APPENDIX A

Internal Audit Service

Key Outcomes from Internal Audit Reports Issued Between October 2016 and March 2017

May 2017

1 Introduction – the Framework of Governance, Risk Management and Control

1.1 Internal Audit is an independent and objective assurance function designed to add value and improve an organisation's operations. Under the Public Sector Internal Audit Standards (PSIAS), Internal Audit is required to help an organisation accomplish its objectives by "bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

1.2 It is important that the Audit Committee receives regular updates on key findings and governance themes from Internal Audit's work. This is also emphasised in the PSIAS which requires the Chief Internal Auditor to provide an annual opinion on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control, and to report on emerging issues in year.

1.3 In our organisation, the Chief Internal Auditor's formal opinion is reported to the Audit Committee each May, timed to support preparation of the Authority's Annual Governance Statement. 'Opinion' in this context does not mean 'view', 'comment' or 'observation'; it means that Internal Audit must have performed sufficient, evidenced work to form a supportable conclusion about the activity it has examined.

2 Purpose of this Report

2.1 This report summarises the outcomes from Internal Audit reports which were finalised in consultation with management and issued in the six month period October 2016 to March 2017. Reporting on this period allows management the opportunity to have implemented and embedded recommendations; and Internal Audit to have then reviewed this implementation and to form a judgement on whether the control issues identified have been satisfactorily addressed. Information has been provided on the level of assurance for each audit (described below), the number of recommendations made (classified according to priority), areas of good practice identified, and main findings. The progress made/action taken by management in respect of key issues identified from each audit has also been included. As discussed at previous meetings of the Audit Committee, Internal Audit has also followed up and evidence checked reported progress, on a sample basis weighted according to priority and materiality.

2.2 It is intended that, by providing regular reports on key outcomes from Internal Audit's work, this will enable the Audit Committee to develop an ongoing awareness of the soundness of the framework of governance, risk management and control, in addition to receiving the Chief Internal Auditor's annual opinion on this matter each May.

3 Opinion on the Framework of Governance, Risk Management and Control (May 2017)

3.1 On the basis of Internal Audit work performed and described in this report, the report of the preceding period considered by the Audit Committee in November 2016, and work performed from the approved Strategic Audit Plan for 2016/17, the Chief Internal Auditor's opinion is that the organisation's internal systems of governance, risk management and control are **satisfactory**. This is a positive opinion for the organisation.

3.2 In this report, details of four audit opinions are presented. Of these, three (75%) were 'moderate assurance' opinion classification or higher. No 'critical priority' recommendations were made.

4 Opinion Framework

4.1 A framework of opinion classifications is used in Internal Audit reporting. The framework applies an overall assurance judgement to each system audited, as defined below.

Full Assurance	There is a sound system of control with key controls consistently applied.
Significant Assurance	There is a sound system of control, although there are some minor weaknesses in the system and/or occasional non-compliance with key controls.
Moderate Assurance	While there is a basically sound system of control, there are some weaknesses in the system and evidence of regular non-compliance with key controls.
Limited Assurance	The system of control is insufficient.
No Assurance	There is no system of control in place.

Note: With effect from April 2017, use of the Moderate Assurance opinion classification is being discontinued.

4.2 The opinions given to audits issued during this period are shown in **Section 5**.

4.3 In addition to the overall opinion given on every internal audit, individual recommendations within each report are classified as critical, high, medium or low priority. This prioritisation is designed to assist management in assessing the importance of each recommendation. The definitions of these priority classifications are set out in the following table:

Priority	Description
1* Critical	Action considered imperative to ensure the organisation is not exposed to unacceptable risks.
1 High / Fundamental	Action that is considered imperative to ensure that the service area / establishment is not exposed to high risks.
2 Medium / Significant	Action that is considered necessary to avoid exposure to considerable risks.
3 Low / Less Significant	Action that is considered desirable or best practice and would result in enhanced control or better value for money.

4.4 Prioritisation of Internal Audit recommendations is controlled through Internal Audit's quality control and file review processes.

4.5 In addition to performing internal audits of existing systems within the Authority and responding to queries on the operation of such systems, Internal Audit has a significant and increasing role in advising on new systems within the Authority. Programme assurance and project boards supported by Internal Audit are shown below. Whilst time spent on such assurance work reduces the number of available audit days, it is considered an efficient use of Internal Audit resource, in that assurance is obtained that effective controls are incorporated into new systems from the outset. In turn, this minimises the risk of weaknesses in systems and strengthens the control environment. Internal Audit has supported the following Project Boards (in a programme assurance role) and Working Groups during the period under review:

- Information Security Group
- ICT Performance and Prioritisation Board
- Customer Journey and Digital Strategy Delivery Board
- Sundry Debtors System Replacement
- Social Care Case Management System Replacement
- Office 365 & SharePoint (collaborative tooling solution)
- Robotic Process Automation
- Business Reporting and Analytics
- Oracle iSupplier
- Cashless Projects
- Academy Converters Working Group

4.6 Internal Audit has also supported a several special investigations and management requests in this time period. Due to the nature of this work, it is not appropriate to report findings in detail (as this may weaken the control environment) at this juncture. However, key themes arising from this work will be included in Internal Audit's annual report.

