Audit Committee

18 September 2018: 10:30am

London Councils offices are wheelchair accessible

Location: Meeting Room 4, London Councils, 59½ Southwark Street, London SE1 0AL

Contact Officer: Alan Edwards

Telephone: 020 7934 9911 **Email:** Alan.e@londoncouncils.gov.uk

****** Appendices attached separately

* **Declarations of Interests**

If you are present at a meeting of London Councils' or any of its associated joint committees or their sub-committees and you have a disclosable pecuniary interest* relating to any business that is or will be considered at the meeting you must not:

- participate in any discussion of the business at the meeting, or if you become aware of your disclosable pecuniary interest during the meeting, participate further in any discussion of the business, or
- participate in any vote taken on the matter at the meeting.

These prohibitions apply to any form of participation, including speaking as a member of the public.

It is a matter for each member to decide whether they should leave the room while an item that they have an interest in is being discussed. In arriving at a decision as to whether to leave the room they may wish to have regard to their home authority's code of conduct and/or the Seven (Nolan) Principles of Public Life.

*as defined by the Relevant Authorities (Disclosable Pecuniary Interests) Regulations 2012

If you have any queries regarding this agenda or are unable to attend this meeting, please contact:

Alan Edwards
Governance Manager
Corporate Governance Division
Tel: 020 7934 9911
Email: alan.e@londoncouncils.gov.uk

Minutes of the Meeting of the Audit Committee
21 June 2018

Cllr Roger Ramsey was in the Chair

Members Present:

Cllr Roger Ramsey (LB Havering)
Cllr Stephen Alambritis (LB Merton)
Cllr Victoria Mills (LB Southwark)

In Attendance:

Jerry Mullins, Audit Manager, City of London
Martha Franco-Murillo, Senior Auditor, City of London
Stephen Lucas, Senior Manager, KPMG

London Councils' officers were in attendance.

1. Apologies for Absence

Apologies for absence were received from Councillor Yvonne Johnson (LB Ealing) and Councillor Robin Brown (LB Richmond).

2. Declarations of Interest

There were no declarations of interest.

3. Minutes of the Audit Committee meeting held on 22 March 2018

The minutes of the Audit Committee meeting held on 22 March 2018 were agreed as being an accurate record.

4. Internal Audit Reviews

The Audit Committee received a report that provided members with an update of the internal audit reviews completed by the City of London's Internal Audit section since the last meeting held in March 2018.

David Sanni, Chief Accountant, London Councils, introduced the report, which updated members on the 2017/18 Internal Audit Plan, the implementation of recommendations and reviews that had occurred in earlier years. He informed Audit Committee that there were 11 amber priorities and no red priority recommendations.

David Sanni said that there had been some slippage on the 2017/18 plan. *Appendix 1* showed that the review of financial controls for petty cash, inventories and procurement cards had been completed and the report presented at the last meeting. Draft reports had been issued for the reviews of controls on ICT remote access and mobile devices and the grants scheme, officers are in the process of preparing the management response to the reviews. The fieldwork for the final review on parking and traffic is due to be completed this month and all three outstanding reviews will be presented to the Audit Committee on 18 September 2018.

David Sanni said that *Appendix 2* highlighted previous years' audit recommendations that were followed-up during 2017/18. He informed members that four recommendations had yet to be implemented. Three recommendations arose from the information management and security review, including improvements around password controls, disposal of devices which hold personal data and encryption of portable media devices. The timetable for these had slipped, with a revised implementation dates of September 2018. The reason for the delay in following-up on the three 2013/14 recommendations was the transfer of IT support from in-house to the City of London contract with Agiliysis. The fourth recommendation regarding the UPS backup power supply had now been implemented.

The Chair said that the Audit Committee on 18 September 2018 was likely to have a full agenda and asked whether the outstanding audit reviews could be brought to a later meeting. Jerry Mullins, Audit Manager, City of London, said that he was working with colleagues to ensure that there was a more even spread of audit work. He said that the problem was down to how the City of London scheduled its audit work, and had nothing to do with London Councils. There was currently a bottleneck situation with the audit work. Jerry Mullins said that he had met with David Sanni and would be putting in firm dates for audit reviews. These would be staggered more evenly in the future and monitored.

The Chair asked if the outstanding ICT recommendations affect General Data Protection Regulation (GDPR) compliance. Frank Smith confirmed that this was not the case and that the recommendations enhanced existing controls.

The Audit Committee noted the internal audit reviews report.

5. Review of the Annual Governance Statement (AGS)

The Audit Committee received a report that (i) reviewed each element of the AGS, (ii) highlighted any continuing and potentially new areas for development (and those from previous years), and (iii) made recommendations for revisions that would be contained in the AGS to be included in the audited accounts for 2017/18.

David Sanni introduced the report, which gave a review of the draft Annual Governance Statement (AGS) for the 2017/18 annual accounts. The report also gave a summary of the internal audit reviews undertaken in 2017/18. The AGS had been prepared in accordance with the CIPFA/SOLACE framework to comply with Accounts and Audit Regulations. There had also been some minor changes to key elements in paragraph 7 of the report, incorporating more accurate descriptions of arrangements.

David Sanni informed members that *Appendix A* detailed the AGS that was in the audited accounts for 2016/17, along with recommended changes shown in red using track changes. *Appendix B* was a summary of the internal audit reviews completed in the 12 months to 31 March 2018 and the Head of Internal Audit and Risk Management's opinion on the overall control environment at London Councils. *Appendix C* was a "clean" version of the draft 2017/18 AGS. The Chair acknowledged that no issues had arisen as a result of the substantial changes caused by GDPR coming into effect.

The Audit Committee:

- Noted the summary of the internal audit reviews undertaken during 2017/8 and the opinion of the Head of Audit and Risk Management at the City of London on the overall control environment, as detailed in Appendix B of the report; and
- Approved the recommended changes to the AGS for 2016/17, as detailed in Appendix A of the report, to produce the AGS for 2017/8 for inclusion in London Councils' accounts for 2017/18, as detailed in Appendix C.

6. Risk Management: Services Risk Register

The Audit Committee received a report that presented the current Services Directorate Risk Register for consideration by members.

Yolande Burgess, Strategy Director, London Councils, introduced the risk register report, which was divided into six sections for Services: General Risks, Transport & Mobility, London Tribunals, Grants, Community Services and Young People, Education & Skills (YPES).

Stephen Boon, Chief Contracts Officer, London Councils, introduced sections B and C of the Services Risk Register. Two new risks were B12A and B12B (page 48 of the report). B12A related to a “Lorry Control System Failure” (if the new LLCS system case management and permission application system failed). B12B related to “Key Person Risk for Contractor” and referred to a possible over reliance of key contractor personnel. The Chair asked for details about the contractor risk. Stephen Boon confirmed that a control had been put in place whereby London Councils could gain access to the system keys should anything go wrong (keys needed to decrypt encrypted data, which was held in escrow). Councillor Alambritis said that SMEs needed to be supported, although there were always greater risks when dealing with smaller contractors.

Stephen Boon informed members that risks had been updated for B15 and B16 for the London European Partnership for Transport (LEPT). Brexit (B15) and TfL funding (B16) were the main risks, and the impact on both these risks was set to a 3-rating. Risk B18 “Taxicard Procurement” outlined the risk in procuring the new service. The contract had now been awarded and the risk had been downgraded to fairly low. Stephen Boon said that the new contract should generate savings of approximately 5% plus.

Stephen Boon said that risk numbers C6 and C7 related to “back office” functions. C6 referred to the newly awarded Northgate contract for operating London Tribunals, where there had been some initial teething problems. A number of appeals had been lodged, but had not been heard. Measures had been taken to control this and legal advice had been sought. The supplier would be responsible for any compensation to the appellants, and not the boroughs. The problems had now been rectified and the risk ratings had been reduced from 4 to 2.

Yolande Burgess said that changes to controls had been put in place for the Grants Programme (risk number D3). A risk from the previous year, relating to the failure to find sufficient match funding to draw down additional European Social Fund (ESF) monies, was no longer deemed a risk and had been removed. Controls had been improved and revised for risks E2, E3 and E4.

Yolande Burgess said that the rating for risk F4 which relates to London not adequately meeting the statutory requirements for young people with Special Education Needs and Disabilities had been reduced to reflect current circumstances. Risk F6 which related to the LEP funding of YPES had been removed as the funding had ceased (having been time-limited to the lifespan of the LEP).

The Audit Committee noted the current Services Directorate Risk Register and the changes contained in the cover report.

7. Implementing the General Data Protection Regulation (GDPR) and Data Protection Act 2018

The Audit Committee considered a report that provided members with an update on the London Councils work on the General Data Protection Regulation and the Data Protection Bill 2018.

Frank Smith introduced the report and informed members that a more detailed GDPR report had been presented to Audit Committee in March 2018. A report had initially been presented to London

Councils’ Executive on 16 January 2018. This report updated Audit Committee on where London Councils currently stood with regards to implementing the GDPR.

Frank Smith said that, although the date for GDPR coming into force had now passed (25 May 2018), the work on GDPR for London Councils will be an on-going process of continuous review. Local authorities would now be looking at how the Information Commissioner applies penalties for breaches of the new laws. Frank Smith said that indications are that the Information Commissioner wanted local authorities to demonstrate that they have taken steps to review and improve their data protection arrangements, rather than go in heavy handed and dish out significant fines.

Frank Smith informed members that London Councils had identified a total of 98 contractors which had varying risks with regards to the use of personal data. All 98 contractors had been contacted and given the latest GDPR guidance, and no objections had been received to date. Frank Smith said he would be supporting Emily Salinger who would be policing GDPR on behalf of London Councils.

Emily Salinger informed the Committee that she had been appointed the Data Protection Officer for London Councils. The Chair asked whether London Councils had any privacy notices. Emily Salinger said that London Councils had a number of these. The Chair asked whether there was a link to privacy notices on emails sent to the public. Emily Salinger said that the latest e-bulletin was on the website, and this would be used to enable people to sign up to a new mailing list in the future. She said that there was one distribution list that London Councils felt uncomfortable about sending information to and had, therefore, been discontinued, with a notice posted on the relevant website page informing users to indicate if they wish to receive information in the future.

Frank Smith reminded members that a decision was required on how often they would like to receive updates on GDPR. The Chair said that GDPR should be on the agenda for each Audit Committee meeting, until further notice.

The Audit Committee:

- Noted the work done in relation to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18); and
- Agreed that GDPR updates would be presented to all future Audit Committee meetings, until further notice.

The meeting finished at 11:05am

Action Points

None	Action	Progress
7. Implementing the GDPR and DPA 2018	*To ensure that a GDPR update was brought to every Audit Committee meeting until further notice*	Ongoing

Audit Committee

Annual Audit Report 2017/18 Item no: 04

Report by:	David Sanni	**Job title:**	Chief Accountant
Date:	18 September 2018		
Contact Officer:	David Sanni		
Telephone:	020 7934 9704	**Email:**	david.sanni@londoncouncils.gov.uk

Summary

This report presents the annual audit report to those charged with governance (ISA260) prepared by KPMG, London Councils' external auditor, in respect of the 2017/18 financial year.

Stephen Lucas, from KPMG, will attend the meeting to present the report to members.

Recommendations

The Audit Committee is asked:

- To note the contents of the annual audit report included at Appendix A; and
- To approve the draft letter of representation included at Appendix B.

Annual Audit Report 2017/18

Introduction

1. At its meeting on 22 March 2018, the Audit Committee approved an external audit plan prepared by KPMG which set out the scope and approach for the audit of London Councils 2017/18 accounts. KPMG has completed majority of its audit work and is required to report the outcome of its audit to those charged with governance in accordance with the International Standards of Auditing (UK and Ireland). The audit report summarises the key findings arising from the audit of London Councils 2017/18 accounts and is included at Appendix A to this report.

Audit outcome

2. KPMG anticipate issuing an unqualified opinion on the financial statements subject to the satisfactory conclusion of outstanding issues such as the final quality review process and the receipt of letters of representation. KPMG will provide an oral update on these matters. KPMG will also report that the Narrative Report and Annual Governance Statements are consistent with the financial statements and its understanding of London Councils.

3. There were no audit adjustments to the primary statements identified during the course of the audit. However, there are some presentational adjustments identified in the notes to the financial statements in relation to officers remuneration and related party transactions which are detailed on page 14 of the audit report.

4. There were no recommendations on improvements to internal controls included in the audit report.

Management representation

5. The draft management representation letter can be found at Appendix B of this report. The letter declares, to the best of the management's knowledge, that the financial statements and other information provided to the auditor are sufficient and appropriate and have not omitted any facts that are material to the financial statements. A management representation letter will be required for all three sets of accounts. The letter will be signed by the Director of

Corporate Resources and the Committee is asked to approve the draft letter of representation.

Financial Implications for London Councils

None

Legal Implications for London Councils

None

Equalities Implications for London Councils

None

Appendices

Appendix A – External Audit Report for 2017/18
Appendix B – Draft management representation letter for 2017/18 accounts

Background Papers

Final accounts working files 2017/18

London Councils External Audit Plan for 2017/18

External Audit Report 2017/18

London Councils

DRAFT: 5 September 2018

Content

Contacts in connection with this report are:

Neil Hewitson
Director, KPMG LLP

Tel: 020 7311 1791
neil.hewitson@kpmg.co.uk

Steve Lucas
Senior Manager, KPMG LLP

Tel: 020 7311 2184
stephen.lucas@kpmg.co.uk

Taryn Retief
Assistant Manager, KPMG LLP

Tel: 0777 0620049
taryn.retief@kpmg.co.uk

Page

This report is addressed to London Councils and has been prepared for the sole use of London Councils. We take no responsibility to any member of staff acting in their individual capacities, or to third parties.

External auditors do not act as a substitute for the audited body's own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

We are committed to providing you with a high quality service. If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Neil Hewitson, the engagement lead to London Councils, who will try to resolve your complaint..

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Important notice

Circulation of this report is restricted. The content of this report is based solely on the procedures necessary for our audit. This report is addressed to London Councils and has been prepared for your use only. We accept no responsibility towards any member of staff acting on their own, or to any third parties.

External auditors do not act as a substitute for London Councils' own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

Basis of preparation: This Report is made to London Councils' Audit Committee in order to communicate matters as required by International Audit Standards (ISAs) (UK and Ireland) and other matters coming to our attention during our audit work on the Joint Committee, Transport and Environment Committee and Grants Committee financial statements that we consider might be of interest and for no other purpose. To the fullest extent permitted by law we do not accept or assume responsibility to anyone (beyond that which we may have as auditors) for this Report or for the opinions we have formed in respect of this Report.

Limitations on work performed: This Report is separate from our audit opinion and does not provide an additional opinion on London Councils' financial statements nor does it add to or extend or alter our duties and responsibilities as auditors. We have not designed or performed procedures outside those required of us as auditors for the purpose of identifying or communicating any of the matters covered by this Report. The matters reported are based on the knowledge gained as a result of being your auditors. We have not verified the accuracy or completeness of any such information other than in connection with and to the extent required for the purposes of our audit.

Status of our audit: Our audit is not yet complete and matters communicated in this Report may change pending signature of our audit reports. We will provide an oral update on the status of our audit at the Audit Committee meeting. Aspects of our final closedown procedures including final quality review processes and receiving the management representation letters are still ongoing.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Summary

Financial statements audit – see section 2 for further details

Subject to the final closedown being satisfactorily completed we intend to issue an unqualified audit opinion on London Councils' Joint Committee, Transport and Environment Committee and Grants Committee financial statements, following the Audit Committee adopting them and receipt of the management representations letters.

We have completed our audit of the consolidated Joint Committee financial statements which comprises the Joint Committee, Transport and Environment Committee, Grants Committee and London Councils Limited financial statements, and the Transport and Environment Committee and Grants Committee financial statements. We have read the Narrative Report and reviewed the Annual Governance Statements (AGS). Our key findings are:

- There are no unadjusted audit differences.
- We agreed presentational changes to all three financial statements with officers. These changes mainly related to compliance with the Code of Practice on Local Authority Accounting in the United Kingdom 2017/18.
- We are not seeking any specific management representations beyond those considered as standard for any of the three Committees;
- We reviewed the Narrative Reports and Annual Governance Statements and have no matters to raise with you.

Other matters

ISA 260 requires us to communicate to you by exception 'audit matters of governance interest that arise from the audit of the financial statements' which include:

- Significant difficulties encountered during the audit;
- Significant matters arising from the audit that were discussed, or subject to correspondence with management;
- Other matters, if arising from the audit that, in the auditor's professional judgment, are significant to the oversight of the financial reporting process; and
- Matters specifically required by other auditing standards to be communicated to those charged with governance (e.g. significant deficiencies in internal control; issues relating to fraud, compliance with laws and regulations, subsequent events, non disclosure, related party, opening balances, etc.).

There are no other matters which we wish to draw to your attention in addition to those highlighted in this report or our previous reports relating to the audit of London Councils 2017/18 financial statements.

