

Division(s): N/A

AUDIT and GOVERNANCE COMMITTEE – 6 September 2017

INTERNAL AUDIT 2017/18 PROGRESS REPORT

Report by the Director of Finance

INTRODUCTION

1. This report provides an update on the Internal Audit Service, including resources, completed and planned audits and an update on counter-fraud activity.

RESOURCES

2. A full update on resources was made to the Audit and Governance Committee in April 2017 as part of the Internal Audit Strategy and Plan for 2017/18. There have been no changes to resources since that update. We agreed to cover the 6 month maternity leave absence of the Principal Auditor with a seconded resource from an external firm. This placement has been arranged and will commence in September.
3. The two Auditors within our team are currently undertaking professional study, both are undertaking the IIA's Certified Internal Auditor Qualification, both have passed their second exams and are due to sit further exams in December.

2017/18 INTERNAL AUDIT PLAN - PROGRESS REPORT

4. The 2017/18 Internal Audit Plan, which was agreed at the 26 April Audit & Governance Committee, is attached as Appendix 1 to this report. This shows current progress with each audit.
5. There have currently been no amendments to the plan for 2017/18. The plan and plan progress will be reviewed with the individual directorate leadership teams during September and October.
6. There have been 6 audits concluded since the last update (provided to the April meeting of the Audit and Governance Committee); summaries of findings and current status of management actions are detailed in Appendix 2. The completed audits are as follows:

Directorate	2017/18 Audits	Opinion
ICT	Cyber Security	Amber
ICT	Disposal of ICT equipment	Amber
Adults	Payments to Residential and Home Support Providers	Amber
Corporate / ICT	Digital First Platform - Programme Governance Review	Amber
Corporate	Travel and Expenses - proactive fraud review	Green
Corporate	Procurement Cards - proactive fraud review	Amber

PERFORMANCE

7. The following performance indicators are monitored on a monthly basis.

Performance Measure	Target	% Performance Achieved for 17/18 audits (as at 21/8/17)	Comments
Elapsed time between start of the audit (opening meeting) and Exit Meeting.	Target date agreed for each assignment by the Audit manager, stated on Terms of Reference, but should be no more than 3 X the total audit assignment days (excepting annual leave etc)	100%	Previously reported year-end figures: 2016/17 60% 2015/16 58% 2014/15 52%
Elapsed Time for completion of audit work (exit meeting) to issue of draft report.	15 days	100%	Previously reported year-end figures: 2016/17 94% 2015/16 96%

			2014/15 83%
Elapsed Time between issue of Draft report and issue of Final Report.	15 days	85%	Previously reported year-end figures: 2016/17 75% 2015/16 48% 2014/15 69%

The other performance indicators are:

- % of 2017/18 planned audit activity completed by 30 April 2018 - reported at year end.
- % of management actions implemented (as at 21/8/17) - 72%.
Of the remaining there are 9% of actions that are overdue and 19% of actions not yet due.

(At 26 April 2017 A& G Committee the figures reported were 72% implemented, 7% overdue and 21% not yet due)

- Extended Management Team satisfaction with internal audit work - reported at year end.

COUNTER-FRAUD UPDATE

8. The 2017/18 Counter-Fraud Plan, which was agreed at the 26 April Audit & Governance Committee, is attached as Appendix 3 to this report. This shows current progress.
9. Internal Audit are continuing to work with Adult Social Care to provide Fraud Awareness Training as part of the directorate's direct payment training. Adult Social Care has determined this to be mandatory training for all staff involved in direct payments.
10. Development of arrangements for working with the City Council Investigation Team, for Counter-Fraud continues. The arrangement is working well and they have provided excellent support to our team by undertaking several reactive fraud investigations on our behalf. This has demonstrated clear benefits of having properly trained and skilled fraud investigators and has had very successful results. Work is currently being scoped with the City Council Investigation Team for them to lead on the work required to update the fraud risk register and delivery of proactive counter-fraud activities. They continue to work on

Single Person Discount initiative, which delivered excellent results during 2016/17.

