central midlands audit partnership

Derby City Council – Internal Audit Progress Report

(Covering the period November 2016toFebruary2017)

Audit & Accounts Committee: 22nd March 2017

Our Vision

Through continuous improvement, the central midlands audit partnership will strive to provide cost effective, high quality internal audit services that meet the needs and expectations of all its partners.

Contents

Contacts

Richard Boneham
Head of the Audit Partnership
c/o Derby City Council
Council House
Corporation Street
Derby
DE1 2FS
Tel. 01332 643280
richard.boneham@derby.gov.uk

Adrian Manifold
Audit Manager
c/o Derby City Council
Council House
Corporation Street
Derby
DE1 2FS
Tel. 01332 643281
adrian.manifold@centralmidlands audit.co.uk

CMAP central midlands audit partnership

Providing Excellent Audit Services in the Public Sector

Derby City Council – Internal Audit Progress Report

Summary

Role of Internal Audit

The Internal Audit Service for Derby City Council is provided by the Central Midlands Audit Partnership (CMAP). The Partnership operates in accordance with standards of best practice applicable to Internal Audit (in particular, the Public Sector Internal Audit Standards – PSIAS). CMAP also adheres to the Internal Audit Charter.

The role of internal audit is to provide independent assurance that the organisation's risk management, governance and internal control processes are operating effectively.

Recommendation Ranking

To help management schedule their efforts to implement our recommendations or their alternative solutions, we have risk assessed each control weakness identified in our audits. For each recommendation a judgment was made on the likelihood of the risk occurring and the potential impact if the risk was to occur. From that risk assessment each recommendation has been given one of the following ratings:

- Critical risk.
- Significant risk.
- Moderate risk.
- Low risk.

These ratings provide managers with an indication of the importance of recommendations as perceived by Audit; they do not form part of the risk management process; nor do they reflectthe timeframe within which these recommendations can be addressed. These matters are still for management to determine.

Control Assurance Definitions

Summaries of all audit reports are to be reported to Audit & Accounts Committee together with the management responses as part of Internal Audit's reports to Committee on progress made against the Audit Plan. All audit reviews will contain an overall opinion based on the adequacy of the level of internal control in existence at the time of the audit. This will be graded as either:

- **None** - We are not able to offer any assurance. The areas reviewed were found to be inadequately controlled. Risks were not being well managed and systems required the introduction or improvement of internal controls to ensure the achievement of objectives.
- **Limited** - We are able to offer limited assurance in relation to the areas reviewed and the effectiveness of the controls found to be in place. Some key risks were not well managed and systems required the introduction or improvement of internal controls to ensure the achievement of objectives.
- **Reasonable** - We are able to offer reasonable assurance as most of the areas reviewed were found to be adequately controlled. Generally risks were well managed, but some systems required the introduction or improvement of internal controls to ensure the achievement of objectives.
- **Comprehensive** - We are able to offer comprehensive assurance as the areas reviewed were found to be adequately controlled. Internal controls were in place and operating effectively and risks against the achievement of objectives were well managed.

This report rating will be determined by the number of control weaknesses identified in relation to those examined, weighted by the significance of the risks. Any audits that receive a None or

Derby City Council – Internal Audit Progress Report

Limited assurance assessment will be highlighted to the Audit & Accounts Committee in Audit's progress reports.

Audit Coverage

Progress on Audit Assignments

The following tables provide Audit & Accounts Committee with information on how audit assignments were progressing as at 28thFebruary 2017.

Audit Plan Assignments	Type of Audit	Current Status	% Complete
Independent Living Funds	Systems/Risk Audit	In Progress	65%
Transition to Adult Services for Disabled Young People	Systems/Risk Audit	Allocated	5%
SEND - Local Offer - Travel & Other Support	**Systems/Risk Audit**	**Final Report**	**100%**
Looked After Children (LAC) Strategy & Reviews	Systems/Risk Audit	Allocated	0%
Fostering Services	**Systems/Risk Audit**	**Final Report**	**100%**
Child Protection - Local Authority Designated Officer (LADO)	**Systems/Risk Audit**	**Final Report**	**100%**
Priority Schools Building Programme	Systems/Risk Audit	Cancelled	0%
Public Health - Pooled Budgets	Systems/Risk Audit	Fieldwork Complete	80%
Integrated Commissioning	Systems/Risk Audit	In Progress	55%
Business Intelligence	Systems/Risk Audit	Fieldwork Complete	80%
Data Quality & Performance	Governance Review	In Progress	35%
People Management	Systems/Risk Audit	Draft Report	95%
Grant Certification Work 2016-17	Grant Certification	Reviewed	90%
Main Accounting Systems 2016-17 - Reconciliations	Key Financial System	In Progress	75%
Treasury Management 2016-17	Key Financial System	In Progress	70%
Fixed Assets	Key Financial System	Allocated	5%
Taxation 2016-17	Systems/Risk Audit	In Progress	55%
Procurement Monitoring	Procurement/Contract Audit	In Progress	75%
Procurement Control	Procurement/Contract Audit	Allocated	0%
Capital Contracts	Procurement/Contract Audit	Allocated	5%
Revenue Contracts	Procurement/Contract Audit	Allocated	15%
Housing Benefits & Council Tax Support 2016-17	Key Financial System	In Progress	75%
Council Tax 2016-17	Key Financial System	Fieldwork Complete	80%
NDR 2016-17	Key Financial System	In Progress	75%
Revenues and Benefits System Project	Advice/Emerging Issues	In Progress	15%
Payroll 2016-17	Key Financial System	Fieldwork Complete	80%
Information Governance	**Governance Review**	**Final Report**	**100%**
Cyber Security	IT Audit	In Progress	70%
Liquid Logic Security Assessment	**IT Audit**	**Final Report**	**100%**
Website Review	IT Audit	Draft Report	95%
Income Management (Civica ICON)	IT Audit	In Progress	75%
MiPeople Application	**IT Audit**	**Final Report**	**100%**

Derby City Council – Internal Audit Progress Report

Active Directory	**IT Audit**	**Final Report**	**100%**
Derby Arena	**Systems/Risk Audit**	**Final Report**	**100%**
Section 106 Agreements	**Systems/Risk Audit**	**Final Report**	**100%**
Refuse Collection & Recycling	Systems/Risk Audit	In Progress	10%
Licensing	**Systems/Risk Audit**	**Final Report**	**100%**
Trading Standards	**Systems/Risk Audit**	**Final Report**	**100%**
Health & Safety	Governance Review	Draft Report	95%
Economic Regeneration	Systems/Risk Audit	In Progress	40%
External Funding	Systems/Risk Audit	In Progress	75%
Commercial Rents	Systems/Risk Audit	Draft Report	95%
Property Maintenance	Systems/Risk Audit	Allocated	30%
Highways & Engineering	Systems/Risk Audit	In Progress	50%
Peartree Junior School	Investigation	Draft Report	95%
Investigation - Residential Care Requisition	Investigation	In Progress	75%
Purchase Cards	**Anti-Fraud/Probity/Ethics**	**Final Report**	**100%**
Morleston Day Centre	**Anti-Fraud/Probity/Ethics**	**Final Report**	**100%**
Various Cash-ups	Anti-Fraud/Probity/Ethics	In Progress	65%
Farmers Market	**Anti-Fraud/Probity/Ethics**	**Final Report**	**100%**
Registrars	Anti-Fraud/Probity/Ethics	Reviewed	90%
Schools SFVS Self Assessment 2016-17	Schools	In Progress	75%
18 Schools SFVS Assessments (15 final report, 1 reviewed, 2 fieldwork complete)	Schools	Allocated	Various