IA/AHM/KM/SC
May 2017

5 Main Outcomes – Audit Reports Issued During the Period October 2016 to March 2017

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	**High**	**Medium**	**Low**
1	IT Service Management (ITSM) System Review	To determine whether the systems and procedures in operation for ITSM are functioning satisfactorily and are in accordance with legislation and the stated priorities within the Council Plan. To further determine whether the system supports the principles of the Target Operating Model and self-service.	**Significant**	0	0	2	5

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• Tables have been identified and enabled for auditing. Both pre and post changes can be viewed and users can not amend or switch off the audit functionality. • ITSM provides its users with built in searches which can be easily adapted for ad hoc reporting and exported into a spreadsheet.	• ITSM is only used by ICT and one of the organisation's decentralised system support teams. There is a risk that the organisation may not benefit from a consistent approach to the recording and management of support calls. • ITSM does not support the principles of the Target Operating Model in relation to the organisation's drive for self-service. ITSM is regarded as an 'end of life' system and there are no plans by the software supplier to enhance the current version of the application. ITSM may not meet the organisation's future needs.	Four of five low priority recommendations have been self-certified as complete by ICT. Action to address the remaining low priority recommendation and both medium priority recommendations is dependent on replacing ITSM with a new application by the agreed target date of 01/04/2018. ICT has advised that a replacement for ITSM is proposed within the capital plan for 2017/18 but indications are that demand will exceed available budget and as such it is unlikely that an ITSM replacement will be funded in 2017/18. ICT's decision to delay replacing ITSM has been taken following a risk assessment of all projects in the proposed 2017/18 capital plan and on the basis that ITSM is still supported by the supplier and meets the basic business need.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
2	Perimeter Security	To determine whether the organisation's systems of control provide adequate protection against the risks associated with virus / hacking attacks, are in accordance with legislation and the stated priorities within the Council Plan.	**Moderate**	0	1	10	14

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• Strong authentication controls are in place to minimise the risk of inappropriate access to the corporate firewalls and the ability for firewall rules to be modified. • The corporate network is subject to independent penetration testing and vulnerability scans to identify weaknesses which are reported to ICT Services for corrective action. • 'Mimecast' software scans all incoming Internet mail before it enters the organisation's network minimising the potential risk of spam or virus infected emails. 52% of all email sent to the organisation are rejected. • Devices are configured to check Sophos for new virus definitions multiple times during each day to ensure they are protected against the most recent threats. • Universal Serial Bus (USB) devices must be approved by ICT Services before they can be used. All devices are automatically checked for viruses before access to stored data is permitted.	• Approximately 10% of the organisation's Microsoft Structured Query Language (SQL) servers and operating systems estate is unsupported. Software vulnerabilities are at greater risk of being exploited once support ceases, as security patches are no longer released. • There is no process in place to verify that Sophos anti-virus client software is installed during the Windows server build process and no assurance that it has been installed on all desktop devices. • The organisation's Windows servers and desktop devices and firewalls were not protected with the latest security updates and are at increased risk of malware attack. • ICT Security training available via the Learning Pool is not mandatory and less than half of the organisation's computer users have completed it. • Password controls to access tablet devices and mobile phones which can access corporate email are weaker than the standard applied to desktop and laptop devices and do not meet the requirements of the Information Computer Security Policy. • Not all tablets are managed by the corporate mobile device management solution and ICT Services employees have not been trained in its use since it was implemented in 2014.	ICT has confirmed that work to address the high priority recommendation relating to unsupported software impacting Public Services Network (PSN) compliance is on-going. Evidence checking has confirmed that four of ten medium priority recommendations have been implemented with a further two part implemented and four not implemented. Implementation of the Dell KACE management system is on-going and agreement for software patching windows has been obtained to enable the Authority to maintain a high level of protection against external threats. Eight of fourteen low priority recommendations have been self-certified as complete by ICT with a further three part implemented and three not implemented. Action to address three of the recommendations that have not been implemented (two medium and one low priority recommendation) are dependent on determining whether comparable functionality is available within the Authority's chosen collaborative working solution (Office 365). As such, ICT's decision to defer action to address these recommendations until an implementation partner for 365 is appointed is considered reasonable.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
3	ICT Business Continuity Planning (BCP) and Disaster Recovery (DR)	To determine whether the controls and procedures in place to maintain access to the Authority's computerised systems, applications and information are adequate and operating effectively. To further determine whether, in the event of a disaster or significant event causing major disruption to the Authority's data processing capabilities, ICT has business continuity management and disaster recovery plans in place that will minimise any disruption to processing of business critical applications.	**Limited**	0	0	11	10

