evidence of authorisation by the line manager. No exceptions noted.
Leaving user access to the network and remote access is withdrawn on instruction from HR	Inspected leaver's forms for a selection of employees (permanent and temporary) who had left the organisation and noted that their access had been revoked upon receipt of the forms / email from HR (permanent) or the IT Administration team (temporary). No exceptions noted.
Unused accounts are identified weekly using automatic reports showing current user accounts which haven't logged on for >= 30 days & >= 90 days. Accounts appearing in the former are disabled & those in the latter are removed. Actions recorded in Remedy. The process are reviewed by IT Security. Unused accounts appearing in the 30-day list are escalated as potential leavers.	For a selection of weekly reports showing users that have not logged on for 30 days and 90 days or more, inspected the associated Remedy tickets and noted evidence of the check and follow-up action (through to closure) by IT Helpdesk. Further noted that the report had been reviewed by IT Security and that unused accounts had been escalated as potential leavers after 30 days. No exceptions noted.

Twice yearly, IT Helpdesk (or delegated to IT Admin) reconciles the list of personal Windows accounts against legitimate reasons for their existence. The criteria are the account owner is a payroll employee, under contract or a BNYM employee. IT Security approves the reconciliation.	Inspected a selection of network access reconciliation reports and noted that the network accounts were reconciled by the IT Helpdesk team. Further noted that IT Security had approved the reconciliation and exceptions identified during the reconciliation were actioned upon by the IT Helpdesk team. No exceptions noted.
Systems admin access (Access to ADM groups) is granted via an approval workflow and approved by system owner. ADM access is granted via membership of SUPP admin groups. The SUPP Group membership is checked weekly in IT Security intrusion check. Changes to these groups taking place outside the workflow system are reported in a weekly report (IT Security weekly checks) and investigated if seen.	For a selection of systems administrator accounts, inspected the access requests and noted that the access was approved by the system owner. For a selection of dates, inspected the security check reports and associated Remedy tickets and noted that changes to the system administrator access was reported to the IT Security officer by the IT Helpdesk team. Further noted that the IT Security officer had reviewed the security check report and exceptions were followed up. No exceptions noted.
Insight users are provided with remote access to workstations. All remote access is authenticated at two levels: 1) RSA tokens using PINs and one-time token codes; and 2) Windows identity Remote connections from “untrusted” connections (home computers) do not allow access to administrative tools.	Observed the process for initiating a remote access session via VPN to Insight’s network from Insight laptops and noted that users were required to input a User ID and authenticate through a random pass code generated by an RSA token along with a PIN number. For a selection of new joiners granted remote access to Insight’s network from Insight laptops, inspected evidence of approval by IT Security. No exceptions noted.

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

As detailed above, System log-on IDs and passwords are assigned to individual users by means of user accounts. These accounts are authorised by the relevant line manager or department PA as part of the joiner’s process and set-up by the IT Operations team. Hard copies of joiner’s forms are archived and on-line forms retained on the system. Reviews of user access rights are performed by IT Administrator team on a semi-annual basis and sent to the IT Security Manager for approval. Logical system controls on relevant trading, payment processing and messaging systems prevent input and approval functionality as defined by the user profiles.

Detailed Controls	Tests Performed by KPMG LLP and Results
Roles exist within thinkFolio that segregate duties between Fund Managers who can approve orders and those that can't and Dealers. Fund Managers registered with the FCA (and approved by Risk) can authorise their own orders. They would then be passed on to a separate dealing function. Permissions within Sapphire are granted on a per instrument basis. Users are prevented from proposing, approving and executing their own orders. A "segregation of duties" matrix is in place that defines the permitted roles for each function associated with order management and trading. This matrix is reviewed by the Corporate Risk team against the user access rights granted by line managers on an annual basis. It mitigates the risk of line managers assigning and/or approving incorrect access levels. Permissions for IT staff for thinkFolio and Sapphire may be changed subject to IT Operations management signoff, typically to support approved software upgrades and production support issues. Permissions will be revoked within 1 business day. Weekly reports for permissions changes to thinkFolio and Sapphire are reviewed by Corporate Risk (for business users) and by the Head of IT Operations (for IT users). Weekly reports of IT activities in thinkFolio and Sapphire are reviewed by the Head of IT Operations.	Inspected the segregation of duties matrix and noted that permitted roles for order management and trading were defined and the matrix was reviewed and signed-off by Operational Risk. Inspected the segregation of duties matrix and noted the following: • Roles exist within ThinkFolio that segregate duties between Fund Managers who can approve orders and those that can't; and Dealers. • Fund Managers registered with the FSA (and approved by Risk) can authorise their own orders, which would be passed on to a separate dealing function. • Permissions within Sapphire are granted on a per instrument basis. • Roles are defined such that users are prevented from proposing, approving and executing their own orders. Inspected system access permissions for a selection of users and noted that the roles were configured as per the job function. For a selection of weeks, inspected the permission changes to thinkFolio and Sapphire and noted that the reports had been reviewed by Corporate Risk for business users and Head of IT Operations for IT users. For a selection of weeks, inspected the report of IT activities for thinkFolio and Sapphire and noted that the report had been reviewed by the Head of IT Operations. No exceptions noted.
IT Admin provides user access review reports for the above applications to the desk heads on an annual basis for their review. Evidence of review is via sign-off and return of these reports, including any changes to access required.	Inspected and noted evidence of user access reviews performed by the desk heads. Also noted that exceptions identified during the review had been actioned upon by IT Helpdesk. No exceptions noted.
Currency Risk Management trades are model generated and executed by Pareto's Trading team. Roles within the trade execution platform, CTS, define those individuals authorised to execute trades. On a quarterly basis Pareto's Currency Trading System permissions are reviewed by Corporate Risk.	Inspected the roles within CTS and noted that the roles defined the access rights of individuals to execute trades. Inspected both CTS permissions reviews and noted that the reviews had been carried out by Corporate Risk. No exceptions noted.

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

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

Automated processes are in place to process data changes. These are deployed across various platforms and controlled via a central scheduler. An in-house monitoring solution for software failures has been implemented (called 'Lighthouse') to monitor intra-day and weekend batch schedules and to alert support teams to any failures.

Failures are sent, by email, to the support team responsible for the application that has failed.

The team members are then responsible for picking up the failure and ensuring resolution. Each support team has a manager responsible for ensuring that issues are being picked up by the team and resolved in an appropriate timescale.

Detailed Controls	Tests Performed by KPMG LLP and Results
Deployment of technology monitoring toolsets is in place for all production infrastructure, batch schedules and time-critical (e.g. supporting trade-flow) application services.	Inspected the technology monitoring toolsets (e.g. Lighthouse and Control M) configurations for monitoring jobs for the in scope applications and noted that the toolsets were configured to monitor critical batch schedules and production infrastructure and alert relevant support teams if necessary. For selection of events identified, inspected the alert emails and noted that the emails had been distributed to relevant support teams and followed through to resolution. No exceptions noted.
Daily and overnight batch jobs are scheduled and run via automated job scheduling tools (e.g. Control M). Changes to job schedules are tested and approved by management via the change management process.	For a selection of changes, inspected the change tickets and noted that they had been approved by management via the Insight change management process. No exceptions noted.

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

Insight has many third party data suppliers and recipients to whom daily file transfer is an integral business as usual activity.

We predominantly use FTP as a means for electronic data transfer as well as the MQ Series for real time updates.

Bulk data transmissions are performed using software with data integrity management controls, and an in-house built monitoring process highlights late delivery of data. Errors are automatically reported to the application infrastructure team by email during the day and overnight. This team is responsible for resolving any issues.

The confidentiality of data transmissions with external parties is controlled using private or encrypted links. The Risk Management team maintains a list of fixed external connections (private links) and the Corporate Risk Assessment of new projects identifies cases where critical data should be encrypted. Firewall rules limit access to and from third party organisations to the traffic needed for the link to function. Third party authenticity is assured through the use of fixed links or application-specific means. Controls exist to secure access to applications that process data transmissions (see section 4.7.1.2).

Detailed Controls	Tests Performed by KPMG LLP and Results
The completeness, accuracy and timeliness of data transmissions are automatically monitored using software, and any errors are reported by email to the application infrastructure team for resolution.	Inspected the configuration of data transmissions for the in scope applications and noted that File Transfer Protocol is used to ensure completeness and accuracy of the data transfer. Inspected the configuration of the alerting tool used to monitor data transmission jobs for the in scope applications and noted that each job was configured to send email alerts on failure of the job processing to run completely and accurately during the scheduled time, to the application infrastructure team. Inspected a selection of email alerts and noted that the email had been communicated to the application infrastructure team and were resolved. No exceptions noted.
External links are terminated on the firewalls and documented in the firewall ruleset. Project teams engage with IT security to determine encryption requirements.	Observed the configuration of security mechanisms for a selection of data transmission connections and noted that they were secured through encryption or dedicated lines. For a selection of new external connections setup in the review period, inspected the outcome of the Operational Risk Assessment carried out by the risk team to determine whether the data should be encrypted. For a selection of change requests related to external links, noted evidence of e-mail approval from the IT Security manager on technical controls around the external links. No exceptions noted.

