Pension Board

Monday, 26 June 2023 at 10.00 a.m.
Committee Room - Tower Hamlets Town Hall, 160 Whitechapel Road, London E1 1BJ

Supplemental Agenda

8 .9 Review of Internal Controls at Investment Managers and Custodian (Pages 3 - 16)

Contact for further enquiries:

Farhana Zia, Democratic Services Officer,
farhana.zia@towerhamlets.gov.uk
020 7364 0842
Town Hall, 160 Whitechapel Road, London, E1 1BJ
http://www.towerhamlets.gov.uk/committee

This page is intentionally left blank

Non-Executive Report of the: **Pensions Committee** Monday 3 July 2023	TOWER HAMLETS
Report of Caroline Holland, Interim Corporate Director Resources	**Classification:** Unrestricted
Review of Internal Controls at Investment Managers and Custodian	

Originating Officer(s)	Miriam Adams, Interim Head of Pensions & Treasury
Wards affected	All wards

Summary

This report presents the finding of the review of the adequacy of internal control measures put in place by the fund managers that hold the Fund's assets in management. Officers have reviewed the available AAF 01/06 and SSAE3402 (which signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm).

The review of these reports and bridging letters has identified no significant changes in the internal control environment for the period 1 April 2022 to 31 March 2023.

The Fund managers' internal control reports have been audited and approved by external auditors and from the reports issued they are satisfied that adequate controls are in place for managing and reporting of the Fund's assets.

Recommendations:

The Pensions Committee is recommended to:

1. Note the report contents; and

2. Note that the current position for London CIV.

1. REASONS FOR THE DECISIONS

1.1 There are no alternative decisions to be made.

2. ALTERNATIVE OPTIONS

2.1 The review of fund managers' AAF 01/06 and ISAE 3402 reports should provide some assurance to the Pension Fund (Members and Trustees) that fund managers have adequate controls and safeguards are in place to for managing the Fund's assets. It is appropriate for the committee and Fund members to be kept abreast of any risks identified through this process and the likely impact of such risks to the Fund.

3. DETAILS OF REPORT

3.1 The Pensions Regulator Code of Practice 9 Internal Controls requires Trustees to review internal controls as part of risk management.

3.2 There are a range of internal control reports produced in different countries I response to local and regulatory pressures. The guidance allows service organisations to disclose their controls activities and processes to their clients and the auditors of their clients in a uniform reporting format.

3.3 The publication of a service auditor's report prepared in accordance with a country's authoritative guidance indicates that a service organisation has had its service control objectives and control activities examined by an independent accounting and auditing firm.

The importance of these assurance reports is that they can provide appropriate audit evidence under ISA (UK & I) 402.

3.4 In December 2009, the IAASB published Internal Standard on Assurance Engagement 3402 (ISAE 3402), Assurance Reports on Controls at a Service Organization. This is effective for service auditors' reports covering periods ending on or after 15 June 2011 and replaces the previous AAF01/06 and SAS70 reports. This standard should now be the basis for all internal control reports, whichever country they have been issued in.

3.5 This authoritative guidance allows pension fund managers to disclose their control activities and processes in a universally recognised reporting format, which is updated annually.

3.6 The Fund has always required that fund managers prepare and provide internal control reports as part of their reporting requirement to the Fund. These reports provide some assurance to the Fund that fund managers' internal controls/safeguarding measures are adequate. These reports are subject to annual audits, and consequently officers also review the updated reports annually to ensure that any changes are acceptable to the Council and will not expose the Fund's assets to undue risk.

Review of Fund Managers' and Custodian Internal Control Reports

3.7 Each of the Fund's investment managers prepares an annual report having regard to ISAE 3402 and AAF 01/20. Under these protocols the directors/partners prepare a report focussing on key environmental business and process issues and make commitments along the following lines:

- The report describes fairly the control procedures that relate to their stated control objectives;
- How risk is controlled in the provision of investment management or custody services;
- The control procedures are suitably designed such that there is reasonable assurance that the specified control objectives would be achieved if the described control procedures are complied with satisfactorily; and
- The control procedures described are operating with sufficient effectiveness to provide assurance that the related control objectives were achieved during the period specified.

