FINAL INTERNAL AUDIT REPORT

CORPORATE SERVICES DEPARTMENT

IT SERVICES CONTRACT AUDIT 2016-17

Issued to:	**Mark Bowen, Director of Corporate Services** **Peter Turner, Director of Finance** **Stuart Elsey, Head of Information System Services** **Dee Jackson, Contract Monitoring ISD Manager**
Prepared by:	**Senior IT Audit Manager (Mazars LLP on behalf of LBB)**
Date of Issue:	**16 March 2017**
Report No.:	**CX/073/01/2016-17**

INTRODUCTION

1. This report sets out the results of our IT Services Contract audit. The audit was carried out in Q4 as part of the programmed work specified in the 2016-17 Internal Audit Plan agreed by the Section 151 Officer and Audit Sub-Committee.
2. The audit examined the control framework that we expect to see in place to help minimise the Council's exposure to a range of risks associated with IT Service and Delivery Contract management. Weaknesses in controls that have been highlighted will increase the associated risks and should therefore be corrected to assist overall effective operations.
3. The original scope of the audit was outlined in the Terms of Reference issued on 10/11/2016.
4. The third party partner for IT Services Delivery activities transitioned to Contractor A during 2016 as part of the new IT Services Contract and the new LBB contract compliance management monitoring arrangements.

AUDIT SCOPE

5. The scope of the audit is detailed in the Terms of Reference.

AUDIT OPINION

6. Overall, the conclusion of this audit was that substantial assurance can be placed on the effectiveness of the overall controls. Definitions of the audit opinions can be found in Appendix C.

MANAGEMENT SUMMARY

7. Controls were in place and working well in that a contract was in place, to outline the Service Scope and Delivery Principles. The contract service performance delivery activities are monitored for achievement on monthly basis via the use of appropriate and agreed key performance indicators.

8. The audit examination and assessment of the controls that have been established and applied in the areas set out in the audit scope noted the following:

- The contract management governance roles and responsibilities – While a heavy reliance is placed on the constant availability of key personnel roles are clearly defined and communicated in the Information Systems Department job descriptions and organisational chart including all payment authorisation and budget management activities.
- The contract management monitoring arrangements – were confirmed as largely effective after examination of the monthly management monitoring meeting and payment records where the contract service performance delivery activities are monitored for achievement via appropriate and agreed key performance indicators. One recommendation for further improvement was agreed in this area regarding the adoption of an appropriate key performance indicator for virus and malware detection and resolution solutions and mobile phone device patch management activities.
- Contract hand over arrangements – the LBB IS management team effectively documented all the IS assets and systems in detail prior to transitioning the management and support arrangements from Contractor B to Contractor A. In addition, the effectiveness of the network hardware configuration settings were examined and documented to baseline the security status of these assets at transition and to assist the ongoing monitoring of security improvements. It was also confirmed that the Contractor A delivery management team had completed their own in depth due diligence arrangements for the handover.
- IT Risk management arrangements – are largely effective as the nine high level risks, that are documented in the IT Risk Register, includes the risk of the “New IT Supplier failing to meet the IT delivery performance levels” and the risk of failing to meet regulatory requirements. However, although risk owners are assigned, the responsibilities and target achievement dates for risk mitigation officer activities are not transparently assigned to assist the risk owners to track and monitor the risk mitigation status and a recommendation was raised to help improve this control area.

SIGNIFICANT FINDINGS (PRIORITY 1)

9. None.

DETAILED FINDINGS / MANAGEMENT ACTION PLAN

10. The findings of this report, together with an assessment of the risk associated with any control weaknesses identified, are detailed in Appendix A. Any recommendations to management are raised and prioritised at Appendix B.

ACKNOWLEDGEMENT

11. Internal Audit would like to thank all staff Contracted during this review for their help and co-operation.

IT SERVICES CONTRACT AUDIT 2016-17

APPENDIX A

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
1	**Key Performance Indicator Reports** The use of appropriate key performance indicator reports helps to ensure that ICT performance delivery and solutions are adequately monitored for effectiveness. Examination of the IT Contract documentation and the monthly management monitoring meeting records identified IT service performance delivery arrangements are largely effective. However, while patch management reports are available for review by the LBB Contract Management and Security Management Officers, no similar management monitoring report was found in place to advise management on the effectiveness and trends in a) antivirus and malware detection and resolution solutions; or b) mobile phone device security patch management update activities.	The risk of data leakage and virus or ransomware threats impacting upon the Council is increased because the ability of the LBB Contract Management and Security Management Officers to efficiently monitor the effectiveness and trends of the antivirus / malware detection and resolution solutions may be compromised unless appropriate KPI reports are established for a) Anti-Virus activity and b) Mobile phone device patch management.	The LBB Contract Management and Security Management Officers should seek to ensure that appropriate KPI reports are developed to monitor the effectiveness of a) antivirus / malware detection resolutions; and b) mobile phone device patch management activities.