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

Appropriate measures are implemented to counter the threat from malicious electronic attack. Insight uses:

- Firewalls to implement a boundary between internal and external networks
- Software and execution control methods to limit scope for malware installation and attacks
- Malware detection software to identify and control malicious code on internal machines
- Operates a patching policy to reduce vulnerability to newly discovered attack exploits by applying hot fixes to servers

Firewalls are used to provide a boundary between Insight and external networks. They are managed to restrict connectivity to traffic authorised for delivery of external services. For example, Internet access, trading platforms, market feeds from Bloomberg and Reuters. The process to enable external connections is segregated between the firewall administrators and a separate IT Security function. Machines which can be removed from the network (laptops) run a software firewall to reduce the scope for Internet-hosted attacks to reach them when they are outside the Insight boundary firewall.

Standard workstation users have limited access to the administrative functions of the machines to reduce the scope for malicious installations to take place as a result of browsing. Access to removable media like floppy disks and USB sticks is restricted. Users can be granted read-only or read-write access to removable media. The process includes line managers' approval and Risk oversight.

Anti-virus software has been deployed across the IT estate and is part of the standard build for all servers and workstations. Insight IT actively manages the AV software to ensure that it is up to date and functional. This is monitored through a tool that generates lists of out of date installations. This list is fed to the support teams for rectification on a weekly basis by the IT Security manager who oversees compliance. Internet downloads are passed through a separate malware filter in the network perimeter before they reach workstations.

Email malware controlled in email through Postini gateways and Trend Exchange AV software on mail servers. Internet malware controlled through signature detection and website category blocks on Internet proxies. Malware installation controlled through limitation of administrative privilege on workstations, limitation of access to servers and McAfee AV software on servers and workstations.

Hotfix vulnerability assessment and deployment tool is used to deliver patches to servers and workstations. Patches are delivered to affected platforms following a defined timetable. Insight applies software updates supplied by vendors to correct security vulnerabilities. The update process follows a defined process to defend the operational integrity of Insight systems in the face of defective or surprising patches. The patch calendar shows test servers patched before production, and workstation population patched in multiple phases. Insight runs vulnerability management tools to ensure that correct patches are applied.

Detailed Controls	Tests Performed by KPMG LLP and Results
Firewalls are in place to protect Insight IT environment from unauthorised access.	Inspected the network diagram and noted that firewalls were in place to protect the Insight IT environment. Inspected firewall configurations and noted that firewalls were configured to protect the Insight IT environment from unauthorised access. No exceptions noted.
The Office Wi-Fi network that provides internet access only is segregated from the Insight network via Firewall rules.	Inspected the network diagram and noted that firewalls were in place to segregate the Office Wi-Fi network from the Insight network. No exceptions noted.
Firewall changes that remove access are subject to the change management process. Firewall changes that grant access are authorised through the IT Security Approval process.	Inspected approval evidences for a selection of firewall changes made and noted that the IT Security Manager / IT Security Engineer were obtained prior to implementing the changes. No exceptions noted.
Insight laptops run a software firewall to protect the Insight IT environment from unauthorised access when the laptops are directly connected to the Internet.	Inspected the laptop build configuration and noted that the software firewall was included within the standard build configuration for laptops. No exceptions noted.

Standard workstations include software to control access to removable media (including floppy disks, USB flash devices, and CD/DVD). Users can be granted read-only or read-write access to removable media, requiring approval by the Risk team.	For a selection of workstations, observed and noted that software was in place to control access to removable media. Inspected the workstation build configuration and noted that the Lumension software for controlling access to removable media was included within the standard build configuration for workstations. For a selection of users granted with read-only or read-write access to removable media, inspected their access request forms and noted that they had been approved by the risk team. No exceptions noted.
Anti-virus (AV) software is part of the standard build and runs on all desktops and servers. It is automatically updated at least daily.	Inspected system screenshots and noted the anti-virus software was configured to be updated automatically and there was monitoring in place to detect out of date installations. Inspected the AV server console and noted that the antivirus software was in place for desktops and servers. Further noted that the AV software was configured to automatically update on at least daily basis. No exceptions noted.
Email malware is controlled in email through Mimecast gateways and McAfee software on the email transport server. Internet malware is controlled through signature detection and website category blocks on Internet proxies. Malware installation controlled through limitation of administrative privilege on workstations, servers, McAfee AV software on servers and Symantec AV software on workstations.	Inspected the configuration of the Enterprise Email Servers and noted that MS Forefront Exchange and Mimecast were used to control email malware. Inspected the email malware software settings and internet malware software settings and noted that Internet malware was controlled through signature detection and website category blocks. Inspected the malware installation control and noted that it was restricted due to the limitation of administrative privilege on workstations servers and Symantec AV and McAfee AV. No exceptions noted.
Insight runs vulnerability management tools to ensure that correct patches are applied appropriately to Insight servers and PCs. IT Security vulnerability test results are passed to support teams. External security tests are performed quarterly and the results are assessed by the Head of IT Security. Issues are followed up via an issue tracker maintained by the Head of IT Security and Remedy tickets are raised to address any issues requiring action.	Inspected the workstation and server build configuration and noted that the software for vulnerability management was included within the standard build configuration for workstations and servers. For a selection of months, inspected the patch reports from the vulnerability management software and noted that servers with outdated patches had been identified and updated. For a selection of quarters, inspected the external security test reports and noted evidence of assessment and follow up by the IT Security Manager. Further inspected the issues tracker defined to track the issues requiring action and the Remedy tickets and noted that the remediation steps were identified for the issues. No exceptions noted.

4.7.2.4 The physical IT equipment is maintained in a controlled environment

Insight's physical IT equipment is located in purpose built communications rooms. Insight's communications rooms are protected with temperature control, uninterrupted power supply (UPS) and fire suppression systems.

Air conditioning in the communications rooms is designed to have a one air conditioning unit contingency and is monitored centrally by the building facilities team who investigate and correct any faults.

All Insight communications rooms are supplied with UPS as part of the core building functionality. The backup power is activated immediately in the event of a mains power failure. The generators have the capacity to operate for 3 days before refuelling.

Inergen fire suppression systems are installed in all Insight communications rooms. Between 10pm and 6am these activate automatically in the event of a fire in any communications room. Between 6am and 10pm the security team monitor all detection units through a central console and, in the event that one is triggered, they manually invoke fire suppression.

Detailed Controls	Tests Performed by KPMG LLP and Results
Insight's physical IT equipment is located in purpose built communications rooms. Insights' communications rooms are protected with temperature control, uninterrupted power supply (UPS) and fire suppression systems.	Observed the Insight communication rooms and noted the following environmental controls were in place within the room: • Temperature control • UPS • Fire suppression systems No exceptions noted.

4.7.3 Maintaining and developing systems hardware and software

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

The system infrastructure is logically partitioned into Development (DEV), User Acceptance Testing (UAT) and Production (PROD) environments with 'write' access to each restricted to approved IT staff through the defined user access groups. A documented change management process defines how changes to UAT and PROD environments are controlled.

Development and implementation of new systems, applications and software, including any data migration or modification, will be governed by Insight's Project Management process if anticipated to be greater than 15 man days. All projects are approved by the Project Management Group chaired by the Chief Operating Officer. All system projects are implemented through the Change Management Release (CMR) process (see below). Development and implementation of new systems, applications and software or data migration / modification estimated to be less than 15 man days follow the Change Request process.

The Change Request process consists of a weekly meeting attended by business support managers and business sponsors. It is chaired by the Head of IT Operations, and authorises and prioritises the list of change requests. If a new IT requirement is identified, Change Requests can be raised by anybody in the Business if approved by a line manager.

The authorisation of Change Requests permits the development activity to commence and a Change Management Release (CMR) form is initiated when testing in the UAT environment is ready to commence. A weekly CMR meeting reviews all proposed releases to both the UAT and PROD environments for approval and scheduling. These meetings are chaired by the Head of IT Operations (or a delegate) and minutes are retained.

There is a Change Register used to keep a record of all changes made to either environment. Changes to the PROD environment cannot be made unless tested in the UAT environment first. Only specific colleagues from Business Support have the necessary permissions to release source code into UAT and PROD.

The change management process includes an emergency approval route to allow timely resolution of urgent problems.

Emergency changes must be approved by the Head of IT Operations (or in his absence, the Head of Projects and Development).

Application source code is managed using PVCS. This provides development and support staff with the appropriate access required to make changes, promote code and manage implementations. Access to raw data files is controlled via the standard file access control procedures.

An audit trail of software changes can be tracked and is a standard feature of the PVCS toolset. Each version is labelled with a corresponding reference that can be traced through each release stage (DEV, UAT, PROD). An audit trail of software changes can be tracked and is a standard feature of the PVCS toolset. Each version of a file is labelled with a corresponding change management reference that can be traced through UAT and PROD.