We have made no recommendations as a result of our 2017/18 work.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Financial statements audit

We audit your financial statements by undertaking the following:

	Accounts production stage		
Work Performed	**Before**	**During**	**After**
1. Business understanding: review your operations	✓	✓	–
2. Controls: assess the control framework	✓	–	–
3. Prepared by Client Request (PBC): issue our prepared by client request	✓	–	–
4. Accounting standards: agree the impact of any new accounting standards	✓	✓	–
5. Accounts production: review the accounts production process	✓	✓	✓
6. Testing: test and confirm material or significant balances and disclosures	–	✓	✓
7. Representations and opinions: seek and provide representations before issuing our opinions	✓	✓	✓

We have completed the first six stages and report our key findings below:

1. Business understanding	In our 2017/18 audit plan we assessed your operations to identify significant issues that might have a financial statements consequence. We confirmed this risk assessment as part of our audit work. We provide an update on each of the risks identified later in this section.
2. Assessment of the control environment	We assessed the effectiveness of your key financial system controls that prevent and detect material fraud and error. We found that the financial controls on which we seek to place reliance are operating effectively. We reviewed work undertaken by your internal auditors, in accordance with ISA 610 and used the findings to inform our work.
3. Prepared by client request (PBC)	We produced the PBC to summarise the working papers and evidence we ask you to collate as part of the preparation of the financial statements. We discussed and tailored our request with the Chief Accountant and this was issued as a final document to the finance team. We are pleased to report that this has resulted in good-quality working papers with clear audit trails.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Financial statements audit

4. Accounting standards	We work with you to understand changes to accounting standards and other technical issues. For 2017/18 these changes related to: • Updates to the presentation of the Comprehensive Income and Expenditure Statement and the Movements in Reserves Statement and the introduction of the new Expenditure and Funding Analysis; • Amended guidance on the Annual Governance Statement. There were no issues arising from these changes that we need to report to you.
5. Accounts Production	We received complete draft accounts for all three Committees on 23 July 2018. The accounting policies, accounting estimates and financial statement disclosures are in line with the requirements of the Code of Practice on Local Authority Accounting in the United Kingdom 2017/18. We thank Finance for their cooperation throughout the visit which allowed the audit to progress and complete within the allocated timeframe.
6. Testing	We have summarised the findings from our testing of significant risks and areas of judgement in the financial statements on the following pages. During the audit we identified only minor presentational issues which have been adjusted.
7. Representations	You are required to provide us with representations on specific matters such as your going concern assertion and whether the transactions in the accounts are legal and unaffected by fraud. We provided a draft of this representation letter to the Chief Accountant on 5 September 2018. We draw attention to the requirement in our representation letter for you to confirm to us that you have disclosed all relevant related parties to us. We are not seeking any specific management representations beyond those considered as standard.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Financial statements audit

ISA 260 requires us to communicate to you by exception ‘audit matters of governance interest that arise from the audit of the financial statements’ which include:

- Significant difficulties encountered during the audit;
- Significant matters arising from the audit that were discussed, or subject to correspondence with Management;
- Other matters, if arising from the audit that, in the auditor's professional judgment, are significant to the oversight of the financial reporting process; and
- Matters specifically required by other auditing standards to be communicated to those charged with governance (e.g. significant deficiencies in internal control; issues relating to fraud, compliance with laws and regulations, subsequent events, non disclosure, related party, opening balances, public interest reporting, questions/objections, etc.).

There are no others matters which we wish to draw to your attention in addition to those highlighted in this report or our previous reports.

To ensure that we provide a comprehensive summary of our work, we have over the next pages set out:

- The results of the procedures we performed over the annual IAS 19 valuation which was identified as a significant risk within our audit plan;
- The results of our procedures to review the required risks of the fraudulent risk of revenue recognition and management override of control; and
- Our view of the level of prudence applied to key balances in the financial statements.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Financial statements audit

SIGNIFICANT audit risk	Account balances effected	Summary of findings
All three Committees: Pension assets and liabilities	Net Pension Liability as at 31 March 2018 – Joint Committee: Pension assets £52.72 million PY £50.47 million Pension liability £80.72 million PY £80.45 million Net pension liability £28.02 million, PY £29.99 million	The net pension liability represents a material element of London Councils' balance sheet. London Councils is an admitted body of London Pension Fund Authority which had its last triennial valuation as at 31 March 2016. This forms an integral basis of the valuation as at 31 March 2018. The valuation of the Local Government Pension Scheme relies on assumptions, most notably around the actuarial assumptions, and actuarial methodology which results in London Councils' overall valuation. There are financial assumptions and demographic assumptions used in the calculation of London Councils' valuation, such as the discount rate, inflation rates, mortality rates etc. The assumptions should reflect the profile of the entity's employees, and should be based on appropriate data. The basis of the assumptions is derived on a consistent basis year to year, updated to reflect changes. There is a risk that the assumptions and methodology used in the valuation of London Councils' pension obligation are not reasonable. This could have a material impact to net pension liability accounted for in the financial statements. We evaluated the competency, objectivity and independence of Barnett Waddingham, your actuarial expert. We used our KPMG actuarial expert to review the appropriateness of the key assumptions made, compared them to expected ranges and found them to be appropriate. We reviewed the methodology applied in the valuation by Barnett Waddingham As part of our work we corresponded with the auditors of the administrating authority to gain assurance over the controls operated by the administrating authority, as well as the value and composition of scheme assets and scheme performance as at 31 January 2018 as passed to the actuary. We checked the disclosure in the financial statements were complete and supported by appropriate evidence. Our review did not identify any issues to bring to your attention. We set out our view of the assumptions used in valuing pension assets and liabilities at page 10.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Financial statements audit

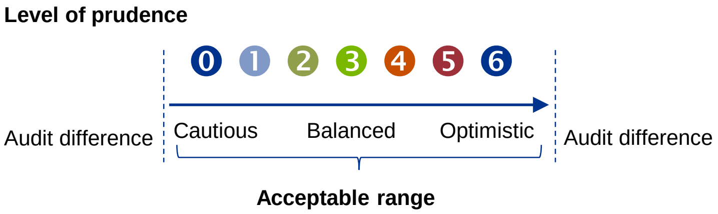
Risks that ISAs require us to assess in all cases	Why	Our findings from the audit
All three Committees Fraud risk from revenue recognition	Professional standards require us to make a rebuttable presumption that the fraud risk from revenue recognition is a significant risk. We do not consider this to be a significant risk for any of the committee's income as there is unlikely to be an incentive to fraudulently recognise revenue.	There are no matters arising from this work that we need to bring to your attention.
All three Committees Fraud risk from management override of controls	Management is typically in a powerful position to perpetrate fraud owing to its ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Our audit methodology incorporates the risk of management override as a default significant risk. In line with our methodology, we carry out appropriate controls testing and substantive procedures, including over journal entries, accounting estimates and significant transactions that are outside the normal course of business, or are otherwise unusual. We have not identified any specific additional risks of management override relating to this audit.	There are no matters arising from this work that we need to bring to your attention.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Financial statements audit

Judgements in your financial statements

We consider the level of prudence in key judgements in your financial statements. We summarise our view below using the following scale:



Level of prudence

Acceptable range

Assessment of subjective areas				
Asset / liability class	**CY**	**PY**	**Balance (£m)**	**KPMG comment**
Accruals	③	③	£1.70M PY:£3.38M	For each committee, we agreed a sample of the accruals recorded in the financial statements to supporting documentation, including confirmation of post-year end payment. We reviewed a sample of post-year end payments to check the cut-off of expenditure recorded in the period and ensured there are no unrecorded liabilities at the year end. We believe London Councils assessment for all three committees represent a balanced view of future payables.
Pensions liability	④	③	£28.02M PY £29.99M	We used our KPMG actuarial expert to review the actuarial assumptions used in the IAS 19 valuation and concluded they are reasonable. Barnett Waddingham (expert used by London Councils) was provided with fund returns from London Pension Partnership (PPP) to 31 January 2018 and the fund returns for the period 1 February 2018 to 31 March 2018 were estimated based on returns on market indices weighted by the Fund's asset allocation. The estimated return over this period was -3%. After the report was produced, Barnett Waddingham received the actual fund returns for those two months and the actual return experienced over this period was -1%. In addition they were notified after the production of the reports that some earlier months' Fund returns had been recalculated and updated by LPP as part of the year-end process. Combined, the overall impact is to reduce the total return over the year from 6% to 5%. Updating this would reduce London Councils' pension fund assets by around £500k. This difference in the estimate is below materiality and therefore is acceptable although our assessment of management's estimate is that they have been slightly optimistic when making the estimate.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Financial statements audit

Narrative Report and Annual Governance Statement

We reviewed London Council's Narrative Report and Annual Governance Statement and confirmed that it is consistent with the financial statements and our understanding of the entity.

Audit fees

Our fee for the audit was £35,100 exc. VAT (£35,100 exc. VAT in 2016/17). This fee was in line with that highlighted in our audit plan approved by the Audit Committee in March 2018. Our fee for London Councils Limited was £900 exc. VAT (£900 exc. VAT in 2016/17).

We have not performed any non-audit work outside of that already disclosed to you as part of our audit planning.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Appendix 1

Materiality and reporting of audit differences

The assessment of what is material is a matter of professional judgment and includes consideration of three aspects:

- Material errors by **value** are those which are simply of significant numerical size to distort the reader's perception of the financial statements. Our assessment of the threshold for this depends upon the size of key figures in the financial statements, as well as other factors such as the level of public interest in the financial statements;
- Errors which are material by **nature** may not be large in value, but may concern accounting disclosures of key importance and sensitivity, for example the salaries of senior staff; and
- Errors that are material by **context** are those that would alter key figures in the financial statements from one result to another – for example, errors that change successful performance against a target to failure.

Materiality for the Joint Committee consolidated accounts was set at £1.3 million which equates to around 2% percent of gross expenditure. We design our procedures to detect errors in specific accounts at a lower level of precision. For the Joint Committee core statements we have used £190k for materiality.

Materiality for the Transport and Environment Committee accounts was set at £850k which equates to around 2% percent of gross expenditure.

Materiality for the Grants Committee accounts was set at £160k which equates to around 2% percent of gross expenditure.

We design our procedures to detect errors in specific accounts at a lower level of precision.

Reporting to Audit Committee

Whilst our audit procedures are designed to identify misstatements which are material to our opinion on the financial statements as a whole, we nevertheless report to the Audit Committee any misstatements of lesser amounts to the extent that these are identified by our audit work. Under *ISA 260*, we are obliged to report omissions or misstatements other than those which are 'clearly trivial' to those charged with governance. *ISA 260* defines 'clearly trivial' as matters that are clearly inconsequential, whether taken individually or in aggregate and whether judged by any quantitative or qualitative criteria. *ISA 450* requires us to request that uncorrected misstatements are corrected.

In the context of London Councils, an individual difference could normally be considered to be clearly trivial if it is less than £65,000 for the Joint Committee overall with £9,000 for its core activities, £8,000 for the Grants Committee and £40,000 for the Transport and Environment Committee.

Where management have corrected material misstatements identified during the course of the audit, we will consider whether those corrections should be communicated to the Audit Committee to assist it in fulfilling its governance responsibilities.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Appendix 2

Audit differences

Unadjusted audit differences

Under UK auditing standards (ISA (UK&I) 260) we are required to provide the Audit Committee with a summary of unadjusted audit differences (including disclosure misstatements) identified during the course of our audit, other than those which are ‘clearly trivial’, which are not reflected in the financial statements.

We are pleased to report that there are no unadjusted audit differences.

Adjusted audit differences

To assist the Audit Committee in fulfilling its governance responsibilities we present below a summary of non-trivial adjusted audit differences (including disclosures) identified during our audit.

We are pleased to report that there are no adjusted audit differences to the primary financial statements.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Audit differences

Presentational adjustments

We identified presentational adjustments required to ensure that London Councils' financial statements for the year ending 31 March 2018 are fully compliant with the Code of Practice on Local Authority Accounting in the United Kingdom 2017-18 ('the Code'). Whilst the majority of these adjustments were not significant, we identified adjustments of a more significant nature and details of these are provided in the following table.

Presentational adjustments	
#	Basis of audit difference
1	Salaries The Employers Pension Contribution in the Officers' Remuneration disclosure in the Joint Committee accounts (Note 24) for the Chief Executive had been incorrectly calculated by £354. This was adjusted The Chief Executive's remuneration was also included in the incorrect band for officers remuneration. This was adjusted.
2	Related parties transactions in Joint Committee accounts (Note 27) included income of £675k from Central Government. Upon review of the transaction listing used to prepare this figure, European Social Fund (ESF) grant funding was incorrectly classified as Central Government related party transactions. The Central Government related party disclosure was corrected to £280k.

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Audit independence

ASSESSMENT OF OUR OBJECTIVITY AND INDEPENDENCE AS AUDITOR OF LONDON COUNCILS

Professional ethical standards require us to provide to you at the conclusion of the audit a written disclosure of relationships (including the provision of non-audit services) that bear on KPMG LLP’s objectivity and independence, the threats to KPMG LLP’s independence that these create, any safeguards that have been put in place and why they address such threats, together with any other information necessary to enable KPMG LLP’s objectivity and independence to be assessed.

In considering issues of independence and objectivity we consider relevant professional, regulatory and legal requirements and guidance, including the provisions of the Code of Audit Practice, the requirements of the FRC Ethical Standard and the requirements of Auditor Guidance Note 1 - General Guidance Supporting Local Audit (AGN01) issued by the National Audit Office (‘NAO’) on behalf of the Comptroller and Auditor General.

This Statement is intended to comply with this requirement and facilitate a subsequent discussion with you on audit independence and addresses: general procedures to safeguard independence and objectivity; breaches of applicable ethical standards; independence and objectivity considerations relating to the provision of non-audit services; and independence and objectivity considerations relating to other matters.

General procedures to safeguard independence and objectivity

KPMG LLP is committed to being and being seen to be independent. As part of our ethics and independence policies, all KPMG LLP partners, Audit Directors and staff annually confirm their compliance with our ethics and independence policies and procedures. Our ethics and independence policies and procedures are fully consistent with the requirements of the FRC Ethical Standard. As a result we have underlying safeguards in place to maintain independence through: instilling professional values; communications; internal accountability; risk management; and independent reviews.

We are satisfied that our general procedures support our independence and objectivity.

Independence and objectivity considerations relating to other matters

There are no other matters that, in our professional judgment, bear on our independence which need to be disclosed to the Audit Committee.

Confirmation of audit independence

We confirm that as of the date of this report, in our professional judgment, KPMG LLP is independent within the meaning of regulatory and professional requirements and the objectivity of the Audit Director and audit staff is not impaired.

This report is intended solely for the information of the Audit Committee of London Councils and should not be used for any other purposes.

We would be very happy to discuss the matters identified above (or any other matters relating to our objectivity and independence) should you wish to do so.

KPMG LLP

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Appendix 4

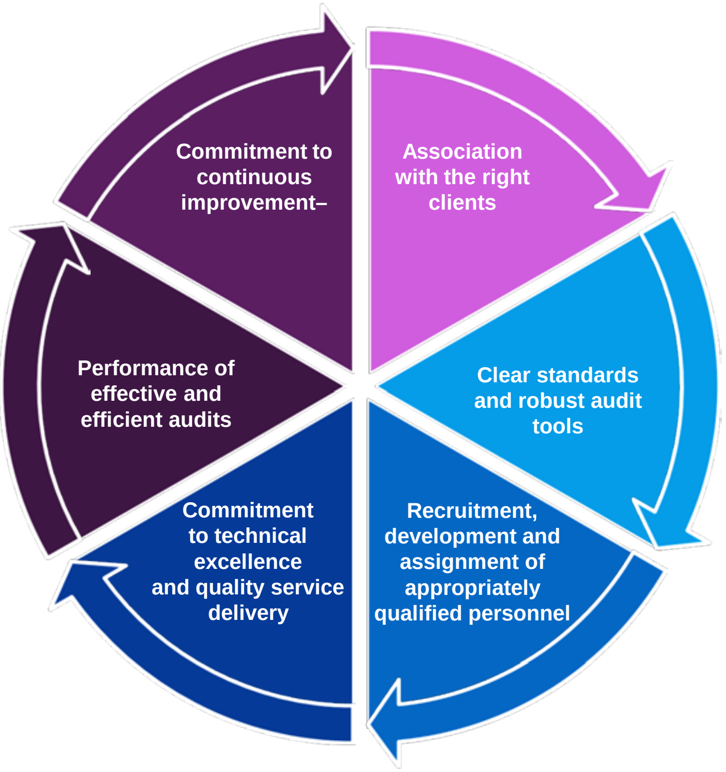
Audit quality framework

Audit quality is at the core of everything we do at KPMG and we believe that it is not just about reaching the right opinion, but how we reach that opinion. To ensure that every partner and employee concentrates on the fundamental skills and behaviours required to deliver an appropriate and independent opinion, we have developed our global Audit Quality Framework

- Comprehensive effective monitoring processes
- Proactive identification of emerging risks and opportunities to improve quality and provide insights
- Obtain feedback from key stakeholders
- Evaluate and appropriately respond to feedback and findings

- Professional judgement and scepticism
- Direction, supervision and review
- Ongoing mentoring and on the job coaching
- Critical assessment of audit evidence
- Appropriately supported and documented conclusions
- Relationships built on mutual respect
- Insightful, open and honest two way communications

- Technical training and support
- Accreditation and licensing
- Access to specialist networks
- Consultation processes
- Business understanding and industry knowledge
- Capacity to deliver valued insights


Commitment to continuous improvement–
Association with the right clients
Clear standards and robust audit tools
Recruitment, development and assignment of appropriately qualified personnel
Commitment to technical excellence and quality service delivery
Performance of effective and efficient audits

- Select clients within risk tolerance
- Manage audit responses to risk
- Robust client and engagement acceptance and continuance processes
- Client portfolio management

- KPMG Audit and Risk Management Manuals
- Audit technology tools, templates and guidance
- Independence policies

- Recruitment, promotion, retention
- Development of core competencies, skills and personal qualities
- Recognition and reward for quality work
- Capacity and resource management
- Assignment of team members and specialists

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
The KPMG name and logo are registered trademarks or trademarks of KPMG International.

APPENDIX B

KPMG LLP
15 Canada Square
London
E14 5GL

Contact:	David Sanni
Direct line:	020-7934 9704
Email:	david.sanni@londoncouncils.gov.uk
Our reference:	
Your reference:	
Date:	18 September 2018

DRAFT

Dear Sirs,

This representation letter is provided in connection with your audit of the financial statements of London Councils Joint Committee (“the Committee”), for the year ended 31 March 2018, for the purpose of expressing an opinion:

i. as to whether these financial statements give a true and fair view of the financial position of the Committee as at 31 March 2018 and of the Committee’s expenditure and income for the year then ended;

ii. whether the financial statements have been prepared properly in accordance with the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2017/18.

These financial statements comprise the Consolidated Expenditure and Funding Analysis, the Consolidated Comprehensive Income and Expenditure Statement, the Consolidated Movement in Reserves Statement, the Consolidated Balance Sheet, the Consolidated Cash Flow Statement and the related notes.

I confirm that the representations I make in this letter are in accordance with the definitions set out in the Appendix to this letter.

I confirm that, to the best of my knowledge and belief, having made such inquiries as considered necessary for the purpose of appropriately informing myself:

Financial statements

1. I have fulfilled my responsibilities, as set out in the Accounts and Audit Regulations 2015, for the preparation of financial statements that:

    i. give a true and fair view of the financial position of the Committee as at 31 March 2018 and of the Committee’s expenditure and income for the year then ended;

ii. have been properly prepared in accordance with the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2017/18.

2. The financial statements have been prepared on a going concern basis.

3. Measurement methods and significant assumptions used by the Committee in making accounting estimates, including those measured at fair value, are reasonable.

4. All events subsequent to the date of the financial statements and for which IAS 10 *Events after the reporting period* requires adjustment or disclosure have been adjusted or disclosed.