11. There have been a minor number of issues received during 2017/18, these have been referred to the relevant service area and are currently being investigated. Internal Audit will monitor and report on the outcome of these as completed.
12. Proactive work is underway in Public Health, reviewing a small number of contracts to look at whether there are any data accuracy issues and to see whether the contract monitoring is sufficient to identify any potential anomalies.
13. The pro-active reviews of purchasing cards and travel and expenses have now been completed and the final reports issued. The executive summary of the reports are included within the Appendix 2 of this report.

National Fraud Initiative (NFI)

14. A number of match reports have now been worked through and closed, however there is still further work to be done on duplicate creditor records, blue badge matches, concessionary travel and residential parking permits. £29k was identified and recovered from a duplicate creditor payment. Additionally £270k has been identified in overpayments to residential care homes, for residents that have passed away. Of that £270k, £97k was recovered as a part of the NFI exercise, the rest had already been recovered as part of the normal processes. These matches are being reviewed closer to see whether additional work is needed within care homes that have been an issue across several exercises. A small number of pension cases have also been identified, these are currently being reviewed with the Pensions Manager and further action will be taken to investigate if needed.

RECOMMENDATION

15. **The committee is RECOMMENDED to note the progress with the 17/18 Internal Audit Plan and 17/18 Counter Fraud Plan and the outcome of the completed audits.**

Sarah Cox
Chief Internal Auditor

Background papers: None.
Contact Officer: Sarah Cox : 07393 001246

APPENDIX 1 - 2017/18 INTERNAL AUDIT PLAN - PROGRESS REPORT

INTERNAL AUDIT PLAN PROGRESS 2017/18

Directorate	Audit	Planned start	Status	Conclusion
People	Safer Recruitment	Q2	Scoping	
People	Transitions - from Childrens to Adults Service	Q4		
Adults	Payments to Residential and Home Support Providers	Q1	Final Report	Amber
Adults	Client Charging (including ASC debt)	Q3		
Adults	Personal budgets including Direct Payments	Q4		
Adults	Mental Health	Q4		
Adults	Adult Mental Health Practitioner Service	Q2	Fieldwork	
Childrens	Thriving Families - Grant Claims	Q2 & Q4	Fieldwork	
Childrens	CEF Contract Management	Q3		
Childrens	Fostering Service	Q2	Fieldwork	
Childrens	EDT	Q4		
ICT / Childrens	Childrens Social Care IT System Replacement	Q4		
Schools	Thematic Review	Q3		
Public Health	Combined Contract Management Audit / Counter Fraud Review	Q2	Fieldwork	
Communities & Resources	Capital Programme - including follow up of 16/17 audit findings	Q3		
Communities	S106	Q1	Draft Report	
Communities	Supported Transport	Q2	Fieldwork	

Communities	Research and Innovation	Q3		
Communities	Highways Contract Payment - follow up	Q3		
Finance	Pensions Administration	Q3		
Finance	Pensions Fund	Q3		
Finance	Accounts Receivable	Q4		
Finance	Payroll	Q4		
Finance	Purchasing / Procurement (including pre-paid cards)	Q3		
Finance	Feeder systems	Q2		
Finance	Insurance	Q4		
Finance / Corporate	Grant Certification	Q1- Q4	5 complete	
Finance / Corporate	Security Bonds	Q2	Scoping	
Corporate	Contract Management System	Q3		
Corporate	Programme Management Office	Q3		
Corporate / ICT	Fit for the Future - Digital First Platform	Q2- Q4	Part 1 Programme Governance Review - Final Report	Amber
HR / Corporate	Sickness management	Q1/Q2	Fieldwork	
HR / Corporate	Establishment control / HR data	Q1/Q2	Fieldwork	
HR / Corporate	Recruitment	See above		
ICT	Cyber Security	Q2	Final Report	Amber
ICT	Disposal of Equipment	Q1	Final Report	Amber
ICT	PSN compliance (Public Services Network)	Q3		

ICT	Mobile Computing	Q3	Fieldwork	
ICT	ICT backup and recovery	Q3		
ICT	ICT incident management	Q3		
ICT / Childrens	Childrens Social Care IT System Replacement	See above		

APPENDIX 2 - EXECUTIVE SUMMARIES OF COMPLETED AUDITS

ICT Disposal of Equipment 2017/18

Opinion: Amber	05 June 2017	
Total: 08	Priority 1 = 0	Priority 2 = 08
Current Status:		
Implemented	08	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	0	

All actions have been reported as implemented since finalisation of this report.

