Division(s): N/A

AUDIT and GOVERNANCE COMMITTEE – 16 SEPTEMBER 2015

INTERNAL AUDIT 2015/16 PROGRESS REPORT

Report by the Chief Finance Officer

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.
2. The Internal Audit Plan is attached as Appendix 1 to this report. This reports on the progress against the quarter 1 and quarter 2 plan and the proposed quarter 3 plan.
3. The proposal for restructuring the current resources of the Internal Audit Service is now complete. Three distinctive teams have been created, to protect the role and independence of an Internal Audit Service; to provide a clear strategy and resource for the management of Counter-Fraud; and, to create capacity to manage the corporate responsibility for Risk Management and a new a Business Assurance function.
4. The key outcome of the change is to provide a structure that can contribute to and report on the Council's combined assurance that ensures the effectiveness of the governance, risk management and the system of internal control.
5. The Internal Audit function is looking to recruit a Trainee Auditor post, this recruitment will commence in September.
6. The new Risk and Business Assurance function is currently recruiting to two vacant Compliance Officer posts. The advert for the two posts closes at the end of August. The team currently has an interim Compliance Officer in place working wholly on undertaking internal check procedures on the file upload process for feeder systems to the main accounting system.
7. The team have also commissioned 100 days from the Council's insurance provider (Zurich) to assist in reviewing and updating the Council's Risk Management Strategy, Strategic Risk Register and to develop a methodology for assurance mapping the organisation's critical services.
8. The agreement with Oxford City to provide counter-fraud support has been drafted and will be operational by the end of September.

9. Now the team structure has been finalised, the work plans for compliance, counter-fraud and internal audit activity will be developed in respect of financial risks and key financial systems, during Q3 and delivered during Q3 and Q4.

10. There is currently a critical piece of work on-going following the transfer of services to the Hampshire IBC; the audit needs assessment for retained services and processes is being created from which the assurance based activity with be determined as either a need for compliance checking, proactive counter-fraud audits, or systems based internal audit. In addition the expectations of the IBC systems are being captured and will be discussed with the Chief Internal Auditor of Hampshire CC, including the IBC, to ensure they will be able to provide independent assurance on the system of control to Oxfordshire.

2014/15 AUDIT PLAN PROGRESS

11. There have been 5 audits concluded since the last update (provided to the July 2015 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	**2014/15 Audits**	**Opinion**
SCS	Adult Social Care Management Controls	Amber
Directorate	**2015/16 Audits**	**Opinion**
SCS	Management Letter - Provider Investigation - post investigation review of controls.	N/A
EE - ICT	Cyber Security	Amber
EE - ICT	ICT Disposal of Equipment	Red
EE - ICT	ICT Change Management	Amber

PERFORMANCE

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

Performance Measure	**Target**	**% Performance Achieved**	**Comments**
Elapsed Time for completion of audit work (exit meeting)	15 days	75%	

to issue of draft report.			
Elapsed Time between issue of Draft report and issue of Final Report.	15 days	50%	For the audits that did not meet this PI, there were known delays in finalisation due to key staff being on holidays.

The other four performance indicators are:

- % of 2014/15 planned audit activity completed by 30 April 2016 - reported at year end.
- % of management actions implemented (measured from 13/14 to date) = 77%. Of the remaining 23% - there are 51 actions that are overdue, and 110 actions not yet due.
- Effectiveness of Internal Audit - reported at year end.
- Extended Management Team satisfaction with internal audit work - reported at year end.

COUNTER-FRAUD

13. The external potential frauds being investigated within Social and Community Services are still on-going and a full update will be given at the conclusion of the investigations. For one of the cases, the investigation has been passed across to the Police and their investigation is underway.

14. The minor financial irregularity relating to additional payments made to an ex-employee concluded with no further action to take. The available evidence was reviewed by management and found to be inconclusive. It was considered, on the balance of the evidence available and that no significant values were involved, that no further action was required.