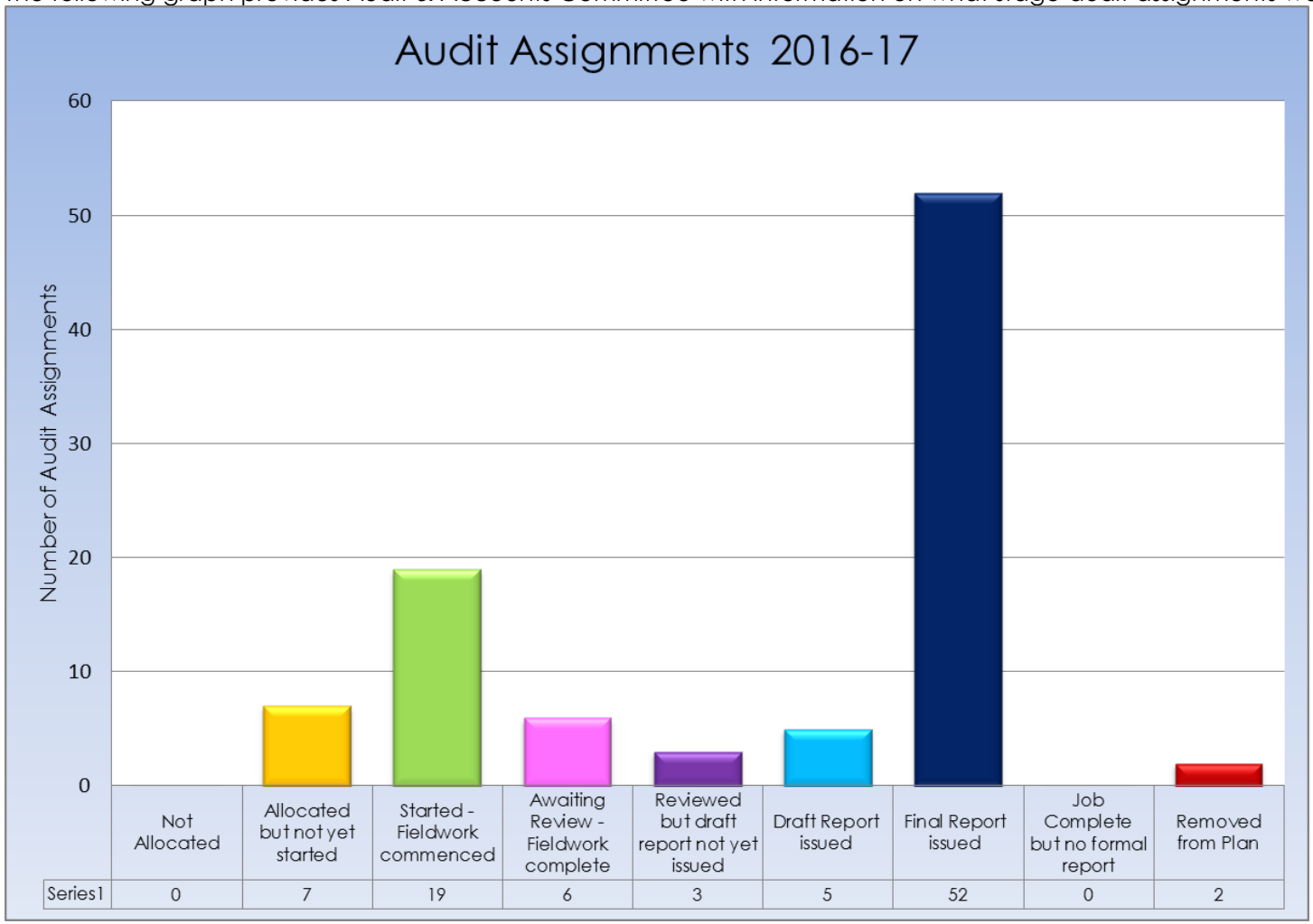
A further 23 finalised audits (not shown above) have already been reported to this Committee.

Derby City Council – Internal Audit Progress Report

Audit Coverage

Progress on Audit Assignments Chart

The following graph provides Audit & Accounts Committee with information on what stage audit assignments were atas at 28th February2017.



Derby City Council – Internal Audit Progress Report

Audit Coverage

Completed Audit Assignments

Between 12th November 2016and 28thFebruary2017 Internal Audit has completed the following 14 audit assignments for Derby City Council as well as 15 Schools SFVS reviews:

Audit Assignment	Overall Assurance Rating
SEND - Local Offer	Comprehensive
Foster Care	Reasonable
Child Protection	Reasonable
Information Governance	**Limited**
Liquid Logic Security Assessment	**Limited**
MiPeople Application	Reasonable
Active Directory	**Limited**
Derby Arena & XN Leisure System	**Limited**
Section 106 Agreements	Reasonable
Licensing	Reasonable
Trading Standards	Reasonable
Purchase Cards	**Limited**
Morleston Day Centre	**Limited**
Farmers Market	Reasonable

All audits leading to a rating of "Limited" or "None" will be brought to the Committee's specific attention. Accordingly, the 6 Limited assuranceaudit assignments highlighted above are brought to Committee's attention from this period.

We no longer provide full details of any Low risk recommendations where management has decided not to take any mitigating actions. These will still be highlighted to this Committee in the assignment summaries provided in these Progress reports. However, we will continue to provide full details of any Moderate, Significant or Critical risk issues where management has decided not to take any mitigating actions.

The following summarises the internal audit work completed in the period and seeks to highlight issues which Committee may wish to review in more detail at the next meeting.

Peoples

SEND - Local Offer

Overall Control Assurance Rating:**Comprehensive**

This audit focused on three different aspects of the SEND (Special Educational Needs and Disability) Local Offer; the controls and authorisation of home-to-school transport for qualifying students, the adequacy of controls on the provision of short breaks, and the effectiveness of the mediation service provided under legislative requirements.

From the 12 key controls evaluated in this audit review, 11 were considered to provide adequate control and 1 contained weaknesses. This report contained 1 recommendation which were considered to present a low risk.The following issue was considered to be the key control weakness:

- Some direct payments to parents/guardians of short break recipients had been subject to delay. (Low Risk)

The issue raised within this report was accepted and action was agreed to be taken by 1stApril 2017.

Foster Care

Overall Control Assurance Rating:**Reasonable**

This audit focused on reviewing the adequacy of controls within the systems in place for authorising, processing and monitoring of payments to Foster Carers in Derby.

From the 21 key controls evaluated in this audit review, 10were considered to provide adequate control and 11contained weaknesses. This report contained 8 recommendations, 6 of which were considered to present a low risk, the other 2 presenting a moderate risk.Another 2 minor risk issues have been highlighted for management's consideration.The following issues were considered to be the key control weaknesses:

- There was no cover for the Accountancy Officer which could lead to the Council being unable to fully process Foster Care payments in the event of an extended absence.(Low Risk)
- Details of rates paid to Carers were incorrect on the Council's website.(Low Risk)
- Details of payments on the Softbox system were being used to inform budget monitoring even though it did not include petty cash payments and overpayments recovered using Accounts Receivable invoices.(Low Risk)
- The current filing systems in use and the lack of a structured formal approach to defining the contents of emails in the subject field was both ineffective and inefficient leading to a waste of staff time.(Low Risk)
- Payment rates input manually to the Softbox system (for example when calculating staying put allowances) were out-of-date. There was no procedure in place to review rates used in ad-hoc calculations when rates were updated.(Low Risk)
- There was no evidence that payment runs were being checked for accuracy and completeness. (Moderate Risk)
- There were insufficient controls to prevent the creation of and payments to an unauthorised Carer. (Moderate Risk)
- Two remittance advice notes were being sent for one payment which could lead to confusion and additional work as a result of enquiries from Carers. (Low Risk)

All 8 issues raised within this report were accepted. Action had already been taken to address 4 of the issues raised by the end of the audit with action being taken to address the 2 moderate risk issues by 1st January 2017 and the remaining 2 issues by 31stMarch 2017.

Organisation & Governance

Information Governance

Overall Control Assurance Rating:**Limited**

This audit focused on ensuring that a sound and robust system was in place for responding to Subject Access Requests (SAR), in accordance with the Data Protection Act 1998. The audit also reviewed the processes in place regarding the Information Governance Sold Service to Schools.

From the 21 key controls evaluated in this audit review, 8 were considered to provide adequate control and 13contained weaknesses. This report contained 12 recommendations, 9 of which were considered to present a low risk, the other 3 presenting a moderate risk.The following issues were considered to be the key control weaknesses:

- The Council's Data Protection Act Policy was out-of-date and had not been reviewed in line with the documented timescale in May 2015. (Low Risk)
- The Council had not established a formal Code of Practice in support of its Data Protection Policy 1998, but had instead provided supplementary information in separate documents, which were not necessarily subject to review on a regular basis. (Low Risk)
- Whilst the Council had established a standard template form for a Subject Access Request (SAR), there were disparities between the information recorded on this form (available on the Council's website), a similar form on the internal intranet site and on the information pages relating to Data Protection both on the website and intranet. (Low Risk)
- As of November 2015, the Council was in the process of reviewing and updating its Records Retention Schedule. The

document continued to be a work in progress at the time of publishing and so did not include information that was required to ensure appropriate processes and controls were in place. (Low Risk)

- A process or guidance for undertaking checks on personal data had not been established. As such, some departments were undertaking checks to ensure personal data held was accurate, whilst others weren't. (Low Risk)
- All of the Rights of Individuals under Principle 6 of the Data Protection Act had not been detailed within key Data Protection documents or on the Council's website. (Low Risk)
- Redacted files and documents supplied to the requester were not checked by a second officer prior to issue.(Low Risk-**Risk Accepted**)
- Responses to SAR's were not currently being provided within the 40 calendar day statutory timeframe. (Moderate Risk)
- The Council had not yet established an Information Asset Register which would help speed up the process of locating the information required to respond to SAR's. (Moderate Risk)
- No checks were undertaken by Information Governance to ensure the schools requesting the Data Protection and Information Security Advice sold service had paid the appropriate charge. (Low Risk)
- The twice yearly newsletter, promoting awareness of information security, good practice tips and any legal issues, produced as part of the Schools sold service package, had not been produced since 2013. (Moderate Risk)
- The register of data controllers, maintained by the Information Governance team was not up-to-date, reflecting historic expiry dates where registrations had been found to have been renewed. In one case, a school had overlooked renewing its registration, resulting in an approximate 3 month delay before it was displayed as registered on the Information Commissioners website. (Low Risk)

All 12 issues raised within this report were accepted. Action had already been taken to address 5 of the issues raised by the end of the audit, with action being taken by 31st March 2017 to address a further 6 issues. Management decided to accept the risk in respect of the remaining issue raised and take no further action.