Overall Conclusion is Amber

The previous audit of this area in 2015 identified significant risks, including potential breach of the Data Protection Act 1998, and resulted in a Red overall conclusion. It is pleasing to report that ICT have addressed many of the risks, resulting in an improved control framework. However, some risks remain as detailed below.

A corporate policy on the disposal of ICT equipment was documented following the 2015 audit but has never been published, presenting a risk that it may not be known to relevant ICT staff/teams. The policy also missed its annual review in January 2017.

All equipment identified for disposal is collected from user areas and held in a secure room until it is ready to be collected by the third-party disposal company. Details of the equipment are recorded in an inventory which was reviewed and found to be up to date. A Collection Form is used to reconcile the number of items being disposed to the number of items collected by the disposal company and is signed by both parties. However, our testing identified one form from the last six collections where the number of items collected had not been recorded. We also found that the asset register is not updated to reflect equipment that has been disposed of. For each collection, the supplier should issue a Billing Report detailing their charges before they submit their invoice. A Billing Report has not been received for any collection since October 2016, although we found that one of the collections has been invoiced and paid. Paying invoices without a Billing Report increases the risk of incorrect payments being made.

Data is wiped from hardware using a certified tool that has been approved by the National Cyber Security Centre. Where hardware cannot be made data safe, the magnetic media is degaussed and shredded. The disposal company issue an itemised inventory of the hardware they have disposed of, but there is no evidence that this is checked and reconciled to the inventory held by ICT of the equipment they sent for disposal. We also found that the disposal

company has not issued a Certificate of Data Sanitisation or Certificate of Destruction for the two most recent collections in January and February 2017. This should be followed up with them to ensure all equipment was sanitised and/or destroyed.

There is a formal contract with the third-party disposal company that covers areas such as Environmental Protection Act 1990, waste regulations, Data Protection and security. The contract was signed in January 2016 and is for a three-year period. However, a site visit of the disposal company has not been undertaken to review their operational procedures from a compliance perspective, as advised by the Information Commissioner's Office.

Cyber Security Review 2017/18

Opinion: Amber	28 June 2017	
Total: 20	Priority 1 = 0	Priority 2 = 20
Current Status:		
Implemented	06	
Due not yet actioned	01	
Partially complete	02	
Not yet Due	11	

Overall Conclusion is Amber

Cyber threats are not new, but the focus on cyber security has increased because of a number of high profile disruptive and damaging security incidents and breaches. The most recent of these is the WannaCry ransomware attack which began on Friday 12 May 2017 and within a day was reported to have infected more than 230,000 computers in over 150 countries. In the UK, the attack made headline news as it severely impacted parts of the NHS.

This review has focussed on a number of key risk areas relating to cyber security. However, it is important to note that other computer audit reviews also provide assurance in this area, including reviews planned in 2017/18.

All organisations using digital systems are vulnerable to cyber-attacks and must operate strong security controls to minimise the risk of any attack being successful. Cyber risks are included on the ICT risk register but responsibility for cyber security has not been formally assigned; this should be reviewed in light of the increased threat.

The procurement of new IT services/systems does not include a cyber security assessment to ensure suppliers/partners operate adequate controls to protect OCC systems and data from cyber risks.

There is a documented Acceptable Use Policy and ICT have processes for alerting users to the latest cyber-attacks via the Intranet and ICT Security Hub.

All users are required to undertake an e-learning course on the Acceptable Use of Information, although we found that people who have not completed it are not followed up. There is a corporate Information Security Incident Policy and all security incidents are investigated by the Information Services Team and reported to the Corporate Information Governance Group.

Anti-virus software, vulnerability scanning and system patching is in place, although there is scope to further strengthen the controls in these areas.

All new user accounts have to be authorised by a manager and network passwords are changed on a regular basis, although some exceptions have been noted and reported.

Payments to Residential & Home Support Providers 2017/18

Opinion: Amber	17 July 2017	
Total: 11	Priority 1 = 01	Priority 2 = 10
Current Status:		
Implemented	01	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	10	

Overall Conclusion is Amber

OCC paid £21m for home support and £124m¹ for residential in 2016/17 (this includes health funded care packages). The home support payments are mostly paid from actual visit data from the Electronic Time Management System (ETMS) whereas residential payments are paid based upon planned care packages.