Information provided

5. I have provided you with:

   - access to all information of which I am aware, that is relevant to the preparation of the financial statements, such as records, documentation and other matters;
   - additional information that you have requested from the Committee for the purpose of the audit; and
   - unrestricted access to persons within the Committee from whom you determined it necessary to obtain audit evidence.

6. All transactions have been recorded in the accounting records and are reflected in the financial statements.

7. I confirm the following:

   I have disclosed to you the results of its assessment of the risk that the financial statements may be materially misstated as a result of fraud.

   Included in the Appendix to this letter are the definitions of fraud, including misstatements arising from fraudulent financial reporting and from misappropriation of assets.

8. I have disclosed to you all information in relation to:

   a) Fraud or suspected fraud that I am aware of and that affects the Committee and involves:

      - management;
      - employees who have significant roles in internal control; or
      - others where the fraud could have a material effect on the financial statements; and

   b) allegations of fraud, or suspected fraud, affecting the Committee’s financial statements communicated by employees, former employees, analysts, regulators or others.

   In respect of the above, I acknowledge my responsibility for such internal control as I determine necessary for the preparation of financial statements that are free from material misstatement, whether due to fraud or error. In particular, I acknowledge my

DRAFT

responsibility for the design, implementation and maintenance of internal control to prevent and detect fraud and error.

9. I have disclosed to you all known instances of non-compliance or suspected non-compliance with laws and regulations whose effects should be considered when preparing the financial statements.

10. I have disclosed to you and have appropriately accounted for and/or disclosed in the financial statements, in accordance with IAS 37 *Provisions, Contingent Liabilities and Contingent Assets*, all known actual or possible litigation and claims whose effects should be considered when preparing the financial statements.

11. I have disclosed to you the identity of the Committee's related parties and all the related party relationships and transactions of which I am aware. All related party relationships and transactions have been appropriately accounted for and disclosed in accordance with IAS 24 *Related Party Disclosures*.

12. Included in the Apendix to this letter are the definitions of both a related party and a related party transaction as I understand them as defined in IAS 24 and the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2017/18.

13. I confirm that:

    a) The financial statements disclose all of the key risk factors, assumptions made and uncertainties surrounding the Committee's ability to continue as a going concern as required to provide a true and fair view.
    b) Any uncertainties disclosed are not considered to be material and therefore do not cast significant doubt on the ability of the Committee to continue as a going concern.

14. On the basis of the process established by the Committee and having made appropriate inquiries, I am satisfied that the actuarial assumptions underlying the valuation of defined benefit obligations are consistent with its knowledge of the business and are in accordance with the requirements of IAS 19 (Revised) *Employee Benefits.*

    I further confirm that:

    a) all significant retirement benefits, including any arrangements that are:

        - statutory, contractual or implicit in the employer's actions;
        - arise in the UK and the Republic of Ireland or overseas;
        - funded or unfunded; and
        - approved or unapproved,

    have been identified and properly accounted for; and

    b) all plan amendments, curtailments and settlements have been identified and properly accounted for.

DRAFT

This letter was tabled and agreed at the meeting of the Audit Committee on 18 September 2018.

……………………………………………………………..
Frank Smith, CPFA
Director of Corporate Resources
For and on behalf of London Councils Joint Committee
18 September 2018

DRAFT

Appendix to the Representation Letter of London Councils Joint Committee: Definitions

Financial Statements

A complete set of financial statements comprises:

- A Comprehensive Income and Expenditure Statement for the period;
- A Balance Sheet as at the end of the period;
- A Movement in Reserves Statement for the period;
- A Cash Flow Statement for the period; and
- Notes, comprising a summary of significant accounting policies and other explanatory information and the Expenduture and Funding Analysis.

An entity may use titles for the statements other than those used in IAS 1. For example, an entity may use the title 'statement of comprehensive income' instead of 'statement of profit or loss and other comprehensive income'.

Material Matters

Certain representations in this letter are described as being limited to matters that are material.

IAS 1.7 and IAS 8.5 state that:

> “Material omissions or misstatements of items are material if they could, individually or collectively, influence the economic decisions that users make on the basis of the financial statements. Materiality depends on the size and nature of the omission or misstatement judged in the surrounding circumstances. The size or nature of the item, or a combination of both, could be the determining factor.”

Fraud

Fraudulent financial reporting involves intentional misstatements including omissions of amounts or disclosures in financial statements to deceive financial statement users.

Misappropriation of assets involves the theft of an entity’s assets. It is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorisation.

Error

An error is an unintentional misstatement in financial statements, including the omission of an amount or a disclosure.

Prior period errors are omissions from, and misstatements in, the entity’s financial statements for one or more prior periods arising from a failure to use, or misuse of, reliable information that:

DRAFT

a) was available when financial statements for those periods were authorised for issue; and
b) could reasonably be expected to have been obtained and taken into account in the preparation and presentation of those financial statements.

Such errors include the effects of mathematical mistakes, mistakes in applying accounting policies, oversights or misinterpretations of facts, and fraud.

Management

For the purposes of this letter, references to “management” should be read as “management and, where appropriate, those charged with governance”.

Related Party and Related Party Transaction

Related party:

A related party is a person or entity that is related to the entity that is preparing its financial statements (referred to in IAS 24 *Related Party Disclosures* as the “reporting entity”).

a) A person or a close member of that person’s family is related to a reporting entity if that person:
   i. has control or joint control over the reporting entity;
   ii. has significant influence over the reporting entity; or
   iii. is a member of the key management personnel of the reporting entity or of a parent of the reporting entity.
b) An entity is related to a reporting entity if any of the following conditions applies:
   i. The entity and the reporting entity are members of the same group (which means that each parent, subsidiary and fellow subsidiary is related to the others).
   ii. One entity is an associate or joint venture of the other entity (or an associate or joint venture of a member of a group of which the other entity is a member).
   iii. Both entities are joint ventures of the same third party.
   iv. One entity is a joint venture of a third entity and the other entity is an associate of the third entity.
   v. The entity is a post-employment benefit plan for the benefit of employees of either the reporting entity or an entity related to the reporting entity. If the reporting entity is itself such a plan, the sponsoring employers are also related to the reporting entity.
   vi. The entity is controlled, or jointly controlled by a person identified in (a).
   vii. A person identified in (a)(i) has significant influence over the entity or is a member of the key management personnel of the entity (or of a parent of the entity).
   viii. The entity or any member of a group of which it is a part, provides key management personnel services to the reporting entity or to the parent of the reporting entity.

DRAFT

A reporting entity is exempt from the disclosure requirements of IAS 24.18 in relation to related party transactions and outstanding balances, including commitments, with:

a) a government that has control, joint control or significant influence over the reporting entity; and
b) another entity that is a related party because the same government has control, joint control or significant influence over both the reporting entity and the other entity.

Related party transaction:

A transfer of resources, services or obligations between a reporting entity and a related party, regardless of whether a price is charged.

DRAFT

Audit Committee

Financial Accounts 2017/18 Item no: 05

Report by:	David Sanni	**Job title:**	Chief Accountant
Date:	18 September 2018		
Contact Officer:	David Sanni		
Telephone:	020 7934 9704	**Email:**	david.sanni@londoncouncils.gov.uk

Summary

This report presents the audited statement of accounts for 2017/18 for approval.

The accounts to be approved comprise of London Councils Consolidated Statement of Accounts for 2017/18, London Councils Transport and Environment Committee Statement of Accounts for 2017/18 and London Councils Grants Committee Statement of Accounts for 2017/18.

Recommendations

The Audit Committee is asked:

- To approve the statement of accounts, as detailed at Appendices A to C of this report.

Introduction

1. This report presents the annual audited statements of accounts for approval. The accounts to be approved comprise of London Councils Consolidated Statement of Accounts for 2017/18, London Councils Transport and Environment Committee Statement of Accounts for 2017/18 and London Councils Grants Committee Statement of Accounts for 2017/18. London Councils' financial regulations require the Director of Corporate Resources to present the audited statement of accounts to the Audit Committee for approval by 30 September each year.

2. KPMG has completed the audit of the provisional consolidated accounts for London Councils (incorporating the activities of London Councils Limited) and the separate statutory accounts for both the Grants Committee and the Transport and Environment Committee for 2017/18. The Audit Committee is therefore asked to approve these audited accounts.

Audited Financial Results 2017/18

3. The London Councils' Executive noted the pre-audited financial results for 2017/18 at their meeting on 19 June 2018. This report showed the provisional levels of income and expenditure for the year, and compared the results against the approved budget. The movement in the provisional surplus of £712,000 from £4.374 million, as reported to that meeting, and the audited surplus of £3.662 million for the year, is summarised in Table 1 below:

Table 1 – Movement in surplus position for 2017/18

	£000
Provisional surplus for the year	**(4,374)**
Transfer to 2020 Freedom Pass Re-issue Reserve	377
Provision for potential shortfall in borough funded ESF programmes	344
Understated LEPT income	9
Audited surplus for the year	**(3,662)**

4. The version of accounts presented to KPMG for their final audit were already adjusted to reflect the movements above which relate to:

- the TEC sub-committee's approval of the transfer of £377,000 to the 2020 Freedom Pass Re-issue Reserve at their meeting on 19 July 2018;

- a provision for the potential shortfall in funding in relation to the borough ESF funded programme services of £344,000. Measures were introduced in 2017/18 to mitigate the extent of potential losses on the ESF borough funded commissions. Any actual loss incurred will be offset by the £99,000 transferred from the Grants Committee reserves to the Joint Committee reserves approved by Leaders Committee on 6 December 2016; and

- an understatement of £9,000 worth of income in relation to the London European Partnership for Transport (LEPT).

5. The finalised revenue outturn for 2017/18, split across the three funding streams, is highlighted in Table 2 below:

Table 2 - Audited surplus 2017/18 split across funding streams

	Grants	**TEC**	**Core**	**Consolidated**
	£000	**£000**	**£000**	**£000**
Total Expenditure	7,636	44,977	9,336	61,949
Total Income	(7,983)	(45,676)	(8,370)	(62,029)
Interest income/expense	29	236	480	745
(Surplus)/Deficit for the year before transfer from reserves	**(318)**	**(463)**	**1,446**	**665**
Transfer from General Reserves	(231)	(855)	(1,542)	(2,628)
Transfer to Specific Reserve	-	377	-	377
Transfer from Unusable Reserves	(107)	(633)	(1,336)	(2,076)
Audited surplus for the year after transfers from reserves	**(656)**	**(1,574)**	**(1,432)**	**(3,662)**

6. In accordance with Local Authority Accounting (LAA), the use of reserves during the year is excluded from each of the Comprehensive Income and Expenditure Statements featured in the audited accounts so that the statements only reflect the income and expenditure due in the relevant financial year. LAA also requires that actuarial gains or losses on the pension scheme during the year are included in the statement to derive the Total Comprehensive Income and Expenditure. These gains or losses which have not been realised arise due to the actual experience or events differing from the assumptions adopted by the actuary at the previous valuation. The effect of these requirements on the audited accounts is summarised in Table 3 below:

Table 3 – Adjusted position 2017/18 as shown in the statutory accounts

	Grants	**TEC**	**Core**	**Consolidated**
	£000	**£000**	**£000**	**£000**
(Surplus)/Deficit for the year before transfer from reserves	**(318)**	**(463)**	**1,446**	**665**
Actuarial losses on pension assets/liabilities	(274)	(732)	(3,014)	(4,020)
Total Comprehensive Income and Expenditure	**(592)**	**(1,195)**	**(1,568)**	**(3,355)**

7. London Councils set a balanced budget for all three funding streams for 2017/18. An analysis of the main variances was included in the pre-audited report presented to the Executive in June. An update on the audited position will be presented at the next meeting of the Executive. An analysis of the main variances that contributed to the audited surplus of £3.355 million is included for information for the Committee in Table 4 below:

Table 4 – Analysis of revenue account surplus 2017/18

	£000
Grants Committee	
Underspend on 2016/17 main scheme liabilities	(119)
Underspend on ESF match funded programme	(501)
Transport & Environment Committee	
Underspend on Freedom Pass non-TfL bus services	(478)
Net surplus on Freedom Pass Survey & Reissue costs	(377)
Net surplus on Lorry Control Scheme administration & PCN income	(360)
Net surplus on parking appeals	(284)
Net underspend on London Tribunal administration	(172)
Core Joint Committee	
Underspend on employee costs	(572)
Underspend on Challenge Implementation Fund	(501)
Addition income from various sources	(325)
Underspend on research and commissioning	(267)
Net surplus on central recharges	(109)
Borough ESF funded programmes	344
Residual variances across all funding streams	59
Audited surplus for the year	**(3,662)**

8. Detailed explanation of these variances can be found in the Narrative Report on pages 21 to 26 of the Consolidated Statement of Accounts at Appendix A.

9. Another requirement of LAA is the separation of reserves between Usable Reserves and Unusable Reserves. Usable Reserves comprise of resources that can be used in the provision of services including reserves with spending restrictions. London Councils' Usable Reserves consist of the General Reserve and the 2020 Freedom Pass Re-issue Specific Reserve. The Unusable Reserves cannot be used in the provision of services and are set up to deal with instances where income and expenditure are recognised against General Fund balances on a statutory basis which is different from that expected by accounting standards adopted by LAA. London Councils' Unusable Reserves consist of the Pensions Reserve and the Accumulated Absence Reserve which serve to offset the impact of the IAS19 Pension Liability and Accumulated Absence Liability on the General Reserve.

10. The level of Usable Reserves for each funding stream as at 31 March 2018 has been confirmed as follows:

Table 5 – Audited position on Usable Reserves as at 31 March 2018

	Grants	TEC	Core	Consolidated
	£000	£000	£000	£000
Audited Usable Reserves at 1 April 2017	**2,018**	**5,075**	**5,417**	**12,510**
Transfer from General Reserve	(231)	(855)	(1,542)	(2,628)
Transfer to Specific Reserve	0	377	0	377
Surplus for the Year	656	1,574	1,432	3,662
Audited Usable Reserves at 31 March 2018	**2,443**	**6,171**	**5,307**	**13,921**

11. The Unusable Reserves at 31 March 2018 amounted to a negative balance of £28.154 million consisting of a Pension Reserve of £28.019 million and an Accumulated Absences Reserve of £135,000. As mentioned in paragraph 9 above, the reserves offset the impact of their associated liabilities on the General Reserve. The Pension Liability has decreased from £29.989 million as at 1 April 2017 to £28.019 million as at 31 March 2018, a decrease of £1.97 million. The reason for the decrease in the pensions liability is due to a marginal return across all asset classes, including equities, offset by an increase in the defined benefit obligation as a result of a reduction in the discount rate (which is based on corporate bond yields) used in the calculation of the obligation. This liability will continue to be recovered through future employers' pension contribution rates and anticipated improved returns on existing pension fund assets and will not, therefore, be a first call on existing London Councils General Reserves.

The Audited Accounts

12. The audited accounts can be found at Appendices A – C. The accounts consists of the following core statements:

- **Expenditure Funding Analysis**
  This statement shows the adjustments to the net expenditure chargeable to the Usable Reserves to arrive at the amounts included in the Comprehensive Income and Expenditure Statement. The adjustments arise due to differences in accounting treatments based on generally accepted accounting practices and the funding basis under regulations.

- **Comprehensive Income and Expenditure Statement**
  This statement shows the accounting cost in the year of providing services in accordance with generally accepted accounting practices.

- **Movement in Reserves Statement**
  This statement shows the movement in the year on the different reserves held by the Committee, analysed into usable reserves and unusable reserves.

- **Balance Sheet**
  The Balance Sheet shows the value as at the Balance Sheet date of the assets and liabilities recognised by the Committee. The net assets of the Committee (assets less liabilities) are matched by the reserves held by the Committee.

- **Cash Flow Statement**
  The Cash Flow Statement shows the changes in cash and cash equivalents of the Committee during the reporting period.

13. The statement of accounts include a number of notes that provide further detail to the cost, income and balances shown within the core statements.

14. Each statement also contains a Narrative Report which provides a review of the Committee's activities during the year, and a summary of the financial outturn. It also includes an Annual Governance Statement (AGS) which is a description of the key elements of the systems and processes that comprise the governance arrangements and the procedures applied to maintain and review their effectiveness. London Councils' AGS for 2017/18 was approved by the Audit Committee at their meeting on 21 June 2018.

Financial Implications

The financial implications are contained in the body of the report.

Legal Implications

London Councils' financial regulations require the Director of Corporate Resources to present the audited statement of accounts to the Audit Committee for approval by 30 September each year.

Equalities Implications

None

Appendices

Appendix A:	London Councils Joint Committee Consolidated Statement of Accounts for the year ended 31 March 2018
Appendix B:	London Councils Transport and Environment Committee Statement of Accounts for the year ended 31 March 2018
Appendix C:	London Councils Grants Committee Statement of Accounts for the year ended 31 March 2018

Background papers

2017/18 Final accounts working files

Audit Committee

London Councils' Corporate Risk Register

Item no: 06

Report by:	David Dent	**Job title:**	Principal Corporate Governance Officer
Date:	18 September 2018		
Contact Officer:	Christiane Jenkins		
Telephone:	020 7934 9540	**Email:**	Christiane.jenkins@londoncouncils.gov.uk

Summary

London Councils' Risk management Framework provides that the Corporate Risk register will be presented to the Audit Committee on an annual basis.

Recommendations

The Audit Committee is asked to:

- Note London Councils' Corporate Risk Register for 2018/19 which can be found attached at Appendix 2.

London Councils’ Corporate Risk Register

1. Background

1.1.1 It is widely accepted that it is good governance and practice to have and maintain an organisational risk register. London Councils has had a Risk Management Strategy and Framework in place for a number of years and this was last reviewed by London Councils’ Audit Committee in September 2017.

1.1.2 The approach is proportionate to the organisation and establishes a framework for identifying and periodically monitoring risk. The types and definitions of risks used in London Councils’ risk assessments are attached at Appendix 1.

1.2 As set out in the Risk Management Framework, the Corporate Risk register is reviewed annually by the Audit Committee.

1.3 The Directorate and Corporate Risk registers are reviewed quarterly by the Corporate Governance Officer Group and half-yearly by London Councils’ Corporate Management Board (CMB). This review process ensures that the risk registers continue to support London Councils’ corporate priorities.

2. Current Position on Risk Registers

2.1 There are three directorate registers:

- Chief Executive (includes the Corporate Resources and Corporate Governance Divisions)
- Services (which includes the Transport & Mobility Division and the Community Services and grants and YPES Division)
- Policy & Public Affairs

2.2 The Divisional and Directorate Risk registers and the Corporate Risk register were last considered and agreed by CMB on 29 August 2018. The 2018/19 Corporate Risk register is attached at Appendix 2.