3.8 Each of the managers has engaged a leading firm of auditors to report on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives.

3.9 The internal controls report for the following fund managers have been received and reviewed:

- Schroders
- LCIV
- Legal & General
- Goldman Sachs
- Insight

3.10 This process has not identified any significant change in risk to the Fund. However, a report from the London CIV in their capacity as investment manager which complies to the Standard is currently being awaited.

Legal and General (LGIM) – Low Carbon Global Equities investments

3.11 LGIM provided Assurance report on Internal Controls for the period 1 January 2022 to 31 December 2022. In respect of the Pension Fund accounts a bridging letter covering the period 1 January 2023 to 31 March 2023 was also received.

3.11.1 The report is based on the framework set out in the technical releases International Standards for Assurance Engagements (ISAE) 3402, issued by the international Auditing and Assurance Standards Board (IAASB (and the Audit and Assurance Faculty (AAF) 01/20 on assurance reports on the internal controls of service organisations made available to third parties. Issued by the Institute of

3.11.2 There were no issues of material concerns flagged by KPMG who are the LGIM auditors.

The report only covers the control activities, policies and procedures in relation to the unitised funds in the following areas of operation – accepting clients, authorising and processing transactions, maintaining financial and other records, safeguarding of assets, managing and monitoring compliance and outsourcing, reporting to clients, restricting access to systems and data, maintaining integrity of the systems, maintaining and developing systems hardware and software, recovering from processing interruptions and managing and monitoring compliance and outsourcing.

3.11.3 Cyber security – LGIM maintains and continually improves a cyber and information security framework ensuring integrity of operations and confidentiality of information Cyber incident response plans are routinely maintained and tested to validate security posture.

Eight control objectives tested required management responses.

London CIV (LCIV)

Portfolio managers internal control reports

3.12 At the time of writing this report, LCIV report is yet to be received. The LCIV has been contacted about this.

Goldman Sachs (GSAM) (pooled fixed income investments)

3.13 The manager provided reports for the period 1 October 2021 to 30 September 2022 and a bridging letter for the period 1 October 2022 to 31 March 2023. There were no significant issues raised by the external auditor PricewaterhouseCoopers LLP (PWC).

3.13.1 The report covered Goldman Sachs Asset Management group's description of its Investment Management system for processing user entities transactions throughout the period October 1, 2021, to September 30, 2022, and the suitability of the design and operating effectiveness of the controls.

3.13.2 The report acknowledges limitations of testing, but no qualifications or major issues reported. PWC concluded that the controls operated effectively to provide reasonable assurance that the control objectives state in the description were achieved throughout the period. Management acknowledged that asset management is reliant upon the use of internal and third-party information processing technologies in conducting its investment management activities. As a result, most of the processing of transactions for accounts is automated.

Investment management focus areas are client relationship management, strategic client services, compliance, operations and portfolio management.

3.13.3 Control objective 11- controls provide that provide reasonable assurance that logical access to production programs, data files and IT infrastructure is restricted to authorised and appropriate users. Two of the tests conducted required management response to sample exceptions.

Asset Management Controls	PricewaterhouseCoopers Tests	Results of Tests
f. Access permissions to applications and supporting infrastructure are recertified on a periodic basis to ensure access is commensurate with the individual's current job function/role. Access is re-approved or revoked in a timely manner.	**Inspection** Inspected evidence to determine whether a periodic access recertification was performed for all access permissions. **Inspection** For a sample of access permissions requested to be revoked as a result of the periodic access recertification, inspected evidence to determine whether the access permissions were revoked in a timely manner. **Inspection** For a sample of access permissions requested to be retained as a result of the periodic access recertification, inspected evidence to determine whether the reviewer and access permission was appropriate.	**Exceptions noted.** For the user access recertification performed for the SecDb platform, 4 out of 162 teams were not included in the recertification.
g. Production access events are pre-approved and are monitored and reviewed in a timely manner by appropriate personnel to ensure that the access events are performed by authorized individuals.	**Observation** Observed a production access event to determine whether the production access event was captured by the Production Access Control Tool ("PACT") completely and accurately, and routed to appropriate personnel for review. **Inspection** For the population of production access events, inspected evidence to determine whether the production access events were reviewed in a timely manner.	**Exceptions noted.** For the population of 3,526 production access reviews performed during the period, 270 production access reviews were not performed in a timely manner.

