London Councils – Internal Audit Recommendations Log (June 2016) **Appendix C**

ICT Review (February 2014)

Risk rating	Recommendations	Accepted	Implemented	Outstanding
Red	0	0	0	0
Amber	7	7	6	1
Green	12	11	9	2
	19	**18**	**15**	**3**

Issue, Risk & Recommendation ICT Review (February 2014)	Management Response	Current Position at June 2016
Recommendation 1 Issue: A current ICT strategy does not exist. Risk: The lack of a current ICT strategy and therefore lack of planning can result in risk of failure to achieve business objectives. Risk rating: Amber Recommendation: Formalise and document the ICT strategy in line with the business requirements.	The current ICT Strategy was ratified in June 2005 so is due for revision. The Corporate Management Board has agreed that the revised strategy will be consulted upon and produced post April 2014. This will give the organisation sufficient time to instigate and complete critical mail, server and infrastructure improvement projects by March 2014. Responsibility: Frank Smith, Director, Corporate Resources Target Implementation Date: August 2014 Progress note (September 2014): The critical projects led by the City of London ICT and Agilisys had been delayed hence the delay in completion of the task. The mail migration project and server tasks noted were finally were only delivered early September 2014 with a revised date proposed of October 2014 for the infrastructure recommendations. Revised date for strategy completion, January 2015.	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 2 Issue: A staff data security and sensitive data awareness training programme does not exist thus staff potentially unaware of the data security aspects related to their environment. Risk: Data loss due to insufficient training with a potential for loss of reputation. Risk rating: Green Recommendation: LC are recommended implement an appropriate programme of training in line with industry guidelines.	London Councils has been trying to implement an appropriate programme of training in line with what the City of London does for some time. However, the on-line/e-learning courses on protecting Information and Data Security which City of London employees are required to complete is only now available to London Councils staff. The DPA and FOI modules are not. A training package will be developed which combines what is available on-line via the e-portal with a bespoke London Councils element, which will be delivered to all staff at Southwark Street/Angel Square. Responsibility: Christiane Jenkins, Director, Corporate Governance Target Implementation Date: August 2014	Recommendation implemented
Recommendation 3 Issue: Computer room does not conform to best practice guidelines and generally needs improving such as suitable preventative measures in place. For example the cooling mechanism needs an approved permanent solution, computer cables need labelling and tidying, etc. Audit is aware there is an on-going improvement programme underway in this area as part of the LC report by CoL and most parts are being already being dealt with. Risk: Partial or total loss of the computer room and/or services thus adversely affecting the business with a potential for loss of reputation.	All redundant kit and cabling has already been removed from the computer room and as exiting server hosts are being virtualised remaining redundant hardware will be decommissioned. The mail server hosts will be decommissioned post the Office365 migration in April/May 2014. A UPS has also been installed to support the new virtual server environment. The remaining phone and PBX servers will also be virtualised. A second permanent air cooling unit was commissioned and installed in January 2014 providing the required air cooling temperature throughout this space.	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Risk rating: Amber Recommendation: LC are recommended to review all aspects of the computer room and improve/align them with industry best practice guidelines.	Any other required improvements are building works changes. As the building is owned by the City of London Corporation, it is suggested that the City Surveyors provide costs for these improvements, as a refurbishment of the server room together with any 3rd party equipment should be completed as a single project. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: January 2015 Progress note (September 2014) Activities met February to August 20014; • Avaya PBX upgraded alongside associated patch cabling and voice networking • Three additional physical data and production servers have now been virtualised, with only one server (DOCSERVER) remaining on-site scheduled for migration to new virtual platform post the Office 365 migration September 2014. BlackBerry (BBERRY)server now decommissioned (hosted within Office 365 cloud service) and old telephone server (PHONESERVER) decommissioned and new admin and voicemail server for new Avaya phone platform rebuilt as a virtual Windows 2008 server • Activities to be completed post September 2014; • Destruction and removal of all redundant server data on decommissioned physical servers hardware and safe collection and disposal organised	

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
	• As part of the London Councils PATAS (parking & Traffic Appeals Service) service tender a Lot has been incorporated for the provision of a full managed ICT services at London Councils from June 2015. This would include the management and hosting of the complete London Councils server infrastructure into IaaS platform which means the Southwark Street site would become infrastructure free from June 2015. We will know more regarding the award of this lot once contract has been awarded in November 2014	

