

Pensions Committee
Hackney Service Centre
1 Hillman Street
London
E8 1DY

Direct line +44 (0)7747 764 529
Email mark.kirkham@mazars.co.uk
27th February 2026

Dear Pension Committee Members,

London Borough of Hackney Pension Fund 2024-25 audit of financial statement conclusion of pending matters – Audit Completion Report

As required by International Standards on Auditing (UK and Ireland), I am writing to communicate the conclusion of those matters that were marked as outstanding within the Audit Completion Report dated February 2026 and presented to the Audit and Governance Committee on 24th February 2026.

The outstanding matters and the conclusions reached are detailed below:

Matter	Conclusion reached
ITGC testing	We have now completed this work with no issues arising.
Risk disclosure testing	We have now completed this work with no issues arising.
IAS 19	We have now completed this work with no issues arising.
IAS 26	We have now completed this work with no issues arising.
Final review procedures	We have now completed this work with no issues arising.
Events after the reporting period	We have now completed this work with no issues arising.

If you wish to discuss these or any other points, then please do not hesitate to contact me.

Yours sincerely,

Mark Kirkham
Key Audit Partner

Appendix 1 – Deficiencies in internal control finalised after the ACR was issued

This appendix outlines the control recommendations for the consideration of Those Charged With Governance that were finalised after the ACR was issued. These do not include those detailed in Section 4 of the Audit Completion Report.

Fund manager reconciliations

Description of deficiency

Quarterly reconciliations between the Fund Manager and GL have not been taking place due to disagreements about the figures.

Potential effects

This means that the assertions of Existence, Rights and Obligations, and Valuation have not been accurately assessed on a regular basis which may impact internal budgets. A year-end reconciliation has been taking place, which means that the scope for material deficiencies is limited.

Recommendation

In order to improve the controls process, there should be adequate discussions with the custodian in order to come to a consensus for quarterly reconciliations to still take place. This helps to ensure that the value of investments remains accurately valued.

Management response

The Pension Fund changed custodian in September 2023, the processes and reporting of investments by the custodian has changed over time following the transition. The historic arrangement meant some transactions were payments directly to the fund managers from the Pension Fund such as purchases for private market capital calls and some income, capital distributions from fund managers were paid directly to the Fund's bank account rather than the custodian. This had led to some differences between what the fund manager reports compared to the custodian. Fund officers have taken steps to implement the more common model whereby all transactions go through the custodian. We have had some success but the custodian would not implement capital calls due to LGPS pooling now underway.

Fund officers use a combination of custodian reports, fund manager reports and cashflows for completeness when carrying out reconciliations on investments and assess whether appropriate valuation of investments have been reported in the custodian reports prior to posting transactions to the general ledger.

Officers engaged with the custodian in October 2024 to undertake monthly fund manager reconciliations which commenced in December 2024, this was only possible for the segregated bond mandate for which they provide custody. The remaining fund managers were pooled investments and reported to the custodian and Fund on a monthly or quarterly basis. The custodian provides quarter reporting in addition to annual reporting to assist officers in reconciliations.

Officers have continued to engage with the custodian to align valuation methods and improve on the recording of cash flows such as directing investment distributions from the fund manager to the custodian. Officers will continue to engage with the custodian to find a solution that improves the timeliness of reporting, resolving discrepancies and approval of reconciliations. We recognise that the custodian and fund managers may have differences in valuation methods, officers will ensure that reconciliations include reasons for differences.

Related parties

Description of deficiency

Not all councillors (including Pension Fund Committee Councillors) completed their related parties forms during the financial statement closing process despite the efforts of the finance team to obtain these. The CIPFA Code of Practice Guidance Notes detail that sole reliance on the statutory register of interests requires recording of transactions as well as relationships, and therefore we consider the operation of both of these controls necessary to ensure the completeness of the related parties note. We consider that the control is currently deficient.

Some Pension Fund Committee members declaration forms are included in this and so the control recommendation also applies to LBHPF.

Potential effects

Related party note might be incomplete or inaccurate.

Recommendation

We recommend the Council strengthens processes and controls in place to meet 100% compliance during the financial statement closing process in the filling out of related party forms by councillors.