It is acknowledged that Management are already aware of a number of issues that are highlighted in the report and are already taking action primarily through the Business Efficiencies System Improvement group (BESI) which is tasked with the oversight of improving some of the payments to provider processes and the availability of robust management information. For example, the checks undertaken by the Care Service Administrators (CSAs) between the planned versus actual home support care delivered is currently under review and therefore was not tested during this audit, likewise the BDU Interface for uploading payments to SAP is due to be replaced by a direct interface between Controcc and SAP.

A: Payment Accuracy

Delays in authorising Support Plans can result in delays to payment to providers and sample testing undertaken during the audit identified that these

¹ The residential care homes figure includes health funded care package payments processed by OCC, eg FNC and CHC packages

delays had impacted on payments made. Delays are monitored via a weekly report sent to managers, however given the high volume of overdue Support Plan tasks on the report, it is clear that a significant issue remains with late or non-completion of Support Plans. There was also a lack of clarity amongst ASC staff regarding when the Funding Authorisation Form (FAF) should be used, particularly in relation to home support placements when a Referral for Domiciliary Care Form has already been completed.

Ideally, all payments to residential and home support providers should be made via ContrOCC to ensure transparency and linkages to the service user records. However, SAP reports show that in 2016/17, Purchase Orders were used to pay £2.5m of home support payments (including Extra Care Housing) and £782k to residential providers. Whilst this includes some payments to providers that currently would not be expected to go through ContrOCC, for example to pay for services or contracts not relating to an individual's care, there are still payments relating to service users' care, made by purchase order. This has resulted in a small number of duplicate payments which have recently been identified. However, the key issue is the efficiency and consistency of processes; this is already recognised by management, with the subsequent introduction of a payments policy and further work being led by BESI to investigate these payments further with a view to reducing these.

Extra Care Housing payments are made up of core payments and payments for visits. Unlike other home support providers, ECH do not use ETMS to record actual visits, therefore payment amounts are made based upon care packages, which may or may not be accurate. This also applies to external day care services. This is being reviewed further by BESI.

Deletion or date amendments to CPLIs have to be processed by ICT at the request of social care or finance teams. There is a risk of payment errors where a CPLI is deleted or amended without a correct CPLI being in place, which has occurred in some recent cases. As a result, ICT are now required to alert the Payments team of any CPLI amendments or deletions that will have a material impact upon payments (over £10k or from more than 3 months ago). This process has only recently been implemented, and is being overseen by BESI, so no targeted testing was undertaken. There is ongoing work to review the whole system administration and where these tasks will be managed in the future.

Home Support

The pick-up rate amongst the H2LAH providers reduced significantly during 2016/17 and was much lower than the budgeted volumes than the advance payments had been calculated upon, leading to these payments being too high. In the last 4 months these payments have been reduced accordingly, the previous overpayments clawed back and advance payment amounts are now reviewed and updated more regularly. Whilst this issue has now been rectified, one provider has subsequently gone into administration prior to being able to reclaim the advance payments, resulting in a reported impairment of £335k in the 2016/17 accounts and a claim has now been submitted to the Liquidator. (Note that £212k relates to payments made under

the contract and £123k related to additional direct and opportunity costs of arranging alternative service provision). Contract Management have implemented a strengthened monitoring of advance payments against actuals, and are working more closely with Finance colleagues. Providers are able to request to change from advance payments to a payment in arrears arrangement, and communications have been sent out to this effect; some care providers have now elected to take this option. There are also improvements being implemented whereby the financial stability of the main providers is monitored more closely.

Residential

Residential payments are paid based upon care package. There are controls which help mitigate the risk of paying for a service user no longer resident. Whilst the audit has identified weaknesses in the application of these controls, it should be noted that the evidence provided via the NFI (National Fraud Initiative) data match has identified only a very small percentage of overpayments has occurred where death of a service user is not notified by the providers. (Early figures from the current exercise show 48 potential overpayments, totalling £270k, with half of these appearing to be where the home has not notified OCC, or notified OCC some-time after the death of the service user.)