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 4 Issue: Email is running on outdated fragile hardware. Email software is two versions out of date and on extended support until April 2014. Email is critical to LC for performing the daily business operations. Risk: Email service failure or Email is unsupported. Risk rating: Amber Recommendation: LC and CoL are aware of the risks (from the LC technology report) of the current software and timescales. A project to replace the Email system (implementation scheduled for first quarter of 2014) with the cloud based Office 365 is underway, however delays are already occurring. The project and the interdependencies need to be carefully and regularly monitored to ensure delays are minimised otherwise an interim solution should be investigated and implemented prior to the expiry of the extended support date.	These issues will be resolved with migration of LCs email stores to cloud storage (Office 365). This project is has been scoped in conjunction with CoL and cloud consultants Content & Code. Progress and project plan is reviewed weekly with controls in place. Tests will begin with a testing group during February 2014 with full roll-out projected to be completed early April 2014. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: April 2014	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 5 Issue: The IP network at the Southwark Street currently utilises a public IP range. The use of a public IP range is not considered best practice and can cause issues with a network that has connection to the Internet. Risk: Future IP conflicts are possible with the reallocation of the IP range. LC systems using this range will become unusable. Risk rating: Green Recommendation The London Councils Reports highlighted this issue however a proposed solution has not been confirmed yet. Consider implementation of a proper IP subnet to improve security and conform to best practice standards to avoid future problems.	The London Councils network in its present topology could support multiple subnets however additional or replacement networking equipment would be required to achieve this. Agilisys, the City of London's ICT contractor can provide London Councils with a proposal for this network infrastructure upgrade and the project plan for migrating to a new IP addressing scheme. This would be a new service request that would need to be further scoped. City estimates are at present around £40,000 for this piece of work. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: January 2015 Progress note (September 2014) Cost estimates and network proposals from City of London ICT and Agilisys quoted to accomplish this activity have not altered. As an element of the London Councils PATAS service we have requested the tenders to propose options for the networking infrastructure piece so it may be prudent to explore the models and solutions being proposed by the managed service tenders if contract is awarded to another ICT provider. The tenderers on the Lot 3 shortlist have proposed solutions which we would then work on in detail post contract award in November 2014.	In conjunction with City of London ICT and Agilisys partners, the technical solutions for this activity has been recrafted to incorporate the corporate project LAN and network upgrade/refresh and the two factor authentication project with a revised and combined delivery date of 29th July 2016.

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 6 Issue: Password security standards for LC does not exist therefore security within a number of systems is probably less than best practice. Risk: Risk of unauthorised access to systems and sensitive data. Risk rating: Green Recommendation: Establish and implement LC password security standard in line with industry best practice and apply to all systems.	London Councils Active Directory domain logons follow a best practice password policy adopted from the City of London. London Councils will carry out a further scoping exercise of all our existing systems that do not meet best practice password policies and this can be managed as separate project. All staff are issued with a password and all the Internet/Email/Telephone Policy states: "individuals are required to follow the necessary security disciplines and to keep their passwords totally confidential". London Councils will periodically remind staff that this is the case. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: January 2015	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 7 Issue: Remote Access is permitted requiring only the computer IP, username and password to gain access. Additional security verification is not enforced with use of a security fob or similar. Risk: The system is less secure and vulnerable to malicious access by allowing an easier entry point to the LC systems and data. Risk rating: Green Recommendation: Install suitable access measures which include two factor authentication which requires the current user logon and password, and additionally a security fob or similar.	London Councils are in the process of migrating their remote access solution onto a server farm built on Windows Server 2008. Staff will now be required to access the remote service using a secure desktop icon which contains additional security and gateway data. The IP address gateway access will be switched off in March 2014. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: March 2014 Progress note (September 2014) The above activity was completed in February 2014 and is in full use by the business. However, a remote access security breach in September 2014 has resulted in reconsideration of the level of risk acceptance of this area by London Councils. A scoping and costing exercise for 2FA has been requested from the CoL IS department as a matter of urgency.	In conjunction with City of London ICT and Agilisys partners, the technical solutions for this activity has been recrafted to incorporate the corporate project LAN and network upgrade/refresh and the two factor authentication project with a revised and combined delivery date of 29th July 2016.