15. The investigation into the potential misuse of a direct payment is on-going. An audit of the Direct Payments processes is now underway and has a focus on what controls the Council has in place to protect against, or highlight, direct payment funds being used for anything other than their intended purpose.

16. At the last update it was reported that the Income Team had alerted Audit to an irregularity whereby a company had informed them they had been asked to make payment in the name of an individual as opposed to the Council. The systems were updated immediately following this and the Finance Business Partner obtained initial assurances that the individual had not received or cashed cheques into a personal account, and that it was a lack of knowledge of correct

process. A full detailed analysis is still to be done, however assurances thus far have proved sufficient that there has been no loss and no deliberate attempt at committing fraud.

17. Internal Audit has been made aware of a potential procurement card misuse. This was investigated by HR and management and found to be a wider issue of lack of procedural knowledge, which constituted the misuse. Whilst no disciplinary action is being taken, the individual in question is now paying back the money spent inappropriately on their card and the control issues that are highlighted by this case are being reviewed in the current audit of Childrens Social Care Payments.

18. National Fraud Initiative (NFI)

    The matches from the 2014/15 exercise have been released. In total OCC have had 15,266 matches returned, of which 6,850 are recommended to be looked at. Key officer and Councillor checks have been completed and no issues have been identified. Data matches are now being reviewed by individual teams across the Council and Internal Audit.

RECOMMENDATION

The committee is RECOMMENDED to approve the Q3 Internal Audit Plan.

Lorna Baxter
Chief Finance Officer

Background papers: None.
Contact Officer: Ian Dyson, Chief Internal Auditor, 01865 323875

APPENDIX 1

Progress against Quarter 1 Internal Audit Plan

Directorate	Qtr Start	Audit	Status
CEF	1	**CEF Safeguarding (Children's Social Care Management Controls)** The detailed scope of the audit will be agreed with the Deputy Director. The audit will look to provide assurance over the processes in place for the monitoring and escalation of missing children, including children missing from school.	**Directorate requested deferral until quarter 3.** **Fieldwork start date planned for November 2013.**
CEF	1	**CEF Thriving Families** The revised Thriving Families Framework requires internal audit verification of each claim. New processes have also been developed by the team. Internal Audit plan to review the new processes in April / May and then complete the required verification work of both the summer and winter claims.	**Initial review of processes has been completed. Summer claim not made. Verification work will therefore be undertaken by Internal Audit for the Winter Claim.**
SCS	1	**SCS Personal Budgets / Direct Payments** The audit will provide assurance on the effectiveness of the Self Directed Support process, including personal budget allocations and accounting, care plan delivery and client documentation. The audit will specifically review controls in respect of direct payments. This will include review of the processes and recording via the new Adult Social Care I.T. System.	**Fieldwork stage.** **Due for completion by end of September 2015.**

Directorate	Qtr Start	Audit	Status
SCS	1	**Adult Social Care Information System** A follow up audit of the audit of the IT system implementation audit that was undertaken in February 2015 will be undertaken in quarter 1 to provide assurance that the weaknesses identified in the area of testing have been sufficiently addressed prior to go-live.	**The implementation of the new system was deferred from May 2015 to November 2015. This audit will therefore now start in quarter 2.** **The follow up audit has now been completed and is at draft report stage.**
SCS	1-4	**LEAN / Responsible Localities** This is a major programme looking at improving the care pathway of clients and introducing improved ways of working. The Audit Manager will continue to work with the Finance Business Partner for SCS in reviewing the newly designed processes and also look to provide assurance on the overall programme governance. This will include review of the care management processes and recording via the new Adult Social Care I.T. System.	**On-going**
SCS	1-4	**SCS Implementation of the Care Bill** From April 2015 the new Care Bill will go live. This will include changes to the collection of deferred payments, larger volume of care assessments, changes to eligibility, improvements required to information and advice, etc. The required changes are being managed as a major programme by the SCS directorate. Internal Audit will look to provide assurance on the on-going programme governance arrangements and implementation plans.	**On-going**