Detailed Controls	Tests Performed by KPMG LLP and Results
Insight has documented change management procedures which require all changes prior to migration to the user acceptance testing (UAT) and production (PROD) environments to be tested and signed off by relevant parties (including both IT and business users).	For a selection of changes implemented, inspected the relevant testing and approval evidences and noted that the required testing had been performed per control description and Business and IT authorisation had been received prior to migration. No exceptions noted.
The change management process and records are online and all changes are logged and processed electronically. The names of the approvers are contained on the form to ensure that the identities of accountable personnel are visible and a full audit history is kept that reflects all workflow approvals applied during the history of a change.	For a selection of changes implemented, inspected the change records and noted that the names of the approvers were recorded along with a history of workflow approvals applied during the history of the change. No exceptions noted.
The weekly Change Management Release meeting chaired by the Head of IT Operations (delegate) approves and or schedules changes to the UAT and PROD environments. Meeting minutes are retained.	For a selection of weeks, inspected the minutes of the Change Request meetings and noted that updates were made to the change management workflow to evidence input from business support managers and business sponsors and approvals and prioritisation of changes. No exceptions noted.
Developers do not have access to the test or production environment to migrate changes. Access is restricted to the following support groups: Desktop Services, Business Application Support, Application Infrastructure, Infrastructure Services and DBA.	Inspected the list of users with access to the development and production environment for the in-scope applications and noted that developers did not have access to the production environment. Further noted that access to the test or production environment to migrate changes was restricted to the following support groups: Desktop Services, Business Application Support, Application Infrastructure, Infrastructure Services and DBA. No exceptions noted.

Source version control tools are used for version management control. Each version of a file is labelled with a corresponding change management reference that can be traced through the test environment to production.	Inspected the Dimensions and Stash software tool and noted that Dimensions and Stash version numbers are automatically tracked within the tool to provide an audit trail of software changes. For a selection of change requests, inspected evidence that each file is labelled and can be traced through UAT and Production in Dimensions or Stash for CTS changes. No exceptions noted.
The Project Management Group approves all projects anticipated to be greater than 15 man days. Approvals are evidenced by PMG meeting minutes.	For a selection of projects greater than 15 man days, inspected the Project Management Group (PMG) meeting minutes and noted the approvals for the projects. No exceptions noted.
BAU development and change requests are approved and prioritised by representatives from the business and IT teams via one of the following three forums which meet monthly: Risk Control Committee and OTC Pricing Committee and the NT Change Management Committee.	For a selection of changes, inspected the relevant forum minutes for a selection of BAU changes and noted that the changes had been approved and prioritised by the committees, in line with the control description. No exceptions noted.
The change management process includes an emergency approval route to allow timely resolution of urgent problems. Emergency changes must be approved by the Head of Business Application Support, the Head of Infrastructure Services or the Customer Services Manager. In any of their absence, emergency sign-off will be provided by the Head of IT Operations.	For a selection of emergency change request forms, inspected the forms and noted evidence of pre-approval from the Business Application Support Manager. No exceptions noted.

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

Data migration or modification is treated as a software change and is processed using the change management process detailed above (see section 4.7.3.1). As part of the process to ensure complete and accurate data migration or modification, the data would be reconciled back to the source data.

Detailed Controls	Tests Performed by KPMG LLP and Results
Data migration tasks are performed under the same change management process used for systems and are consequently subject to approval by IT operations managers.	Enquired of IT Operations Manager regarding management process for data migration tasks and were informed that they follow the same change management process used for systems and were consequently subject to approval by IT operations managers. Inspected data migration approvals from IT managers for a selection of tasks to determine if the approvals had been granted as per the change management policy. Limitation of Scope: KPMG was unable to ascertain the operating effectiveness of this control as there were no instances of data migration during the period under review.

4.7.4 Recovering from processing interruptions

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

Storage Area Network (SAN) technology is employed for 'real time' back up of critical systems' data onto fileservers at the disaster recovery site (see section 4.7.4.3 below). A daily procedures checklist is completed by the infrastructure team to ensure that the SAN is synchronised each morning and that the daily backups have been completed successfully. Backup policies are in place and reviewed regularly by application owners and approved by business data owners to ensure that all production systems are backed up on tapes on a daily basis. The tape library resides at the DR site.

The infrastructure service team check all critical system backups as part of the routine morning check. The results of their check are sent to the '$IT Checks' mailing list which includes all support teams. Each support team is responsible for identifying and invoking the appropriate corrective actions should one of their backups fail. Data is recovered from backup at least 3 times per week as a result of routine support and development requests. Critical systems data is restored as a result of UAT environment refreshes at least twice a year.

Detailed Controls	Tests Performed by KPMG LLP and Results
Systems and data are backed up on a daily basis through the use of specialised tools, following pre-defined schedules. The infrastructure service team check all critical system backups as part of routine morning checks.	Inspected the configuration of the enterprise data backup software and noted that backup schedules were defined for the in-scope applications. For a selection of days, inspected the routine morning check emails and noted that the critical system backups had been checked as part of the routine morning checks. No exceptions noted.
Backup policies documented and reviewed as part of BCP procedures. They stipulate the daily and monthly requirements for all systems. A storage area network is used to back up production data to DR site. Backup tapes are stored offsite at the DR site.	Inspected the BCP procedures document and noted that the document stipulated the daily and monthly requirements for backup of the in-scope applications. Inspected the BCP procedures and noted that the document had been reviewed during the year of testing. Inspected the configuration of the enterprise data backup software and noted that the backup schedule for the in-scope applications was in accordance to the backup policy and the backup of the production data was replicated via storage area network to the DR site. Observed that Backup tapes were stored offsite at the DR site. No exceptions noted.

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

Daily health checks are performed by each IT support team every morning to ensure that all critical systems are working correctly. The Infrastructure checks are emailed to the '$IT Checks' distribution list so that the relevant IT team responsible to take corrective action is alerted.

Systems Centre Operations Manager (SCOM) is the automated tool used for hardware and systems monitoring. Alerts are reported to a central console and emailed to the infrastructure support teams who are responsible for correcting any failures.

The manager of the infrastructure support team is responsible for monitoring the overall failure rate and ensuring that all failures are resolved in a timely manner.

Detailed Controls	Tests Performed by KPMG LLP and Results
Health checks are performed on critical infrastructure services every morning. The results are sent to the Head of Infrastructure Services and Head of IT Operations and any failed checks are addressed with action appropriate to the type of failure.	For a selection of days, inspected the daily check emails and noted that daily checks had been performed and failures addressed as required. No exceptions noted.
Operational issues identified by support teams and users are logged as Remedy tickets. Calls are managed to resolution by IT operations team members. Key Performance Indicators for call and service management are reported at the OMG (Operations Management Group) on a monthly basis.	For a selection of operational issues, inspected remedy tickets and noted that the issues were logged and tracked to resolution. Inspected the KPI reports for a selection of months and noted that the KPI reports had been prepared and reported to the OMG (Operations Management Group) and contained information pertaining escalated issues and service outage. No exceptions noted.

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

Insight's Business Continuity (BC) planning is designed to allow business processes to continue through emergencies. Insight plans to avoid any significant disruption that may prevent it from continuing to operate effectively for clients, satisfying the FCA's threshold conditions and compliance with the Principles for Businesses. As such, Business Continuity and Crisis Management are fundamental to Insight's internal control mechanisms.

Insight has endorsed and complies with the Group BC Policy. The policy defines the framework and principles for BC Management. Compliance with this policy is assessed annually by Group through their benchmarking process. The Technology Information Risk Committee (TIRC), chaired by the Chief Risk Officer, formulates Insight's BCM strategy, co-ordinates testing schedules, assesses test results and evaluates emerging risks. The attendees of the Group include, but are not limited to, the Head of IT Operations, the Head of IT Security, Head of Distribution Technology and Operations and the BCM Manager. The output and deliverables from the TIRC are distributed to Insight's Risk Management Committee and the Group Business Continuity. The TIRC meets every month.

Insight's Crisis Management Team (CMT), chaired by the Chief Risk Officer, manages a crisis situation from discovery to BAU. Members of the CMT include all the Insight Executive Officers and the Head of IT Operations. Each member has at least one nominated delegate in the event of absence. Dependent on the nature of the crisis, this team will interact with the CMT, Emergency, and Intelligence Services.

CMT plans state clearly the activation process for executing the plan. The plan includes:

- The conditions for activation
- Emergency procedures and liaison with the emergency services to reduce the impact on colleagues
- Alternative locations and relocation to the sites
- Key contacts

Insight's Disaster Recovery (DR) plan clearly states the recovery and restoration process of all critical systems and applications.

The plan includes the:

- Responsibilities of colleagues, describing who is authorised to take actions during recovery from a technology incident
- Activities and timeframes required to re-establish the technology necessary to support critical business processes

The Recovery Time Objectives (RTO) for all critical systems is 8 hours, and 4 hours for the trading specific applications.

Business Continuity plans, IT Disaster Recovery plans and Crisis Management Plans are living documents that are maintained, tested and updated on a regular basis. The plans are approved by their respective owners.

Testing process

The testing process verifies that plans are up to date and match the needs of the business.

The principle types of testing:

- Table top functional level testing using scenarios
- Call-out cascade activation
- Technical, telephony and business recovery to our DR sites

The 'table top' testing covers both specialist areas and the CMT.

A DR technical test took place in November 2014 which was also successful. The results from the tests are recorded.

Insight Business Continuity also works with our third party suppliers to ensure that their BC planning is robust and in the event of an incident would have minimal impact on us. The diversification of certain elements of our operations to third party suppliers mitigates our overall exposure to Business Continuity risk.

DR site and systems architecture

Insight has an ongoing contract with a third party to provide BC services. The contract currently provides us with seats in a secondary site, hardware, telecommunications and a dedicated communications room. The business requirements as identified by the Business Impact Analysis (BIA) exercise are covered by the contract.