Issue, Risk & Recommendation **ICT Review (February 2014)**	**Management Response**	**Current Position at June 2016**
Recommendation 8 Issue: Lack of recording and monitoring of LC network logins. Risk: Invalid and potentially malicious access attempts going undetected and unreported. Risk rating: Green Recommendation: LC are recommended to implement a procedure to include logging, monitoring and reporting to allow assessment of the data for corrective action.	Agilysis and the City of London have been asked to provide a proposal for additional security for the monitoring of network logons, which will be reviewed by the ICT and Facilities Manager. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: January 2015 Progress notes (September 2014) Still awaiting costs and proposals from City of London and Agilisys.	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 9 Issue: Internet access is almost unrestricted thus allowing access to unsuitable sites and social media sites. Risk: Inappropriate use of the internet and possibility of download of malware as well as wastage of staff time. Risk rating: Amber Recommendation: Create an responsible internet access policy and disseminate to staff.	London Councils has a well-documented and intranet accessible Internet/Email/telephone Policy which clearly sets out what is acceptable/not acceptable. Access to unacceptable sites was blocked in 2010 and allowable access was discussed at length by London Councils Corporate Management Board and as a consequence the Internet/Email/telephone Policy alongside the equally accessible Social Media Guidelines are considered adequate for London Councils. The current Ironport web proxy and URL filtering system is currently not filtering due to a fault. The implementation of Webroot would allow London councils to enforce its internet access policy. Webroot testing is due to start in February with implementation later that month. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: February 2014 Progress notes (September 2014) After a detailed review of projects March 2014 in particular our key infrastructure projects and deliverables being managed by the City of London and Agilisys, it was agreed that there would be reduced risk if this activity was completed post Office 365 mail migration and tenancy project. As the Office365 project only completed in September 2014 and implications for the new London Councils website and intranet portals that go live during October, deployment of Webroot across the organisation has now been rescheduled for late October 2014.	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 10 Issue: Hardware such as CD drives and USB ports are unsecured thus data can be copied onto portable devices. Risk: Sensitive data may be copied and carried off the premises thus risking data breach. Risk rating: Amber Recommendation: Consider restricting access to administration users only and locking down PC's so data cannot be easily copied and additionally implement a process to enable data copy requests with suitable controls.	Agilysis have been asked to provide a proposal for installing appropriate software to make the use of portable media more secure. The proposal will be considered by the ICT and Facilities Manager. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: July 2014 Progress notes (September 2014) This task has not commenced. In conjunction with CoL and Agilisys rescheduled for completion January 2015.	Recommendation implemented
Recommendation 11 Issue: Inadequate monitoring and management of storage capacity for the email system. Risk: System downtime. Risk rating: Amber Recommendation: Implement suitable controls for monitoring and management of disk capacity for the email system and other critical systems.	Daily checks are in place monitored by the City ICT team for LCCOMMS as this server has had some disk space issues. Further work is due to be carried out to reduce mailbox database sizes prior to migration to the cloud services. Mutiny alert software is currently used on all systems to alert on disk usage over 80%. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: May 2014	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 12 Issue: The existence of an FTP server. The exact use and user restrictions are unknown and until recently it was in an unrestricted area. FTP data transfer is still possible. Risk: Transfer of data in an unsecure manner. Risk rating: Green Recommendation: The LC are aware of this issue from the report produced by CoL which resulted in the move of the FTP server into more secure area, however, further improvements are recommended. As a minimum modify the server to only allow only secure data transfer using Secure File Transfer Protocol (SFTP) as opposed to FTP. Implement a process for assessing and authorising use of this facility and document user and data transfer information.	This server is now decommissioned and only secure data transfer will now be permitted. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: December 2013	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 13 Issue: The percentage of support calls completed within SLA targets is lower than expected (65-80%). Risk: The support provided is inadequate. Risk rating: Green Recommendation: A monthly review of support calls that exceed SLA is advised with a view to identifying problem areas and acceptable delays for a more accurate assessment of the level of service provided.	Since January 2014 Agilisys have now have implemented a new service management tool Hornbill which will be available to provide more accurate information on SLA and areas where call resolution is not meeting targets. The ICT & Facilities Manager, who is responsible for the client-side management of the ICT service provided by the City, now has access to the City's call logging portal so is now able to monitor all logged and breached incidents and service requests. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: February 2014	Recommendation implemented
Recommendation 14 Issue: A single source of information on ICT contracts and agreements information does not exist. This can result in critical renewal dates being missed. Risk: Possible interruption of service or potentially a poorer service. Risk rating: Green Recommendation: Consolidate important information into a ICT contracts register with a procedure to regularly review and update the contents.	Contract data is being compiled and will be held in a single contracts register.	Recommendation implemented