d. Production access events are monitored and reviewed in a timely manner by appropriate personnel to ensure that changes are authorized.	**Observation** Observed a production access event to determine whether the production access event was captured by the Production Access Control Tool ("PACT") completely and accurately, and routed to appropriate personnel for review. **Inspection** For the population of production access events, inspected evidence to determine whether the production access events were reviewed in a timely manner.	**Exceptions noted.** For the population of 3,526 production access reviews performed during the period, 270 production access reviews were not performed in a timely manner.

3.13.4 Management response to control test f above: The exclusion of the four teams from the recertification was a result of an oversight during the setup of the recertification process. Upon identification of the oversight, the recertification for the excluded teams was performed with no access changes requested.

Management response to control test g and 12d above: The increased oversight in production access reviews has resulted in fewer extended unreviewed events, however, this reviews not performed within 21 days SLA exceeded the determined the access events were performed by authorised individuals and approved management prior to each use. Oversight and escalation have now increased to 14 days to meet the 21- day SLA.

3.13.5 Although not covered by the external audit of controls, the report noted that there are information barriers both within asset management and between asset management and other areas of the firm that serve to control the flow of

confidential and proprietary information as well as protect asset management client confidential information. The firm's information barriers, which segregate asset management from the firm and its affiliates, are audited annually by Internal Audit.

Schroders (Commercial Real Estate investments)

3.14 Report provided by this manager covered Synthetic Equity, Equity protection and Real Estate mandates. Period covered was 1 October 2021 to 30 September 2022. The manager issued a bridging letter covering 1 October 2022 to 31 March 2023. The period covered by the report differs to the period covered by report issued in previous years. This new reporting period was adopted by Schroders to make report available to clients in January each year.

3.14.1 EY the managers auditors reported no significant issues but acknowledges that their report did not cover security controls. EY concluded that control activities stated in management's report were suitably described to provide reasonable assurance that the specified control objectives would be achieved.

3.14.2 The controls described by Schroders and audited by EY covers investment management, property investment management and information technology activities conduced in Schroders Group investment centres onbehalf of clients. The report does not cover the activities or controls of outsourced functions or third-party fund managers in the Schroders Real Estate fund.

3.14.3 The service auditor also provided assurance on European Market Infrastructure Regulation (EMIR).

Insight Investments (Pooled Fixed Income Investments)

3.15 The manager's report covered the period 1 October 2021 to 30 September 2022. A bridging letter was provided by the manager to cover period between 1 October 2022 to 31 March 2023.

3.15.1 No material adverse changes to the control environment and/or objectives was reported by KPMG. KPMG procedures included testing the operating effectiveness and suitability of those controls that they consider necessary to provide reasonable assurance that the control objectives were achieved.

Controls tested included account set up, guideline coding, trade execution, counterparty set up and monitoring, trade settlement, corporate actions, proxy voting, new money and withdrawals, investment income and valuations.

3.15.2 The test of controls does not include subservice organisations who provide Insight with supporting technology, back office and proxy voting services to their investment management service.

KPMG issued reasonable assurance report however there were a number of controls which required management responses.

3.15.3 Guideline coding control objective 3 - test to provide reasonable assurance that investment limits and restrictions are established. The test inquired of Insight management as to whether any investment management agreement for currency risk management portfolios (Japanese) had been signed during the period. Although management represented that there was none during the, KPMG were unable to test the operating effectiveness of the control. The Fund has no Japanese market fixed income investments with Insight.

3.15.4 Stable value controls – account opening was tested. Control objective 22 (1 and 2) – controls tested to provide reasonable assurance that stable value account opening activities are authorised and completed accurately and timely. Although management represented that there were no new client accounts opened or closing during the period, auditors were unable to test the operating effectiveness of the control.