Directorate	Qtr Start	Audit	Status
EE (OCS)	1	**Externalisation Programme** The audit will follow on from 2014/15 IBC On Boarding audit and the related projects (Impacts and Business Readiness). The review will focus on programme and project governance and the design of any new internal control mechanisms introduced by the Council that will interface with the IBC.	**On-going**
EE (OCS)	1	**Cyber Security** The audit will provide assurance that the Councils ICT environment, systems and data are adequately protected and secure against cyber threats	**Final Report**
Planned Quarter 2 audit, brought forward and undertaken in quarter 1:			
EE (OCS)	2	**ICT Disposal of Equipment** This area has not been subject to any previous internal audit review and there is a responsibility under the Data Protection Act 1998 to ensure all personal data is securely wiped from all redundant equipment. To evaluate the controls over the disposal of ICT equipment, including the security wiping of data.	**Final Report**

Progress against Quarter 2 Internal Audit Plan

Directorate	Qtr Start	Audit	Status
CEF	2	**CEF MASH (Multi Agency Safeguarding Hub)** The audit will look to provide assurance on the new processes and governance arrangements in place.	**Fieldwork**
CEF	2	**CEF Social Care Payments** The audit will review the accuracy and integrity of the various payment types made by CEF social workers, for example emergency payments, which are made via the Facilities Management Offices.	**Fieldwork**
CEF	2	**CEF Foster Payments** The audit will review the processes in place for payments to foster carers. The scope will be agreed with the Directorate, however will include both internal and external foster placement arrangements.	**Fieldwork**
EE	2	**EE Planning** The audit will review the processes in place for managing and consulting on planning applications. The audit will also review the relationship with the District Council's in supporting their planning process and the use of the Single Response system.	**Rescheduled for later in 2015/16**
EE	2	**EE Energy Recovery Facility** The audit will review the financial management and performance monitoring arrangements in place for the Energy Recovery Facility.	**Rescheduled for later in 2015/16**

Directorate	Qtr Start	Audit	Status
		Testing will include a detailed review of payments made; tracking details back to source documentation.	
EE (ICT)	2	**ICT Change Management** A new change process is being implemented. To ensure there are formal processes for managing changes to the ICT environment and that all such changes are appropriately authorised and tested prior to being implemented.	**Final Report**
EE (ICT)	2	**Broadband Project** To review the implementation of the broadband project. This is a key ICT project that is running until 2017.	**Fieldwork**
EE	2 / 3	**Capital Programme Governance & Delivery** The audit is a high level review of the capital programme aimed at testing the Council's approach to progressing identified schemes and to ascertain the management of the capital programme and its delivery. Detailed scoping is yet to take place, but the review will test capital programmes from across the Council.	**Planned start for quarter 3**
EE	2 / 3	**Highways Contract** In conjunction with the contract management team, this audit will review the management and operation of the Highways Contract with Skanska.	**Fieldwork**

Proposed quarter 3 Internal Audit Plan

NB. Audits deferred from quarter 1 & 2 and now planned to start in quarter 3 are listed above. The following are additional audits for quarter 3.

Directorate	Qtr Start	Audit	Status
SCS	3	**SCS Pooled Budgets** The audit will look to provide assurance over the governance and operational arrangements in place to manage joint risks, shared decision making and work undertaken on behalf of each other. The audit will include reviewing the arrangements in conjunction with the introduction of the Better Care Fund.	**To start quarter 3**
EE	3	**City Deal** The audit will review the governance and financial arrangements in place for managing and monitoring the City Deal, including delivery within established targets or timeframes.	**To start quarter 3**
Corporate	3	**OLEP Governance Framework** The audit will review the design and application of the OLEP's Assurance Framework, following the guidance issued by the Department for Business, Innovation & Skills in December 2014 that is aimed at guiding local decision making to support accountability, transparency and value for money.	**To start quarter 3**

Directorate	Qtr Start	Audit	Status
EE (ICT)	3	**Commissioning of ICT Services** A number of key services have been, or will be, externally commissioned, including services relating to the data centre, wide area network and SAP system. To ensure ICT services provided by external parties are adequately managed and monitored.	**To start quarter 3**

APPENDIX 2

Summary of Completed Audits (since last update to July 2015 Audit Committee)

(Status at end of August 2015)

ADULT SOCIAL CARE MANAGEMENT CONTROLS 2014/15.