Issue, Risk & Recommendation **ICT Review (February 2014)**	**Management Response**	**Current Position at June 2016**
Recommendation 15 Issue: Security is not enforced for voicemail on telephones. Risk: Private and sensitive voicemails are accessible by all LC staff. Risk rating: Green Recommendation: Enforce voicemail pin code functionality which is already available.	London Councils currently manage telephony and voicemail system. All telephones are accessible for all staff to use and to monitor and pick-up and to ensure any voicemail messages are dealt with. London Councils does not consider that a voicemail pin code is necessary – this will mitigate staff being able to cover for one another and provide a proper service to our customers/stakeholders.	Recommendation not accepted.
Recommendation 16: Issue: The database for the LC GIFTS system not patched to latest security level. Risk: The systems are exposed to known and fixable vulnerabilities. Risk rating: Green Recommendation: Install latest security patches and implement a procedure to regularly patch all systems.	An SCCM server is currently in place and will be configured to automate the MS Windows Server patching. MS SQL servers are not patched automatically due to the complexity and impact of patches across a MS SQL server hosting multiple databases. A review of existing 3rd party database application will be carried and the MS SQL server patches will be applied Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: Already in place	Recommendation implemented

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 17 Issue: There is a lack of resilience, for example, only a single firewall in place at both LC and CoL sites. Risk: Single points of failure would result in service interruption. Risk rating: Amber Recommendation: Investigate infrastructure for all points of failure and initiate a project to improve resilience otherwise include reasons for risk acceptance. In the meantime ensure the firewall configuration is backed up regularly.	The City of London site is the DR site for London Councils and the need for dual firewalls at this site may not be cost effective. The London Councils site firewall is managed by a third party (BIS) who provide backups of the firewall configuration and an SLA for hardware faults. The existing Virgin media Internet link currently has an SLA call out target of 8 hours. Aglisys have estimated an additional annual cost of £10,000 for a fully resilient internet fail-over connection. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: July 2014 Progress notes (September 2014) Cost estimates and design architecture proposed by the City of London ICT and Agilisys have not changed. As part of the London Councils PATAS service retender we have requested the tenders propose options for a fully managed or infrastructure free service for London Councils and a managed service DR site therefore it may be prudent to explore those models proposed if contract is awarded to another ICT provider. The service providers on the Lot 3 shortlist have proposed solutions which include IaaS which we would then work into detail post contract award in November 2014.	In conjunction with City of London ICT and Agilisys partners, the technical solutions for this activity has been recrafted to incorporate the corporate project LAN and network upgrade/refresh and the two factor authentication project with a revised and combined delivery date of 29th July 2016.

Issue, Risk & Recommendation ICT Review (February 2014)	**Management Response**	**Current Position at June 2016**
Recommendation 18 Issue: LC BCP plan last updated 16 months ago. The Angel Square site BCP is more current but needs updating to reflect latest changes (eg staff changes). Risk: The plan is out of date and may jeopardise business continuity in a disaster. Risk rating: Green Recommendation: Update the current BCP plans and regularly review (at least annually).	Both documents for 59½ Southwark Street and Angel Square are in the process of consultation and review. This will be conducted in conjunction with Recommendation 19. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: June 2014 Progress notes (September 2014) This activity has not started due to delays and additional work required to complete Office 365 and server decommissioning projects. Revised date February 2015. The lease on Angel Square comes to an end in July 2015 therefore a new plan will be constructed for the new PATAS service, location yet to be finalised.	Recommendation implemented .
Recommendation 19 Issue: A single comprehensive DR plan does not exist although some individual systems undergo DR. Risk: DR is inadequate or not possible thus recovery could be severely delayed. Risk rating: Green Recommendation: Produce a comprehensive DR plan inclusive of testing.	In conjunction with Recommendation 18 a single comprehensive DR with test plan will be devised. A test of the DR plan will be undertaken post the Office365 implementation. Responsibility: Roy Stanley, ICT & Facilities Manager Target Implementation Date: June 2014 Progress notes (September 2014) This activity has not started due to delays and additional work required to complete Office 365 and server decommissioning projects. Revised date February 2015.	Recommendation implemented