Liquid Logic Security Assessment

Overall Control Assurance Rating:**Limited**

This audit focused on the security and management of the Liquid Logic applications (LAS and LCS), as well as all server side components of the application, including application servers, database servers, and data warehouses. Testing covered all production, test and user acceptance testing deployment environments, where extracts of sensitive data about vulnerable adults and children were stored.

We were not able to provide assurances on the security of the universe used to report and analyse data within the Liquid Logic data warehouse environments, as evidence could not be provided within audit testing deadlines. When using Business Objects applications to query and report on a data warehouse, these applications access the database through a middle layer known as a universe, which also requires appropriate access controls.

An audit memo was issued on the 9th June 2016 relevant to this audit which detailed some urgent security issues for Management to address. These issues included unsupported database server software in operation, servers missing numerous critical Windows security updates, and a backup copy of the database exposed to every user in the network due to default access control lists. Although these security vulnerabilities were addressed during the audit, similar security vulnerabilities have been identified by audit testing conducted later in the assignment and these have again given rise to further recommendations in this report. This raises concerns about the adequacy of the actions being taken to address the underlying control weaknesses, if they are allowing such security vulnerabilities to reoccur.

Derby City Council – Internal Audit Progress Report

From the 69 key controls evaluated in this audit review, 47were considered to provide adequate control and 22 contained weaknesses. This report contained 10 recommendations 5 of which were considered to present a low risk and 5 presenting a moderate risk. Another 2 minor risk issues were also highlighted for management's consideration.The following issues were considered to be the key control weaknesses:

- There were a small number of users in Business Intelligence roles who had been assigned the DCC System Admin profile in the live LAS/LCS application. This did not appear to be appropriate or necessary based on their duties.(Low Risk)
- There were a number of SQL Server authentication accounts on the Liquid Logic SQL Servers, relating to users, which were not subject to password complexity or expiry policies.(Low Risk)
- There were a number of SQL Server accounts on the live, test and UAT database and data warehouse instances that had weak corresponding passwords, as they were set to "password", "Password01", mirrored the username, or "Controcc". This included 2 accounts on the PROD server with securityadmin server role permissions. (Moderate Risk)
- There were a large number of enabled accounts (40) who had been assigned sysadmin permissions on the live and test Liquid Logic database servers. This included officers in roles such as a finance assistant, which would typically not require complete unrestricted sysadmin level access over all databases on the production or test database server. (Moderate Risk)
- Over 100 accounts had been granted securityadmin server role permissions over the test Liquid Logic database server, and over 40 accounts had been assigned this server role over the live database server. This again included users in finance and accountancy roles. These permissions allow users to give themselves permissions to absolutely anything in these database servers, including access to any sensitive data in any table or view. (Moderate Risk)
- The SQL Server GUEST account was enabled in LCS_Live and LAS_Live databases on the production Liquid Logic database server. This means any accounts with access to any other databases on this instance (such as Controcc) can access these databases via the GUEST account, which may expose personal data to unauthorised access.(Low Risk)
- The transaction log was larger than the data file for a few databases on the production Liquid Logic database server, indicating that the transaction log backups are not being performed or not performed often enough, or insufficient capacity has been assigned. This had caused service outages for Controcc in recent weeks. (Low Risk)
- Both the live and UAT data warehouses were running an unsupported version of SQL Server (missing service pack 3, and 4 for SQL Server 2008 R2). The live and test database servers were also operating unsupported versions of SQL Server. This means they are not patched against newly discovered security vulnerabilities, and therefore the data is vulnerable to unauthorised exposure. The audit memo issued earlier in this assignment had already identified issues with security updates and software support which were addressed during this audit. (Moderate Risk)
- Unencrypted backups of the live Liquid Logic data warehouse were being written to a file share accessible to every user in the DerbyAD domain (almost 5000 accounts). This could expose highly personal and sensitive data to unauthorised access leading to data protection breaches. The audit memo issued earlier in this assignment had already identified an open backup, on a different file share housing a backup of the live Liquid Logic database, which was addressed during this audit. (Moderate Risk)
- None of the databases on the live data warehouse had been subject to a recent DBCC CHECKDB. It is a recommended

best practice to run these at minimum once every 2 weeks to identify data corruption issues as early as possible. (Low Risk)

All 10 of the issues raised were accepted and positive action had already been taken to address 6 of the issues raised by the end of the audit. The final 4 issues were agreed to be addressed by the 24thFebruary 2017.

MiPeople Application Audit

Overall Control Assurance Rating:**Reasonable**

This audit focused on reviewing the security, management and hosting of the MiPeople application, including the quality of service provided by the hosting and software providers.

We were unable to assess the security posture of the hosting provider's infrastructure, including specifically the application and database servers that provided the production environment for the instance of the MiPeople application used by Derby City Council. We were not permitted access to their infrastructure to run our own security assessment, and requesting the results of any vulnerability assessments and security analysis was identified as chargeable work by the hosting providers. The Council was not prepared to fund the chargeable work, and as such the scope was reduced to focus on the application security and the quality and contractual compliance of the service provision by the provider.

From the 23 key controls evaluated in this audit review, 18 were considered to provide adequate control and 5 contained weaknesses. This report contained 5 recommendations 4 of which were considered to present a low risk and 1 presenting a moderate risk.The following issues were considered to be the key control weaknesses:

- A number of unused accounts were still enabled in the System at the time of testing. This increases the risk of unauthorised access to personal and sensitive payroll data, which could lead to data protection breaches.(Low Risk)
- There was no formally defined, documented or implemented data retention policy for records processed by the application, such as personal and sensitive information about former employees, or personally identifiable data about unsuccessful job applicants. This could ultimately lead to non-compliance with data protection requirements (Low Risk)
- The Council did not have effective plans in operation for unexpected termination of the contract with the Provider (e.g. company goes out of business or the Council experiences unsatisfactory performance or costs).(Moderate Risk)
- There were no service level agreements specific to availability (uptime) in the contract.(Low Risk)
- The Council was not receiving sufficient information from the supplier to enable them to effectively monitor the quality of service being provided, including compliance against service level agreements.(Low Risk)

All 5 of the issues raised were accepted and positive action had already been taken to address 3 of the issues raised by the end of the audit. Of the 2 remaining issues, 1 moderate risk issue was agreed to be addressed by the end of February 2017, with the final issue being addressed by the end of March 2017.

Active Directory

Overall Control Assurance Rating:**Limited**

This audit focused on the security, design, configuration and management of the Council's Active Directory environment, including the DerbyAD (DerbyAD.net) and Partners (Partners.DerbyAD.net) domains.

From the 71 key controls evaluated in this audit review, 49 were considered to provide adequate control and 22 contained weaknesses. This report contained 10 recommendations 5 of which were considered to present a low risk and 5 presenting a moderate risk.Another 5 minor risk issues were also highlighted for

management's consideration.The following issues were considered to be the key control weaknesses:

- 656 accounts that were still enabled in the domain had not logged into the DerbyAD domain in over 90 days (or sometimes ever) and did not have an account expiration date value. From a sample of 25 stale accounts reviewed, some were found to have left the Council based on their payroll record, and others could not be found on Payroll or iDerby phonebook at all.(Moderate Risk)
- Accounts were being created and access related service requests actioned on the basis of requests from non-managerial officers, which violates the current policy that requires authorisation by line managers. (Low Risk)
- There were 187 devices in DerbyAD, and 10 devices in Partners, which had not logged into the domain in over 90 days, yet were still enabled in Active Directory. (Low Risk)
- Users with membership to high privilege security groups such as administrators or domain admins, did not appear to have a secondary lower privilege account for day to day activities, such as accessing Email or browsing the Internet.(Moderate Risk)
- It was possible to browse the Internet from a domain controller. (Low Risk)
- Access to high privilege security groups such as domain admins had not been restricted to authorised and current administrators. There were a large number of accounts in the domain admins group in DerbyAD which did not appear to be actively in use, and when challenged could not be justified. In general, the number of accounts in the group also seemed excessive, with over 100 accounts in the domain admins group in DerbyAD.(Moderate Risk)
- There were over 100 accounts with an associated @derby.gov.uk mailbox who had been configured with the password never expires option. This included a number of senior officers and Councillors. A general security concept is the longer a password goes unchanged the less protection it offers, and therefore granting this exemption to the policy to a large number of users, increases the risk to the Council's private network. (Low Risk)
- There were a small number of enabled domain admin accounts in both domains with weak corresponding passwords, which if compromised would give complete administrator access to every server and computer in the domain.(Moderate Risk)
- There were 4 enabled devices in the DerbyAD, (all of which had been in recent use), running Windows XP operating systems and 8 servers running Windows 2003 Server operating systems, both of which are no longer supported by Microsoft. Unsupported operating systems on computers and servers joined to the DerbyAD domain provide a security weakness, as newly discovered vulnerabilities are not patched by Microsoft.(Moderate Risk)
- The Domain Controller's OU (organisational units) in Partners domain and a number of OUs in both domains were not protected from accidental deletion. Furthermore, the AD recycle bin had not been enabled in either domain. Both of these go against best practice designs to reduce the impact and downtime of administrator error. (Low Risk)