Installed in the DR site communications room are replicas of the essential production servers and systems used at Queen Victoria Street. A Storage Area Network (SAN) based solution is employed to replicate the data from Queen Victoria Street to the DR site on a synchronous basis. In the event of an invocation, the replication is suspended, and critical systems are recovered from the mirrored data and operating systems at the DR site.

This architecture also enables a very quick recovery to the loss of an individual server at our primary site, without full scale invocation.

Detailed Controls	Tests Performed by KPMG LLP and Results
DR plans are maintained by the Business Continuity Manager, reviewed and tested at least annually. Any issues from the tests are escalated to the BC Steering Group and actions are monitored to closure. BCP tests are carried out periodically throughout the year on an as-required basis. A documented set of business incident management procedures are detailed in the Insight Disaster Recovery, Business Continuity, and Crisis Management Teams Plans.	Inspected the DR plans and noted that the document was reviewed and maintained by the Business Continuity Manager. Inspected the annual restoration test report and noted that restoration of critical applications was successfully completed. Inspected the Disaster Recovery, Business Continuity and Crisis Management Team Plans and noted that documented included a set of business incident management procedures. No exceptions noted.

5. REPORT BY THE REPORTING ACCOUNTANTS

KPMG LLP
Financial Services
15 Canada Square
Canary Wharf
London E14 5GL
United Kingdom

Tel +44 (0) 20 7311 1000
Fax +44 (0) 20 7311 0426

Private & confidential
The Board of Directors
Insight Investment Management Limited
160 Queen Victoria Street
London
EC4V 4LA

22 May 2015

Dear Sirs,

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

Use of report

This report is made solely for the use of the directors, as a body, of Insight Investment Management Limited ('Insight'), and solely for the purpose of reporting on the internal controls of Insight, in accordance with the terms of our engagement letter dated 8 December 2014 and attached as appendix 1 (together with Additional Terms of Business appended thereon).

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 Insight ('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 Insight and issued in connection with the internal controls of Insight, 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 Insight for our work, for this report or for the conclusions we have formed.

Scope

We have been engaged to report on Insight's description of its investment management activities and internal controls throughout the period 1 January 2014 to 31 December 2014 ('Description'), and on the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description.

Service organisation's responsibilities

Insight is responsible for: preparing the Description and the accompanying assertion set out on page 3, including the completeness, accuracy, and method of presentation of the Description and the assertion; 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 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. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 and 3402, and ICAEW Technical Release AAF 01/06. That standard and guidance require that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed, implemented and operating effectively to achieve the related control objectives stated in the Description throughout the period 1 January 2014 to 31 December 2014.

Our work involved performing procedures to obtain evidence about the presentation of the Description and the design and operating effectiveness 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.

Inherent limitations

Insight'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 system 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.

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.

Opinion

In our opinion, in all material respects, based on the criteria including specified control objectives described in the directors' assertion on page 3:

(a) the description on pages 10 to 55 fairly presents the investment management activities that were designed and implemented throughout the period from 1 January 2014 to 31 December 2014;

(b) the controls related to the control objectives stated in the description on pages 10 to 55 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 2014 to 31 December 2014; 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 2014 to 31 December 2014.

Description of test of controls

The specific controls tested and the nature, timing and results of those tests are listed on pages 10 to 55.

Yours faithfully,

KPMG LLP

KPMG LLP
Chartered Accountants
15 Canada Square
London E14 5GL
United Kingdom
22nd May 2015

APPENDIX 1 – ENGAGEMENT LETTER

KPMG LLP
Financial Services
15 Canada Square
Canary Wharf
London E14 5GL
United Kingdom

Tel +44 (0) 20 7311 1000
Fax +44 (0) 20 7311 6426
DX 157460 Canary Wharf 5

Private & confidential
The Board of Directors
Insight Investment Management Limited
160 Queen Victoria Street
London
EC4V 4LA

8 December 2014

Dear Sirs

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

We are writing to confirm the terms of the engagement by Insight Investment Management Limited and its subsidiaries, Insight Investment Management (Global) Limited and Pareto Investment Management Limited (together "Insight" or "you") of KPMG LLP ("KPMG" or "we") to deliver ISAE 3402 / AAF 01/06 Type II Assurance Services to you in connection with a report on the controls system applicable to the investment management services undertaken by Insight Investment Management Limited and its subsidiaries Insight Investment Management (Global) Limited and Pareto Investment Management Limited (together "Insight"), at the business unit located at 160 Queen Victoria Street, London, UK, EC4V 4LA as of 31.12.2014. In this letter, references to Insight's "management" means the directors of Insight and those employees to whom the directors of Insight have properly delegated day-to-day conduct over matters for which the directors of Insight retain ultimate responsibility.

1 Scope of the Services

We set out below details of the services to be delivered. Any work already performed in connection with this engagement before the date of this letter will also be governed by the terms and conditions of this letter.

We will conduct our examination having regard to standards established by the International Auditing and Assurance Standards Board (IAASB) and in accordance with Technical Release AAF 01/06, issued by the Institute of Chartered Accountants in England and Wales (ICAEW). The following paragraphs describe the objectives of our engagement and the nature and limitations of the services we will provide.

The "specified period" for this engagement, being the period of operation of the system which will be the subject of our examination, will be 1 January 2014 until 31 December 2014.

Our objective will be to conduct an examination that will include procedures to obtain reasonable assurance, in all material respects and based on suitable criteria, to enable us to express an opinion (Type II Reporting Accountants' Assurance Report) as to whether:

- Insight's management description of its system fairly presents the 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 controls included in the aforementioned description were suitably designed throughout the specified period to provide reasonable assurance that the control objectives specified in the description would be achieved if the described controls were complied with satisfactorily; and
- Such controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the specified period.

The control objectives for this examination are specified by Insight's management and are described in Appendix 1.

In conducting the examination we will examine, on a test basis, evidence supporting Insight's description of controls, including the operating effectiveness of the related controls, and perform other procedures as we consider necessary in the circumstances to provide a reasonable basis for our report. Our examination will not include other systems, controls, operations or services not specified herein including internal control at user organisations and, accordingly, we will express no opinion on such items.

2 Responsibilities

Management of Insight acknowledges and accepts its responsibility for providing a written assertion about whether in all material respects, and based on suitable criteria:

- Management's description of Insight's system fairly presents the system that was designed and implemented throughout the specified period;
- The controls related to the control objectives stated in management's description were suitably designed throughout the specified period to achieve those control objectives; and
- The controls related to the control objectives stated in management's description operated effectively throughout the specified period to achieve those control objectives.

This written assertion will be included in, or attached to, management's description of Insight's system, and provided to user entities as part of the final report issued by management. In the event that we are unable to satisfy ourselves that your written assertion is complete in all material respects and based on suitable criteria, we will work with management to resolve such issues. If

we are unable to resolve such issues, we will either disclaim an opinion or withdraw from the engagement without issuing a report.

Additionally, management of Insight acknowledges and accepts its responsibility for:

- Preparing its description of its system and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion;
- Having a reasonable basis for its assertion;
- Selecting the criteria to be used and stating them in the assertion;
- Specifying the control objectives and stating them in the description; and
- Identifying the risks that threaten the achievement of the control objectives and designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the controls objectives stated in the description will be achieved.

Insight agrees that all actual or claimed malfunction, breach, error or problem associated with the description of its system subject to our examination, and assertion, will be disclosed to us promptly once we begin our work, and you will procure the full cooperation of Insight personnel.

Insight's management will provide us on request, for the purposes of our report, with a representation letter that, among other things, will confirm management's responsibility for its assertion and description of its system, and that all records, documentation, and information relevant to the description have been made available to us under the terms of this letter including any and all actual or claimed malfunction, breach, error or problem associated with the systems and processes subject to our examination. Management's responses to our enquiries, written representations, and the results of our other examination procedures comprise the evidential matter we will rely upon in forming our opinion.

The management of Insight is responsible for the implementation and reliability of information systems, processes and controls described in the description of its system. The management of Insight is also responsible for the description of Insight's system, written assertion and all representations contained therein. Because of the importance of management's assertion and representations to the effective performance of our services, Insight releases this firm, our partners/members/directors and our employees from any claims, liabilities, costs and expenses incurred by Insight relating to our services under this letter that are solely attributable to any misrepresentations in the representation and assertion letter referred to above.

An examination is planned and performed to obtain reasonable assurance of detecting both intentional and unintentional misstatements that are material to the description of the system taken as a whole and whether the related controls were not operating with sufficient effectiveness to achieve the control objectives throughout the specified period. Absolute assurance is not attainable because of factors such as the need for judgment regarding the areas to be tested and the nature, timing, and extent of tests to be performed; the concept of selective testing of the data;

the nature of fraud; and the inherent limitations of the controls applicable to the control objective. Therefore, there is a risk that fraud or a material misstatement may exist or that the controls are not operating effectively and not be detected by an examination performed in accordance with professional standards. Also, an examination is not designed to detect matters that are not material to the description or operating effectiveness of controls. In addition, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

If we conclude that the description of controls contains material omissions or material misstatements of fact, that controls are not operating effectively, or if we determine that there is evidence that fraud may exist, or if we determine that an illegal act may exist, we will report the matter to the Directors of Insight Investment Management Limited.