London Councils – Internal Audit Recommendations Log (June 2016) **Appendix C**

Key Financial Controls (December 2015)

Risk rating	Recommendations	Accepted	Implemented	Outstanding
Red	0	0	0	0
Amber	1	1	0	1
Green	0	0	0	0
	1	**1**	**0**	**1**

Issue, Risk & Recommendation Key Financial Controls (December 2015)	Management Response	Current Position at June 2016
Recommendation 1 Issue: The inventory record is not fully compliant with Financial Regulation paragraph 14.9 related to the control of assets. Risk: Non-compliance with Financial Regulations. Insurance arrangements may be compromised by poor/incomplete information related to assets. Assets cannot easily be accounted for due to poor / incomplete management information. Risk rating: Amber Recommendation: Inventory maintenance should be undertaken in accordance with Financial Regulation 14.9.	The omitted information will be incorporated into the inventory listing if available. There are instances where items such as the date and cost of purchase are unavailable due to the age of the items some of which were acquired prior to the creation of the organisation in its current form. However, an estimated replacement value will be assigned to each item for insurance purposes. Responsibility: Roy Stanley, ICT and Facilities Manager Target Implementation Date: February 2016	**Partially implemented** - All items included on the inventory list have been assigned a replacement value in accordance with the financial regulations. New and recent purchases also have the date and cost of purchase included on each record. However, there is an ongoing exercise to identify information that relates to more historic purchases.

London Councils – Internal Audit Recommendations Log (June 2016) **Appendix C**

Risk Management and Business Continuity Planning (May 2016)

Risk rating	Recommendations	Accepted	Implemented	Outstanding
Red	0	0	0	0
Amber	1	1	1	0
Green	2	2	1	1
	3	**3**	**2**	**1**

Issue, Risk & Recommendation Risk Management and Business Continuity Planning (May 2016)	Management Response	Current Position at June 2016
Recommendation 1 Issue: The Risk Management Strategy & Framework was last formally reviewed and approved by the Audit Committee in May 2012. Risk: The Risk Management Strategy & Framework is not reflective of current organisational processes. Risk Management Strategy & Framework not in alignment with the Business Plan 2015-16. Risk rating: Green Recommendation: The Risk Management Strategy & Framework should be scheduled for review and update every three years to ensure that it is reflective of current organisational processes and subsequently approved by the Audit Committee.	Management is happy for a recommendation to be made to the Audit Committee when this Internal Audit Report is reported, that the Risk Management Strategy & Framework is formally reviewed during the course of 2016/17 and any proposed changes are reported to Audit Committee for approval and that it is then reviewed on a periodic basis. Responsibility: Christiane Jenkins, Director, Corporate Governance Target Implementation Date: September 2016	Recommendation to be implemented by September 2016.

Issue, Risk & Recommendation **Risk Management and Business Continuity Planning** **(May 2016)**	**Management Response**	**Current Position at June 2016**
Recommendation 2 Issue: Test results of the Business Continuity Plan are not scheduled to be presented to Audit Committee. Risk: Business Continuity processes in place are insufficient to protect London Councils from potential disruption. Risk rating: Green Recommendation: When the Business Continuity Plan is tested, the results should be recorded and presented to Audit Committee. This requirement should be updated in the Business Continuity Plan.	The results of the Business Continuity Plan (BCP) tests will be recorded and reported to the Audit Committee. The BCP will be updated to reflect this. Responsibility: Roy Stanley, Information & communications technology and facilities manager Target Implementation Date: Completed	Recommendation implemented.
Recommendation 3 Issue: The draft Business Continuity Plan does not contain information to enable effective business continuity arrangements to be undertaken. Risk: The Business Continuity Plan is not effective in the event of an incident. Risk rating: Amber Recommendation: Prior to the finalisation of the Draft Business Continuity Plan the following should be considered for inclusion: • Review and approval process of the Business Continuity Plan	The recommendation is accepted and the listed items have been considered and incorporated as follows: • Review and approval process of the Business Continuity Plan – The plan is scheduled for review every three months by the ICT and Facilities Manager (the Core Plan Owner) and any relevant information such as structure charts and contact details updated. Any significant changes to the plan layouts will be referred to CMB for approval. • Scenario testing timetable – This timetable will be included within Appendix A which has been redrafted. It will be split into quarterly projected tasks over the next twelve months. • Reporting results of scenario testing – A third	Recommendation implemented.