2.3 In accordance with Audit Committee requirements, risk registers are reported to Committee in rotation. Future dates are as follows:

21 March 2019	PaPA Risk Register
June 2019 (date TBA)	CEX Risk Register
September 2019 (date TBA)	Corporate Risk Register
March 2020 (date TBA)	Services Risk Register
June 2020 (date TBA)	PaPA Risk Register

2.4 The Corporate Risk Register has also been referred to Internal Audit and our external Auditors for information.

3. Implications

Financial Implications for London Councils

There are no financial implications arising from this report.

Legal Implications for London Councils

There are no legal implications arising from this report.

Equalities Implications for London Councils

There are no specific equalities implications arising from this report, although when compiling the Divisional, Directorate and Corporate Risk Registers, equalities issues may be identified and will be recorded, reported and managed as necessary.

4. Recommendations

Audit Committee is asked to:

- Note London Councils' Risk Register for 2018/19 which can be found attached at Appendix 2.

Appendices:
Appendix 1 – Criteria for risks within London Councils
Appendix 2 – Corporate Risk Register for London Councils for 2018/19

Background Papers:

- London Councils Risk Management Strategy and Framework 2016;
- Directorate and Divisional Risk Registers 2018/19;
- Corporate Risk Register 2017/18.

Appendix 1 – Criteria for risks within London Councils
(extract from London Councils Risk Management Strategy & Framework, approved March 2012)

Types of risks

The main types of risk that London Councils is likely to encounter are:

Risk	Definition
Compliance	Risk of failing to comply with statutory requirements.
External	Risks from changing public or government attitudes.
Financial	Risks arising from insufficient funding, losing monetary resources, spending, fraud or impropriety, or incurring unacceptable liabilities
Operational	Risks associated with the delivery of services to the public and boroughs arising, for example, from recruitment difficulties, diversion of staff to other duties, or IT failures, loss or inaccuracy of data systems or reported information
Project	Risks of specific projects missing deadlines or failing to meet stakeholder expectations.
Reputation	Risks from damage to the organisation's credibility and reputation.
London	Risks to our stakeholders that need to be taken into account in our planning and service provision
Strategic	Risks arising from policy decisions or major decisions affecting organisational priorities; risks arising from senior-level decisions on priorities.
Contractual Risks	Risks related to the management of service contracts
Internal	Risks that relate to HR/People risks associated with employees, management and organisational development

Assessing and scoring risks

To assess risks adequately London Councils will identify the *consequences* of a risk occurring and give each risk a score or *risk rating*.

A means of comparing risks is needed so that efforts can be concentrated on addressing those that are most important. Each risk will be given a score, depending on its likelihood and its impact, as shown below. A risk may meet some, or all, of a description of likelihood or impact. These descriptions provide guidance rather than a prescriptive formula for determining risk ratings. Scoring a risk is a judgement call based on knowledge, understanding and informed guesswork.

Any risks which are both very likely to occur and will have a high impact are the ones that demand immediate attention.

Risk assessment			
Rating	**Likelihood**	**Impact**	**Rating**
Very High 4	**70% chance of occurrence** Almost certain (the risk is likely to occur within 6 months or at a frequent intervals). The event is expected to occur as there is a history of regular occurrence.	Huge financial loss; key deadlines missed or priorities unmet; very serious legal concerns (e.g. high risk of successful legal challenge, with substantial implications for London Councils); major impact on Boroughs or Londoners; loss of stakeholder public confidence.	*Very High 4*
High 3	**40% - 70% chance of occurrence** Probable, the risk is likely to occur more than once in the next 12 months. A reasonable possibility the event will occur as there is a history of frequent occurrence.	Major financial loss; need to renegotiate business plan priorities; changes to some organisational practices due to legislative amendments; potentially serious legal implications (e.g. risk of successful legal challenge); significant impact on the Boroughs or Londoners; longer-term damage to reputation.	*High 3*
Medium 2	**20% - 39% chance of occurrence** Possible, the risk may occur in the next 18 months. Not expected but there's a possibility it may occur as there is a history of casual occurrence.	Medium financial losses; reprioritising of services required; minor legal concerns raised; minor impact on the Boroughs or Londoners; short-term reputation damage.	*Medium 2*
Low 1	**<20% chance of occurrence** Rare, the risk may occur in exceptional circumstances.	Minimal financial losses; service delivery unaffected; no legal implications; unlikely to affect the Boroughs or Londoners; unlikely to damage reputation.	*Low 1*

Risk scores

Risk Assessment

Very High (4)	4	8	12	16
High (3)	3	6	9	12
Medium (2)	2	4	6	8
Low (1)	1	2	3	4
	Low (1)	**Medium (2)**	**High (3)**	**Very High (4)**

Impact

It is recognised that the scores at different levels of the register (project/team, directorate/ divisional, corporate) will reflect the importance of the risk in the context of the level of the register. For example, an individual officer's project register may reflect a high impact score on the project if an element is delivered late, but this will not necessarily correspond to a high impact on the organisation as a whole. This incremental approach to impact allows risks to be appropriately scored at each level to enable effective prioritisation of management and mitigation actions.

Mitigating risks

In addressing risks, a proportionate response will be adopted – reducing risks to 'As Low a Level as is Reasonably Practicable' in the particular circumstances
(known as the ALARP approach).

In identifying actions to address a risk, at least one of the 4 T's; treat, transfer, tolerate or terminate should apply.

Treat – treating the risk is the most common response, taking action to lessen the likelihood of the risk occurring. Treatment can also mean planning what you will do if the risk occurs, therefore minimising the impact. The purpose of 'treatment' is not necessarily to terminate the risk but, more likely, to establish a planned series of mitigating actions to contain the risk to an acceptable level.

Transfer – transferring the risk might include paying a third party to take it on or having an insurance policy in place. Contracting out a service might mitigate the risk but create new risks to be managed.

Tolerate – the ability to take effective action against some risks may be limited, or the cost of taking action may be disproportionate to the potential benefit gained. In this instance, the only management action required is to 'watch' the risk to ensure that its likelihood or impact does not change. This is an acceptable response as long as the risk has been properly identified and toleration is agreed to be the best option. If new management options arise, it may become appropriate to treat this risk in the future. London Councils may choose to tolerate a high residual risk if the activity involves presents a significant, yet risky, opportunity for the organisation. This should be explained in the description of the countermeasures.

Terminate – by doing things differently, you remove the risk.

London Councils Corporate Risk Register

Responsibility - CMB	Reviewed by; Corporate Governance Group	Date last reviewed **:July 2018**
	Reviewed by; CMB	Date last reviewed **: February 2018**

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
Corp 1	Loss of borough support	Financial, Reputational and Strategic	Inability to demonstrate value to London local government resulting in boroughs withdrawing support for London Councils.	4	4	16	London Councils has a range of controls in place and regularly reports to Leaders' Committee, the Executive, its sub Committees, TEC and Grants Committees and through the party group leaders to influence and shape the priorities of the organisation. A member communication programme is in place that offers online and tailored services to all members in the form of exclusive, policy-based member briefings, a free events programme and a bespoke members' website. In addition, London Councils officers engage and work with relevant officer groups across London, including but not limited to CELC, ADASS, ALDECS and SLT. Targeted briefing and engagement events are being arranged for the start of the new cycle. The London Challenge process has helped to inform the organisation's consideration of what it needs to be capable of delivering on behalf of	John O'Brien, Chief Executive	3	2	6

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
						🟥	London local government over the next five years.				🟥
Corp 2	Business Continuity/ Disaster Recovery Plans not in place or inadequate	Operational, Reputational, Financial	IT systems, utilities and/or buildings access cannot be restored following a system failure or disaster scenario resulting in an inability to continue day-to-day business.	4	2	8	London Councils' Business Continuity Plan (BCP) was updated and approved by CMB in April 2016. An internal audit review of the BCP has recently been completed and the recommendations were incorporated into the final version. The BCP includes adequate arrangements to ensure that all areas of service could continue in the event of a system failure or disaster. Nominated Gold, Silver and Bronze team members are the main points of contact for help or advice on contingency and emergency procedures and continuity arrangements. Each Directorate has considered its business continuity risks which are reflected in the business risk impact analysis and identified appropriate contingency plans. The BCP includes details of scenario testing, communication plans and examples of the types of scenarios to be considered in recovery/disaster recovery situations. An annual report from the BCP will be considered by CMB in February 2019 and Audit Committee in March 2019.	Frank Smith, Director of Corporate Resources	1	2	2

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
Corp 3	Inadequate corporate governance	Compliance, Financial, Reputational	London Councils policies including HR policies, not compliant - risk of prosecution and damage to London Councils reputation for failure to comply with current legislation, including compliance with information legislation, Freedom of Information Act 2000, GDPR and the Data Protection Act 2018; inability to meet statutory and best practice requirements; non compliance with external auditor recommendations, lack of a corporate governance framework, information management issues; lack of robust financial systems, including grant funded organisations.	2	3	6	The organisation has a number of controls in place to address its statutory responsibilities. The financial controls have been approved by the external auditors and there is robust budget monitoring and reporting of monthly salaries forecasts to Corporate Management Board and detailed quarterly budget monitoring reports to the Executive and funding stream committees (performance management framework in place to rectify poor performance of grant funded organisations, supplemented by robust monitoring). There is also a rolling internal audit programme. An annual governance statement is in place and is approved by the Audit Committee and outlines corporate governance arrangements, policies and procedures. In addition, an annual Corporate Governance report goes to CMB outlining the work completed and development areas for the following year. Guidance on data protection and for responding to requests for information is available for all staff on the intranet. Information Management policies are in place and a corporate led information governance programme has been put in place to support the organisation as it prepared for the introduction of the General Data Protection Regulations in May 2018. All staff are required to attend an appropriate information	Frank Smith, Programme Director, Corporate Resources Christiane Jenkins, Programme Director, Corporate Governance	2	2	4

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
							security/data protection training session. Further support on all information governance matters is available from Corporate Governance and, where necessary, legal advice can be obtained from the City of London.				
Corp 4	Non-delivery of pan London mobility services	Operational, Reputational	Failure to manage/retain the funding and delivery of the Freedom Pass, Taxicard and concessionary fares would impact directly on London's older and disabled residents and possibly borough budgets.	2	4	8	Contracts, negotiations, governance and management processes are in place monitoring cost and performance. Members receive regular committee reports. Back office data management systems underpin both schemes.	Spencer Palmer, Director Transport and Mobility	1	2	2
Corp 5	Non delivery of London Tribunals (formerly the Parking and Traffic Appeals service known as PATAS)	Strategic, Operational, Reputational, Financial	One of London Councils' Transport and Environment Committee's (TEC) statutory responsibilities is to provide the Environment and Traffic Adjudicators (ETA) Tribunal via London Tribunals (which also comprises the Road User Charging Adjudicators (RUCA) who deal with appeals against penalty charge notices for the London congestion charge and the Low Emission Zone (LEZ) schemes). A	3	4	12	Closely specified and managed contract for administrative support; with strong KPIs and management arrangements internally.	Spencer Palmer, Director Transport and Mobility	2	2	4

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
			failure to run the support services to the independent adjudicators effectively impacts the adjudicators and users of the Tribunals (i.e. appellants and enforcement authorities, as parties to appeals). Service failures therefore have reputational consequences for TEC, London councils and the adjudicators and financial consequences on the boroughs and TfL directly, as they fund the Tribunal services. There may also be direct impacts on enforcement authority processes, which could lead to further reputational and financial losses for them as well as inconvenience to the public.			🟥					🟨

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
Corp 6	Ineffective relationships with key stakeholders, key decision makers and the media	External Project Reputation Strategic	Failure to develop effective relationships is likely to reduce our ability to influence key audiences and the quality of policy and service developments which could lessen the impact of the work, in particular, inability to stabilise productive relationships with the Mayor and Mayoral Advisers and current Government.	2	2	4	Key partners identified during business planning process; continuing dialogue during commissioning of services, monitoring of delivery, sharing of knowledge and intelligence.	CMB*	1	1	1
Corp 7	Inability to be flexible with resources to ensure appropriate responses to changing circumstances	Strategic, Operational, Reputational, Financial	Insufficient response to economic, social, legal, political changes in society rendering existing work less relevant and/or missing opportunities to have a greater impact.	4	2	8	Regular engagement with Members to ensure that any changes to organisational priorities are supported; effective work programmes and robust corporate business planning to enable flexibility to respond to changing circumstances. Flexible deployment of resources. Regular engagement with member Portfolio holders.	CMB*	2	2	4
Corp 8	Failure to deliver a robust Grants Scheme that delivers members requirements	Strategic, Operational, Reputational, Financial	Loss of confidence in the grants programme by London boroughs, the voluntary sector and other private and voluntary sector funders and the	3	3	9	Close liaison with Members, lawyers, services, other funding bodies and the voluntary sector.	CMB*	2	2	4

No	Risk	Risk Type	Risk description	Risk Rating without control (1-4)			Controls in place	Responsible Officer	Risk rating with control (1-4)		
				L	I	O			L	I	O
			recipients of the programmes/interventions; ineffective consultation and delivery of equalities and boroughs' objectives.								
Corp 9	Failure to deliver ongoing efficiency savings	Reputational, Financial and Operational	Efforts to secure ongoing efficiency savings.	4	3	12	Managing proposals to ensure proper consideration is given to options for savings and enough information is given to Members to enable informed decisions on the impact of any proposed savings.	CMB*	3	2	6
Corp 10	Failure to lead and manage change effectively flowing from London Council's Challenge	Strategic and Operational	Failure to lead and coordinate change activity with staff in the Organisation in a way which is effective.	4	4	16	Robust planning for and implementation of organisational change arising from specific London Councils' Challenge projects is supported by good levels of staff engagement and clear communication.	CMB*	3	2	6

*CMB members are John O'Brien (Chief Executive), Dick Sorabji (Corporate Director, Policy & Public Affairs), Christiane Jenkins (Director – Corporate Governance) Yolande Burgess (Strategy Director), Spencer Palmer (Director, Transport and Mobility), Jim Odling-Smee (Director of Communications) and Frank Smith (Director of Corporate Resources)

LONDON COUNCILS

Audit Committee

Internal Audit Reviews

Item no: 07

Report by:	Pat Stothard	**Job title:**	Head of Audit & Risk Management (City of London Corporation)
Date:	18 September 2018		
Contact Officers:	Martha Franco Murillo, Senior Auditor (City of London Corporation) Email: Martha.Franco-Murillo@cityoflondon.gov.uk Jeremy Mullins, Audit Manager (City of London Corporation) Email: jeremy.mullins@cityoflondon.gov.uk Pat Stothard, Head of Audit & Risk Management (City of London Corporation) Email: pat.stothard@cityoflondon.gov.uk		

Summary

The purpose of this report is to provide the Committee with an update of internal audit work that has been undertaken since the last committee meeting in June 2018.

Recommendations

The Audit Committee is asked to note and comment on the contents of the report and appendices.

Background

1. London Councils internal audit service is provided by the City of London's Internal Audit section under the terms of the service level agreement for financial support services. The Audit Committee approves an internal audit plan for each financial year and the purpose of this report is to provide an update on the progress of the 2017/18 and 2018/19 audit plans.

Internal Audit Plan 2017/18

2. Work on the 2017-18 Internal Audit Plan has progressed as follows: there were four full assurance audits one has been fully completed: Financial Controls for Petty Cash, Inventories and Procurement Cards, two completed to final report stage, ICT Remote Access and Mobile Devices and Grant Monitoring and Payments; and the fieldwork has been completed for one remaining audit, Parking and Traffic, the draft report is currently under review. A follow up on previous recommendations was also completed and the outcomes reported to the Committee in June 2018.

3. The Internal Audit Plan Progress Report for 2017/18 is attached at Appendix A.

Internal Audit Reviews

Remote Access and Mobile Devices

4. The objective of the audit was to provide assurance on the adequacy of the arrangements for managing mobile devices and access to the London Councils network through remote working.

Policies and Procedures

5. Internal Audit confirmed that policies and supporting procedures on the use of mobile devices and remote access to the London Councils network are available to staff via the London Councils intranet. Audit examination of these documents identified a number of areas for improvement and amber priority recommendations have been raised in respect of the following:

   - Insufficiently detailed guidance on mobile device usage;
   - Policy documentation has not been reviewed periodically to ensure content remains current and relevant, and to align with good practice;
   - Guidance does not specifically mention how devices should be managed during transit or the use of mobile devices in public places;
   - The 'Device Receive Form', signed by the recipient at the point of handover, does not refer to policies that apply with respect to the device, or general guidance on device safe-keeping and secure use in public, and
   - Policy and procedural information on remote access and mobile devices is not mandatory reading for new starters.

Mobile Device Framework

6. This audit established that London Councils have a framework in operation for mobile devices and their connectivity to applications/systems. The framework arrangements are

contained within the Information Security policy, which identifies the specific types of mobile devices permitted to connect to the London Councils network. The following areas for improvement were identified:

- Asset/inventory information is maintained in separate documents, which means that to ascertain assets held, a number of registers/documents need to be accessed; and
- Audit sample testing identified that some asset information was missing from the asset register.

Monitoring

7. Audit testing established that regular monitoring is not undertaken with respect to remote access and mobile device usage. Internal Audit was advised that should monitoring information be required, it would be provided upon request by Agilisys. London Councils has purchased a tool called RADAR365 which is used to provide some local monitoring information on Office365 elements such as Active User mailboxes, licences and mailbox sizes. The London Councils ICT Manager stated that that the current arrangements are adequate, since only approved devices can connect to the London Councils in the first instance. While a range of controls are already in place about security and access restriction, recommendations have been raised to strengthen control in respect of the following issues:

   - There is no requirement for staff to change password immediately a device is lost/stolen;
   - Data held on laptops cannot be remotely wiped off;
   - Laptops storage is not encrypted, and
   - There is no documented procedure for actions to be taken in order to update the asset register for lost/stolen devices.

8. The full report on the review of Remote Access and Mobile Devices is attached at Appendix B.

Grant Monitoring and Payments

9. The purpose of this audit was to examine the monitoring arrangements to ensure that beneficiary organisations fully deliver grant funded projects and to review the grant funding payments arrangements to ensure validity and timeliness.

Monitoring Delivery of Grant Funded Projects

10. Internal Audit testing confirmed that, overall, there are appropriate arrangements in place for monitoring grant delivery in relation to the main grants programme. The audit also confirmed that grant agreements include terms to safeguard grant funding, and that there are appropriate arrangements for reporting on grant delivery to Senior Management and Members.