3 Deliverable

After we have carried out our work under this letter we will report in writing. Our report will be addressed to the Directors of Insight Investment Management Limited. We will report on the controls based on enquiry, observation, and inspection of documentation, and other methods of testing such as re-performance. Our report will be described as our Independent Reporting Accountants' Assurance Report (ISAE 3402 / AAF 01/06 Type II). The report prepared by management will contain:

- Our reporting accountants' assurance report (KPMG opinion letter);
- Your written assertion (Insight Management Assertion);
- A description of the system (Management's System Description) applicable to the defined scope of services to which our report relates including:
  - An overview of Insight activities and services;
  - A general description of the flow of transactions through the process(es);
  - A description of the information systems and operational processing controls; and
  - A brief description of control considerations that should be adopted by user organisations.
- A description of control objectives and the controls in place that satisfy the control objectives, including relevant changes throughout the specified period (Insight Description of Control Objectives and Related Control Procedures and Controls);
- The results of control testing (our description of tests performed by us and test results);
- A description of any additional tests performed, and the results of those tests (our description of supplemental testing by us of additional criteria / subject matter); and

- Additional information Insight management wish to provide to user organisations (Other information provided by Insight).

We will also provide you, separately from our report, with a private annual management letter containing any concerns regarding missing or ineffective controls and management's plans to address those issues.

We will discuss all the findings and recommendations resulting from our reviews with appropriate business unit management before finalising the report.

4 Timetable

A provisional timetable for the delivery of our services will be agreed with you before the commencement of our work. The timing of our work and its performance will be dependent on all relevant information and documentation and access to personnel being made available to us promptly as and when required by us. We shall use all reasonable endeavours to meet any agreed timetable.

5 KPMG resources

This engagement will be led by Neil Palmer and day to day operation will be the responsibility of Derek Kimmerle. We will involve others in the work as appropriate. Our engagement team will include personnel provided by other KPMG network firms. Such personnel will work as members of the team assigned to this engagement by KPMG. You may have direct contact with them, but all services delivered under this engagement letter will be provided by KPMG.

6 Our charges

We will agree our fees for these services with you separately in a fee letter (which shall form part of this Engagement Letter).

Invoices will be payable on presentation.

If the timetable slips because of delays in making information or documentation or personnel available to us, we may charge additional fees for any work performed outside of the original timetable on the basis of our normal hourly rates in force when the relevant work is done.

7 Terms of Business

We accept this engagement on the basis that our General Terms of Business, as set out in Appendix 2, will apply to this work and govern our relationship with you, together with the Additional Terms: Reports under ISAE 3402 and AAF 01/06 in Appendix 3. This letter is the "Engagement Letter" mentioned in our General Terms. Please read these Terms carefully. There are various exclusions and limitations on our liability and associated obligations imposed on you.

Through our contract with you we aim to clarify your and our obligations and responsibilities and we seek to protect ourselves, other members of the KPMG organisation and our people. We draw your attention in particular to the following clauses and amendments of our General Terms:

Clause 4: We set out here the obligations imposed on us in respect of your Confidential Information. For our marketing or publicity purposes we are permitted to make general references to our relationship with you and to work performed for you.

Clause 7: We confirm here that our work is performed for you alone and we set out various restrictions on the extent to which you may share with others the product of our work or refer to our name. This is qualified by clause 7 of the Additional Terms (as noted below).

Clauses 18 to 24: These set out our position where your interests may conflict with our other clients' interests and clarify our responsibilities in relation to Confidential Information (as defined in clause 4) in the circumstances identified.

Clauses 31 to 35: We set out here the principal exclusions and limitations on our liability to you. Our liability to you in connection with this engagement for losses shall be limited, on the basis set out in our General Terms, to a maximum aggregate of £500,000. If you wish to bring a claim against us, you must do so within 4 years.

Clause 42: For the purposes of this clause and this engagement, the following shall be treated as Other Beneficiaries: Insight Investment (Global) Limited and Pareto Investment Management Limited.

We draw your attention to the following clause of our Additional Terms (Appendix 3):

Clause 7: This sets out the basis on which we consent to your release of our report to "Customers" of Insight Investment Management Limited (meaning clients of Insight Investment Management Limited who have signed contracts in place as users of the services which are the subject of the Report) and their auditors. We set out in section 9 below, *Special arrangements*, the basis on which we consent also to your release of our report to "Prospective Customers" (meaning any potential client or clients who have approached Insight Investment Management Limited in respect of Insight Investment Management Limited taking on business that is the subject of the Report and for whom a signed contract is not yet in place in relation to that business).

Clause 10: This sets out your agreement to indemnify us in respect of any claims by third parties (including Customers of Insight Investment Management Limited) arising out of this engagement for amounts over and above the agreed limitation on the amount of our liability to you (as recorded above).

8 Special arrangements

We understand that, in addition to release to Customers as referred to above, you wish to make a copy of our report ("the KPMG Report") available to Prospective Customers, which is not envisaged by the standards to which we refer in section 1 above, *Scope of the Services*.

We are willing to agree to disclosure of the KPMG Report to Prospective Customers as well as to Customers, provided that you have obtained our approval as to the form of disclosure and its context, subject to the conditions and on the basis set out below.

KPMG's consent for release of our report to Prospective Customers is given on condition that our report is released under the cover of a transmittal letter in the form of Appendix 4, which should be issued on the letterhead of Insight Investment Management Limited.

KPMG consents to the disclosure of the KPMG Report (in full only) to Prospective Customers in all cases to enable Prospective Customers to verify that a report on the matters discussed has been commissioned by you and issued by KPMG in connection with the internal controls of Insight Investment Management Limited without assuming or accepting any responsibility or liability to them on our part, and subject to the further conditions detailed below. This section of this engagement letter qualifies clause 7 of our General Terms.

It is a condition of our willingness to agree to disclosure of the KPMG Report to Prospective Customers that the Directors of Insight Investment Management Limited and Insight Investment Management Limited , the Directors of Insight Investment (Global) Management Limited and Insight Investment (Global) Management Limited, the Directors of Pareto Investment Management Limited and Pareto Investment Management Limited each accept the risk, and will not hold KPMG responsible, if the disclosure of the KPMG Report to Prospective Customers or any public reference (virtual or otherwise) to our name or our work results in or leads to (i) the termination or alteration to the terms of the existing relationship of the Directors or Insight Investment Management Limited with Prospective Customers, (ii) the termination or alteration to the terms of any transaction or proposed transaction involving Insight Investment Management Limited, (iii) any action or claim against the Directors or Insight Investment Management Limited , or (iv) any other adverse consequences for the Directors or Insight Investment Management Limited.

In addition, to the fullest extent permitted by law, Insight Investment Management Limited agrees to indemnify and hold harmless KPMG and all other KPMG Persons (as defined in the General Terms at Appendix 1) against any and all actions, proceedings and claims brought or threatened against any KPMG Person by any persons other than Insight Investment Management Limited, and all loss, damage and expense (including legal expenses) relating thereto, where any such action, proceeding or claim in any way relates to or concerns or is connected with the KPMG Report and its disclosure to any Prospective Customers.

9 Confirmation

Please confirm your agreement to and acceptance of the terms of this letter and the attachments on your own behalf and as agent for the Other Beneficiaries by signing and returning to us the enclosed copy. If there are any aspects that you wish to discuss, please let us know.

Yours faithfully

Neil Palmer, *KPMG LLP*

Attached:

1 Control Objectives
2 General Terms of Business
3 Additional Terms: Reports under ISAE 3402 and AAF 01/06
4. Form of transmittal letter

I have read and understood the terms and conditions of this letter and attachments and I agree to and accept them.

Signed:

Name: C FARQUHARSON

Position: DIRECTOR

Date: 8.1.15

Duly authorised, for and on behalf of Insight Investment Management Limited and as agent, duly authorised, for and on behalf of Insight Investment Management (Global) Limited and Pareto Investment Management Limited.

Appendix 1

4.1.1 Accounts are set up and administered in accordance with client agreements and applicable regulations
4.1.2 Complete and authorised client agreements are operative prior to initiating investment activity
4.1.3 Client take-ons including in-specie transfers, are monitored, documented and opening positions are accurately reported to clients
4.1.4 Investment limits and restrictions are established
4.2.1 Investment strategy is set and implemented in a timely manner
4.2.2 Investment transactions are properly authorised, executed and allocated in a timely and accurate manner
4.2.3 Transactions are undertaken only with approved counterparties
4.2.4 Commission levels and transaction costs are monitored.
4.2.5 Investment and related cash transactions are completely and accurately recorded and communicated for settlement a timely manner
4.2.6 Corporate actions are processed and recorded accurately and in a timely manner
4.2.7 Proxy voting instructions are generated and recorded and carried out accurately and in a timely manner
4.2.8 Client new monies and withdrawals are processed and recorded completely and accurately; withdrawals are appropriately authorised
4.3.1 Investment income and related tax are accurately recorded in the proper period
4.3.2 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
4.3.3 Cash and investment positions are completely and accurately recorded and reconciled to third party data
4.3.4 Investment management fees and other account expenses are accurately calculated and recorded
4.4.1 Uninvested cash is managed with regard to diversification of risk and security of funds
4.5.1 Client portfolios are managed in accordance with investment objectives, monitored for compliance with investment limits and restrictions and performance is measured

Appendix 1

4.5.2 Outsourced activities are properly managed and monitored and conflicts of interest identified to clients
4.5.3 Transaction errors (including guideline breaches) are rectified promptly and clients treated fairly
4.5.4 Counterparty exposures are monitored
4.6.1 Client reporting in respect of portfolio transactions, holdings and performance, commission and voting is complete and accurate and provided within required timescales
4.7.1.1 Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals
4.7.1.2 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
4.7.1.3 Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles
4.7.2.1 IT processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner
4.7.2.2 Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure
4.7.2.3 Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g. firewalls, anti-virus etc.)
4.7.2.4 The physical IT equipment is maintained in a controlled environment
4.7.3.1 Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented
4.7.3.2 Data migration or modification is authorised, tested and, once performed, reconciled back to the source data
4.7.4.1 Data and systems are backed up regularly, retained offsite and regularly tested for recoverability

4.7.4.2 IT hardware and software issues are monitored and resolved in a timely manner
4.7.4.3 Business and information systems recovery plans are documented, approved, tested and maintained

APPENDIX 2 – ADDITIONAL TERMS

KPMG

General Terms of Business

These General Terms of Business ("**General Terms**") apply to the delivery of services by KPMG to a client pursuant to a letter enclosing these General Terms and recording the engagement ("**the Engagement Letter**").