Whilst each overpayment is investigated in full and the monies recovered, in comparison to the amounts paid annually to residential providers, the amounts are not material and do not suggest a large scale issue regarding the accuracy of payments made. This has therefore been considered by management and proportionate action has been agreed when considering the operation of current controls.

B: Overpayments

ContrOCC, in accordance with the contracts, automatically adds 7 days onto residential care package end dates where 'deceased' is selected as the reason for deactivation. From checking a sample of 5 care packages where the end date was later than the date of death, in 2 cases the service user died in respite, however in the other 3 cases the end date was entered too late, resulting in overpayments (two of which had previously been identified and corrected, the third had not been identified prior to the audit and resulted in an overpayment of £700). There is currently no cross checking between dates of death in LAS to care package end dates for deceased service users, which would identify where the incorrect end date had been entered.

In one case in the residential payments sample, a reduction in funding had been agreed in 2014 but this had not been processed as a new Annex 2 was not completed, resulting in an additional £8k being paid for the service user's care, since the date the care package should have been reduced. This individual case is now being reviewed by ASC.

C: Follow Up

Out of the 10 actions agreed at the 2015/16 audit, two are still recorded as open, these are allowing the Placement Officers to authorise Annex 2s (this has not yet been implemented in full, as block contracts are now been authorised as part of a trial but the process will not be put in place for spot contracts until after this has been completed) and to strengthen the 6-monthly remittance quality control process to ensure all residential providers submit their current residents lists (this process has stopped, as reported above).

Of the 8 actions reported as implemented 4 have been fully implemented; 4 not re-tested in this audit.

Travel & Expenses Review 2017/18

There are no management actions for this audit

Overall Conclusion is Green

Data analytics were carried out on all travel and expense claims submitted in 2016/17. Sampling was then targeted to samples of employees of those with high claims, those that were 50% greater than the previous year, those that had a monthly claim 50% higher than average claim, claims made against a cost centre without a nominated manager and claims made whilst on sick leave/annual leave. Each employee was asked to provide justification for the mileage incurred and receipts for expenses claimed for the month requested.

Improvements have been noted since the last review, and whilst there are still issues with information that management can see within the IBC system, there was no evidence found of any claims that appeared to be deliberately falsified.

All individuals sampled could support the need for the expenses and could provide justification for the journeys undertaken. Positive assurance (based on the sample tested) can be provided that there were fewer issues with claims noted during this review than the previous one. Only very minor issues were found with mileage claims, which were corrected by the individuals during the review (two over-claims of 30 miles and 10 miles, respectively). There were also two instances whereby individuals had not kept receipts to support expense claims; however they could demonstrate that the expenses were legitimate.

The visibility of management information within IBC is still an issue and has not been resolved since the previous review. Management are still unable to view staff members that have submitted expense only claims. This has been acknowledged by the IBC and is part of their change programme to rectify.

The Fit for the Future Programme Board is due to have oversight of Council-wide travel and expenses management information, which will give greater

visibility and challenge over spending. Quarterly reports are also planned to be presented to CLT to provide strategic information.

8 management actions were agreed in the previous audit, of those 8; 1 is referred to above re strategic oversight of Council-wide information and is currently being implemented. 3 have been implemented in full, 2 have been superseded and a further 2, whilst not implemented, are included as part of the IBC's improvement change programme and therefore a fix is planned.

Digital First Platform - Programme Governance Review 2017/18

Opinion: Amber	26 July 2017	
Total: 08	Priority 1 = 0	Priority 2 = 08
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	08	

Overall Conclusion is Amber

Digital First is one of three workstreams in the Fit for the Future transformation programme and is designed to build and implement digital solutions to help services improve and automate their business processes. The Digital Platform is a key component of the Digital First workstream and provides a set of common tools that can be used by customers to transact with the council e.g. apply, report, pay, book etc.

Digital First forms part of OCC's Digital Strategy 2016-2020 which was developed in response to a corporate objective of going digital by default. The Digital Strategy was approved by CCMT in July 2016.

At the time of the audit the Digital First workstream comprised of five projects, although this was being reviewed. A PMO function was created in April 2017 and they have developed a process for approving and prioritising projects within the Fit for the Future programme.