All 10 of the issues raised were accepted and positive actions were agreed to address 1 issue by the end of February 2017, 1 issue by the 10thMarch 2017, 6 issues by the end of March 2017, 1 issue by the end of April 2017, and the final issue by the end of May 2017.

Communities & Place

Derby Arena & XN Leisure System

Overall Control Assurance Rating:**Reasonable**

This audit focused on:

- Reviewing the adequacy of controls in place around income collection, recording and banking

- Establishing that charges are accurately made for all chargeable services
- Reviewing the accuracy and completeness of membership records
- Understanding how usage of the Arena is monitored and addressed where necessary.

We have performed our work through discussion with officers, observation of processes, review of documentation, and sample testing where necessary.

The XN Leisure system is key to a number of the areas of focus above, and we have therefore performed additional testing over the system itself. The recommendations made based on this work are relevant across all three of the Council's leisure centres, as are a number of the other recommendations made in this report.

From the 69 key controls evaluated in this audit review, 45 were considered to provide adequate control and 24 contained weaknesses. This report contained 22 recommendations, 19 of which were considered to present a low risk, the other 3 presenting a moderate risk. Another minor risk issue was also highlighted for management's consideration.The following issues were considered to be the key control weaknesses:

- Discrepancies in float amounts were not recorded as being investigated. (Low Risk)
- Unders/overs reported during cashing up were not being consistently investigated by management. (Low Risk)
- Amounts on payment schedules could be amended by Customer Service Assistants without requiring Manager authorisation. (Low Risk)
- Void transactions were not being appropriately monitored by management. (Low Risk)
- The reconciliation between café income recorded and income received in the bank was not fully operational. (Low Risk)
- Lost property records were not accurate and complete. Valuable items were stored in the safe but not recorded, and valuable items recorded as lost property could not be located. (Low Risk)
- The ability to amend pricing was not appropriately restricted: any leisure centre manager was able to make amendments to the master prices held within XN Leisure. (Low Risk)
- Appropriate evidence was not always sought to confirm eligibility for concessionary membership.(Moderate Risk)
- Payment was not always received in advance of meetings or events booking. (Low Risk)
- Membership cancellation forms were not being processed promptly in all cases. (Low Risk)
- Membership suspensions were not always processed in response to unpaid direct debits and cancellations were not always processed when outstanding direct debit debts were not settled. (Low Risk)
- Notes were required on XN Leisure when a payment schedule was amended, however these were not always of sufficient quality to provide a clear rationale for the amendment. (Low Risk)
- Membership home sites were not being reviewed regularly to ensure they accurately reflect usage. (Low Risk)
- There were several file shares on the DCC-TLMSWEB01 server of the XN leisure application, that were openly accessible, often with full control, to every user in the DerbyAD domain, which at the time of the audit was over 5000 accounts. These shares included personal information about members, as well as financial information for BACS runs, including bank account names, numbers and sort-codes.(Moderate Risk)
- The XNLEISURE instance was operating a dangerous build of SQL Server, and was missing service pack 3. Whereas the current service pack level is supported until 10th January 2017, service pack 3 was released in 2015 and addresses a

number of dangerous known bugs which are corruption related. (Low Risk)

- There was a SQL authentication account on the XNLEISURE instance which had a weak corresponding password, as it mirrored the username. This account was found to have db_owner privileges over 4 databases on the XNLEISURE instance, which could be misused to corrupt the integrity of the data, which would impact the System and therefore end users.(Moderate Risk)
- Auto-shrink was enabled on a number of live databases on the XNLEISURE instance. This setting is a bad practice, and is well known to cause database fragmentation, which can ultimately lead to performance issues, and possible even service outages, which would affect the availability of the system, and therefore impact service delivery. (Low Risk)
- Page verification was set to TORN_PAGE and NONE on a number of live databases on the XNLEISURE instance. This is bad practice, especially where set to NONE, as the Council could face a situation where corrupt data is not recoverable without reverting back to old backups (pre-corruption), leading to major data loss to the system, and causing a significant disruption to service delivery. (Low Risk)
- The GUEST account was enabled in 16 databases on the XNLEISURE instance. Enabling the GUEST account in user databases on the XNLEISURE instance could expose sensitive data to unauthorised access. (Low Risk)
- We identified over 60 active accounts with no recent login activity within the past 6 months. When the list was provided, over 40 of these were immediately disabled by the systems administrator. There is a risk that failing to disable accounts when access is no longer required increases the likelihood that the personal and sensitive information processed by the application may be exposed to unauthorised users. (Low Risk)
- 3 users had been assigned the super admin security role, despite not being administrators of the system. And an ex administrator still had local admin rights over DCC-TLMSWEB01 server, which acted as the web server for the application. Failing to restrict administrator access at any tier of the system risks the availability, integrity and confidentiality of the system, which could impact Council service delivery. (Low Risk)
- There was no formally defined, documented or implemented data retention policy in place for the records processed by the System. This increases the likelihood that the Council could fail to comply with Principle 5 of the Data Protection Act. (Low Risk)

All 22 issues raised within this report were accepted and action had been taken to address 6 of the recommendations at the time of finalising the report. Action was agreed to address 11 of the issues by 21stFebruary 2017, 1 issue by 31stMarch 2017, 1 issue by 1stApril 2017, and the remaining 3 issues by 30thApril 2017.

Section 106 Agreements

Overall Control Assurance Rating:**Reasonable**

This audit focused on the policy and procedures relating to Section 106 agreements, monitoring arrangements, management of funds and ensuring that expenditure of Section 106 monies was in accordance with the terms of the agreement. Finally, the audit sought to ensure that appropriate monitoring arrangements were in place in respect of non-financial contributions.

From the 25 key controls evaluated in this audit review, 19 were considered to provide adequate control and 6 contained weaknesses. This report contained 6 recommendations all of which were considered to present a low risk. The following issues were considered to be the key control weaknesses:

- Detailed procedures had been established, but were dated April 2010 and made reference to officers who no longer worked at the Council. (Low Risk)
- The Planning Team maintained a database for recording information relevant to each Section 106 agreement, but not

all information, particularly in relation to key dates, was being recorded. (Low Risk)

- Calculations for index linked payments and late payment charges were not being checked by a second officer to ensure they were accurate. (Low Risk)
- Checks were being undertaken on S106 monies received by the Council, but there was no evidence to demonstrate that these checks were being undertaken. (Low Risk)
- Four Section 106 contributions had not been spent, despite the "use by" date being 31 July 2016. (Low Risk)
- No monitoring was being undertaken in respect of planning obligations relating to non-financial contributions. (Low Risk)

All 6 issues raised within this report were accepted. Action had already been taken to address one of the issues raised by the end of the audit with action being taken to address 2 issues by 31st January 2017 another by 28th February 2017; a further issue will be addressed by 1st June 2017 with action taken on the remaining issue by 1st September 2017.

Licensing

Overall Control Assurance Rating:**Reasonable**

This audit focused on reviewing processes within the Council's Licensing Team (in relation to animal welfare, exhumations, charitable collections and Mobile Home sites) and associated financial management, to provide assurance as to the adequacy of controls within the processes.