Issue, Risk & Recommendation **Risk Management and Business Continuity Planning** **(May 2016)**	**Management Response**	**Current Position at June 2016**
• Scenario testing timetable • Reporting results of scenario testing • Business Impact Analysis review and update timetable • Roles and responsibilities of City of London, Agilisys and London Councils • Identification of critical systems and associated recovery time objective (RTO) • Relevant stakeholders	column will be added to Appendix A outlining the test results. • Business Impact Analysis (BIA) review and update timetable – This will be the responsibility of each of the BIA plan owners and the overall responsibility of the Silver Team leads as outlined in Sections 2 and 4 of the plan. • Roles and responsibilities of City of London, Agilisys and London Councils – This level of detail will be outlined within the 'Critical Systems and Associated RTO' document, currently being drafted, which will hold the more technical details to the plan. Their roles and responsibilities are also outlined in section 4 of the current ICT Strategy 2015-18 documents. • Identification of critical systems and associated recovery time objective (RTO) – This level of detail will also be outlined within the 'Critical Systems and Associated RTO' document which will hold the more technical details to the plan. • Relevant stakeholders – This is detailed within the current ICT Strategy 2015-18 document. Responsibility: Roy Stanley, Information & communications technology and facilities manager Target Implementation Date: Completed	

London Councils – Internal Audit Recommendations Log (June 2016) **Appendix C**

ICT Strategy (May 2016)

Risk rating	Recommendations	Accepted	Implemented	Outstanding
Red	0	0	0	0
Amber	1	1	0	0
Green	2	2	0	0
	3	**3**	**0**	**0**

Issue, Risk & Recommendation ICT Strategy (May 2016)	Management Response	Current Position at June 2016
Recommendation 1 Issue: No evidence was obtained of Disaster Recovery test exercises having been performed. Risk: Assurance cannot be provided that the IT element of Business Continuity will ensure availability of key services in the event of a disaster. Risk rating: Amber Recommendation: Disaster Recovery test exercises should be scheduled at the earliest opportunity to ensure continuity.	Recommendation accepted. London Councils have added a comprehensive testing plan to be carried out in conjunction with the City of London and Agilisys. The test plan along has been ratified by London Councils CMB and will reside in the current Business Continuity Plan (Appendix A, page 62-63) activity to commence April 2016. Testing results will be available in the quarterly updates of the BCP plan next due in July 2016. This will be implemented by August 2016. Responsibility: Roy Stanley, ICT and facilities manager Target Implementation Date: August 2016	Recommendation to be implemented by August 2016.

Issue, Risk & Recommendation **ICT Strategy** **(May 2016)**	**Management Response**	**Current Position at June 2016**
Recommendation 2 Issue: Disk storage thresholds are not documented. Additionally historical growth charts have not been provided to London Councils. Risk: Without formally documented arrangements LC cannot be sure the thresholds are as expected and potentially lower thresholds can result in system unavailability. Risk rating: Green Recommendation: Usage criteria should be formalised and regular review of storage utilisation considered by management.	Recommendation accepted. The activity will be carried out by Agilisys and reviewed at our monthly SLA meetings between CoL and Agilisys and commence during second quarter 2016/17 meetings. Responsibility: Roy Stanley, Roy Stanley, ICT and facilities manager Target Implementation Date: August 2016	Recommendation to be implemented by August 2016.
Recommendation 3 Issue: Checks are not performed to ensure third party compliance. Risk: Without periodic checks and provision of evidence such as compliance certificates it cannot be guaranteed that London Councils' interests are adequately safeguarded. Risk rating: Green Recommendation: Where compliance is the responsibility of a third party an annual compliance certificate should be obtained.	Recommendation accepted. Most if not all our principle third part contracts such as Lorry Control and ESP are up for renewal this year. London Councils will ensure these checks and evidence of compliance certificates are made available and incorporated into the requirements for renewal or into the new contracts. This will be actioned by September 2016 Responsibility: Roy Stanley, Roy Stanley, ICT and facilities manager Target Implementation Date: September 2016	Recommendation to be implemented by September 2016.

Priority risk rating key:

Green:	Low risk and/or weakness already been addressed
Amber:	Medium risk requiring mitigation and prompt action
Red	High risk, urgent action required