Management response

Two councillors did not submit their related party forms; one was on maternity leave, and the other did not engage, indicating a minor lapse in our otherwise robust processes. Despite this, we are committed to achieving 100% compliance with the CIPFA Code of Practice going forward, ensuring all relevant relationships and transactions are fully disclosed in the financial statements.

Password Security

Description of deficiency

Inconsistencies were identified within the password security policy and best practice principles relating to restricted reuse of passwords for users, password expiry timeframes and number of characters passwords. This control is to be included in the follow-up letter to the audit completion report.

Potential effects

There is a risk that passwords may be weaker and more susceptible to cyber-attack which would impact the operational effectiveness of the entity.

Recommendation

We recommend the Council ensures that password policy is in line with best practice standards that parameters on google workspace and account sign-on are consistent with password policies.

Management response

The IT Department is currently conducting a comprehensive review of our existing password policy to ensure continued alignment with industry best practices and evolving security standards.

Currently, our Google Workspace and Single Sign-On (SSO) protocols mandate a "Strong Password" configuration—requiring a combination of letters, numbers, and symbols—with a minimum length of nine characters. This policy also strictly prohibits password reuse and enforces Multi-Factor Authentication (MFA).

While our current standards meet many foundational security requirements, we will be increasing the minimum password length to 12 characters. This technical modification will be applied to Google Workspace and all integrated sign-on systems to ensure consistent enforcement. These proactive measures are vital to bolstering our defence against sophisticated cyber-attacks and maintaining the integrity of our operations.

User Access Review

Description of deficiency

ITGC testing of User Access Reviews of in-scope IT systems identified that there was no implementation of the user review policy which requires System Leads to review licence access and user access requirements in line with roles. Whilst the council provided verbal assurance that these reviews were taken and there were no users with inappropriate access given on either iTrent or CedAR systems there was no formal documentation in place.

Potential effects

here is a risk that users may not have their access reviewed in a timely and appropriate manner which may result in inappropriate privileges being given to individuals beyond the scope in which the access originally agreed or beyond that changes to roles would permit.

Recommendation

We recommend the Council document regular reviews of user access lists and security access levels dependent on role with evidence of inquiry as part of the process and document any actions taken in response to review with authorisation by the system lead in line with the Council's User Access Policy.

Management response

To strengthen internal controls, the Council is transitioning from a verbal assurance model to a mandatory, documented review process for user access.

System Leads will be required to regularly review user access lists against current roles and responsibilities and formally sign off on these reviews. A standardised template will be introduced to record all inquiries made to other service areas and the resulting actions, such as revoking access. This new process will be incorporated into the Council's User Access Policy to guarantee that user privileges consistently align with the scope of their individual roles.

CedAR E5 Journals System Fault

Description of deficiency

Journals testing on the main council identified 7 instances in which the journal inputter's user ID was the same as the reviewer ID. This was caused by a system fault in CedAR e5, where the reviewer ID overwrites the initial poster ID. We cannot ascertain how many journals overall may be impacted by this issue. There were no indications of management override of controls or fraud in the journals selected for testing because they had the same user and approver. Due to the shared ledger system this control deficiency applies to both the Council and the Pension Fund audits.

Potential effects

There is a risk that journals could be edited or manipulated, and segregation of duties controls which are largely effective could be circumvented without detection.

Recommendation

We recommend the Council review the reporting function in CedAR and ensure that reporting accurately reflects the journal uploader, reviewers and authoriser as well as ensure that journal upload templates are updated for all manual journals to ensure consistency.

Management response

The Council is aware of a system glitch in the CedAR e5 finance system where the 'input user' field incorrectly displays the reviewer's ID instead of the original poster's ID upon review of an unposted journal. We are currently collaborating with the supplier to correct this anomaly. However, we reject the assertion that this represents a control weakness. This is solely a visual display error within CedAR e5. It has no impact on the underlying Segregation of Duties (SoD) controls. System permissions are strictly enforced: individuals with inputter roles cannot approve uploads, and authorisers cannot upload journals. Since technical roles remain separate and siloed, it is impossible to override the Segregation of Duties controls.