Stable value controls – investment guidelines were tested. Control objective 23.1 – controls in place to provide reasonable assurance that investment guidelines and amendments to investment guidelines are input completely and accurately, and compliance with the guidelines is monitored on a timely basis.

3.15.5 Management represented that there were no new or amended investment guidelines document for Stable Value Accounts during the period, the auditors were unable to test the operating effectiveness of the control. The same applied to two of the tests conducted for control objective 24 – controls provide reasonable assurance that stable value controls – transaction authorisation. Sample tests 24.3 and 24.5 could not be tested because there were no traditional GIC trades for stable value accounts.

3.15.6 KPMG also tested controls for single entity controls. Control objective 31 – controls provide reasonable assurance that Guaranteed Investment Contracts (GICs)/Medium Term Notes (MTN) balances maintained in Ares are complete and accurate. The operating effectiveness of test 31.5 could not be conducted because according to management there were no failures during the period.

3.15.7 The same applied to testing of control objective 32.3 – controls provide reasonable assurance that instructions are sent from properly authorised personnel.

IT General Controls Tested

- Testing of physical access – control objective 34 – controls providing reasonable assurance that physical access to computer equipment, storage media and program documentation in data centre is restricted to properly authorised individuals. Testing 34.1 conducted showed that for 3 of 25 users granted building access, access had not been requested by HR and approved by the Operations Administrations team, for 1 of 25 users granted building access, access was granted prior the approval of the Operations team and for 1 of 25 users granted building access, access was not approved by the Operations Administration team. Management provided responses.

- Testing of segregation of duties – control objective 36 – controls providing reasonable assurance that segregation of duties is defined,

implemented, and enforced by logical security controls in accordance with job roles. Three of five weekly reports of IT activities tested for 36.2 had no evidence of review performed by the Head of IT Operations.

- Management will implement a mechanism to evidence and retain the evidence of review of the weekly reports for permission changes and IT activities in the services affected.

Northern Trust Corporation (NT) – Global Custodian

3.16 NT provided internal controls report for the year to 30 September 2022, covering custody and fund service transactions like account coding, transaction events, authorisation, trade communication and settlements, vault security, tax withholding and reclamation, fund accounts, global sub-custodian management and client and performance reporting all of which are key areas that affect their work for the Fund.

3.16.1 It is understood from the report provided that the audit conducted by KPMG did not include audit of any third-party data centres used by NT.
Some processes included disaster control, IT controls and fraud prevention.

The table below shows internal control responsibilities that NT believe each client should have in place for their accounts.

NT Expectations on Clients	LBTH Controls
Clients, and their appointed representatives (e.g., investment manager), are responsible for providing complete and accurate holding and valuation information on assets not custodied by Northern Trust but held on record in client accounts, including timely notification of security and derivative trades not executed by Northern Trust	All investment managers provide NT with monthly or quarterly reports. LBTH is informed when reports are received late or not received
Clients are responsible for the accuracy and source of prices provided to them to Northern Trust for special-type assets where prices are otherwise unavailable	Quarterly reconciliation of manager and custodian data. Review of source pricing for non-publicly available asset pricing.
Clients are responsible for maintaining the integrity of any connection to Northern Trust from any other network connection, (e.g., the internet, leased line, etc). This should be achieved via the deployment of control mechanisms (e.g., firewalls, routers, switches, etc) to monitor and manage traffic between the client network and the client connection points with Northern Trust network(s) and by limiting access to client systems to only appropriate individuals	The administering Authority inhouse IT is responsible for the IT environment the Fund operates in.

Clients should maintain adequate records (e.g., data files, paper trail, etc) to recover transactions entered since the last processing (i.e., file transmission) and backup cycle.	Copies of reports are saved on the shared teams drive and password protected. Back of the IT environment is managed by the administering authorities internal IT.
Clients are responsible for implementing security administration procedures necessary to properly restrict access of client personnel to Northern Trust systems and provide timely written notification to Northern Trust of changes to employee access privileges.	Access to NT system is restricted to officers in pensions and treasury team who have responsibilities for investment or accounting related duties. Request for access to NT passport system is signed off by authorised signatories of the pension fund.
Clients are responsible for maintaining the confidentiality of assigned IDs and passwords relating to Northern Trust applications and ensuring that such IDs and passwords are not shared resulting in the compromise of system authorities or information security	Password to NT spreadsheet is restricted to officers in the team who have responsibilities for accounting or investment related tasks. Officers on the NT mailing list are also restricted.