From the 20 key controls evaluated in this audit review, 11 were considered to provide adequate control and 9 contained weaknesses. This report contained 7 recommendations all of which were considered to present a low risk. Another 2 minor risk issues were highlighted for management's consideration.The following issues were considered to be the key control weaknesses:

- A review had not recently been undertaken to update procedural guidance in place to support the process to administer licences relating to animal welfare and the process to oversee an exhumation. (Low Risk)
- A record to evidence the presence of the Environmental Health Officer, at an exhumation administered by Bereavement Services was not being maintained. (Low Risk)
- The cost of Licensing Officers' (EHO) time for attendance at exhumations was not being included in the calculation of the fee charged to the Licensee. (Low Risk)
- Invoices for the annual billing for licence fees and fee renewals, numbering around 600, were being raised manually and input to the system individually, which was resource intensive. (Low Risk)
- The Licensing Team was not receiving reports on the income suspense account from Accountancy for them to monitor and identify income belonging to them. (Low Risk)
- Debts submitted for approval for write-off had not been fully investigated as they included existing customers in receipt of other Council services for which either normal payments were being made or arrangements to repay debts were in place. (Low Risk)
- Mobile home sites had not been inspected to ensure that the number of homes on site and other licence conditions were being adhered with. (Low Risk)

All 7 issues raised within this report were accepted. Positive action had already been taken to address 6 recommendations by the end of the audit. Further positive action was agreed for the remaining recommendation to be addressed by 1st April 2017.

Trading Standards

Overall Control Assurance Rating:**Reasonable**

This audit focused on reviewing the adequacy of controls over the process in place for:

- Devising the annual planned programme of inspections undertaken by Trading Standards.

- The logging and managing of referrals and complaints.
- The management monitoring and reporting arrangements.

From the 26 key controls evaluated in this audit review, 16 were considered to provide adequate control and 10 contained weaknesses. This report contained 8 recommendationsall of which were considered to present a low risk. Another minor risk issue was highlighted for management's consideration. The following issues were considered to be the key control weaknesses:

- Although there were standard criteria used to assess each business, the rationale for determining the risk assessment score was not summarised and recorded in a clear and concise manner as part of the formal risk assessment process. (Low Risk)
- The 2016/17 Food and Feed Law Enforcement Plan had not been authorised by the Director of Environmental and Regulatory Services and approved by Members on a timely basis. (Low Risk)
- A standard format was not being used consistently for reporting back to traders, the outcomes and recommendations from inspections undertaken by Trading Standards Officers.(Low Risk)
- Access permissions to documents that were relevant to trading standards inspection and investigations were not properly restricted. (Low Risk)
- The Council website had a dedicated webpage on scam alerts but did not have a dedicated telephone number with answer phone that would be available for the public 24 hours a day. (Low Risk)
- The routine updates on the operational activities and the status of all the jobs that had been allocated were not recorded in a standard format that were consistently reviewed and updated on a regular basis. (Low Risk)
- There were no formal periodic reporting arrangements in place to update senior management on departmental performance and the progress made to achieve the annual plan. (Low Risk)
- There was no hospital accident scheme in place whereby the Council's Trading Standards team would be notified of injuries caused by unsafe goods and services. (Low Risk)

All 8 control issues raised within this report have been accepted and positive action has been agreed to address one by 16thDecember 2016 and the other 7 by 1stApril 2017.

Anti-Fraud / Probity Work

Purchase Cards

Overall Control Assurance Rating:**Limited**

This audit focused on the issue and appropriate use of corporate purchase cards. This audit took place as part of a wider audit probity programme and was not notified to management in advance of the audit.

From the 16 key controls evaluated in this audit review, 8 were considered to provide adequate control and 8 contained weaknesses. This report contained 7 recommendations, 1 of which was considered to present a low risk, the other 6 presenting a moderate risk. Another minor risk issue was highlighted for management's consideration. The following issues were considered to be the key control weaknesses:

- The Procurement Card Policy was still in draft and as such had not been published.(Moderate Risk)
- A number of purchase cards had been issued to staff without authorisation of the Director of Finance. (Moderate Risk)
- Not all current purchase card holders had signed the purchase card acknowledgement/agreement.(Moderate Risk)
- The purchasing activity of individual cardholders was not reviewed which may mean that cards which were rarely or never used had not been highlighted. This may afford a

greater opportunity for the card to be lost or used fraudulently.(Moderate Risk)

- Cardholders were using their cards to purchase goods which were available through corporate food provision contracts. (Low Risk)
- Transactions logs were not always submitted promptly to Accountancy, to enable expenditure posted to the miscellaneous budget code on the General Ledger to be reallocated appropriately.(Moderate Risk)
- There were inconsistencies in the retention of receipts to validate expenditure and not all transaction logs had been authorised.(Moderate Risk)

All 7 of the control issues raised within this report were accepted and positive action had already been taken for 2 of the issues by the end of the audit. For the remaining issues, action was agreed to be undertaken by 1stApril 2017 for 2, another by 2ndMay 2017 with the remaining 2 issues actioned by 1stOctober 2017.

Morleston Day Centre

Overall Control Assurance Rating:**Limited**

This audit focused on the controls in operation over various financial procedures at Morleston Day Centre. This was an unannounced visit that took place as part of a wider audit probity programme.

From the 50 key controls evaluated in this audit review, 32 were considered to provide adequate control and 18 contained weaknesses. This report contained 13 recommendations, 7 of which were considered to present a low risk, the other 6 presenting a moderate risk. The following issues were considered to be the key control weaknesses:

- Auditors were allowed to enter restricted parts of the Centre and given access to cash without being asked for identification. (Low Risk)
- The number of safe key holders exceeded the limits prescribed in the Council's Cash Handling Policy. (Moderate Risk)
- The overnight insurance limit for cash held in the safe at the Centre was being exceeded. (Low Risk)
- A note of the receipt number issued to customers who had made a payment was not being logged on the attendance register. (Low Risk)
- There was no assurance that a large proportion of customers were making the correct level of contribution towards their use of the day centre.(Moderate Risk)
- The banking sheet was not signed dated and countersigned by the responsible officer and senior manager. The transfer of monies between staff was not formally recorded. (Low Risk)
- Receipt pads were not being kept securely when not in use.(Moderate Risk)
- A stock record of receipt pads held at the Centre was not maintained.(Moderate Risk)
- Banked income was not being recorded and allocated to the correct budget in the E Return system. (Low Risk)
- A formal Advisory Committee had not been established for the Amenity Fund. (Low Risk)
- Quarterly Statements were not being prepared for the Amenity Fund and there was no evidence of independent scrutiny of the account's transactions or balances.(Moderate Risk)
- An annual statement had not been produced for the Amenity fund. (Low Risk)
- The Centre Manager had pre-signed some blank cheques for the Amenity Fund and cheque payments were not being recorded in the transaction log.(Moderate Risk)

All 13 of the control issues raised within this report were accepted and positive action had already been implemented for 8 of the

issues by the end of the audit. Action will be taken by 31st January 2017 for 2 of the issues. For the other 3 issues, action was agreed to be undertaken by 28th February 2017.

Farmers Market

Overall Control Assurance Rating: **Limited**

This audit focused on the controls in operation over various financial procedures relating to income collection at the Farmers Market. This was an unannounced visit that took place as part of a wider audit probity programme.

From the 6 key controls evaluated in this audit review, 1 was considered to provide adequate control and 5 contained weaknesses. This report contained 5 recommendations all of which were considered to present a moderate risk. The following issues were considered to be the key control weaknesses:

- A stock record of controlled stationery items (receipt pads) was not being maintained.(Moderate Risk)
- Receipt pads were not being kept securely.(Moderate Risk)
- The register of stallholders' attendance and payment methods was not being matched to records of receipts issued or to income records for confirmation that income due from all stall holders had been collected/received. The spreadsheet was also not adequately protected from potential unauthorised amendments. (Moderate Risk)
- There were no formal records of signatures obtained when money was transferred between employees of the Council as per Financial regulations.(Moderate Risk)
- Income records were not being reconciled with the General Ledger to provide assurance that all income collected was being allocated to the correct cost centre.(Moderate Risk)

All 5 of the control issues raised within this report were accepted and positive action had already been taken for 4 of the issues by the end of the audit. For the remaining issue, action was agreed to be undertaken by 1st January 2017.