There is a programme structure in place that includes a monthly Digital Workstream Board and fortnightly Digital Management Support Team. An Implementation Sponsors Working Group has also recently been established and is responsible for managing the interdependencies between the different Fit for the Future workstreams. We have identified that the terms of reference for the Digital Workstream Board needs to be reviewed and that there are no terms of reference for the Digital Management Support Team. The responsibilities of key roles, such as the Workstream Sponsor and Programme Manager, should also be further defined. A Communications and Engagement Plan has been approved and a resource has recently been identified to help implement it.

A programme level risk log and issues log is maintained and Highlight Reports are used for reporting to the Fit for the Future Transformation Board, Digital First Board and Digital Management Support Team. However, a review of the risk log found that risks are not being correctly rated as they are currently based on their impact alone and without any assessment of how likely they are to occur.

A high-level programme plan has been prepared but individual project plans were not developed for any of the current Digital First projects. There should be clear guidance on when project plans are required. The programme plan includes milestones and these are monitored by the Programme Manager and any missed milestones are reported to the Digital First Board and Digital Management Support Team. This was tested and confirmed.

The budget for the Digital First workstream has been refined over the last 6-9 months as costs have become clearer and currently stands at £2.5 million. In 2016/17, programme costs were charged to general ICT codes and recharged at the end of the year and ICT are now working with Finance colleagues to put in place a revised coding structure to help distinguish Digital First costs from the cost of other ICT programmes. We have found that responsibility for managing the Digital First budget has not been formally assigned and the level of financial reporting to the Digital First Board should also be improved.

Purchasing Cards Review 2017/18

Opinion: Amber	21 August 2017	
Total: 05	Priority 1 = 0	Priority 2 = 05
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	05	

Overall Conclusion is Amber

In 2015/16 the Council spent approximately £2.7m on purchasing cards, increasing to £3.2m in 2016/17. The Purchasing Card system is run through RBS and administered by the IBC in Hampshire. Managers are required to approve cardholders' transactions on a monthly basis. A proactive fraud review of the Purchasing Card system was last undertaken in 2015/16.

The objective of the review was to consider the sufficiency and clarity of policies and procedures in this area, adequacy and availability of the internal control processes (particularly in relation to approval of expenditure) and to complete targeted testing on a sample of cardholders' purchases, including foreign transactions, questionable expenditure, high value transactions, transactions occurring after leaving date, etc.

Key findings:

Usage of the RBS system to review and approve transactions has improved significantly since the previous review. Both review and approval levels were previously around 20% in the system. For 2016/17 the review level was at 71% and the approval level was at 32% (A number of schools are still using the paper sign off method).

Purchasing card policy and guidance has further scope to be strengthened from a fraud prevention point of view. Issues were noted whereby cards had been linked to online purchasing platforms (such as PayPal), and payment for non-OCC related purchases made. Further issues were also noted with card sharing. There is also a need to make the policy and guidance more accessible and visible to schools, as there were a number of issues noted with purchases not in line with the policy, such as meals, gifts and alcohol.

15 actions were raised in the previous proactive fraud review. 14 of those have been implemented, one still remains outstanding (noting the OCC policies in the e-learning package).

APPENDIX 3 - 2017/18 COUNTER FRAUD PLAN - PROGRESS REPORT

Activity	Planned Qtr Start
Review and update of fraud risk register. Identification of new fraud risk areas.	Ongoing
NFI 2016 match - review and investigation of data matches	Q1 - ongoing
Reactive investigations - continued from 2016/17 plus new referrals.	Ongoing
Fraud awareness sessions.	Ongoing
Proactive Fraud Review - Travel and Expenses	Complete - Final Report Green
Proactive Fraud Review - Procurement Cards	Complete - Final Report Amber
Combined contract management audit / proactive fraud review - Public Health	See audit plan entry - Fieldwork
Continue with development of working arrangements with the City Council for Counter Fraud to include: <ul style="list-style-type: none"> - Single Person Discount Review (including extending to other reliefs/discounts) - Support with the NFI 2016 data match (focus on areas which have previously returned positive results) - Support with reactive investigations - Development of a plan of proactive fraud reviews, potential areas for 17/18 include Procurement, Direct Payments, Deprivation of assets/Non declaration of income and Insurance. 	Q1 - Q4