3.16.2 Tower Hamlets investments are via pooled funds and comprise public and private markets. Officers receive internal control reports from all Investment Managers including London CIV. A summary of findings is included in this report. Officers also reconcile manager information reported data on cash, asset price, bid price to custody information on a quarterly basis.

3.16.3 The administering authority is responsible for providing IT platform, access to custody system is restricted and access is password protected. Spreadsheet from NT are also password protected. Changes to cash or asset movement requires the signature of two authorised signatories of the pension fund.

3.16.4 Northern Trust Corporation's control objectives and related controls and KPMG's test of controls and results of tests.
These tests covered a number of areas like account coding, transaction events, transaction authorisation, trade communication and settlement, derivate settlements, active collateral management, cash reconcilement, securities reconcilement, global subcustodian management, vault security, securities lending, benefit payments, asset coding and valuation, corporate actions, income collections, tax withholding and reclamation, client accounting and reporting, investment risk and analytical services (IRAS), insurance investment and accounting reporting, unitised valuations and reporting services, fund accounting, transfer agency, private equity fund administration (PEFA), investment operations outsourcing (IOO), real estate and infrastructure administration and technology. As an investor investing via pooled funds, a large number of the test areas covered did not relate to the custody services provided to Tower Hamlets Pension Fund.

Transfer Agency

3.16.5 KPMG tested 4 transfer agency control objectives, each objective having a number of controls specified by NT. 2 out of 15 tests had exceptions noted in samples collected. The table below includes shows the test, exceptions and management responses. None of these directly impact the service provided by NT.

Controls Specified by Northern Trust	Testing Performed by KPMG LLP	Results of Tests Performed
For traditional and unitized funds, when an address change is made, a confirmation is sent electronically, via fax, or by mail (UK only), to investors by Transfer Agency or a third-party vendor. Where the confirmation is sent via post, this is mailed to both the old and new address.	For a selection of address changes, inspected confirmation statements or system logs to determine address change confirmations were sent to investors. Where the confirmation is sent via post, determined it was mailed to both the old and new address.	For 1 out of the 32 testing selections, a confirmation of the change in address was not mailed to the new address. As required by the control, when an address change is made, a confirmation should be sent to both the old and new address. **Management's Response:** Transfer Agency makes every effort to ensure that when a confirmation is sent via post, it is mailed to both the old and new address. The third party vendor responsible for issuing this via post has been notified of mailing to the same address twice and has indicated they will enhance their processes to ensure this error does not occur in the future. NT is reviewing this case with the systems provider and the print vendor to identify anomalies or processing errors that may have caused this occurrence. The investor is aware of the duplicates sent to the same address and Transfer Agency confirms there is no financial impact as a result of this exception.
For U.S., U.K. and Ireland, certain share register transactions may be requested via telephone. Transactions accepted via telephone are received on recorded telephone lines. A Transfer Agency staff member validates the caller's identity through the use of security questions and verifies that the transaction is permitted to be initiated via the telephone. Transactions are read back to the caller for validation and quality control. For Luxembourg, a Transfer Agency Analyst reviews subscription and redemption transactions accepted via telephone to ensure the party requesting the transaction is authorized to initiate the transaction and evidences by sign-off on the check list or electronically in the workflow/Share Registration System.	For a selection of U.S., U.K., and Ireland share register transactions accepted via telephone, listened to the recorded telephone call to determine that the call was verified in accordance with business unit procedures. For a selection of Luxembourg subscriptions and redemption transactions accepted via telephone, inspected sign-offs on the checklist or electronic sign-off in the Share Registration System to determine that transactions were reviewed by the Transfer Agency analyst to verify the transactions were from an authorized party.	For 1 out of the 25 testing selections, the call was not verified in accordance with business unit procedures. **Management's Response:** The Transfer Agency team acknowledges a deviation from standard procedures; however, the combination of answers including full SSN and address provided NT reasonable assurance of the caller's identity. The Transfer agency team has committed to retraining call center partners to follow procedures as described in the guidelines. No exceptions noted.