11. This audit confirmed that, overall, there are appropriate arrangements in place for monitoring grant delivery in relation to the ESF grant programme. There are appropriate arrangements for reporting on grant delivery to Senior Management and Members.

12. Three recommendations were made to enhance internal control as follows. London Councils should:

    - request regular management accounts as part of the financial due diligence process for recipients of the main grants programme;
    - undertake annual financial due diligence checks for ESF grant recipients at the earliest opportunity; and
    - ensure consistency and timeliness when capturing and following up on actions required by ESF Grant providers.

Grant Funding Payments

13. There are established arrangements in place to ensure that only valid payments are made to grant recipients across both grant programmes. The audit identified scope to improve internal control through instigating arrangements for approving payment schedules uploaded to the GIFTS system, in respect of the main grants programme.

14. The full report on the review of Grant Monitoring and Payments is attached at Appendix C.

Internal Audit Plan 2018/19

15. Work on the 2018-19 Internal Audit Plan is progressing. There are three full assurance reviews: fieldwork for the PAN London Mobility Schemes audit has been completed; the audit of Business Continuity Arrangements has been postponed to quarter 4 at London Councils' and the City of London IT Director's request, due to the on-going transformation project. The ICT Information Governance, including GDPR audit has also been postponed to quarter 4 at London Councils request. The follow up exercise for 2018-19 will be completed in quarter 3 as agreed at March Committee.

16. The Internal Audit Plan Progress Report for 2018/19 is attached at Appendix D.

Conclusion

17. Work on the 2017-18 Internal Audit Plan is completed to draft report stage with one report under review and the annual internal audit recommendation follow up exercise has also been completed. Work is progressing on the 2018-19 audit plan.

Financial Implications for London Councils

None

Legal Implications for London Councils

None

Equalities Implications for London Councils

None

Appendices

Appendix A:	Internal Audit Plan Progress Report for 2017/18
Appendix B:	Internal audit report on Remote Access and Mobile Devices
Appendix C	Internal audit report on Grant Monitoring and Payments
Appendix D:	Internal Audit Plan Progress Report for 2018/19

Background Papers

Audit Committee report on Internal Audit Planned Work 2017/18 dated 23 March 2017
Audit Committee report on Internal Audit Planned Work 2018/19 dated 22 March 2018
Internal audit work files for 2017/18 & 2018/19

Appendix A

London Councils Internal Audit Plan Progress Report 2017/18

AUDIT REVIEW	DAYS	PROGRESS	ASSURANCE RATING	OBJECTIVES	RECOMMENDATIONS			
					RED	AMBER	GREEN	TOTAL
Financial Controls for Petty Cash, Inventories and Procurement Cards	5	Completed	Moderate Amber	This will be a probity audit exercise of compliance with controls and veracity of transactions.	0	1	1	2

Key Conclusions

Petty Cash and Imprest Account Management:

1. Audit testing established that the petty cash and imprest account administration and management is adequately controlled, with a clear chronological transaction audit trail in place, and supplemented by the mandatory documents such as claim forms and receipts. Audit noted that a regular reconciliation exercise is undertaken by the Head of Financial Accounting of petty cash transactions against the remaining cash float, with a final sign-off as confirmation that there are no discrepancies. Audit also established that suitable arrangements are in place to keep the petty cash float secure at all times. A minor recommendation has been made to improve the clarity of the details held in the petty cash claim form (recommendation 1).

2. Established processes were noted to be in place to ensure that appropriate authorisation is obtained for each claim. The processes were determined to be effective by Audit after examination of a sample of five petty cash claims which were randomly selected and all found to be properly authorised.

Inventory Management:

3. On the basis of Audit sample testing it was determined that an adequate inventory management process is in operation. Examination of the inventory data identified it to be current and the inventory details were found to be in line with the current (June 2015) London Council Financial Regulations (section 14.9). The inventory records also include an essential information item, inventory replacement costs, which enables the Finance team to determine the total asset value for (re)insurance purposes.
4. Audit established that two previous audit findings (from a January 2015 audit spot check) with respect to lack of a review of furniture and equipment, and inventory controls not in accordance with London Councils regulations have both been addressed. The spot check findings are detailed in the findings section below.

Procurement Cards:

5. There is only one procurement card in operation at London Councils. From Audit examination of a sample of seven randomly selected card transactions, the arrangements for processing, authorisation and reconciliation of procurement purchases were considered to be well documented and managed. An amber recommendation was made to include procurement card guidelines in the Financial Regulations (recommendation 2) at the next review of the regulations.

6. Documented procedures for procurement card transactions are clearly published on the London Councils intranet, and it is understood from the Head of Financial Accounting that London Councils has adopted some of the guidance from the City of London policy with respect to procurement cards. The CityCard system from Lloyds TSB is utilised for online reporting and transaction management for procurement card transactions.

Management Comments

Recommendation 1: Include printed name(s) and signature(s) as a mandatory requirement for completion of a petty cash claim.

A revised form that includes the full name and signature of the claimant and approving officer has been prepared and issued staff.

Responsibility: Principal Finance Officer
Target Implementation Date: Completed

Recommendation 2: Include procurement card restrictions/guidelines into the London Councils Financial Regulations at the next review of the Regulations.

A section which incorporates the current guidelines on the use of the procurement card will be drafted for inclusion in London Councils' Financial Regulations. The proposed amendment to the regulations will be put forward to the Leaders Committee for approval at its next Annual General Meeting in June 2018.

Responsibility: Head of Financial Accounting
Target Implementation Date: June 2018

AUDIT REVIEW	DAYS	PROGRESS	ASSURANCE RATING	OBJECTIVES	RECOMMENDATIONS			
Grants (2017-18)	20	Final		The purpose of this audit is to follow-up on improvements recommended at the last review and undertake site visits to grant recipients shadowing the work of the grant team on regular monitoring visits.	RED 0	AMBER 3	GREEN 1	TOTAL 4

Key Conclusions

Monitoring Delivery of Grant Funded Projects

1. On the basis of discussion with the Principal Programme Manager (Main Grants Programme), together with a review of standard grant agreements, examination of arrangements for monitoring quarterly grant submissions and conducting monitoring visits, the audit confirmed that, overall, there are appropriate arrangements in place for monitoring grant delivery in relation to the main grants programme. The audit also confirmed that grant agreements include terms to safeguard grant funding, and that there are appropriate arrangements for reporting on grant delivery to Senior Management and Members.

2. On the basis of discussion with the Strategy Director, together with a review of standard grant agreements, and examination of arrangements for managing grant recipient performance, the audit confirmed that, overall, there are appropriate arrangements in place for monitoring grant delivery in relation to the ESF grant programme. There are appropriate arrangements for reporting on grant delivery to Senior Management and Members.

3. Three recommendations were made to enhance internal control as follows. London Councils should:

    - request regular management accounts as part of the financial due diligence process for recipients of the main grants programme (recommendation 1 - amber).

    - undertake annual financial due diligence checks for ESF grant recipients at the earliest opportunity (recommendation 2 - amber).

    - ensure consistency and timeliness when capturing and following up on actions required by ESF Grant providers (recommendation 3 - green).

Grant Funding Payments

4. There are established arrangements in place to ensure that only valid payments are made to grant recipients across both grant programmes. The audit identified scope to improve internal control through instigating arrangements for approving payment schedules uploaded to the GIFTS system, in respect of the main grants programme (recommendation 4 - amber).

5. On the basis of sample testing, the audit confirmed that valid grant payments are being made on a timely basis.

Management Comments

Recommendation 1: The Strategy Director Young People's Education and Skills, Grants and Community Services, should request that grant recipients provide management accounts on a regular basis to improve the arrangements for conducting financial due diligence. As a minimum, it is expected that grant recipients will provide quarterly budget monitoring reports.

Recommendation accepted. The annual and regular due diligence process has been centralised. Quarterly performance reports/workbooks will be reviewed to include a finance section. Management accounts will be requested in line with the risk-based approach to monitoring i.e. high-risk projects regular requests for accounts, low risk projects, scrutiny of financial reporting to determine if management accounts should be requested.

Responsibility: Yolande Burgess, Strategy Director
Target implementation Date: 28 September 2018

Recommendation 2: The Strategy Director Young People's Education and Skills, Grants and Community Services should ensure that annual financial due diligence checks are reinstated and completed at the earliest opportunity for ESF grant recipients.

Recommendation accepted. Annual Accounts are requested and scrutinised (see also management action for recommendation 1).

Responsibility: Yolande Burgess, Strategy Director
Target implementation Date: 28 September 2018

Recommendation 3: The Strategy Director Young People's Education and Skills, Grants and Community Services should instigate formal arrangements to ensure consistency and

	timeliness with capturing and following up on actions required by ESF Grant providers Recommendation accepted. Monitoring visit template re-introduced; staff will be reminded about service expectations following monitoring visits i.e. notes and actions with review/by dates following monitoring visits to grant recipients with two working days; action follow-up to be diarised; line managers to review follow-up activity in 1-2-1 sessions. **Responsibility: Yolande Burgess, Strategy Director** **Target implementation Date: 28 September 2018** **Recommendation 4: The Strategy Director Young People's Education and Skills, Grants and Community Services should instigate arrangements for reviewing and authorising the accuracy of grant payment schedules uploaded to the GIFTS system.** Recommendation accepted. A first (Finance Officer) and second (Strategy Director) tier check will be implemented. **Responsibility: Yolande Burgess, Strategy Director** **Target implementation Date: 28 September 2018**

AUDIT REVIEW	DAYS	PROGRESS	ASSURANCE RATING	OBJECTIVES	RECOMMENDATIONS			
Parking and Traffic	15	Draft report under review		The purpose of this audit is to obtain assurance that there are adequate contract management arrangements in place across the London Tribunals, TRACE and Lorry Control Services. This audit will also examine the adequacy of arrangements in place for making payments to London Tribunals adjudicators and for administering the London Lorry Control Scheme.	RED	AMBER	GREEN	TOTAL
Key Conclusions								

AUDIT REVIEW	DAYS	PROGRESS	ASSURANCE RATING	OBJECTIVES	RECOMMENDATIONS			
ICT Remote Access and Mobile Devices	10	Final	Amber	An evaluation of the adequacy of security controls for staff working from home, and the use of mobile devices such as USB sticks and dongles.	RED 0	AMBER 10	GREEN 0	TOTAL 11

Key Conclusions

Policies and Procedures

1. Internal Audit confirmed that policies and supporting procedures on the use of mobile devices and remote access to the London Councils network are available to staff via the London Councils intranet. Audit examination of these documents identified a number of areas for improvement and amber priority recommendations have been raised in respect of the following:

   - Insufficiently detailed guidance on mobile device usage (Recommendation 1).
   - Policy documentation has not been reviewed periodically to ensure content remains current and relevant, and to align with good practice (Recommendation 2).
   - Guidance does not specifically mention how devices should be managed during transit or the use of mobile devices in public places (Recommendation 3).
   - The 'Device Receive Form', signed by the recipient at the point of handover, does not refer to policies that apply with respect to the device, or general guidance on device safe-keeping and secure use in public (Recommendation 4).
   - On the basis of audit testing performed, policy and procedural information on remote access and mobile devices is not mandatory reading for new starters (Recommendation 5).

Mobile Device Framework:

2. This audit established that London Councils has a framework in operation for mobile devices and their connectivity to applications/systems. The framework arrangements are contained within the Information Security policy, which identifies the specific types of mobile devices permitted to connect to the London Councils network. The following areas for improvement were identified by audit testing and an amber priority recommendation has been raised (Recommendation 6):

   - Asset/inventory information is maintained in separate documents, which means that to obtain a comprehensive assessment of assets, a number of registers/documents need to be accessed.
   - Audit sample testing identified that some asset information was missing from the asset register.

Monitoring:

3. Audit testing established that regular monitoring is not undertaken with respect to remote access and mobile device usage. Internal Audit was advised that should monitoring information be required, it would be provided upon request by Agilisys. London Councils has purchased a tool called RADAR365 which is used to provide some local monitoring information on Office365 elements such as Active User mailboxes, licences and mailbox sizes. The London Councils ICT Manager stated that that the current arrangements are adequate, since only approved devices can connect to the London Councils in the first instance. While a range of controls are already in place with regard to security and access restriction, recommendations have been raised to strengthen control in respect of the following:

Management Comments

Recommendation 1: London Councils should update the 'Internet/Email/Telephone Use Policy' to clearly specify the requirements for mobile device usage and ensure that this is communicated to all relevant staff.

Recommendation accepted. Revised Email and Internet use policy will have the requirements for mobile device usage added and communicated to staff. This is to be delivered as part of the corporate transformation programme that includes the new Microsoft InTune mobile phone policy and migration

Responsibility: Roy Stanley
Target Implementation Date: November 2018

Recommendation 2: London Councils should implement periodic review of documentation, supported by version control and document history information to provide clarity of the content. Consideration should be given to inclusion of the following within policy and procedure documents:

- **review frequency and approval required from (title)**
- **last reviewed date**
- **brief description of modification (e.g. inclusion of GDPR)**
- **reviewed by**
- **approved by**
- **next review dates**
- **key modifications and change history.**

Recommendation accepted. Revised Email and Internet use policy will include review, revision and change control table. This will be delivered as part of the corporate transformation programme that includes the new Windows 10 Direct Access desktop and Microsoft InTune mobile phone policy

Responsibility: Roy Stanley
Target Implementation Date: November 2018

• There is no requirement for staff to change password immediately when a device is lost/stolen (Recommendation 7 – amber priority). • At present laptops cannot be remotely wiped of any data held on them (Recommendation 8 – amber priority). • Laptops storage is not encrypted (Recommendation 9 – amber priority). • There is no documented procedure for what action needs to be taken to update the asset register for lost/stolen devices (Recommendation 10).	**Recommendation 3: London Councils should enhance existing guidance to staff to include good practice related to the use of devices in transit and the use of mobile devices in public places, for example ensuring that screens cannot be overlooked.** Recommendation accepted. Revised Email and Internet use policy will have the requirements for mobile device usage added and communicated to staff. This will be delivered as part of the corporate transformation programme that includes the new Microsoft InTune mobile phone policy and migration **Responsibility: Roy Stanley** **Target Implementation Date: November 2018** **Recommendation 4: London Councils should consider modifying the Device Receive Form to include: 1) related policies to be aware of such as internet/email/telephone policy, and 2) general usage guidelines such as not be overlooked, keep device on your person in public, keep it locked when not in use.** Recommendation accepted. Revised Email and Internet use policy will have the requirements for mobile device usage added and communicated to staff. This is be delivered as part of the corporate transformation programme that includes the new Microsoft InTune policy and migration **Responsibility: Roy Stanley** **Target Implementation Date: November 2018** **Recommendation 5: To ensure there is a consistent, standard message provided to all the directorates with respect to important policies and procedures, consideration should be given to identifying common important policies, and including these as part of the new starter checklist information for every directorate. New starters should sign and date forms to confirm that the necessary reading has been undertaken.** Recommendation noted. The London Councils Personal Assistants (PA's) across all the four directorates who form the London Councils Support Services Group to be made aware of disseminating all corporate policy documents as part of the new starter formal induction process **Responsibility: Support Services Group** **Target Implementation Date: September 2018**

Recommendation 6: London Councils should:

- **Update the asset register with laptop assets information to provide a single, comprehensive record of assets.**
- **Perform periodic checks to ensure all asset details are present in the asset register**

Recommendation accepted. All mobile phone asset data now incorporated within the core asset register in Excel
Responsibility: Roy Stanley
Target Implementation Date: August 2018

Recommendation 7: London Councils should enforce a requirement for staff to change their password when a device is reported as lost/stolen as a security precaution, in line with good practice.

Recommendation accepted. CoL Service desk advised to inform users to change their passwords as soon as device is officially reported stolen and the Information Security Policy updated to reflect the change of password
necessary as soon as users are aware of any loss
Responsibility: Roy Stanley
Target Implementation Date: August 2018

Recommendation 8: London Councils should explore the potential for introducing tools to enable the remote wiping of data stored on mobile devices.

Recommendation accepted. This is be delivered as part of the corporate transformation programme that includes the new Windows 10 Direct Access desktop, BitLocker encryption for all laptop devices and Microsoft InTune for mobile phones
Responsibility: Roy Stanley
Target Implementation Date: November 2018

Recommendation 9: London Councils should ensure that laptops are encrypted in line with standard industry practice.

Recommendation accepted. This is be delivered as part of the corporate transformation programme that includes the new Windows 10 Direct Access desktop, BitLocker encryption for all laptop devices and Microsoft InTune for mobile phones
Responsibility: Roy Stanley

	Target Implementation Date: November 2018 **Recommendation 10: London Councils should formalise and document the process for recording item movements such as leavers and lost/stolen devices. Information to consider adding to the asset register is - a lost/stolen device tab on the asset register with details of who owned the device, when lost etc.** Recommendation noted. Asset register to be updated with recommended fields **Responsibility: Roy Stanley** **Target Implementation Date: August 2018**

AUDIT REVIEW	DAYS	PROGRESS	ASSURANCE RATING	OBJECTIVES	RECOMMENDATIONS			
Follow Ups	5	Completed		Follow up on the implementation of recommendations made in previous reviews.	RED	AMBER	GREEN	TOTAL
Key Conclusions								
Total	**55**							

* Subject to agreement of scope with service managers when preparing the terms of reference.

Appendix B

CITY OF LONDON

CHAMBERLAIN'S DEPARTMENT

INTERNAL AUDIT SECTION

LONDON COUNCILS
REMOTE ACCESS AND MOBILE DEVICES
FINAL REPORT

Date Issued: August 2018

Issued to:	Director of Corporate Resources	-	Frank Smith
	Head of Financial Accounting	-	David Sanni
	Information & Communications Technology and Facilities Manager	-	Roy Stanley

CONTENTS (INDEX)

Audit Fieldwork Completed	April 2018
Draft Report Issued	June 2018
Management Response Received Agreeing Recommendations	August 2018
Final Report Issued	August 2018

SECTION A : EXECUTIVE SUMMARY

Introduction

1. This audit was undertaken as part of the Internal Audit Plan 2017-18.

2. London Councils is supported in provision of its IT function, including Mobile Devices and Remote access, by the City of London (CoL) and Agilisys as part of the 2013 CoL/Agilisys partnership agreement.

3. In 2014 the mobile devices and remote access functions were reviewed as part of a wider internal audit on ICT strategy and security. Since then London Councils has implemented new technology and this audit is to re-examine the adequacy of the arrangements with respect to mobile devices and remote access.