Opinion: Amber	29 July 2015	
Total: 25	Priority 1 = 07	Priority 2 = 18
Current Status:		
Implemented	01	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	24	

Overall Conclusion is Amber

The audit scope covered review of the Safeguarding Alerts process, how complaints and concerns of a safeguarding nature are managed and also considered how safeguarding information in relation to providers is gathered and used in decision making.

OCC faces the challenges of responding to an increasing volume of Safeguarding Alerts and of adequately monitoring a large number of external residential and home support providers. New policies and procedures have been put in place to improve management oversight, information sharing and joint working, in particular the introduction of the Care Governance and Quality Board (CGQB), the Serious Concerns Framework and the Providers Dashboard, which fill a gap in joint oversight. These changes are a very positive step forward and are currently in an embedding phase, after which they should provide a stronger control framework, supported also by improved data management from the new Adult Social Care System. However, currently some weaknesses exist:

- Outdated information management systems, with heavy reliance on multiple spread sheets, and storage of key documents on individual email accounts or restricted team folders instead of shared folders or databases.
- Data inaccuracies in the new Providers Dashboard (designed to improve oversight of provider quality and performance), as providers' traffic light statuses were incorrect.
- The Contracts Team are not routinely informed of all Safeguarding Alerts, and do not regularly and routinely check for new Alerts, thereby limiting their ability to monitor trends effectively and in a timely manner.
- Alerts or referrals have been closed without clearly documented, triangulated evidence retained to support the decision.

- The management of Provider improvement actions plans and contract sanctions is not satisfactory.
- There is a need to develop a stronger quality assurance and performance management system by utilising systematic data analysis of provider service delivery records.

PROVIDER INVESTIGATION MANAGEMENT LETTER 2015/16.

Opinion: N/A	29 July 2015	
Total: 10	Priority 1 = 01	Priority 2 = 09
Current Status:		
Implemented	03	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	07	

The investigation into the provider where there were queries with the visits that the provider has claimed for is on-going.

However Internal Audit and SCS management met to review whether the investigation had highlighted any weaknesses in systems or processes and agree an action plan where internal / management controls require strengthening. This review took into account the management actions agreed in the audit of payments to residential and home support providers undertaken during 2014/15 and looked to build on those agreed actions and capture any additional weaknesses in systems and processes that the investigation highlighted.

Conclusion

A full audit or any detailed testing has not been undertaken however this post investigation review has highlighted areas where improvements are required to strengthen internal controls to reduce the risk of reoccurrence. These include:

- The need to clarify responsibility for the management and coordination of investigations into providers.
- The need to include within the new Serious Concerns Framework, processes for when a provider is placed on red, which ensure that a risk assessment is undertaken on any existing service users, that the providers are asked to voluntarily agree to not take on any more self-funded or direct payment clients until their position improves and for any sub-contracting arrangements they have in place at the time to be reviewed.

- Development through E-Marketplace on how providers are listed to improve transparency and provide better information.
- Work required with the provider of ETMS (Electronic Time Management System) to address system weaknesses identified and to meet the requirement for more robust management reports which will provide assurance to management that providers are using the system correctly.
- Development of a Contract Management Plan to ensure contract monitoring activity is targeted on themed activities and also to providers on a risk based approach.

It should be noted that improvements have already been established by Management, for example the introduction of the Serious Concerns Framework and also considerable progress made by the Contracts and Quality Service Manager in implementing the agreed actions from the Payments to Providers 14/15 audit report.

CYBER SECURITY REVIEW 2015/16.