Technology

3.16.6 KPMG tested 6 technology control objectives, each objective having a number of controls specified by NT. 5 out of 33 tests had exceptions noted in samples collected. The table below includes shows the test, exceptions and management responses. None of these directly impact the service provided by NT.

Controls Specified by Northern Trust	Testing Performed by KPMG LLP	Results of Tests Performed
Employee transfers automatically trigger an access certification review upon systematic notification from Human Resources. The review of the transferred employee's access is completed by the employee's new manager, and the removal of sensitive access is facilitated by Global Access Provisioning.	For a selection of transferred employees, inspected the transfer request and access privileges to determine that sensitive access was removed.	For 1 out of the 67 transfer certification reviews selected for testing, the removal of a high risk entitlement for 1 employee was not completed timely. **Management's Response:** Management has removed access for the 1 employee transfer exception identified prior to the issuance of this report. In addition, management confirmed that the employee did not utilize the access requested to be removed during the period between when the request was initiated to when it was completed. Management recognizes the importance of completing user access removals for employee transfer requests in a timely manner.
Northern Trust computer platforms supporting critical business functions authenticate users' identities. Authentication controls adhere to the requirements defined in Northern Trust's IT risk policy and standards. In the event that particular operating systems or applications cannot conform to Northern Trust password standards due to system limitations, management undergoes formal risk assessment as part of the Technology Risk and Control exception process	Inspected the password management software to determine that settings were in compliance with Northern Trust standards. Inspected operating system password settings to determine that they were in compliance with Northern Trust standards, or that a deviation was approved in accordance with Technology Risk and Control exception process. For a selection of in-scope applications not managed by the password management software or the operating system platform, inspected application-level password settings to determine that they were in compliance with Northern Trust standards, or that a deviation was approved in accordance with the Technology Risk and Control exception process.	No exceptions noted. No exceptions noted. For 1 out of 3 applications tested, the application's authentication controls do not adhere to the requirements defined in Northern Trust's IT risk policy and standards and the deviation was not approved in accordance with the Technology Risk and Control exception process. **Management's Response:** Management was aware that password length and complexity were not met and was prevented by a system limitation. A required waiver from the standard for this situation was not obtained. The risk of a less complex password is mitigated by the requirement to log into the network with a user id and complex password.
Update access to production platforms, including software libraries and files, parameter tables, and sensitive system commands, is restricted to authorized system accounts or individuals.	For a selection of servers from each significant operating system platform, inspected access lists to determine update access to the following items was restricted to authorized system accounts or individuals: • System utilities • Operating system privileges and functions	For 1 user out of the Mainframe Administrators population, access was determined to be inappropriate based on their job title and responsibilities. **Management's Response:** Management confirmed that the inappropriate Mainframe access for the 1 employee has been removed, and that the employee had never logged on to the system. In addition, management reviewed the design of the process for provisioning privileged access and believes that the design is appropriate; however, a change in personnel at the time resulted in the error. Management has reinforced the process with the team members.