4. During the 2014 Audit it was established that only a limited number of staff had remote access whereas now all London Councils staff (anyone with valid network logon credentials) can connect remotely to the London Councils network, thereby increasing the potential risk because of the potentially increased utilisation.

5. The objective of the audit was to provide assurance on the adequacy of the arrangements for managing mobile devices and access to the London Councils network through remote working. Audit testing was carried out to determine the adequacy of arrangements in operation for the following:

   - Policy and procedures are published and made available to staff on the safe use of mobile devices and remote access facility, and staff awareness is maintained to ensure on-going effectiveness of the procedural guidance.

   - A mobile device framework is in operation that includes mobile device information such as devices permitted for general use, the security requirements such as enforced pin or password entry, security maintenance such as patching requirements, and mobile inventory management practices.

   - Monitoring is in operation to ensure mobile device and remote access processes are being adhered to, and issues are addressed.

6. Mobile devices in the form USB devices have been excluded from this audit as a previous audit, completed in 2017, and titled ‘Information Security’ included a review of the usage of USB devices at London Councils.

7. Internal Audit sought to obtain assurance as to the adequacy of the internal control environment. The audit opinion, below, is based upon discussion with key staff, examination of systems and the findings of sample testing, as such, our work does not provide absolute assurance that material error, loss or fraud does not exist.

Assurance Statement

Assurance Level	**Description**
Moderate Assurance ‘Amber’	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.

Recommendations	Red	Amber	Green	Total
Number Made:	0	10	0	10
Number Accepted:	0	10	0	10

Key Conclusions

Policies and Procedures

8. **Internal Audit confirmed that policies and supporting procedures on the use of mobile devices and remote access to the London Councils network are available to staff via the London Councils intranet. Audit examination of these documents identified a number of areas for improvement and amber priority recommendations have been raised in respect of the following:**

- **Insufficiently detailed guidance on mobile device usage (Recommendation 1).**
- **Policy documentation has not been reviewed periodically to ensure content remains current and relevant, and to align with good practice (Recommendation 2).**
- **Guidance does not specifically mention how devices should be managed during transit or the use of mobile devices in public places (Recommendation 3).**
- **The ‘Device Receive Form’, signed by the recipient at the point of handover, does not refer to policies that apply with respect to the device, or general**

guidance on device safe-keeping and secure use in public (Recommendation 4).
- **On the basis of audit testing performed, policy and procedural information on remote access and mobile devices is not mandatory reading for new starters (Recommendation 5).**

Mobile Device Framework:

9. **This audit established that London Councils have a framework in operation for mobile devices and their connectivity to applications/systems. The framework arrangements are contained within the Information Security policy, which identifies the specific types of mobile devices permitted to connect to the London Councils network. The following areas for improvement were identified by audit testing and an amber priority recommendation has been raised (Recommendation 6):**

   - **Asset/inventory information is maintained in separate documents, which means that to obtain a comprehensive assessment of assets, a number of registers/documents need to be accessed.**
   - **Audit sample testing identified that some asset information was missing from the asset register.**

Monitoring:

10. **Audit testing established that regular monitoring is not undertaken with respect to remote access and mobile device usage. Internal Audit was advised that should monitoring information be required, it would be provided upon request by Agilisys. London Councils has purchased a tool called RADAR365 which is used to provide some local monitoring information on Office365 elements such as Active User mailboxes, licences and mailbox sizes. The London Councils ICT Manager stated that that the current arrangements are adequate, since only approved devices can connect to the London Councils in the first instance. While a range of controls are already in place with regard to security and access restriction, recommendations have been raised to strengthen control in respect of the following:**

    - **There is no requirement for staff to change password immediately when a device is lost/stolen (Recommendation 7 – amber priority).**
    - **At present laptops cannot be remotely wiped of any data held on them (Recommendation 8 – amber priority).**
    - **Laptops storage is not encrypted (Recommendation 9 – amber priority).**

- **There is no documented procedure for what action needs to be taken to update the asset register for lost/stolen devices (Recommendation 10).**

SECTION B : AUDIT FINDINGS AND RECOMMENDATIONS

Policy and Procedures:

11. Audit testing confirmed that policies and procedures are published and made available to staff on the safe use of mobile devices and remote access facility. Additionally, Internal Audit was advised that arrangements are in operation to maintain staff awareness through an online learning programme. Recommendations have been made, as set out below, to further strengthen control and to ensure the ongoing effectiveness of relevant guidance.

12. London Councils documentation within the scope of the audit includes a policy on working from home, and this is further supplemented with an Information Security policy which details the systems security elements of remote access. There is a mobile device policy statement included within the "Internet/Email/Telephone Use Policy" which is less detailed than the working from home policy and an amber priority recommendation has been made to strengthen control in this area, particularly as mobile device usage is on the increase (Recommendation 1).

Priority	Issue	Risk
Amber	On the basis of documentation supplied to Internal Audit, limited information is contained within the mobile device usage policy.	Staff are unclear on the policy and their responsibilities to adhere to the policy and inappropriate practices are put into operation, increasing vulnerability of device or data loss.
Recommendation 1: London Councils should update the 'Internet/Email/Telephone Use Policy' to clearly specify the requirements for mobile device usage and ensure that this is communicated to all relevant staff.		

Management Response and Action Plan

Recommendation accepted. Revised Email and Internet use policy will have the requirements for mobile device usage added and communicated to staff. This is to be delivered as part of the corporate transformation programme that includes the new Microsoft InTune mobile phone policy and migration

Responsibility: Roy Stanley

Target Implementation Date: November 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

13. Audit examination of the policy and procedural documentation supplied by London Councils determined that there is no periodic review and this was confirmed by the ICT and Facilities Manager (ICT Manager). An example of this was 'Internet/Email an/Telephone Use Policy' document which was agreed and published in 2014, with no subsequent review. Internal Audit was advised by the ICT Manager that the content remains current and correct, an amber priority recommendation has been made to formalise documentation review and rollout of version control in the interest of good practice (Recommendation 2).

Priority	Issue	Risk
Amber	Evidence was not supplied to Internal Audit to demonstrate that policy documentation has been reviewed periodically to ensure content remains current and relevant, and to align with good practice.	The content referred to by staff may not be current or no longer relevant, resulting in inappropriate or out of date practices.

Recommendation 2:

London Councils should implement periodic review of documentation, supported by version control and document history information to provide clarity of the content. Consideration should be given to inclusion of the following within policy and procedure documents:

- review frequency and approval required from (title)
- last reviewed date
- brief description of modification (e.g. inclusion of GDPR)
- reviewed by

- approved by
- next review dates
- key modifications and change history.

Management Response and Action Plan

Recommendation accepted. Revised Email and Internet use policy will include review, revision and change control table. This is be delivered as part of the corporate transformation programme that includes the new Windows 10 Direct Access desktop and Microsoft InTune mobile phone policy

Responsibility: Roy Stanley

Target Implementation Date: November 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

14. Audit testing determined that policies and procedures could be strengthened by including a new guidance section on the use of mobile devices outside of the office, similar to the section already present that advises staff on 'Use of personal mobile phones in the office'. Documentation supplied to Internal Audit did not mention how to securely use your phone in public, and how to reduce the likelihood of losing a device; an amber priority recommendation has been made (Recommendation 3).

Priority	Issue	Risk
Amber	There is no guidance on how devices should be managed during transit and or the use of mobile devices in public places.	Improper practices are employed by staff whilst using mobile devices in public increasing the risk of data loss/breach.

Recommendation 3:

London Councils should enhance existing guidance to staff to include good practice related to the use of devices in transit and the use of mobile devices in public places, for example ensuring that screens cannot be overlooked.

Management Response and Action Plan

Recommendation accepted. Revised Email and Internet use policy will have the requirements for mobile device usage added and communicated to staff. This is be delivered as part of the corporate transformation programme that includes the new Microsoft InTune mobile phone policy and migration

Responsibility: Roy Stanley

Target Implementation Date: November 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

15. Audit established that when a device is provided to a user, this must be signed for via a 'Device Receive Form'. This process represents an opportunity to reiterate user responsibilities and good practice requirements. An amber priority recommendation has been made to include references to relevant policies on the form itself (Recommendation 4).

Priority	Issue	Risk
Amber	The 'Device Receive Form', signed by the device recipient, does not contain a brief section on important policies that apply with respect to the device or general guidance on how to use mobile devices securely in public, and how to keep device safe.	Staff are unclear on the policy and their responsibilities to adhere to the policy and inappropriate practices are put into operation, increasing vulnerability of device or data loss.

Recommendation 4:

London Councils should consider modifying the Device Receive Form to include: 1) related policies to be aware of such as internet/email/telephone policy, and 2) general usage guidelines such as not be overlooked, keep device on your person in public, keep it locked when not in use.

Management Response and Action Plan

Recommendation accepted. Revised Email and Internet use policy will have the requirements for mobile device usage added and communicated to staff. This is be delivered as part of the corporate transformation programme that includes the new Microsoft InTune policy and migration

Responsibility: Roy Stanley

Target Implementation Date: November 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

16. Audit testing identified that policies and procedures are communicated to staff via intranet content and a previous audit completed in 2017 'Information Security Audit established that all London Councils staff had been in trained in January 2017. Internal Audit was advised that on-going training measures include a "bite sized" learning program which requires staff to complete mandatory online training in small segments to maintain staff awareness.

17. Scope was identified to enhance information provided to new staff as part of an induction process. Internal Audit was advised that the induction process includes a checklist for new starters which includes a checklist of important policies. It was noted, however, that the new starter process varies across London Councils in order to satisfy the differing requirements of the directorates.

18. Internal Audit sought assurance that important policies, (common to all directorates) were in all the induction checklists, although only the new starter process for the Policy and Public Affairs (PAPA) directorate was made available. Audit examination of the PAPA new starter documentation established that 'Working from home' Policy was not present and an amber priority recommendation has been made to ensure that a consistent message is provided to all new starters in terms of key policies and procedures which apply across London Councils (Recommendation 5).

Priority	Issue	Risk
Amber	The list of required reading in the New Starter Activity Schedule for the PAPA directorate did not include all key policies with respect to remote access and mobile device usage.	New staff are unaware of important polices. Inadequate policy/procedural guidance can result in improper or insecure practices being employed such as devices used in public places where the content such as email can be overseen.
Recommendation 5: To ensure there is a consistent, standard message provided to all the directorates with respect to important policies and procedures, consideration should be given to identifying common important policies, and including these as part of the new		

starter checklist information for every directorate. New starters should sign and date forms to confirm that the necessary reading has been undertaken.

Management Response and Action Plan

Recommendation noted. The London Councils Personal Assistants (PA's) across all the four directorates who form the London Councils Support Services Group to be made aware of disseminating all corporate policy documents as part of the new starter formal induction process

Responsibility: Support Services Group

Target Implementation Date: September 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

Mobile Device Framework:

19. Audit testing established that elements of a mobile device framework are in operation at London Councils, the details of which are documented in the Information Security Policy document and supporting procedures. The framework information clearly states that London Councils owned devices and personally owned devices are permitted to connect to the London Councils network via WIFI. For the purposes of this audit mobile devices will be categorised into two areas as follows:

- Mobiles – includes mobile phones, tablets and iPads
- Laptops –incudes personal computers (PCs), laptops and Apple Mac devices.

20. It was noted that each device within a category has the same system access/restrictions irrespective of the individual make and model of the device. The mobiles category is enabled to access only the Office365 systems (email etc), whilst laptops category is enabled to access the full range of London Councils network systems using Remote Desktop Services (RDS) technology. Internal Audit was informed that since laptops are permitted to access a greater range of London Councils systems, secure measures have been implemented such as use of specific operating system versions; only Windows operating system versions 7, 8 and 10, (the last 3 versions released) and Apple Mac OSX are permitted.

21. A requirement of a mobile device framework is the implementation of data controls and data protection to ensure that either data is not able to able copied onto the local device, or that it is fully protected if local storage is permitted. Audit noted that the RDS technology includes this intrinsic security feature and is clearly stated in

the RDS documentation; RDS technology '*allows a personal computer to access windows applications, email and shared folders with a similar look and feel to the office windows 7 desktop. It is a secure desktop therefore will NOT allow you to access files or data on your home PC or vice versa.*'

22. The RDS mechanism is used to access London Councils network and, it is understood through discussion with the ICT Manager, to create a virtual environment to protect London Councils systems. To access this London Councils environment through RDS, Audit confirmed that two factor Authentication is in operation for connectivity. Two factor authentication requires the user to enter information they know (in this case it's a pin that the user has created) and something that they have, in this case it's a number generated via an RSA secure token device. Both together are entered along with user network credentials (username and password) to gain entry to the virtual environment. This practice is in line with standard industry practice for secure operation.

23. Audit testing established that for mobiles, the framework enforces a mandatory pin entry to the device, and without this Office 365 is not accessible. The user is prompted to create a pin (a minimum of 4 characters to a maximum of 8) as part of the configuration and installation process, thereby adding a measure of protection should it be lost or stolen.

24. Audit examination of the assets register identified that this contains a mobile device inventory with 32 London Councils owned mobile phones in circulation. From discussion with the ICT Manager it is understood that a record of the laptops is maintained outside of the asset register. Audit sample tested the details held against three randomly selected mobile items and identified that the details recorded were correct with one exception where the asset number was missing. The following recommendation has been added. An amber priority recommendation has been made to consolidate this information into a single comprehensive asset register and to ensure that all necessary details are captured (Recommendation 6).

Priority	Issue	Risk
Amber	Asset/inventory information is maintained in separate documents, thus to get a comprehensive assessment of assets, multiple registers/documents need to be	Assets cannot easily be accounted for / assets managed where information is incomplete or not readily available.

🟨	accessed. In addition, audit sample testing identified some asset information missing from the asset register.	

<u>Recommendation 6:</u>

London Councils should:

- Update the asset register with laptop assets information to provide a single, comprehensive record of assets.
- Perform periodic checks to ensure all asset details are present in the asset register

Management Response and Action Plan

Recommendation accepted. All mobile phone asset data now incorporated within the core asset register in Excel

Responsibility: Roy Stanley

Target Implementation Date: August 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

25. Internal Audit was informed by the ICT Manager that software patching (implementation of security fixes for example) is not enforceable for personally owned devices and that patching is considered less critical for such devices since access is restricted to preferred operating systems and a virtual environment is created upon establishing a connection; there is therefore no cross-contamination between local device storage and the London Councils systems. Audit was also informed that patching for London Councils owned laptops is undertaken immediately after London Councils servers are patched, and laptops are required to be handed in so that the IT team can install the new patches.

<u>Monitoring:</u>

26. This audit established that monitoring arrangements are limited, and reliance is placed on Agilisys to provide monitoring information upon request. The ICT Manager advised that regular monitoring of remotely connected devices is not performed and that there is no requirement to monitor which devices are connected to the London Councils network as only ICT team approved devices

can connect. Internal Audit noted that a system called RADAR 365 can be used to identify the last time a particular device was used to connect to Office 365 should concerns be raised after a device is lost/stolen.

27. Should mobiles/laptops be lost/stolen the reliance is placed on the existing security features to secure data. The ICT and Facilities Manager has stated that following controls are operated at present:

- user credentials authentication
- user pin authentication for mobile unlocking
- automatic mobile locking after 15 minutes of inactivity
- password change every 30 days
- mobile category devices (not laptop category) wiping if 10 unsuccessful login attempts are made.

28. Whilst these actions are in line with standard accepted practice and help prevent unauthorised access, an amber recommendation has been made to further strengthen control in this areas by enforcing a prompt password change when a device is informed as lost/stolen (Recommendation 7).

Priority	Issue	Risk
Amber	Change of password is not immediately required when a device is lost/stolen.	Unauthorised access by external parties due to inadequate security measures, increasing vulnerability of data loss.
Recommendation 7: London Councils should enforce a requirement for staff to change their password when a device is reported as lost/stolen as a security precaution, in line with good practice.		
Management Response and Action Plan Recommendation accepted. CoL Service desk advised to inform users to change their passwords as soon as device is officially reported stolen and the Information Security Policy updated to reflect the change of password necessary as soon as users are aware of any loss		

Responsibility: Roy Stanley

Target Implementation Date: August 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

29. IT industry standard practice is to remotely wipe the data on the device should a device be lost/stolen, and the general best practice is to encrypt local laptop storage. Audit established that remote wiping capability is not currently present for laptop devices, however, it is understood that London Councils is looking into a mobile device management tool called inTUNE which will enable this functionality. In addition, disk encryption is not in place for laptop devices. Two amber priority recommendations have been made to address these issues (Recommendations 8 and 9).

Priority	Issue	Risk
Amber	At present laptops cannot be remotely wiped of any data held on them.	Data will remain on lost or stolen devices and could get accessed by unauthorised parties, increasing vulnerability of data loss.

Recommendation 8:

London Councils should explore the potential for introducing tools to enable the remote wiping of data stored on mobile devices.

Management Response and Action Plan

Recommendation accepted. This is be delivered as part of the corporate transformation programme that includes the new Windows 10 Direct Access desktop, BitLocker encryption for all laptop devices and Microsoft InTune for mobile phones

Responsibility: Roy Stanley

Target Implementation Date: November 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

Priority	Issue	Risk
Amber	Laptops storage is not encrypted.	The laptop data can be read if it is written to local laptop storage, increasing vulnerability of data loss.

Recommendation 9:

London Councils should ensure that laptops are encrypted in line with standard industry practice.

Management Response and Action Plan

Recommendation accepted. This is be delivered as part of the corporate transformation programme that includes the new Windows 10 Direct Access desktop, BitLocker encryption for all laptop devices and Microsoft InTune for mobile phones

Responsibility: Roy Stanley

Target Implementation Date: November 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

30. Audit established that Agilisys is tasked with disabling network accounts for leavers and subsequently deleting the account associated data, with a documented leaver process provided by Agilisys. The process commences with a Service Request placed by London Councils with the Agilisys Service Desk, this is actioned by Agilisys and on removal of the user account London Councils is sent a resolution email. Audit sample testing of five leavers established that the network accounts for these leavers had been deleted and the service resolution email sent to London Councils afterwards.

31. From discussion with the ICT Manager, Internal Audit ascertained that mobile assets allocated to a leaver are recorded in the asset register. No documented process was identified, however, to provide guidance to staff and ensure continuity of process. An amber recommendation has been made to strengthen control in this area, to include lost / stolen device recording, in recognition of the increasing use of laptops (Recommendation 10).