Opinion: Amber	27 July 2015	
Total: 11	Priority 1 = 2	Priority 2 = 09
Current Status:		
Implemented	02	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	09	

Overall Conclusion is Amber

Cyber threats are not new, but the focus on cyber security has increased as a result of many high profile disruptive and damaging security incidents and breaches. This review has focussed on a number of key risk areas in relation to cyber security, however, it should be noted that other computer audit reviews also provide assurance in this area. This includes audits of Windows Active Directory, PSN Compliance, Mobile Computing, Wireless Networks and IT disaster recovery.

An ICT Acceptable Use Policy (AUP) is documented, and along with other security policies, is available on the corporate Intranet. We have reviewed the AUP and found that it should be bolstered in the areas of password security and malware prevention.
All ICT users are required to undertake a mandatory e-learning course on the Acceptable Use of ICT, however, because there are problems with the delivery system and it is being replaced, users who have not completed the course will not be followed up until the new system is implemented in July 2015. ICT are monitoring completion of the course to allow the follow-up action to be taken.

A Security Incident Management Policy has been documented and was approved in January 2015. Users are required to report all security incidents to the ICT service desk where they are logged and forwarded to the Information Governance team for review and investigation. Details of all security incidents are reported to the corporate Information Governance Group. No key risks have been identified in this area.

The network has a number of external gateways and each is secured using a Cisco firewall. The Internet and WAN firewalls are managed by Vodafone and the third-party firewalls are managed by ICT. The firewalls have a number of interfaces, each of which has a rule base to control and restrict network connections and traffic. However, the rule bases are not documented and there is also an outstanding management action from our PSN Compliance audit relating to the monthly interface review. For the firewalls managed by ICT, there which could lead to any potential cyber-attack going undetected. We understand that the firewalls managed by Vodafone have intrusion detection monitoring, although this was not verified. Our testing also identified that some firewalls have a number of redundant user accounts and insecure management interfaces.

Microsoft Forefront Endpoint Protection (FEP) is deployed on the network to protect against malware threats. In addition, all incoming and outgoing emails are checked for malware using a cloud based solution, which utilises a different scan engine to FEP and is configured to block all high-risk file attachments. However, whilst FEP is updated every 8 hours there are no procedures to check that updates have been successfully applied to all computers. Consequently, there is a risk that computers with out of date protection are not identified and could become infected by malware.
ICT have access to an in-house solution that allows them to undertake vulnerability assessments. The SureCloud solution is configured to perform quarterly scans of external facing computers/devices and of computers on the internal network. However, the scope of these scans has not been reviewed following the recent changes to the network and formal action plans are not developed to address the vulnerabilities that are identified. Such vulnerabilities could be exploited in a cyber- attack.

Desktops and laptops are patched with security updates on a monthly basis. There is a phased deployment of these updates to ensure they are tested before being rolled out to all machines. However, servers are not patched on a regular basis and our testing has identified that a number of key servers are missing critical security updates. There is an outstanding management action to address this risk from our Windows Active Directory audit undertaken in 2014/15. ICT acknowledge that the action has not been implemented in accordance with the agreed timescales and are taking steps to address this.

Standard build images are used for clients and servers and access to these are restricted on System Center Configuration Manager. Domain administrator level access is controlled and restricted and standard users do not have any local administrator rights on their workstations. However, there is an

outstanding management action to review and update build and configuration procedures and we have further found that the server build checklist is not printed, completed and signed-off by engineers and thus there is a lack of assurance that the agreed process is being followed.

New user accounts are requested using an on-line form which has to be approved by a person who is set-up on the SAP system as an approver. However, from our sample testing we found that a number of new accounts had been requested and approved by the same person, thus increasing the risk of unauthorised accounts being created. There is an equivalent leaver form for notifying staff leavers so that accounts can be disabled and ICT have recently introduced a new procedure for identifying dormant accounts. There are documented procedures for user administration, however, they are out of date.

ICT DISPOSAL OF EQUIPMENT 2015/16.