Derby City Council – Internal Audit Progress Report

Audit Performance

Customer Satisfaction

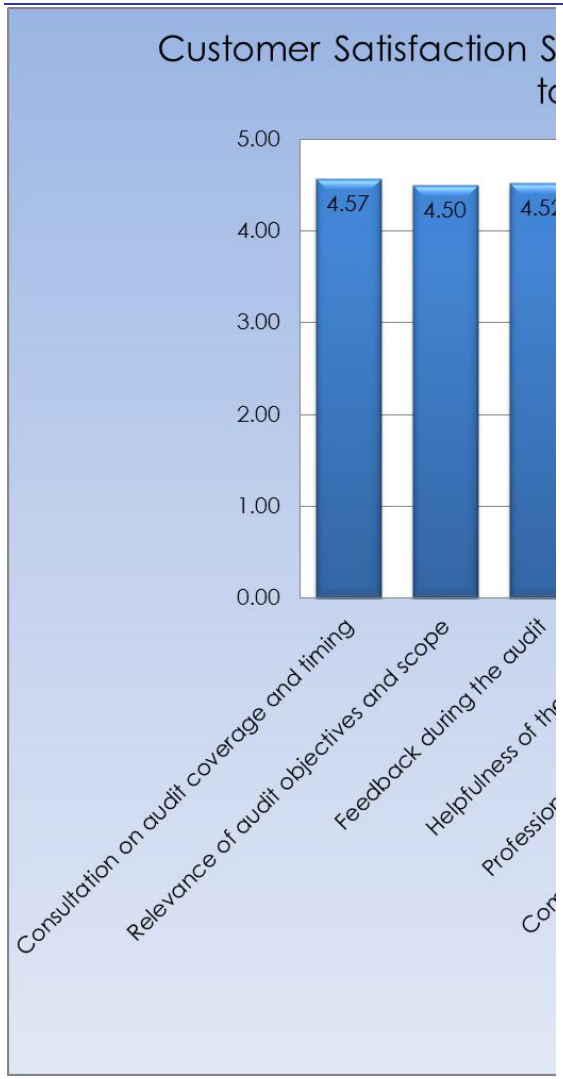
The Audit Section sends out a customer satisfaction survey with the final audit report to obtain feedback on the performance of the auditor and on how the audit was received. The survey consists of 11 questions which require grading from 1 to 5, where 1 is very poor and 5 is excellent. The chart across summarises the average score for each question from the 127 responses received between 1st April 2013 and 10thMarch 2016. The overall average score from the surveys was 50.3 out of 55. The lowest score received from a survey was 29, whilst the highest was 55 which was achieved on 45 occasions.

The overall responses are graded as either:

- Excellent (scores 47 to 55)
- Good (scores 38 to 46)
- Fair (scores 29 to 37)
- Poor (scores 20 to 28)
- Very poor (scores 11 to 19)

Overall 95 of 127 responses categorised the audit service they received as excellent, another 29 responses categorised the audit as good and 3 categorised the audit as fair. There were no overall responses that fell into the poor or very poor categories.

Derby City Council – Internal Audit Progress Report



Derby City Council – Internal Audit Progress Report

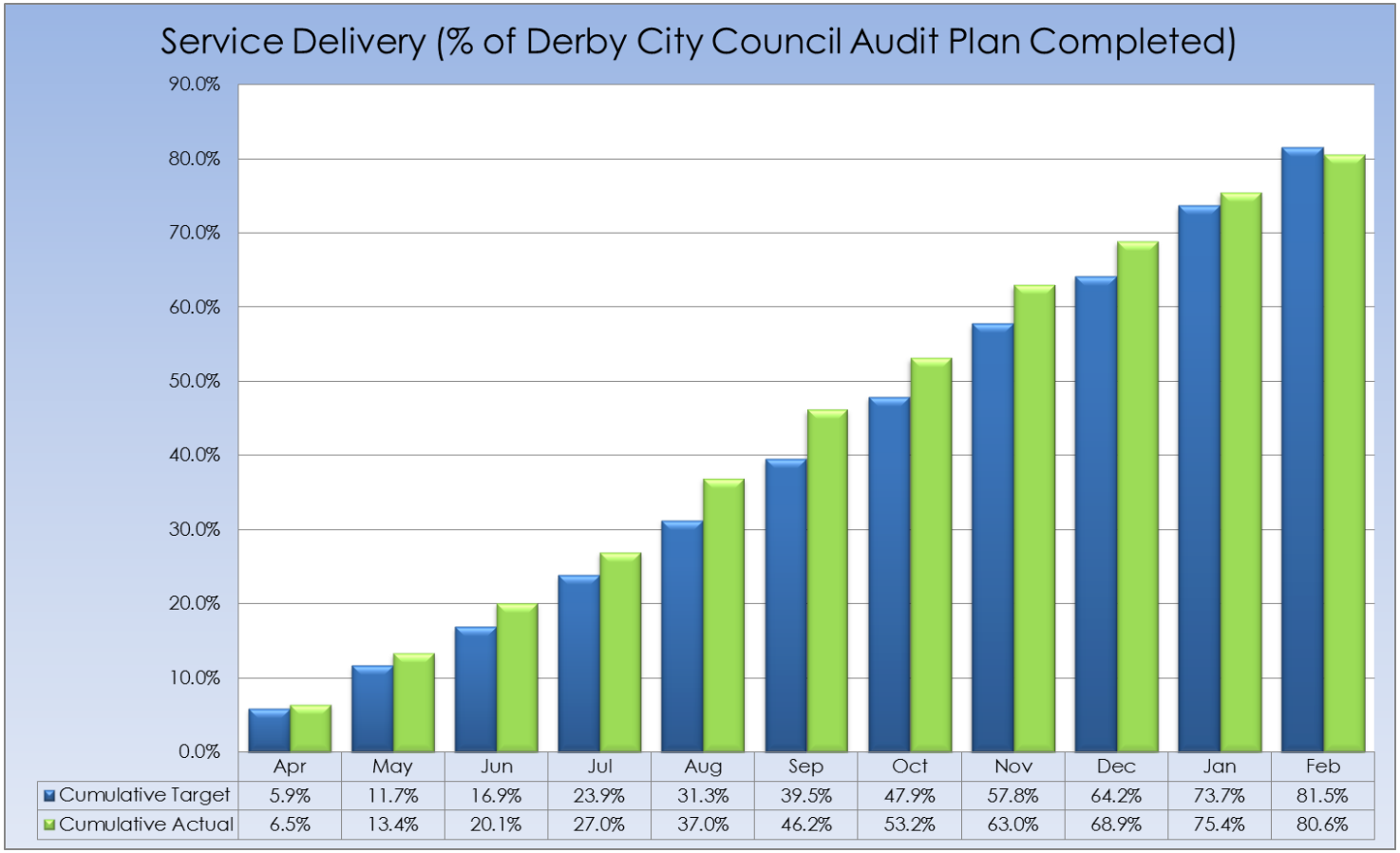
Audit Performance

Service Delivery (% of Audit Plan Completed)

At the end of each month, Audit staff provide the Audit Manager with an estimated percentage complete figure for each audit assignment they have been allocated. These figures are used to calculate how much of each Partner organisation's Audit Plans have been completed to date and how much of the Partnership's overall Audit Plan has been completed.

Shown across is the estimated percentage complete for Derby City Council's 2016-17 Audit Plan (including incomplete jobs brought forward) after 11 months of the Audit Plan year.

For the first time, the monthly target has been profiled to reflect the expected productive time available each month, but still assumes that time will be spent evenly over each partner organisation in proportion with their contributions which is not always the case.



	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb
Cumulative Target	5.9%	11.7%	16.9%	23.9%	31.3%	39.5%	47.9%	57.8%	64.2%	73.7%	81.5%
Cumulative Actual	6.5%	13.4%	20.1%	27.0%	37.0%	46.2%	53.2%	63.0%	68.9%	75.4%	80.6%

Derby City Council – Internal Audit Progress Report

Recommendation Tracking

Follow-up Process

Internal Audit has sent emails, automatically generated by our recommendations database, to officers responsible for action where their recommendations' action dates have been exceeded. We will request an update on each recommendation's implementation status, which will be fed back into the database, along with any revised implementation dates.Each recommendation made by Internal Audit will be assigned one of the following "Action Status" categories as a result of our attempts to follow-up management's progress in the implementation of agreed actions. The following explanations are provided in respect of each "Action Status" category:

- **Blank(Due)** = Action is due and Audit has been unable to ascertain any progress information from the responsible officer.
- **Blank (Not Due)** = Action is not due yet, so Audit has not followed up.
- **Implemented** = Audit has received assurances that the agreed actions have been implemented.
- **Superseded** = Audit has received information about changes to the system or processes that means that the original weaknesses no longer exist.
- **Being Implemented** = Management is still committed to undertaking the agreed actions, but they have yet to be completed. (This category should result in a revised action date)
- **Risk Accepted**= Management has decided to accept the risk that Audit has identified and take no mitigating action.

Implementation Status Details

Reports to Committee are intended to provide members with an overview of the current implementation status of all agreed actions to address the control weaknesses highlighted by audit recommendations made between 1stApril 2013 and 10thMarch 2017. All recommendations made prior to this period have now been resolved.

	Implemented	Being Implemented	Risk Accepted	Superseded	Action Due	Future Action	Total
Low Risk	400	23	23	2	10	41	**499**
Moderate Risk	146	9	8	3	2	23	**191**
Significant Risk	5	2	1	1	0	1	**10**
Critical Risk	1	0	0	0	0	0	**1**
Totals	**552**	**34**	**32**	**6**	**12**	**65**	**701**

The table below shows those recommendations not yet implemented by Dept.