Priority	Issue	Risk
Amber	There is no documented procedure for what action needs to be taken to update the asset register for lost/stolen devices and given that laptops will be used more widely in future it is vital that the asset register captures this information for overall visibility of devices at London Councils.	The asset register is incomplete and becomes inaccurate after a time, which impedes control over the location of assets.

Recommendation 10:

London Councils should formalise and document the process for recording item movements such as leavers and lost/stolen devices. Information to consider adding to the asset register is - a lost/stolen device tab on the asset register with details of who owned the device, when lost etc.

Management Response and Action Plan

Recommendation noted. Asset register to be updated with recommended fields

Responsibility: Roy Stanley

Target Implementation Date: August 2018

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided

APPENDIX 1: AUDIT DEFINITIONS AND RESPONSIBILITIES

Assurance levels

Category	Definition
Nil Assurance 'Dark Red'	There are fundamental weaknesses in the control environment which jeopardise the achievement of system objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.
Limited Assurance 'Red'	There are a number of significant control weaknesses and/or a lack of compliance which could put the achievement of system objectives at risk and result in error, fraud, loss or reputational damage.
Moderate Assurance 'Amber'	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.
Substantial Assurance 'Green'	There is a sound control environment with risks to system objectives being reasonably managed. Any deficiencies identified are not cause for major concern.

Recommendation Categorisations

Priority	Definition	Timescale for taking action
Red - 1	A serious issue for the attention of senior management and reporting to the appropriate Committee Chairman. Action should be initiated immediately to manage risk to an acceptable level	Less than 1 month or more urgently as appropriate
Amber - 2	A key issue where management action is required to manage exposure to significant risks, action should be initiated quickly to mitigate the risk.	Less than 3 months

Green - 3	An issue where action is desirable and should help to strengthen the overall control environment and mitigate risk.	**Less than 6 months**

Note:- These 'overall assurance level' and 'recommendation risk ratings' will be based upon auditor judgement at the conclusion of auditor fieldwork. They can be adjusted downwards where clear additional audit evidence is provided by management of controls operating up until the point of issuing the draft report.

What Happens Now?

The final report is distributed to the relevant Head of Department, relevant Heads of Service, and those involved with discharging the recommended action.

The audit report is provided to the Director of Corporate Resources, Head of Financial Accounting and the Audit Committee. Internal audit will carry out a follow-up exercise of the high priority (red and amber) recommendations approximately six months after the issue of the final audit report. The ongoing progress in implementing each recommendation is reported by Internal Audit to each meeting of the Audit Committee. The final report will be presented at the next meeting of the Audit Committee and the relevant Director or Head of Service will be required to attend the meeting to respond to queries raised by Committee members.

Any Questions?

If you have any questions about the audit report or any aspect of the audit process please contact the auditor responsible (Nirupa Gardner, ext 1298) for the review or Pat Stothard, Head of Audit & Risk Management via email to Pat.Stothard@cityoflondon.gov.uk.

Appendix C

CITY OF LONDON

CHAMBERLAIN'S DEPARTMENT

INTERNAL AUDIT SECTION

LONDON COUNCILS

GRANT MONITORING AND PAYMENTS AUDIT

FINAL REPORT

Date Issued: September 2018

Issued to: Frank Smith, Director of Corporate Resources
Yolande Burgess, Strategy Director: Young People's Education and Skills, Grants and Community Services
Katy Makepeace-Gray, Principal Programme Manager
Sam Armitt, ESF Technical Adviser
David Sanni, Head of Financial Accounting

CONTENTS (INDEX)

SECTION **PAGE**

SECTION A: EXECUTIVE SUMMARY

Introduction

1. This audit was undertaken as part of the agreed 2017-18 internal audit plan.

2. A year-long review and commissioning process resulted in a new, four-year main grants programme of support for Londoners. The 2017-21 main grants programme comprises annual payments of £6.2m split between 13 different projects dedicated to tackling some of the most serious issues affecting the Capital.

3. Applicants to the programme were required to be non-profit organisations that are able to work across more than one borough and able to demonstrate that they provide services in at least one of the key priorities identified by London Councils:

   - Homelessness – offering people various support to prevent them from becoming homeless, as well as, targeted intervention for those who have become homeless, including rough sleepers.

   - Sexual and domestic violence – helping people at risk of harm as well as those who have been subjected to violence.

4. In addition, London Councils also delivers a grants programme to Tackle Poverty Through Employment; the total funding available is £6m. The programme is 50% funded by borough contributions (£3m) and matched by way of a European Social Fund (ESF) grant (£3m). The grants programme covers the period October 2016 to December 2018.

5. It is understood that grant recipients make use of partners to enable delivery of grant programmes. Under these arrangements London Councils funds a lead partner which manages the partnership, handles reporting, and is responsible for distributing funds among the delivery partners.

6. The purpose of the audit was to obtain assurance that there are adequate arrangements in place to ensure that;

   - monitoring arrangements are in place to ensure that organisations fully deliver grant funded projects. In particular, this audit assessed the adequacy of the framework in place for monitoring grants and confirmed the extent to which it is operating in practice. This included reviewing arrangements through which grant recipients report on programme outcomes, together with arrangements for undertaking grant monitoring visits.

   - only valid grant payments are made.

- grant payments are made on a timely basis.

7. The Members of London Councils Grants Committee are responsible for oversight of grant programme delivery.

8. London Councils use the GIFTS system for administering its grants programmes. Grant payments are paid through London Councils' Oracle system.

9. Internal Audit sought to obtain assurance as to the adequacy of the internal control environment. The audit opinion, below, is based upon discussion with key staff, examination of systems and the findings of sample testing, as such, our work does not provide absolute assurance that material error, loss or fraud does not exist.

Assurance Statement

Assurance Level	**Description**
Moderate Assurance 'Amber'	**An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.**

Recommendations	**Red**	**Amber**	**Green**	**Total**
Number Made:	0	3	1	4
Number Accepted:	0	3	1	4

Key Conclusions

Monitoring Delivery of Grant Funded Projects

10. **On the basis of discussion with the Principal Programme Manager (Main Grants Programme), together with a review of standard grant agreements, examination of arrangements for monitoring quarterly grant submissions and conducting monitoring visits, the audit confirmed that, overall, there are appropriate arrangements in place for monitoring grant delivery in relation to the main grants programme. The audit also confirmed that grant agreements include terms to safeguard grant funding, and that there are appropriate arrangements for reporting on grant delivery to Senior Management and Members.**

11. **On the basis of discussion with the Strategy Director, together with a review of standard grant agreements, and examination of arrangements for managing grant recipient performance, the audit confirmed that, overall, there are appropriate arrangements in place for monitoring grant delivery in relation to the ESF grant programme. There are appropriate arrangements for reporting on grant delivery to Senior Management and Members.**

12. **Three recommendations were made to enhance internal control as follows. London Councils should:**

    - **request regular management accounts as part of the financial due diligence process for recipients of the main grants programme (recommendation 1 - amber).**

    - **undertake annual financial due diligence checks for ESF grant recipients at the earliest opportunity (recommendation 2 - amber).**

    - **ensure consistency and timeliness when capturing and following up on actions required by ESF Grant providers (recommendation 3 - green).**

Grant Funding Payments

13. **There are established arrangements in place to ensure that only valid payments are made to grant recipients across both grant programmes. The audit identified scope to improve internal control through instigating arrangements for approving payment schedules uploaded to the GIFTS system, in respect of the main grants programme (recommendation 4 - amber).**

14. **On the basis of sample testing, the audit confirmed that valid grant payments are being made on a timely basis.**

SECTION B: KEY FINDINGS AND RECOMMENDATIONS

Key Findings

Monitoring Delivery of Grant Funded Projects

Main Grants Programme

Grant Agreements

15. On the basis of discussion with the Principal Programme Manager (Main Grants Programme) and examination of standard grant agreements, the audit confirmed that grant agreements set out the following key information. The purpose of grant agreements is to set out the key obligations of London Councils and grant recipients in addition to setting out how grant funding must be spent.

- London Councils standard expectations and requirements;
- The terms and conditions of grant funding;
- Grant outcome and output targets (including targets for each borough (borough spread));
- London Councils grant monitoring arrangements;
- Other key grant information including but not limited to profiled output targets, grant recipients bank account information and the agreed project budget, together with quarterly and annual grant progress report templates, which are provided to grant recipients, as examples.

Submission of Grant Monitoring Reports

16. Through discussion with the Principal Programme Manager and review of quarterly grant monitoring requirements, the audit confirmed that grant providers are required to provide adequate information to enable London Councils to monitor grant delivery effectively. Grant recipients are required to provide the following on a quarterly basis:

- A progress report: The quarterly progress reports require grant recipients to provide details on project progress. This includes, setting out reasons for variances in outcomes achieved against targets, project successes and challenges, arrangements for engaging with boroughs and planned future activities;

- A workbook setting out performance against each outcome target including performance against 'borough spread' targets (this means ensuring that each borough receives services and obtains measurable benefits from the project). The workbook also contains sections for recording equalities monitoring information, borough engagement activity and providing a project budget statement. In addition, grant recipients are also required to 'self-assess' their performance in delivering grant funded projects.

17. Grant recipients also have the option of providing a case study with their quarterly returns, setting out the benefits provided by grant funding.

18. An annual progress report is also required to be submitted, this incorporates a quarterly progress report for the last quarter of the year. The annual progress report requires grant recipients to provide further key details on project management including setting out how projects are publicised, arrangements for project evaluation, how outcomes are evidenced and system in place to capture beneficiary feedback.

19. Through review of quarterly returns (quarter 1 and 2 of 2017/18) for four grant recipients, the audit confirmed that quarterly grant monitoring reports are being provided in accordance with the above arrangements. As 2017/18 is the first year of a four-year grant programme, the first annual reports had not yet been submitted at the time audit fieldwork was completed (due April 2018).

Review of Grant Monitoring Reports

20. London Councils Grant Officers are required to assess performance of grant recipients on a quarterly basis upon receipt of the grant monitoring information stated above. As part of their assessments, Grant Officers are required to assign each grant recipient a 'Red/Amber/Green' (RAG) rating. The RAG rating assessment forms part of the workbooks and is based upon;

    - performance against outcome targets;
    - moderation of provider self-assessments;
    - beneficiary satisfaction survey results;
    - assessment of contract compliance.

21. A standard pro-forma form is in place to ensure consistency of assessments.

22. Though review of grant monitoring evidence for four grant recipients, the audit obtained assurance that grant monitoring is being carried out in accordance with the above arrangements.

Financial Due Diligence

23. Through discussion with the Principal Programme Manager and review of grant agreements, the audit confirmed that London Councils plan to undertake financial due diligence checks on an annual basis throughout the term of the grant; the series of checks to be carried out are documented within grant agreements.

24. The purpose of the financial due diligence checks includes;

    - identifying grant underspends;
    - determining any significant financial issues which may impact grant recipients' ability to continue in operation;
    - determining whether appropriate insurance cover is in place.

25. Through review of grant agreements, the audit confirmed that grant recipients are required to provide an annual return, two weeks after the close of each financial year. They are required to submit the following:

    - annual audited accounts (this need to be submitted nine months after the close of the financial year);
    - annual General Meeting (AGM) minutes;
    - an annual budget update (actuals) including details of any unspent grant;
    - the following financial year's budget;
    - copies of grant recipient's employers and public liability insurance certificates;
    - a copy of the grant recipient's work plan for the following financial year.

26. The audited accounts contain a section 37 statement which sets out how the grant has been spent; this is used to identify grant underspends. It is understood that Grant recipients are required to provide a draft version of the section 37 statement within three months of the financial year.

27. Whilst grant recipients are required to provide an adequate range of information to enable financial due diligence checks to be carried out, the audit identified scope to improve internal control. London Councils should also request that grant recipients provide copies of their management accounts on a regular basis. Management accounts provide London Councils with more recent and, therefore, more relevant information for undertaking financial due diligence checks. Historical annual accounts may not reflect the current financial performance and position of grant providers; this increases the risk that providers in poor financial health go undetected (recommendation 1).

Priority	Issue	Risk
Amber	Whilst the grants financial due diligence checks require grant providers to provide copies of their annual accounts, the accounts reflect historical information in relation to financial performance and position.	Historical information may not reflect the current financial performance and position of grant providers; this increases the risk that providers in poor financial health go undetected.
Recommendation 1: The Strategy Director Young People's Education and Skills, Grants and Community Services, should request that grant recipients provide management accounts on a regular basis to improve the arrangements for conducting financial due diligence. As a minimum, it is expected that grant recipients will provide quarterly budget monitoring reports.		
Management Response and Action Plan Recommendation accepted. The annual and regular due diligence process has been centralised. Quarterly performance reports/workbooks will be reviewed to include a finance section. Management accounts will be requested in line with the risk-based approach to monitoring i.e. high-risk projects regular requests for accounts, low risk projects, scrutiny of financial reporting to determine if management accounts should be requested. **Responsibility:** Yolande Burgess, Strategy Director **Target implementation Date:** 28 September 2018		

28. At the time of the audit, annual financial due diligence had yet to be carried out for the first year of the grant programmes. Grant recipients are required to provide the above information within two weeks of the end of each year i.e. the first round of information was due in April 2018.

Monitoring Visits

29. Grant agreements state that each grant recipient will be subject to one to two monitoring visits each year. Visits will be carried out by Grants Officers, occasionally in conjunction with the Principal Programme Manager, a Borough Officer or a Member of the Grants Committee.

30. There are two types of visits that Grants Officers will undertake:

- Information Monitoring Visits – the purpose of these visits includes, but is not limited to, inspecting records that support quarterly workbook submissions and review issues relating to quarterly and annual reports;

- Delivery visits - the purpose of these visits to review delivery of grants 'in action' and to discuss project delivery issues with grant recipient staff and grant beneficiaries.

31. The audit confirmed that the above arrangements are operating in practice; notes from two delivery visits held in September and October 2017 were obtained. The audit also confirmed that there was an on-going schedule of visits.

Implementing Agreed Actions

32. The audit confirmed that appropriate arrangements are in place to ensure that agreed actions are implemented by grant recipients. Through inspection, the audit confirmed that follow up actions agreed are recorded within the quarterly progress reports. These are followed up as part of the progress report review process.

Safeguarding Grant Funding

33. Through review of the standard grant agreement, the audit confirm that London Councils have incorporated specific terms and conditions to protect funding in the event that grant recipients fail to deliver against agreed grant targets.

34. The Standard Conditions of Grant state that grant recipients have to repay London Councils forthwith on demand:

- if a funded organisation is dissolved, wound-up, disbanded, declared insolvent or bankrupt or otherwise ceases to operate;
- if a funded organisation ceases to be a voluntary organisation or ceases to operate for the purposes in respect of which the grant was paid;
- if a funded organisation fails to comply with any grant conditions or any other obligations under the grant agreement.

35. The Grant Agreement (paragraphs 14.28 and 30) also set out that funding may be withdrawn or ceased as a result of poor performance.

36. It is understood that withdrawal or reduction in funding need to be approved by the Grants Committee, as set out in London Councils Commissioning Performance Management Framework. The Strategy Director has delegated authority to re-profile grant funding.

37. At the time of undertaking the audit fieldwork, it was established that it was too early in the grants programme to make decisions over funding levels. It is understood that London Councils were awaiting submission of Quarter 3 returns before taking decisions on further action required.

Reporting on Grant Delivery to Senior Management and Members

38. Through discussion with the Principal Programme Manager and inspection of the following documents, the audit confirmed that there are adequate arrangements in place for reporting on grant delivery to both Senior Management and Members.

39. The audit confirmed that the following reporting arrangements are in place:

    - Senior Management – The Corporate Management Board receive verbal updates on grant delivery at their weekly meeting. They also receive copies of grant delivery reports presented to Members (see below);

    - Members – through review of reports presented to Members of the Grants Committee, the audit confirmed that updates on grant programme performance is provided in November (covering quarters 1 and 2), March (quarter 3) and July (covering performance relating to the previous financial year). The reports presented to Members include key grant delivery information, including performance against output targets together with the RAG rating for each grant recipient.

ESF Grants Programme

Overview

40. The ESF 'Tackling Poverty through Employment' grant Programme is providing funding across six initiatives to tackle poverty across the capital by helping long-term unemployed and disadvantaged residents into work.

41. In relation to the ESF grant programme, the Strategy Director confirmed that London Councils has faced considerable challenges with grant delivery; over quarters 1 and 2 (quarter ended March 2017) of the grant programme, total performance was only 30 per cent of profile. The Grants Committee have been informed that this has been partly because of some poor advice, guidance and lack of operational management of the programme early on, alongside some performance issues with delivery partners, in particular, assumptions regarding delivery and eligibility, specifically, the eligibility criteria for economically inactive and no option to enrol short-term unemployed. This has particularly impacted on delivery of targets to date;

the loss of some sub-partners; confidence in London Councils by delivery partners. To address this, London Councils has re-based performance targets.

42. The Grants Committee were also informed that significant steps were taken to ensure that Partners have the required tools, guidance and support in place to effectively and successfully deliver projects including but not limited to the appointment of two officers to work with Partners and support with engagement strategies.

Grant Agreements

43. On the basis of discussion with the Strategy Director and inspection of all six signed ESF grant agreements the audit confirmed that the grant agreements set out the following key information.

    - The standard terms and conditions of grant funding;
    - Profiled targets for specific outcomes e.g. enrolment, intervention and engagement, attending training / undertaking education, employment. Enrolment targets are also set out for each borough; organisations delivering within the ESF programme are allocated different target boroughs. Organisations are expected to cross refer individuals to other organisations in their borough, where appropriate.

Submission of Performance Data

44. Through discussion with the Strategy Director, the audit established that grant recipients are required to submit data on performance against targets on a monthly basis, with funding paid on approved submissions. Each month organisations submit actual performance data together with supporting evidence via the ESF database which London Councils Grant Officers download to a spreadsheet. A quarterly progress report is also required to be submitted although, this has no direct impact on funding. The progress report requests commentary on key project information e.g. engagement, delivery, achievement against delivery targets, successes and challenges.

45. A review of data downloaded to the ESF database in July 2017, together with inspection of progress reports for all six grant recipients for the quarter ended September 2017, confirmed that the above arrangements are operating in practice.

46. As funding is paid based on submission of evidence supporting achievement of outputs there is no requirement to submit quarterly or annual monitoring reports as with the main grants programme. Providers are, however, required to submit evaluation reports upon project closure.