Definitions

Services means the services to be delivered by us under the Engagement Letter.

KPMG or **we** (or derivatives) means the KPMG contracting party as identified by the Engagement Letter.

Engagement Team means KPMG Persons (excluding corporate bodies) involved in delivering the Services.

you (and derivatives) means the addressee (or addressees) of the Engagement Letter.

Services Contract means the contract formed by the Engagement Letter and these General Terms, together with any appended other terms applicable to the Services ("**Additional Terms**").

KPMG Persons means the KPMG contracting party, each and all of our partners or directors, employees and agents, together with any other body associated with us and each and all of its partners, directors, employees and agents and "**KPMG Person**" shall mean any one of them.

Other KPMG Person(s) means, collectively or individually, KPMG Persons who are not members of the Engagement Team.

agents (when referable to KPMG) means persons whom we authorise to act on our behalf or whom we treat as our employees, and for whose conduct we accept responsibility, in connection with the Services.

Other Beneficiaries means any person or organisation identified in and for whom you sign the Engagement Letter (other than you) as a beneficiary of the Services or any product thereof.

Our responsibilities

1. The Engagement Letter shall set out the Services to be delivered by us and associated matters and may vary these General Terms.
2. The Services shall be delivered with reasonable skill and care.
3. We shall form an Engagement Team, to include individuals (if any) named in the Engagement Letter. We may substitute any who are named for others of equal or similar skills but we shall consult you before doing so.
4. We may acquire sensitive information concerning your business or affairs while delivering the Services ("**Confidential Information**"). We shall preserve the confidentiality of Confidential Information and we shall not disclose it beyond the Engagement Team unless permitted by you or by this clause. We shall comply with the confidentiality standards of the ICAEW and we shall adhere to the confidentiality restrictions of any other UK authority with powers over us, as well as any obligations imposed on us by English law. We shall be entitled to comply with any requirement of English law, the ICAEW, or any other UK regulatory body with powers over us, to disclose Confidential Information. Information relating to you, to our relationship with you, and to the Services, including Confidential Information, may be shared by us with Other KPMG Persons, and may be accessed by other parties who facilitate the administration of our business or support our infrastructure. We shall remain responsible for preserving confidentiality if Confidential Information is shared with Other KPMG Persons or accessed by such other parties. We may remove, or arrange for the removal of, names and any other identifiers from Confidential Information and then use such anonymised information for lawful purposes chosen at our discretion. This clause shall not apply where Confidential Information properly enters the public domain. This clause shall not prohibit our disclosure of Confidential Information, in confidence, to our professional indemnity insurers or advisers.

   For the purposes of marketing or publicising or selling our services we may wish to disclose that we have performed work (including the Services) for you, in which event we may identify you by your name and we may indicate only the general nature or category of such work (or of the Services) and any details which have properly entered the public domain.
5. We may supply written advice or confirm oral advice in writing or deliver a final written report or make a final oral presentation. We may also supply oral, draft or interim advice or reports or presentations but in such circumstances our written advice or our final written report shall prevail. No reliance shall be placed by you on anything draft or interim. Where you wish to rely on anything provided orally, you shall inform us and we shall supply final documentary confirmation.
6. We shall not be obliged to update any advice, report or other product of the Services, oral or written, for events occurring after the advice, report or product concerned has been issued in final form.
7. Any product of the Services in any form or medium shall be supplied for your benefit and information only. Save as may be required by law or by a competent regulatory authority (in which case you shall, unless prohibited by law, inform us in advance), it shall not be copied, referred to or disclosed by you, in whole (save for your own internal purposes) or in part, without our prior written consent. You shall not quote our name or reproduce our logo in any form or medium without our prior written consent. You may disclose in whole any product of the Services to your legal and other professional advisers if seeking advice in relation to the Services, provided that when doing so you inform them that (i) disclosure by them (save for their own internal purposes or where compelled) is not permitted without our prior written consent, and that (ii) to the fullest extent permitted by law we accept no responsibility or liability to them in connection with the Services.
8. Any advice, opinion, statement of expectation, forecast or recommendation supplied by us shall not amount to any form of guarantee that we have determined or predicted future events or circumstances.

Ownership

9. We shall retain ownership of the copyright and all other intellectual property rights in the product of the Services, whether

oral or tangible, and ownership of our working papers. You shall acquire ownership of any product of the Services in its tangible form on payment of our Charges. For the purposes of delivering services to you or other clients, KPMG, the Engagement Team and Other KPMG Persons shall be entitled to use, develop or share with each other knowledge, experience and skills of general application gained through performing the Services.

Our charges

10. We shall render invoices in respect of the Services comprising fees, outlays and VAT thereon (where appropriate), plus any overseas taxes that might be payable thereon or deductible therefrom ("**our Charges**"). Details of our Charges and any special payment terms shall be set out in the Engagement Letter. Our fees shall be based on the degree of responsibility of Engagement Team members involved in delivering the Services, their skill and time spent by them and the nature and complexity of the Services. Outlays include both directly incurred costs and an amount, equal to 2.5% of the value of time, to cover incidental expenses . Our Charges may differ from any prior estimates or quotations.

11. In return for the delivery of the Services by us, you shall pay our Charges (without any right of set-off), on presentation of our invoice or at such other time as may be specified in the Engagement Letter.

    11.1 We may charge interest on any outstanding balances at the statutory rate from time to time in force (this rate applying after as well as before any court award or judgement in our favour in respect of outstanding balances).

    11.2 If the Services Contract is terminated or suspended, we shall be entitled to payment for outlays incurred and to payment of fees for Services performed, plus VAT thereon (where appropriate). Our fees shall in this event be calculated by reference to our hourly rates at the time of performance of the Services.

    11.3 Where there is more than one addressee of the Engagement Letter, unless the Engagement Letter provides otherwise, all of you shall be liable to pay our Charges in full separately and together as a group.

    11.4 If we are required by any court or regulatory body in any proceedings or forum in which we are not a party or participant but you are, or if we are required by a parliamentary select committee or body, to provide information or to produce documents relating in any way to the Services, you shall pay our costs incurred in preparing for and responding to any such requirement at our standard rates applicable at the time of responding, together with outlays including legal expenses, and VAT thereon (where appropriate).

Your responsibilities

12. Where there is more than one of you, this clause applies to each of you separately and not collectively. Notwithstanding our duties and responsibilities in relation to the Services, you shall retain responsibility and accountability for managing your affairs, deciding on what to do after receiving any product of the Services, implementing any advice or recommendations provided by us, and realising any benefits requiring activity by you.

13. Where you require us or the nature of the Services is such that it is likely to be more efficient for us to perform Services at your premises or using your computer systems or telephone networks, you shall ensure that all necessary arrangements are made for access, security procedures, virus checks, facilities, licences or consents (without cost to us).

14. You shall not, directly or indirectly, solicit the employment of any of our partners, directors or employees, involved in performing the Services, during performance or for a period of 3 months following their completion or following termination of the Services Contract, without our prior written consent. This prohibition shall not prevent you at any time from running recruitment advertising campaigns nor from offering employment to any of our partners, directors or employees who may respond to any such campaign.

Information

15. To enable us to perform the Services, you shall supply promptly all information and assistance and all access to documentation in your possession, custody or under your control and to personnel under your control where required by us. You shall use your best endeavours to procure these supplies where not in your possession or custody or under your control. You shall inform us of any information or developments which may come to your notice and which might have a bearing on the Services. You shall supply information in response to our enquiries (if any) to enable us to comply with our statutory responsibilities to make disclosures to relevant authorities in respect of money laundering and any other criminal activity that we may encounter during performance of the Services and any such disclosures may include Confidential Information.

16. We may rely on any instructions, requests or information supplied, orally or in writing, by any person whom we believe to be authorised by you to communicate with us for such purposes. We may communicate with you by electronic mail where any such person wishes us to do so, on the basis that in consenting to this method of communication you accept the inherent risks, that to the extent permitted by law we may intercept such communications in order to monitor them for internal compliance or other statutory purposes, and that you shall perform virus checks. We may at your request send documents to an electronic storage facility hosted or controlled by you or at your direction, in which event you shall be responsible for security and confidentiality at such facility.