Controls Specified by Northern Trust	Testing Performed by KPMG LLP	Results of Tests Performed
Northern Trust requires all managers to perform an annual review in the Identity and Access Management System (IDM) of their direct reports' access to determine that access rights are commensurate with their job responsibilities. If not completed within 30 days of the due date, the user's access (other than basic access such as email, etc.) is suspended until the review is completed by the manager.	For a selection of managers, inspected annual access reviews and associated IDM access rights to determine that reviews were performed within 30 days of the due date and access changes identified during the reviews were updated as requested. Inspected IDM configuration for delinquent reviews to determine it is configured to automatically suspend accounts if reviews are not completed within 30 days of the due date. In addition, inspected an example of a certification that was not completed within 30 days of the due date to determine the system automatically disabled the user's access. For a selection of in-scope applications, inspected emails of successful import job notifications or incident tickets to determine the feeds were accurately and completely processed and ingested into the IDM for access review purposes, and identified ingestion errors were researched and resolved.	No exceptions noted. No exceptions noted. While no exceptions were identified as part of our testing selection of 38 applications, through other testing we became aware that logical access data was not being refreshed for 1 application that is part of the Document Imaging System. Therefore, the user access reviews were not being performed over complete and accurate data. **Management's Response:** Management refreshed the application data sent to IDM on July 18, 2022. After the data refresh, management reviewed the partners with high risk entitlements to the application, resulting in 1 entitlement being removed for 1 partner. The 1 partner had not used the high risk entitlement. The other production access was determined to be appropriate. Controls T2.1 (user provisioning authorization) and T2.3 (user access removal of terminations) listed on page 135 are the primary controls to provide assurance that partners granted access are authorized by managers and partner access is removed when employment is terminated.
New data center access privilege requests are reviewed and approved by an authorized individual prior to access being granted. Data center access privileges are reviewed by management at least semiannually.	For each data center, inspected a selection of data center access requests to determine the request was properly authorized prior to access being granted. For each data center, inspected a selection of periodic reviews of access privileges, to determine that reviews were performed by management. For a selection of changes identified as a result of the periodic access reviews, inspected access listings to determine changes were made as requested.	For 1 out of the 31 new partner access requests selected for testing, although the user was authorized for temporary privileged access, permanent privileged access to a data center was incorrectly provisioned. **Management's Response:** Management acknowledges that although access was authorized, access was incorrectly granted as permanent rather than temporary. Management validated that permanent access was not used. Partners have been provided supplemental training to prevent this from occurring in the future. No exceptions noted. No exceptions noted.

3.16.7 No matters of significant reason were expressed by KPMG. The Custodian provided a bridging letter to cover the period 1 October 2022 to 31 March 2023.

4. EQUALITIES IMPLICATIONS

4.1 There are no direct equalities implications to this report.

5. OTHER STATUTORY IMPLICATIONS

5.1 This section of the report is used to highlight further specific statutory implications that are either not covered in the main body of the report or are

required to be highlighted to ensure decision makers give them proper consideration. Examples of other implications may be:

- Best Value Implications,
- Consultations,
- Environmental (including air quality),
- Risk Management,
- Crime Reduction,
- Safeguarding.
- Data Protection / Privacy Impact Assessment.

Risk Management Implications

5.2 The review of the AAF 01/06 and SSAE3402 internal control reports of third parties that manage Pension Fund assets ensures that fund managers are able to demonstrate that they are properly managing pension fund assets as stewards of the Fund and are following procedures that do not expose fund assets to any undue risks.

5.3 Pension Fund assets could be exposed to undue risk where AAF 01/06 and SSAE 3402 reports are not in place or adequate internal controls and safeguard measures are lacking in the management of Fund assets.

5.4 The risks arising from this investment performance are included in the Pension Fund risk register.

6. COMMENTS OF THE CHIEF FINANCE OFFICER

6.1 Whilst the performance and effective controls of the investment manager and custodian is of paramount importance in the performance of the Pension Fund, there are no direct financial implications arising from this report.

6.2 The employer's contribution is a significant element of the Council's budget and consequently any improvement in investment performance will reduce the contribution and increase the funds available for other corporate priorities.

6.3 A viable pension scheme also represents an asset for the recruitment and retention of staff to deliver services to the residents.

7. COMMENTS OF LEGAL SERVICES

7.1 This is a noting report for the pension committee. There are no direct legal implications arising from this report. The position regarding the internal controls for the five fund managers set out in 3.9 above is included in the report.

Linked Reports, Appendices and Background Documents

Linked Report

- None

Appendices

- None

Local Government Act, 1972 Section 100D (As amended)
List of "Background Papers" used in the preparation of this report.
Fund Managers AAF 01/06 and ISAE 3402 for Schroder's, Legal & General, Insight, Goldman Sachs. In respect of LCIV a summary report covering all underlying managers was received.
(To be email if required)

Officer contact details for documents:

- Miriam Adams, Interim Head of Pensions & Treasury x4248