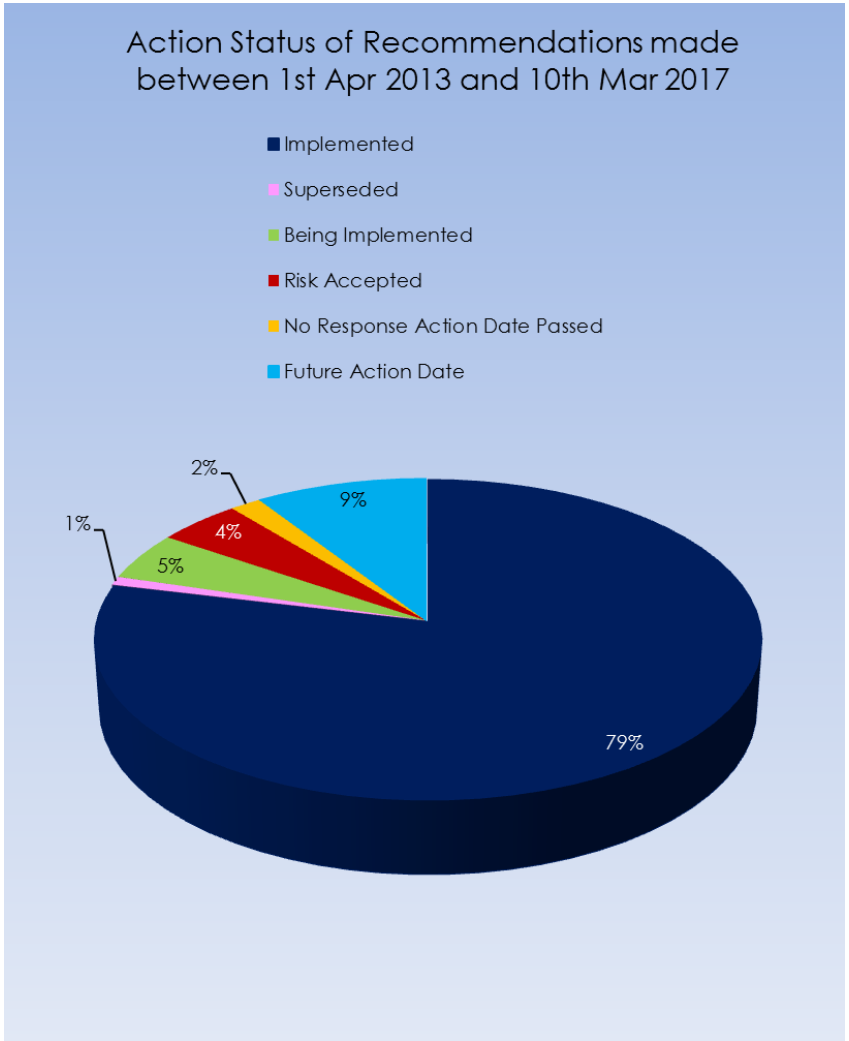
Recommendations Not Yet Implemented	Anti-Fraud & Corruption	People Services	Organisation & Governance	Communities & Place	TOTALS
Being Implemented	4	4	23	3	**34**
Action Due	0	8	3	1	**12**
	4	**12**	**26**	**4**	**46**

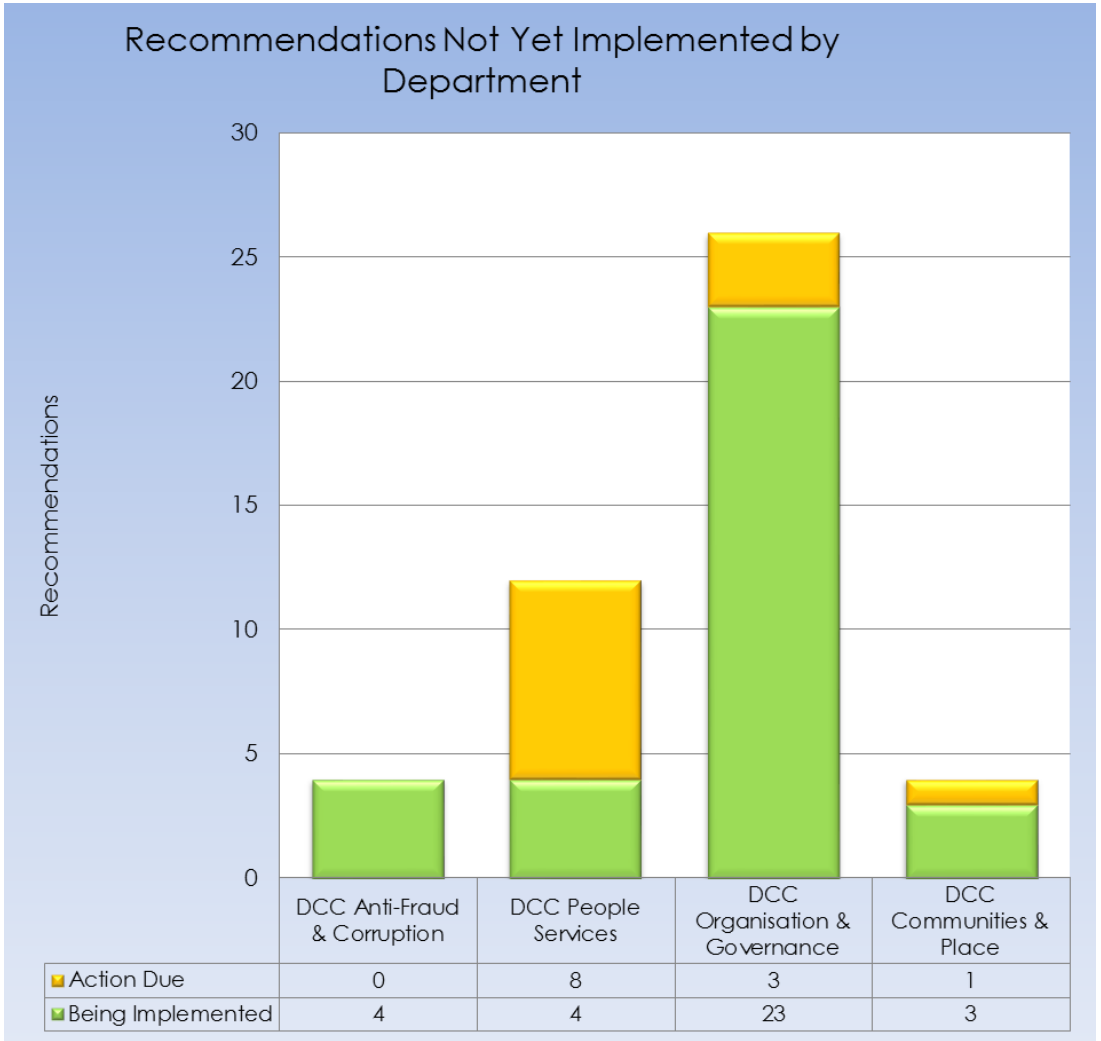
Internal Audit has provided Committee with summary details of those recommendations still in the process of 'Being Implemented' and those that have passed their duedate for implementation. 31 of the risk accepted issues shown above have already been reported to this Committee. Management has chosen to accept the risk on another low risk issue that has been highlighted in the body of this report.

Derby City Council – Internal Audit Progress Report

Recommendation Tracking

Implementation Status Charts





Derby City Council – Internal Audit Progress Report

Recommendation Tracking

Recommendations Not Yet Implemented

Anti-Fraud & Corruption

Audit Assignment	No. of Recs Still Being Implemented	No. of Recs Where Action is Due & we are Unable to Obtain a Response	Final Report Date
Vulnerable Adults Payments	1	0	12-Oct-16
Morleston Day Centre	3	0	23-Dec-16
Total No. of Outstanding Recommendations	**4**	**0**	

People's Services

Audit Assignment	No. of Recs Still Being Implemented	No. of Recs Where Action is Due & we are Unable to Obtain a Response	Final Report Date
Fostering Services	0	3	21-Dec-16
Market Development (Adult Social Care)	4	0	24-Aug-16
Child Protection - Local Authority Designated Officer (LADO)	0	5	18-Nov-16
Total No. of Outstanding Recommendations	**4**	**8**	

Communities & Place

Audit Assignment	No. of Recs Still Being Implemented	No. of Recs Where Action is Due & we are Unable to Obtain a Response	Final Report Date
Derby Arena	0	1	08-Feb-17
Asset Management & Estates	2	0	03-Mar-15
Markets	1	0	19-Nov-13
Total No. of Outstanding Recommendations	**3**	**1**	

Derby City Council – Internal Audit Progress Report

Organisation & Governance

Audit Assignment	No. of Recs Still Being Implemented	No. of Recs Where Action is Due & we are Unable to Obtain a Response	Final Report Date
Creditors 2015-16	1	1	05-Aug-16
Payroll 2015-16	4	0	23-May-16
Information Governance	1	1	18-Nov-16
RIPA	1	0	21-Sep-16
Housing Benefits & Council Tax Support 2015-16	2	0	28-Jan-16
Main Accounting System (MTFP) 2015-16	0	1	10-Nov-16
MiPeople Application Audit	1	0	09-Jan-17
EDRMS Application	1	0	02-Feb-16
Business Support	1	0	28-Aug-15
Configuration Management	3	0	22-Apr-15
Network Access Management	1	0	15-Jul-15
Wireless Network Infrastructure	3	0	31-Mar-16
Active Directory	1	0	18-Jan-17
Data Quality 2013-14	2	0	17-Dec-14
VOIP Security Assessment	1	0	12-Dec-13
Total No. of Outstanding Recommendations	**23**	**3**	

Derby City Council – Internal Audit Progress Report

Recommendation Tracking

Highlighted Recommendations

We have included this section of this report to bring recommendations to your attention for either of the following reasons:

- Any Moderate, Significant or Critical risk recommendations (either being implemented or with no response) that have passed their original agreed implementation date.
- Any Low risk recommendations still being implemented where it has been more than a year since the original agreed implementation date or those with no responsewhere it has been more than 3 months since the original agreed implementation date.