Review of Performance Data Submitted

47. Through discussion with the Strategy Director it was established London Councils adopt a four-tier approach to grant claim verification through examination of supporting records. Grants are verified as follows:

- First tier – grants claims are verified by Grant Officers;
- Second / Third tier – grant claims are verified by the Principal Programme Manager;
- Fourth Tier - grant claims are verified by the Strategy Director and ESF Technical Adviser.

48. Examination of data downloaded to the ESF database in July 2017 confirmed that the four-tier review process is operating in practice.

Financial Due Diligence

49. The Strategy Director stated that due to the considerable challenges in relation to grant delivery, as set out in paragraph 42, annual financial due diligence has not been undertaken since the commencement of the ESF programme. An amber recommendation has been raised to address this (**recommendation 2**).

Priority	**Issue**	**Risk**
Amber	Due to delays in delivery of ESF grants programme, grant recipients have not been subject to financial due diligence checks.	Grant recipients in poor financial health may go undetected; this increases the risk of significant financial loss should providers not be able to continue in operation.
Recommendation 2: The Strategy Director Young People's Education and Skills, Grants and Community Services should ensure that annual financial due diligence checks are reinstated and completed at the earliest opportunity for ESF grant recipients.		
Management Response and Action Plan Recommendation accepted. Annual Accounts are requested and scrutinised (see also management action for recommendation 1). **Responsibility:** Yolande Burgess, Strategy Director **Target implementation Date:** 28 September 2018		

Monitoring Visits

50. On the basis of discussion, the audit confirmed that the Strategy Director and ESF Technical Adviser regularly attend organisations premises to provide informal support and guidance to organisations. Specific feedback on recent grant claims are provided to organisations and their delivery partners at these meetings.

51. Going forward, London Councils is looking to undertake a dual quality assurance process i.e. utilise the option of reviewing the eligibility of participants at grant recipients' premises where it would be beneficial to do so.

52. On the basis that an appropriate assurance of the grant claims submitted can be obtained from reviewing supporting documentation at London Councils premises, the arrangements in place are adequate.

Implementing Agreed Actions

53. The audit established that there are no consistent arrangements in place for ensuring that agreed actions following monitoring are implemented by grant recipients (**recommendation 3**).

Priority	**Issue**	**Risk**
Green	Currently, there are no consistent arrangements in place for capturing and following up actions required by ESF grant recipients, following monitoring.	Agreed actions may not be delivered; this may have a detrimental impact on the quality of ESF programmes delivered.
Recommendation 3: The Strategy Director Young People's Education and Skills, Grants and Community Services should instigate formal arrangements to ensure consistency and timeliness with capturing and following up on actions required by ESF Grant providers		
Management Response and Action Plan Recommendation accepted. Monitoring visit template re-introduced; staff will be reminded about service expectations following monitoring visits i.e. notes and actions with review/by dates following monitoring visits to grant recipients with two working days; action follow-up to be diarised; line managers to review follow-up activity in 1-2-1 sessions. **Responsibility:** Yolande Burgess, Strategy Director **Target implementation Date:** 28 September 2018		

Safeguarding Grant Funding

54. Through examination of standard grant agreement clauses, the audit confirmed that the grant agreement enables London Councils to make changes to ESF programmes; this includes withdrawing funding or re-basing funding as a result of poor delivery. Funding is only paid when appropriate evidence has been obtained to confirm that outputs have been delivered.

Reporting on Grant Delivery to Senior Management and Members

55. The arrangements in place are the same for the main grants programme, as set out above.

Grant Funding Payments

Verifying Grant Recipients Bank Account Information (both grant programmes)

56. On the basis of discussion with the Strategy Director and Principal Programme Manager (Main Grants Programme) the audit confirmed that successful grant applicants are required to provide official 'bank stamp' to verify their bank account details. Through inspection, the audit confirmed that official 'bank stamp forms' were obtained for a sample of four grant recipients across the two grant programmes.

    The audit also confirmed that official bank stamp forms are provided to the Finance Team for the purposes of setting up grant recipients on the Oracle system. It is understood that successful applicants bank information is only uploaded to the Oracle system when payments become due (please see the following two sections of this report).

Grant Payments (Main Grants Programme)

57. On the basis of discussion with the Principal Programme Manager and a walkthrough of the process for making grant payments, the audit confirmed that there is scope to improve the arrangements for uploading grant payment schedules within the GIFTS system.

58. Following Grants Committee approving grant awards, grant payment schedules are input onto the GIFTS system. This is normally undertaken by one of three Officers – the two Principal Programme Managers – Grants, or the Grants Finance Manager. The audit noted that the uploading of grant payment schedules is not subject to review and approval to confirm that the grant payment schedules are accurate. Such

arrangements result in increased risk that inaccurate payment schedules may go undetected; this could result in grant overpayments and therefore, financial loss (**recommendation 5**). Upon initial upload onto the GIFTS system, grant payments are marked as 'contingent' i.e. contingent on the receipt of information such as submission of quarterly workbooks.

Priority	**Issue**	**Risk**
Amber	Following Grants Committee making grant awards, grant payment schedules are input onto the GIFTS system. This could be done by one of three Officers – the two Principal Programme Managers – Grants or the Grants Finance Manager. The uploading of grant payment schedules is not subject to review and approval to confirm that the grant payment schedules are accurate.	Inaccurate payment schedules may go undetected, which could result in grant overpayments and therefore, financial loss.
Recommendation 4: The Strategy Director Young People's Education and Skills, Grants and Community Services should instigate arrangements for reviewing and authorising the accuracy of grant payment schedules uploaded to the GIFTS system.		
Management Response and Action Plan Recommendation accepted. A first (Finance Officer) and second (Strategy Director) tier check will be implemented. **Responsibility:** Yolande Burgess, Strategy Director **Target implementation Date:** 28 September 2018		

59. As set out above, Grant Officers are responsible for reviewing and assessing information sent in by grant recipients. Once Grant Officers have confirmed that satisfactory information has been received the status of grant payments to 'scheduled' on the GIFTS system.

60. Each week, grant payment schedules are run by the Grants Finance Manager; the payment schedules set out all grants that are due for payment. The schedules are subject to review and approval by the Grants Officers and Main Grants Programme Principal Programme Manager before payments are made. Copies of the approved payment schedules are passed to the London Councils Finance Team for payments to be made via Oracle Accounts Payable (AP). The Grants Finance Manager marks the payments as 'scheduled exported' on GIFTS to prevent duplicate payments.

61. The Finance Team provide the Grants Finance Manager and Principal Programme Manager with notification of payments made. Once confirmation is received, the Grants Finance Manager marks payments as 'paid exported' on the GIFTS system.

62. Audit testing confirmed that four grant payments made totalling £840k had been subject to review and approval by the Grants Officers and Principal Programme Manager. The payments related to quarter 2 of the grant programmes.

63. Each payment was made on a timely basis, within one month of final queries being resolved in relation to the quarterly grant monitoring submissions.

64. In relation to notifying London Councils of grant underspends, grant recipients are required to provide a section 37 statement within their annual accounts; section 37 statements set out how grant funding has been utilised. At the time of the audit, grant recipients had not yet submitted their annual accounts for 2017/18; these are due to be submitted by January 2019. It is understood that London Councils will seek to recover grant underspends.

Grant Payments (ESF Grants Programme)

65. Through discussion with the Strategy Director, the audit confirmed that each quarter, output performance data is generated from the ESF database. This is checked for accuracy by the Strategy Director or ESF Consultant. The output performance data is issued to grant recipients in order for them to prepare and submit invoices for the funding due. The payments due are recorded on the GIFTS system.

66. Upon receipt of invoices from grant recipients, the invoices are subject to review and approval by;

    - the Principal Programme Manager (ESF) or Grants Finance Manager and then subject to second approval by:
    - the Strategy Director or ESF Consultant.

67. The invoices are then passed to the Finance Team for payment through Oracle, as set out above.

68. Audit testing confirmed that four grant payments made totalling £57k had been subject to review and approval in accordance with the above arrangements. The payments across quarters ending September and December 2017.

69. Each payment was made on a timely basis, within one week of invoices being submitted by grant recipients.

70. Therefore, ESF funding is paid where grant recipients provide appropriate evidence to confirm achievement of outputs, and this evidence has been verified by London Councils.

APPENDIX 1: AUDIT RESPONSIBILITIES AND DEFINITIONS

Assurance levels

Category	Definition
Nil Assurance 'Dark Red'	There are fundamental weaknesses in the control environment which jeopardise the achievement of system objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.
Limited Assurance 'Red'	There are a number of significant control weaknesses and/or a lack of compliance which could put the achievement of system objectives at risk and result in error, fraud, loss or reputational damage.
Moderate Assurance 'Amber'	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.
Substantial Assurance 'Green'	There is a sound control environment with risks to system objectives being reasonably managed. Any deficiencies identified are not cause for major concern.

Recommendation Categorisations

Priority	Definition	Timescale for taking action
Red – 1	A serious issue for the attention of senior management and reporting to the appropriate Committee Chairman. Action should be initiated immediately to manage risk to an acceptable level.	Less than 1 month or more urgently as appropriate
Amber – 2	A key issue where management action is required to manage exposure to significant risks, action should be initiated quickly to mitigate the risk.	Less than 3 months
Green – 3	An issue where action is desirable and should help to strengthen the overall control environment and mitigate risk.	Less than 6 months

Note:- These 'overall assurance level' and 'recommendation risk ratings' will be based upon auditor judgement at the conclusion of auditor fieldwork. They can be adjusted downwards where clear additional audit evidence is provided by management of controls operating up until the point of issuing the draft report.

What Happens Now?

The final report is distributed to the relevant Head of Department, relevant Heads of Service, and those involved with discharging the recommended action.

A synopsis of the audit report is provided to the Members of the Audit & Risk Management Committee. Internal audit will carry out a follow-up exercise as recommendations become due following issue of the final audit report. The on-going progress in implementing each recommendation is reported by Internal Audit to each meeting of the Audit & Risk Management Committee.

Any Questions?

If you have any questions about the audit report or any aspect of the audit process please contact the auditor responsible for the review, Ryan Wakefield, Senior Auditor, via email to ryan.wakefield@cityoflondon.gov.uk. Alternatively, please contact Pat Stothard, Head of Audit & Risk Management via email to pat.stothard@cityoflondon.gov.uk or Jerry Mullins, Audit Manager via email to jerry.mullins@cityoflondon.gov.uk

Appendix D

London Councils Internal Audit Plan Progress Report 2018/19

AUDIT REVIEW	**DAYS**	**PROGRESS**	**ASSURANCE RATING**	**OBJECTIVES**	**RECOMMENDATIONS**

AUDIT REVIEW	**DAYS**	**PROGRESS**	**ASSURANCE RATING**	**OBJECTIVES**	**RECOMMENDATIONS**			
PAN London Mobility Schemes	15	Fieldwork completed		To determine the effectiveness of controls exercised over the management of the taxi card and the freedom passes schemes. • Freedom passes to focus on contract management • Taxi card scheme to focus on internal controls: eligibility, record keeping and issue of taxi cards.	RED	AMBER	GREEN	TOTAL
Key Conclusions					**Management Comments**			

AUDIT REVIEW	**DAYS**	**PROGRESS**	**ASSURANCE RATING**	**OBJECTIVES**	**RECOMMENDATIONS**			
Business Continuity Arrangements	10	**Postponed to quarter 4 – requested by Chamberlains CoL**.		To evaluate the adequacy of the business continuity arrangements in place, ensuring that the plan is updated on a regular basis, tested for effectiveness, disseminated to Staff, and that staff are provided with adequate and appropriate training.	RED	AMBER	GREEN	TOTAL
Key Conclusions					**Management Comments**			

AUDIT REVIEW	**DAYS**	**PROGRESS**	**ASSURANCE RATING**	**OBJECTIVES**	**RECOMMENDATIONS**			
ICT Information Governance, including GDPR	15	**Postponed to quarter 4 – requested by London Councils**		An audit to determine the transparency and effectiveness of the information governance framework and channels used to manage information, focussing on compliance with GDPR requirements.	RED	AMBER	GREEN	TOTAL
Key Conclusions					**Management Comments**			

AUDIT REVIEW	**DAYS**	**PROGRESS**	**ASSURANCE RATING**	**OBJECTIVES**	**RECOMMENDATIONS**			
Follow Ups	2	On-going		Follow up on the implementation of recommendations made in previous reviews.	RED	AMBER	GREEN	TOTAL
Key Conclusions								

AUDIT REVIEW	DAYS	PROGRESS	ASSURANCE RATING	OBJECTIVES	RECOMMENDATIONS			
Contingency	3	On-going		TBC	RED	AMBER	GREEN	TOTAL
Key Conclusions								
Total	**55**							

* Subject to agreement of scope with service managers when preparing the terms of reference.

Audit Committee

Implementing the General Data Protection Regulation (GDPR) and Data Protection Act 2018 Update

Item no: 08

Report by:	Frank Smith	**Job title:**	Director of Corporate Resources
Date:	18 September 2018		
Contact Officer:	Emily Salinger		
Telephone:	020 7934 9836	**Email:**	Emily.Salinger@londoncouncils.gov.uk

Summary

This item provides the Audit Committee with an update on London Councils work on the General Data Protection Regulation and the Data Protection Act 2018.

Recommendations

The Audit Committee is asked:

- Note the work done in relation to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18).

1. Background

1.1 At the Audit Committee on 21st September 2017 it was agreed to include a General Data Protection Regulation (GDPR) update as a standing item on the Audit Committee agenda.

1.2 In March 2018, the Audit Committee received a report on GDPR preparations which had been considered by the London Councils Executive in January 2018. The Audit Committee also received a verbal update from the Director, Corporate Resources.

1.3 The Audit Committee received a further update report in June 218 and decided to continue to receive reports at each meeting for the foreseeable future.

1.4 The GDPR came into effect on 25th May 2018. Most provisions in the Data Protection Bill 2018 (DPA 2018), which sits alongside the GDPR, also came into effect on 25th May 2018. The legislation replaced the Data Protection Act 1998.

1.5 As reported in June, it is anticipated that focused GDPR/DPA2018 related work will continue through 2018. Beyond then, it is expected the work will focus on the tasks of the Data Protection Officer (DPO) and maintaining a privacy by design culture.

1.6 This report updates the Committee on the work done to meet the requirements of the new data protection legislation.

2. Overview of data protection related work since the last update in June 2018

2.1 In August, London Councils Corporate Management Board approved an updated Data Protection Policy. Many of the staff responsibilities remain the same as our previous policy but it has been updated to reflect changes in legislation and London Councils commitment to the data protection principles within GDPR. The policy sits alongside the Information Security Policy and Information Management Policy which were updated earlier this year. Together the three policies govern how information is managed at London Councils.

2.2 Staff have continued to receive communications on GDPR related topics via our weekly staff newsletter, in particular on breach reporting, raising awareness of our updated policies and on the importance of deleting personal data in line with retention schedules.

2.3 As noted in the previous report, Officers supporting the GDPR/DPA18 preparations risk assessed the work conducted by London Councils and concentrated on the higher risk areas first. Work has continued with lower risk teams, particularly the Policy teams in order to identify the information they hold and ensure they have sound processes for managing it. These teams hold minimal personal data but the process has prompted improvements to information management practices. The work has also increased understanding and awareness of data protection legislation which will help ensure that advice is sought for any new handling of personal data in the future.

2.3 One of the new requirements under GDPR is mandatory reporting of breaches to the Information Commissioners Office. A data breach is defined as;

> A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Breaches must be reported within 72 hours of an organisation becoming aware if there is a risk to individuals' rights and freedoms. London Councils agreed a new breach reporting procedure earlier this year. Staff have received face to face training on the new procedure. Appropriate breach reporting procedures have also been agreed with contractors who process personal data on our behalf.

2.4 As anticipated, there has been an increase in the number of breaches being reported internally compared to those reported in previous years. So far none have met the threshold to be reportable to the ICO. The ICO were contacted in July to ensure the risk assessment London Councils was using was valid and, after talking through a number of breaches, they advised that the approach was appropriate. London Councils will continue to monitor breaches to identify any trends or learning points.

2.5 Another new requirement under GDPR is mandatory data protection impact assessments (DPIA) where a new or changed use of personal data involves a high risk to individuals. The DPIA process involves the identification of risks with a proposal before a new or changed activity takes place. It also includes identification of the mitigating actions planned to reduce the risks to a tolerable level. London Councils has decided, in the short term, to conduct impact assessments in more circumstances than the mandatory requirement to promote understanding of the process. Four DPIA's have been conducted in recent months for a project within the Employment and Inclusion team, a pilot within the Taxicard service and two research projects which involve gathering personal data.

2.6 The information governance work continues to be monitored by the GDPR Preparation Board which includes three members of the Corporate Management Board, including London Councils Senior Information Risk Officer (SIRO), Frank Smith. They provided feedback on the draft data protection policy prior to consideration by the Corporate Management Board.

3 Next steps

3.1 Officers led by the DPO will continue with the programme of work currently underway until every team has risk assessed the information they hold and received specific guidance on managing their information and that new policies and procedures are fully embedded.

3.2 We will continue to monitor new guidance on aspects of the GDPR and DPA18 as well as being aware of how the legislation is being implemented and monitored by the ICO.

3.3 This work will be monitored internally by the GDPR Board and aspects will be audited as part of the internal audit on 'ICT Information Governance including GDPR' towards the end of 2018/19.

4. Implications

Financial Implications for London Councils

None.

Legal Implications for London Councils

None

Equalities Implications for London Councils

None

Recommendations

The Audit Committee is asked:

- Note the work done in relation to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Appendices

None

Background Papers

London Councils Data Protection Policy – updated August 2018

Breach Reporting - Guidance and Template

GDPR Preparation Plan

LONDON COUNCILS

Audit Committee

Dates of Audit Committee Meetings for 2019-20 Item no: 09

Report by:	Alan Edwards	**Job title:**	Governance Manager
Date:	18 September 2018		
Contact Officer:	Alan Edwards		
Telephone:	020 7934 9911	**Email:**	Alan.e@londoncouncils.gov.uk

Summary	This report notifies members of the proposed Audit Committee meeting dates for 2019/20.
Recommendations	It is recommended that members discuss/agree the proposed dates for 2019/20.

Audit Committee Dates for 2019/20

- Thursday 21 March 2019 (at 10.30am)
- Thursday 20 June 2019 (at 10.30am)
- Thursday 19 September 2019 (at 10.30am)
- Thursday 19 March 2020 (at 10.30am)

The above meetings are scheduled to take place at London Councils, 59½ Southwark Street, London SE1 0AL (start times are in brackets)