Opinion: Red	27 July 2015	
Total: 10	Priority 1 = 04	Priority 2 = 06
Current Status:		
Implemented	06	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	04	

Overall Conclusion is Red

OCC as a Data Controller are responsible under the seventh principle of the Data Protection Act 1998 for having appropriate security in place to prevent personal data from being accidently or deliberately compromised. This is relevant to IT asset destruction and recycling processes. In 2013, the Information Commissioner's Office (ICO) imposed a record fine of £200,000 on an NHS organisation for failings in their data destruction procedures which led to personal data being compromised. There are some similarities between this case and control weaknesses we have identified as part of this audit review.

There is no documented corporate policy on the disposal of ICT equipment. Whilst ICT Business Delivery are responsible for disposing of all ICT equipment, a formal policy should be documented to define the approach to be adopted, including minimum security standards for data destruction.

There are no documented procedures covering the disposal process, resulting in a lack of clearly defined roles and responsibilities for specific tasks. The details of all assets identified for disposal are logged on an inventory, although our testing found that it was inaccurate and did not record details of everything that was actually being held for disposal. We also identified discrepancies

between the number of items booked for collection by ICT and the number actually collected by the IT disposal company as per their consignment note. The hardware inventory is also not updated to reflect equipment that has been disposed of.

There is no confirmation of the tools/products used by the IT disposal company for data wiping and hence there is risk that data is not fully wiped from equipment and could subsequently be recovered using specialist tools. The reports issued by the IT disposal company, which include a list of the assets they have disposed of, have not been checked and reconciled since January 2013. As such, there is a risk that exceptions are not identified and followed up on a timely basis.

There is no formal contract between OCC and the IT asset disposal company, KMD Recycling Ltd. This is in direct breach of the Data Protection Act 1998, and as a result, no further equipment should be transferred to them until this is resolved. A site visit of KMD's premises has also not been undertaken to review their operational procedures from a compliance perspective, as advised by the Information Commissioners Office.

ICT CHANGE MANAGEMENT

Opinion: Amber	2 September 2015	
Total:	Priority 1 = 0	Priority 2 = 7
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	07	

Overall Conclusion is Amber

All changes to the ICT environment, including emergency maintenance and patches, should be formally managed and controlled. This helps to manage the risk of negatively impacting the stability or integrity of the "live" environment and the introduction of errors and data corruption.

The documented IT Change Management procedure is dated 2009 and is out of date. It should be reviewed and updated to ensure all relevant staff are aware of the current procedures and processes for making changes to the ICT environment. The change authorisation process and change triage process are documented separately and should be formalised by being included in the revised Change Management procedure.

Change requests are logged and managed on Supportworks, which is ICT's service management tool. There is a daily Change Advisory Board (CAB) which is responsible for reviewing and approving all major/significant changes. However, we identified some exceptions whereby CAB had not approved

major/significant changes as they had either been logged incorrectly or had been approved at a lower level by the change triage process. Our testing also found that some major/significant changes were not supported by a Data Form, which records key information about the change, including a back-out plan, communication plan and test plan. A formal risk assessment of all major/significant changes is also not undertaken.

There is currently no formal reporting on the change management process, although this being addressed through the development of a dashboard that will provide various performance figures for ICT. Changes that have breached their agreed SLA are automatically escalated within Supportworks.

Urgent changes are covered in the existing Change Management procedure but they are not defined and there are no criteria for when they should be used. This could lead to changes being classed as urgent to avoid following the normal change process.

A corporate approach to testing changes has not been documented and hence there is no requirements guidance available to engineers. The Data Form has a section to record the test plan and we found that it had been completed for the sample of changes that were reviewed. However, the lack of any guidance means that the actual testing undertaken is not recorded and evidenced.

When logging a request for change, Supportworks has the facility to identify all documentation that needs to be updated. However, our sample testing found that this information is not entered and there is no evidence of what documentation has been updated, if any, following the change. This increases the risk of the information held in the CMDB (Configuration Management Database) being out of date.