Community & Places

Asset Management & Estates

Control Issue1 - The asset list submitted for insurance did not reflect asset transactions undertaken outside of the Estates Section. The SAM system had not been updated as there was no process for notifying Estates of these changes.

Risk Rating – Significant Risk

Status Update - The revised Corporate Landlord Policy and Procedure is at draft stage and is being reviewed. This will enforce all property transactions to be approved by the Head of Strategic Asset management and estates and will ensure that transactions do not take place outside of the SAM system. There will be some system updates required to allow for full automation of notifications between the various key teams (legal, maintenance, insurance, capital accounts) which will enhance the information flow between teams.

Original Action Date 1 Sep 15 Revised Action Date 31Dec 16

Control Issue5–Some data relating to changes in the commercial property estate was not being routinely shared with other Sections who need the information.

Risk Rating – Low Risk

Status Update –this issue will be resolved when the revised Corporate Landlord Policy and Procedure is in place, as this will ensure that all transactions take place under SAM, and this will include the NDR and GIS information streams.

Original Action Date 1 Sep 15 Revised Action Date 31 Dec 16

Derby City Council – Internal Audit Progress Report

Markets

Control Issue 4 –There was no approved Council policy in place for offering concessions on rental charges to market stall traders in the Council's three markets.

Risk Rating – Moderate Risk

Status Update –Transfer of the Eagle Marker to INTU is imminent and the closure of the Cattle and Wholesale markets is expected to go ahead soon such that in the not too distant future only the Market Hall will be left. It is anticipated that it will be far easier to establish a concessionary model for the Market Hall, especially as leases are shortly due for renewal. It is proposed to establish a Markets Stall Holders Leaflet which it is intended will contain details on any future concessionary model.

Original Action Date 1 Jan 14 Revised Action Date 31 Mar 17

Organisation & Governance

Data Quality 2013-14

Control Issue 6 –There was no documented methodology for the collection and recording of the Street Cleanliness performance data.

Risk Rating – Low Risk

Status Update –The reason for the delay was the planned implementation of a consolidated online form within Lagan and hence a change to the process. This is no longer happening so the process remains the same. Work needs to be undertaken by the Performance and Intelligence Team to try and streamline the reports and add on any extra filters needed to improve the collation and reporting process. New planned date for implementation by the end of March 2017.

Original Action Date 31 Mar 15 Revised Action Date 1 Apr 17

Control Issue 7 –The Compiling Officer was required to undertake additional filtering of the information reported from the Lagan system in order to identify the required information. This process could be open to error and may compromise the integrity of the performance data.

Risk Rating – Low Risk

Status Update –The reason for the delay was the planned implementation of a consolidated online form within Lagan and hence a change to the process. This is no longer happening so the process remains the same. Work needs to be undertaken by the Performance and Intelligence Team to try and streamline the reports and add on any extra filters needed to improve the collation and reporting process. New planned date for implementation by the end of March 2017.

Original Action Date 31 Mar 15 Revised Action Date 1 Apr 17

Network Access Management

Control Issue 2 –We found 50,622,078 instances across the 6 Council File Servers, where a user, group or service account had full control of the contents of a folder. This included 74,180 instances where the Everyone group had full control and 122,222 instances where the BUILTIN\Users group had full control.

Risk Rating – Significant Risk

Status Update –The Head of ICT has discussed this issue with the infrastructure team and full control permission should not now being implemented, formalising this in policies, completed by Q4.

Original Action Date 31Mar 16 Revised Action Date 1Apr 17

Derby City Council – Internal Audit Progress Report

VOIP Security Assessment

Control Issue 1 –We found that neither VoIP data nor signalling media were encrypted to prevent voice conversions being recorded by malicious users.

Risk Rating – Moderate Risk

Status Update –Still busy, implementation in progress

Original Action Date 31 Jul 14 Revised Action Date 1 Apr 17

Creditors 2015-16

Control Issue 1 –Accounts Payable Section was no longer able to undertake regular checks to highlight duplicate payments. Reliance was being placed on the budget monitoring work of Accountancy to highlight potential duplicate payments.

Risk Rating – Moderate Risk

Status Update –No Response Received

Original Action Date 1 Sep 16 Revised Action Date n/a

Payroll 2015-16

Control Issue2–Managers had not been consistently carrying out checks on MOT certificates, driving licences or insurances which contributed to ensuring that officers met the legally required driving standards.

Risk Rating – Moderate Risk

Status Update –Work was progressing in the summer, but the responsible officer has been on long term sick and is just back at work.

Original Action Date 31Oct 16 Revised Action Date 31 Mar 17

Configuration Management

Control Issue 1 –There were no formally defined or documented requirements around configuration management data scope, span or granularity. Without formally defining and documenting requirements around data capture and maintenance within a CMDB (Configuration Management Database), there is no platform on which to identify defects, data quality issues and non-compliance problems.

Risk Rating – Moderate Risk

Status Update –Policies to be reviewed by the end of Q4.

Original Action Date 31Dec 15 Revised Action Date 1Apr 17

Control Issue 4 –There were no formally defined, documented or implemented procedures for auditing and verifying the accuracy of data within the CMDB. Documented audit and verification procedures are crucial to validate and improve the accuracy and completeness of the CMDB, to ensure timely and accurate data is available for resolving IT incidents and considering changes.

Risk Rating – Moderate Risk

Status Update –Policies to be reviewed by the end of Q4.

Original Action Date 31 Dec 15 Revised Action Date 1 Apr 17

Derby City Council – Internal Audit Progress Report

Wireless Network Infrastructure

Control Issue 4 –There was no Intrusion Detection/Prevention System in place on the wireless network despite there being known security vulnerabilities that could be prevented through the deployment of such a system.

Risk Rating – Moderate Risk

Status Update –We will get updata to scope and cost a project and the implementation over an 802.1x policy will be dependant on whether to fund the project. - Data centre move end of march - (the quotation and implementation will be effected by the data centre move scheduled to take place in Q4).

Original Action Date 1 Jun 16 Revised Action Date 1Jun 17

Control Issue 7 –Security vulnerabilities identified in penetration scans undertaken by the third party security consultancy had not been addressed.

Risk Rating – Moderate Risk

Status Update –We will get updata to scope and cost a project and the implementation over an 802.1x policy will be dependant on whether to fund the project. - Data centre move end of march - (the quotation and implementation will be effected by the data centre move scheduled to take place in Q4).

Original Action Date 1 Apr 16 Revised Action Date 1Jun 17

MiPeople Application Audit

Control Issue3–The Council did not have effective plans in operation for unexpected termination of the contract with the Provider (e.g. company goes out of business or the Council experiences unsatisfactory performance or costs).

Risk Rating – Moderate Risk

Status Update –We are exploring how easy it is for someone in Procurement to check the financial position of the provider so we have an early warning system of company financial problems but also looking to re-negotiate the terms of the contract through an early extension so we could discuss this with the provider at the same time.

Original Action Date 28Feb 17 Revised Action Date 31 May 17

Peoples Services

Child Protection

Control Issue6 - The employer was not required to confirm and formally notify the LADO when a referral was reported to the Disclosure and Barring Service, Ofsted and any other regulatory body.

Risk Rating – Moderate Risk

Status Update – No response received.

Original Action Date 28Feb 17 Revised Action Date n/a

Anti-Fraud & Corruption

Morleston Day Centre

Control Issue11 - Quarterly Statements were not being prepared for the Amenity Fund and there was no evidence of independent scrutiny of the account's transactions or balances.

Risk Rating – Moderate Risk

Status Update – The current clerk (from the clerical hub) will no longer be working for us so there is no clerical support. I will raise this at the next management meeting in March 2017.

Original Action Date 28 Feb 17 Revised Action Date 30Mar 17

Derby City Council – Internal Audit Progress Report