IT SERVICES CONTRACT AUDIT 2016-17

APPENDIX A

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
2	**IT Risk Management Mitigation Owners** Effective risk management arrangements helps to minimise or eliminate the probability and impacts of risks. Examination of the departmental risk management arrangements identified that nine high level ICT risks have been documented. These include the risk of the "New IT Supplier failing to meet the IT delivery performance levels" and the risk of failing to meet regulatory requirements (e.g. PSN). However, it was noted that 1) Risk owners are clearly assigned and documented, but the responsibilities and target achievement dates for risk mitigation officer activities are not transparently assigned to assist the risk owners to track and monitor the status of risk mitigations via the departmental risk management arrangements. 2) The best practice "Actions Issues and Risk" (AIR) log being used by the Contractor A Contact Manager is not transparently linked to the departmental risk log references and while it did include estate management actions regarding power supply it did not include mobile device patch management risks.	There is a risk that the effectiveness of IT risk management governance arrangements may be compromised unless the risk management arrangements consider that: a) Quarterly reviews of strengths, weaknesses, opportunities and threats; b) Assigning appropriate risk mitigation action officers, tasks and dates to report on remediation activity to the Risk Owners and the Senior Information Risk Officer.	The risk management monitoring arrangements should consider ensuring that: • Quarterly reviews of strengths, weaknesses, opportunities and threats take place; and • Assigning appropriate risk mitigation action officers, tasks and dates to report on remediation activity to the Risk Owners and the Senior Information Risk Officer.

IT SERVICES CONTRACT AUDIT 2016-17

APPENDIX B

MANAGEMENT ACTION PLAN

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
1	**Anti-Virus Key Performance Indicator Reports** The LBB IT Contract Monitoring and Security Management Officers should seek to ensure that appropriate KPI reports are developed to monitor the effectiveness of • antivirus / malware detection resolutions; and • mobile phone device patch management.	2	AV Reporting – Inflight project will be live with recommendations implemented soon. Mobile Device Security Updates – A CCN will be raised to Contractor A after completion of the above AV software project. It is anticipated that recommendations will be implemented soon after the completion of AV software project.	IT Contract Monitoring and Security Management Officers	June 2017 September 2017

IT SERVICES CONTRACT AUDIT 2016-17

APPENDIX B

MANAGEMENT ACTION PLAN

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
2	**IT Risk Management Mitigation Owners** The risk management monitoring arrangements should consider ensuring that: • Quarterly reviews of strengths, weaknesses, opportunities and threats take place; and • Assigning appropriate risk mitigation action officers, tasks and dates to report on remediation activity to the Risk Owners and the Senior Information Risk Officer (SIRO).	2	The Management Team are working together on improving Risk Management and will be setting up quarterly SWOT review. First meeting happened on 08/03/2017.	Head of ISD	June 2017

OPINION DEFINITIONS **APPENDIX C**

As a result of their audit work auditors should form an overall opinion on the extent that actual controls in existence provide assurance that significant risks are being managed. They grade the control system accordingly. Absolute assurance cannot be given as internal control systems, no matter how sophisticated, cannot prevent or detect all errors or irregularities.

Assurance Level	**Definition**
Full Assurance	There is a sound system of control designed to achieve all the objectives tested.
Substantial Assurance	While there is a basically sound systems and procedures in place, there are weaknesses, which put some of these objectives at risk. It is possible to give substantial assurance even in circumstances where there may be a priority one recommendation that is not considered to be a fundamental control system weakness. Fundamental control systems are considered to be crucial to the overall integrity of the system under review. Examples would include no regular bank reconciliation, non-compliance with legislation, substantial lack of documentation to support expenditure, inaccurate and untimely reporting to management, material income losses and material inaccurate data collection or recording.
Limited Assurance	Weaknesses in the system of controls and procedures are such as to put the objectives at risk. This opinion is given in circumstances where there are priority one recommendations considered to be fundamental control system weaknesses and/or several priority two recommendations relating to control and procedural weaknesses.
No Assurance	Control is generally weak leaving the systems and procedures open to significant error or abuse. There will be a number of fundamental control weaknesses highlighted.