17. We may receive information from you or from other sources in the course of delivering the Services. To the fullest extent permitted by law, we shall not be liable to you for any loss or damage suffered by you arising from fraud, misrepresentation, withholding of information material or relevant to the Services or required by us, or other default relating to such information, whether on your part or that of the other information sources, unless such fraud, misrepresentation, withholding or such other default is evident to us without further enquiry.

Knowledge and conflicts

18. In clauses 18 to 24 "**Barriers**" means safeguards designed to facilitate the protection of each client's interests and may include (for example): separate teams, their geographical and operational separation and/or access controls over data, computer servers and electronic mail systems.

19. The Engagement Team shall not be required, expected or deemed to have knowledge of any information known to Other KPMG Persons which is not known to the Engagement Team.

20. The Engagement Team shall not be required to make use of or to disclose to you any information, whether known to them personally or known to Other KPMG Persons, which is confidential to another client.

21. KPMG Persons may be delivering services to, or be approached to deliver services to, another party or parties who has or have interests which compete or conflict with yours (a "**Conflicting Party**" or "**Conflicting Parties**").

22. KPMG Persons are and shall remain free to deliver services to Conflicting Parties, except that where the interests of the Conflicting Party conflict with yours specifically and directly in relation to the subject matter of the Services: the Engagement Team shall not deliver services to the Conflicting Party; and Other KPMG Persons may only deliver services to the Conflicting Party where appropriate Barriers are put in place. The effective operation of such Barriers shall constitute sufficient steps to avoid any real risk of a breach of our duty of confidence to you.

23. We seek to identify Conflicting Parties in the circumstances set out in clause 22. If you know or become aware that a KPMG Person is advising or proposing to advise such a Conflicting Party, you shall inform us promptly.

24. Where a party has engaged us to deliver services before you have done so and subsequently circumstances change, we may consider that, even with Barriers operating, your interests are likely to be prejudiced and we may not be satisfied that the situation can be managed. In that event we may have to terminate the Services Contract and we shall be entitled to do so on notice taking effect immediately on delivery but we shall consult you before we take that step.

The Services Contract

25. The Services Contract sets out the entire agreement and understanding between you and us in connection with the Services. Without affecting KPMG's responsibilities for other services it is engaged to perform on terms agreed separately in writing, the Services Contract supersedes and relieves you and KPMG from liability (if any) that might otherwise arise for any prior agreements, understandings, arrangements, statements or representations (unless made fraudulently) as to any facts or matters relating to you or to KPMG or the Services. Any modifications or variations to the Services Contract must be in writing and signed by each of us. If there is any inconsistency between the Engagement Letter and any other elements of the Services Contract, the Engagement Letter shall prevail. If there is any inconsistency between these General Terms and Additional Terms that may apply, the Additional Terms shall prevail.

Third party rights

26. Save where the Services Contract confers benefits on KPMG Persons who are not the KPMG contracting party, no-one shall have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any part of the Services Contract. We and you may rescind or vary the Services Contract without anyone else's consent. Other Beneficiaries (if any) shall acquire rights under the Services Contract through signature by the addressee of the Engagement Letter on their behalf.

Circumstances beyond your or our control

27. Neither we nor you shall be in breach of our contractual obligations or incur any liability to the other if we or you are unable to comply with the Services Contract as a result of any cause beyond our or your reasonable control. In the event of any such occurrence affecting one of us, that one shall be obliged as soon as reasonably practicable to notify the other, who shall have the option of suspending or terminating the operation of the Services Contract on notice taking effect immediately on delivery.

Waiver, assignment and sub-contractors

28. Failure to exercise or enforce any rights shall not amount to a waiver of such rights.

29. No-one shall have the right to assign the benefit (or transfer the burden) of the Services Contract to another party.

30. Subject to clauses 4 and 39, we shall have the right to appoint sub-contractors to assist us in delivering the Services but where any such sub-contractors are not KPMG Persons we shall consult you before doing so. Where we appoint sub-contractors under this clause, we may share Confidential Information with them and for all purposes in connection with the Services Contract we shall accept responsibility for their activities which shall form part of the Services.

Limitations on our liability

31. Our liability in connection with the Services Contract and the Services shall be limited in accordance with this clause.

    In the particular circumstances of the Services set out in the Engagement Letter and subject to clause 33 and clause 34 below,

    - the aggregate liability to you and to Other Beneficiaries of each and all KPMG Persons,
    - in contract or tort or under statute or otherwise,
    - for any loss or damage suffered by you (or by any such other party) arising from or in connection with the Services or the Services Contract,
    - however the loss or damage is caused, including if caused by our negligence but not if caused by our fraud or other deliberate breach of duty,

    shall be limited to the amount specified in the Engagement Letter.

32. Where there is more than one beneficiary of the Services ("**Beneficiary**") the limitation on our liability agreed under clause 31 to each Beneficiary shall be apportioned by them amongst them. No Beneficiary shall dispute or challenge the validity, enforceability or operation of clause 31 on the ground that no such apportionment has been so agreed or that the agreed share of the limitation amount apportioned to any Beneficiary is unreasonably low. In this clause, "Beneficiary" shall include you and Other Beneficiaries.

33. Subject always to the aggregate limitation on our liability in clause 31 above, our liability shall in aggregate be limited to that proportion of the total loss or damage, after taking into account contributory negligence (if any), which is just and equitable having regard to the extent of our responsibility for the loss or damage concerned, and the extent of responsibility of any other person also responsible or potentially responsible ("**Other Person**"). In order to calculate the proportionate share of our liability, no account shall be taken of any matter affecting the possibility of recovering compensation from any Other Person, including the Other Person having ceased to exist, having ceased to be liable, having an agreed limit on its liability or being impecunious or for other reasons unable to pay, and full account shall be taken of the responsibility to be attributed to any Other Person whether or not it is before the competent court as a party to the proceedings or as a witness.

34. We accept the benefit of the limitations in clauses 31, 32 and 33 above on our own behalf and in so doing we confer benefits on all KPMG Persons involved in delivering the Services.

    Any parts of the Services Contract which do or may exclude or limit our liability in any respects shall not apply beyond the extent permitted by law.

35. This clause shall apply to claims arising from or under the Services Contract.

    35.1 You and Other Beneficiaries shall not bring any claim against any KPMG Person or anyone else except the KPMG contracting party in respect of loss or damage suffered by you or by Other Beneficiaries arising out of or in connection with the Services. This restriction shall not operate to limit or exclude the liability of the KPMG contracting party for the acts or omissions of anyone involved in delivering the Services.

    35.2 Any claim from you or Other Beneficiaries in respect of loss or damage suffered as a result of, arising from or in connection with the Services Contract, whether in contract or tort or under statute or otherwise, must be made

    - if Services have been delivered, within four years of the date of the activity giving rise to the claim
    - if the Services Contract has been terminated, within four years of the date of termination (subject to the bullet above)
    - if the claim relates to our unauthorised disclosure of Confidential Information, within four years of the date on which the unauthorised disclosure took place

    and in any of these cases that shall be the date when the earliest cause of action (in contract or tort or under statute or otherwise) shall be deemed to have accrued in respect of the relevant claim. For the purposes of this clause a claim shall be made when court proceedings are commenced.

Third parties

36. If you breach any of your obligations under the Services Contract and there is any claim made or threatened against us by a third party, you shall compensate us and reimburse us for and protect us against any loss, damage, expense or liability incurred by us which results from or arises from or is connected with any such breach and any such claim. If any payment is made by you under this clause you shall not seek recovery of that payment from us at any time. In this clause "us" shall include all KPMG Persons and "you" shall include Other Beneficiaries.

Termination

37. Each of us can terminate the Services Contract or suspend its operation by giving 30 days' prior notice in writing to the other at any time. Termination or suspension under this clause shall not affect any rights that may have accrued for either of us before termination or suspension and all sums due to us shall become payable in full when termination or suspension takes effect.

38. Any part of these General Terms which by its nature or implicitly or to give effect to its purpose is to continue in force after expiry or termination of the Services Contract shall survive, such as (for example) restrictions on use or confidentiality or terms protecting against liability.

Data protection

39. The definitions and interpretations in the Data Protection Act 1998 ("**the Act**") shall apply to this clause. We shall process or arrange for processing of personal data on your behalf for the purposes of delivering the Services. For such purposes we shall have your authority to do so in accordance with this clause. We shall act on your instructions only (given for such purposes) and we shall comply at all times with the seventh principle in Part 1 of Schedule 1 to the Act as if applicable to us directly. We may also process or arrange for processing of personal data in order to support the maintenance of quality and standards in our work or to facilitate the administration of our business or to support our infrastructure. We shall answer your reasonable enquiries to enable you to monitor our compliance with this clause. We shall not sub-contract our processing of personal data (unless to KPMG Persons or other parties who are required to take equivalent measures when processing personal data) without your prior written consent.

Notices

40. Any notice under the Services Contract shall be given in writing and delivered by pre-paid first class post (or pre-paid overseas equivalent) to or left at our respective addresses appearing in the Engagement Letter (or such other address as may be notified in writing). Notices delivered by post shall be deemed to have arrived, where posted from and to addresses in the UK, on the second working day and where posted from or to addresses overseas, on the tenth working day, following the date of posting.

Severability

41. Each clause or term of the Services Contract constitutes a separate and independent provision. If any provisions of the Services Contract are judged by any court or authority of competent jurisdiction to be void or unenforceable, the remaining provisions shall continue in full force and effect.

Capacity

42. You agree to and accept the provisions of the Services Contract on your own behalf and as agent for Other Beneficiaries. You shall procure that any Other Beneficiaries shall act as if they had each signed a copy of the Engagement Letter and agreed to be bound by the Services Contract. However, you alone shall be responsible for payment of our Charges.

43. We accept your agreement to and acceptance of the terms of the Services Contract (save for clauses 31, 32 and 33 above) on our own behalf and in so doing we confer benefits on all KPMG Persons.

Regulated activities

44. Where the Services (or part of the Services) amount to "regulated activities" under the Financial Services and Markets Act 2000, or activity that is regulated by the Solicitors Regulation Authority, we shall inform you and set out the implications in the Engagement Letter or elsewhere in writing and Additional Terms shall apply.

Law and jurisdiction

45. The Services Contract shall in all respects be subject to and governed by English law and all disputes arising on any basis from or under the Services Contract shall be subject to the exclusive jurisdiction of the English courts.

Feedback on our performance

46. We aspire to embed in our culture the attributes that we feel distinguish our brand and contribute to the difference that you experience when you engage KPMG. We may invite you to provide feedback on our performance so that we can measure to what extent we meet our goals. If you wish to discuss the Services or complain about them, you are invited to contact any partner or director named in the Engagement Letter. If your problem is not resolved, you should contact David Matthews, our UK Head of Quality & Risk Management, by e-mail to david.matthews@kpmg.co.uk or by writing to him at 15 Canada Square, London E14 5GL or through our website at http://www.kpmg.co.uk/clientcare where you can also find details of information about us that we are required by regulations to make available to you. We investigate any complaints promptly and do what we can to resolve difficulties. If you are still not satisfied, you can refer the matter to the ICAEW and (in respect of "regulated activities" and ancillary services) to the Financial Ombudsman Service and to the Legal Ombudsman in respect of activity that is "reserved legal activity" or "legal activity" under the Legal Services Act 2007, or any complaint that the Legal Ombudsman considers to be about a legal service.

KPMG

Additional Terms: Reports under ISAE 3402 and AAF 01/06

These Additional Terms supplement our General Terms of Business and apply where expressly incorporated in the Engagement Letter.

Where the Services involve the provision of a report (**"the Reporting Accountants' Report"**) having regard to the framework set out by the Institute of Chartered Accountants in England & Wales (**"the Institute"**) in Technical Release AAF 01/06, *'Assurance reports on internal controls of service organisations made available to third parties'* and the International Auditing and Assurance Standards Board (IAASB) in International Standard on Assurance Engagements 3402 *'Assurance reports on controls at a Service Organisation'*, the terms and conditions set out below shall apply.

Duties and responsibilities of directors

1. The directors (**"the Directors"**) of the company in relation to which the Reporting Accountants' Report is to be provided (**"the Company"**) are and shall be responsible for the design, implementation and maintenance of control procedures that provide adequate levels of protection for the data processed by the Company, customers' assets (and, where appropriate, liabilities) and to ensure that all transactions are properly recorded. The Directors are and shall be responsible also for the definition of adequate levels of protection in terms of control objectives and for ensuring that these objectives are achieved by the control procedures in place. The Directors shall describe the system (control objectives and the related control procedures) and provide a written assertion in a report (**"the Directors' Report"**).

2. In drafting the Directors' Report, the Directors shall have regard to, as a minimum, the criteria specified within the Technical Release AAF 01/06 issued by the Institute but they may add to these to the extent that this is considered appropriate in order to meet customers' expectations.

Duties and responsibilities of Reporting Accountant

3. It is and shall be our responsibility to form and set out in the Reporting Accountants' Report an independent opinion on the matters noted in clause 4 below, based on the work carried out in relation to the control procedures of the Company's specified function carried out at the specified business units of the Company as described in the Directors' Report and report this to the Directors. We shall not be responsible for a review of changes to control procedures beyond the period reported upon or for the identification of changes not disclosed by the Directors.

4. The Reporting Accountants' Report shall set out an independent opinion on whether:

   a) The Directors' description of the system fairly presents the system that was designed and implemented; and

   b) The controls included in the aforementioned description were suitably designed;

   at a specified reporting date. Where the Reporting Accountants' Report covers a specified period in time, that opinion shall address those matters throughout the specified period to that reporting date and it shall also set out an independent opinion on whether:

   c) Such controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the specified period.

   The reporting date and, if appropriate, the specified period shall be defined in the Engagement Letter. We shall not be responsible for a review of changes to control procedures beyond the period reported upon or for the identification of changes not disclosed by the Directors.

5. The Directors acknowledge that control procedures designed to address specified control objectives are subject to inherent limitations and, accordingly, errors or irregularities may occur and may not be detected. Such procedures cannot be proof against fraudulent collusion especially on the part of those holding positions of authority or trust. The Directors accept that our opinion set out in the Reporting Accountants' Report shall be based on historical information and the projection of any information or conclusions contained in that opinion or in the Directors' Report, to any future periods shall be subject to the risk that changes in procedures or circumstances may alter their validity.

6. We may seek written representations from the Directors in relation to matters on which independent corroboration is not available. We shall seek confirmation from the Directors that any significant matters of which we should be aware have been brought to our attention.

Use of our report

7. The Reporting Accountants' Report shall, subject to the permitted disclosures set out in these Additional Terms, be made solely for the use of the Directors, and solely for the purpose of reporting on the internal controls of the Company, in accordance with the Services Contract. Our work shall be undertaken so that we might report to the Directors those matters that we have agreed to state to them in the Reporting Accountants' Report and for no other purpose. Our Reporting Accountants' Report shall be issued on the basis that it must not be recited or referred to or disclosed, in whole or in part, in any other document or to any other party, without our express prior written permission. Provided that you have obtained our approval as to the form of disclosure and its context, we permit the disclosure of our Reporting Accountants' Report, in full only, to customers of the Company (**"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 and issued in connection with the internal controls of the Company without assuming or accepting any responsibility or liability to them on our part.

8. You shall not use the Reporting Accountants' Report, or make references to it, in material disseminated to the general public without our express written permission. In any cases where marketing literature is prepared which will refer either to us or to

the Reporting Accountants' Report, you shall seek our consent to those references in advance and we reserve the right to refuse or to give consent subject to conditions.

Third parties

9. We shall accept no responsibility or liability for any loss or damage suffered or incurred by any person other than the Company, including without limitation any customer or regulator of the Company, as a result of any reliance that any such person may place on the Reporting Accountants' Report and we may make this clear in the Reporting Accountants' Report.

10. In consideration for our consent to your making the Reporting Accountants' Report available to third parties under clause 7 above you agree that the Company shall indemnify any KPMG Persons and hold us and them harmless against any loss, damage, expense or liability incurred by us or them as result of, arising from or in connection with any claim made or threatened by a third party (including without limitation any customer or regulator of the Company) which results from or arises from or is connected with the provision of the Reporting Accountants' Report to third parties (whether under the provisions of clause 7 or otherwise) to the extent that such loss, damage, expense or liability exceeds the amount of the limitation of our aggregate liability to you set out in the Services Contract and does not result from our fraud or other deliberate breach of duty. In this clause, "you" shall include the Directors and the Company and any Other Beneficiaries.

General Terms of Business

11. Clause 7 of our General Terms of Business shall apply to the Services Contract subject to clause 7 of these Additional Terms.

Survival on termination

12. Clauses 5, 7, 8, 9, 10, 11 and 12 of these Additional Terms shall survive expiry or termination of the Services Contract.

APPENDIX 3 – TRANSMITTAL LETTER

Appendix 4 – Form of transmittal letter

To be produced on Insight Investment Management Limited or Insight Investment Management (Global) Limited or Pareto Investment Management Limited headed paper

Private & confidential

Prospective Customer of *Insight Investment Management Limited or Insight Investment Management (Global) Limited or Pareto Investment Management Limited*

[Date]

Dear Sirs

ISAE 3402 / AAF 06/01 Type II Reporting Accountants' 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") in accordance with the specific terms of reference agreed between Insight Investment Management Limited ("the Company") and 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 the Company 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 wishes you to be aware that the work it carried out for the directors of the Company was designed to meet our agreed requirements and particular features of the engagement determined by our needs at the time. The Report should not be regarded as suitable to be used or relied on by any party wishing to acquire any rights against KPMG other than the Company 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 the Company, the Report or any judgments, conclusions, opinions, findings or recommendations that KPMG may have formed or made and, to the fullest extent permitted by law, KPMG will accept no liability in respect of any such matters to you. Should you choose to rely on the Report, you will do so at your own risk.

The Report is released to you on the basis that, save as may be required by law or by a competent regulatory authority, it is not to be copied, referred to or disclosed, in whole or in part, without KPMG's prior written consent. *[To be included if the customer or prospective customer is a public body* Please note that the Report is confidential and that this letter is also confidential between you and Insight Investment Management Limited. Any disclosure of the Report beyond you and us, and any disclosure of this letter beyond you and us, will or may prejudice substantially

KPMG's commercial interests. A request for KPMG's consent to any such wider disclosure may result in KPMG's agreement to these disclosure restrictions being lifted in part. If 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, having regard to these actionable disclosure restrictions you should let KPMG know and you should not make a disclosure in response to any such request without consulting KPMG in advance and taking into account any representations that KPMG might make.]

Yours faithfully

Insight Investment Management Limited