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• Responsibility for maintaining the accuracy of ICT's BCP documentation is clearly defined. • ICT's BCP is recorded in multiple documents specific to individual technologies/disciplines that are saved with other BCP documents to encrypted memory sticks held by nominated ICT employees. • Secure back up arrangements exist for all unstructured data held on the storage area network (SAN) and structured data held within business applications. Data is backed up to primary back up media located at the DR site and replicated to secondary back up media located within the primary data centre.	• Infrastructure located at the secondary (DR) data centre currently located within the Killingworth site would not provide a satisfactory level of resilience should BCP/DR plans be invoked. • There is no second site resilience for the Internet, Citrix and multiple business applications hosted on virtual machines (VM). • There is no DR for Windows based applications. • Interdependencies between applications may not have been addressed when determining DR arrangements. • Delays communicating ICT issues including virus alerts may have exposed the organisation to an increased risk of widespread disruption to business processing. • There are single points of failure across ICT should key employees be unavailable. • The level of insurance cover for ICT assets is not based on an assessment of actual value.	Evidence checking has confirmed that two of eleven medium priority recommendations have been implemented with a further four part implemented and five not implemented. One of the part implemented and three of the five not implemented recommendations are yet to reach their target date but discussion with ICT has confirmed that target dates will not be achieved. All of the main issues identified remain outstanding and although resilience for Unix based applications and the Internet has been enhanced, ICT's focus in the period under review has been to stabilise the current infrastructure and address the significant number of issues required to ensure on-going PSN compliance. Six of ten low priority recommendations have been self-certified as complete by ICT with a further two part implemented and two not implemented.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
4	BACS (Bankers' Automated Clearing Service) System Review	To determine whether the systems and procedures in operation for the BACS system are functioning satisfactorily and are in accordance with legislation and Council policy.	**Significant**	0	0	2	24

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• The system provides opportunities to create an effective separation of duties and allows different settings to be applied to each category of user. There are 37 live BACS users (excluding two system administrators) 32 of whom are assigned a specific responsibility (submit or approve) within one of six unique roles. • Sort code and account number field lengths are set within the C-Series BACS application so applying validation over field length and format. C-Series incorporates mandatory modulus checking, which is an arithmetic check that establishes whether there is a valid link between a given sort code and account number range, and the Extended Industry Sort Code Directory (EISCD), which is a monthly download. • There are a number of contingency arrangements in place should there be any loss of links in the BACS transmission process.	• BACS transmissions are a two-stage and two-person process in all service areas with the exception of Employee Services where Payroll transmissions are a two-stage and one-person process. There are five Employee Services employees within the 'PAYROLL ALL' group. Discussion with the Employee Services Manager and the Employee Services employee undertaking BACS transmissions identified that management checks were being undertaken outside the BACS application despite the Employee Services Manager being a BACS user. A single person process may increase the potential for input errors to remain undetected resulting in incorrect transmissions. • Payroll transmissions are typically processed on the last possible day to meet payment deadlines. Timing of the transmissions means that a failure of any link in the BACS process could have rendered the majority of business continuity arrangements unusable meaning that salary and other payroll payments may be delayed. Any failure to pay employees etc. on the correct date may incur additional costs as employees incurring bank charges as a result of late payments would be able to reclaim those costs from the organisation. Late payments may damage the Authority's reputation.	Evidence checking has confirmed that both medium priority recommendations have been addressed and evidenced. Unique Approval and Submit roles have been created in BACS for Payroll users and the 'PAYROLL ALL' group has been disabled to enforce a two-stage and two-person process, thereby reducing the risk of human error. Payroll BACS transmissions have been brought forward whenever possible to provide sufficient time for contingency arrangements to operate as intended should there be a failure at any stage of the BACS process. 17 of 24 low priority recommendations have been self-certified as complete leaving seven low priority recommendations that have exceeded their original target dates. Several low priority recommendations have been classed as complete because ICT has undertaken the agreed action. However, the wider organisation has not responded to requests from ICT to, for example, review their BACS user base to disable obsolete users or create new users to improve resilience. In these cases, the risks to the organisation have not been addressed.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
5	Automation of Key Controls	To identify the main control points and risks in each of the Authority's key financial systems and determine whether these are being effectively monitored and managed. To further determine whether potential exists to automate some of the key controls within each system by implementing a form of continuous auditing through the development and automatic generation of management information (MI) reports that would enhance current reporting arrangements. Financial systems reviewed in the period are Debtors, Procure to Pay and Payroll.	N/A	0	0	0	0

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• The audits identified good practice in each of the business areas reviewed with good use being made of the proprietary reporting tools available within the business applications. • A project is underway to replace the current Debtors system with the Ash Debtors system. An initial review of the Ash reporting suite indicated it was comprehensive.	• Oracle Discoverer is in use for reports generated from the Oracle e-business suite of applications. As Discoverer is no longer supported and scheduled to be replaced, it is unlikely that there will be any appetite for further development of reports until a replacement solution is procured and implemented. • Current reporting tools for each application could be utilised to provide enhanced management information over key controls and to address recurring themes identified in key financial system audits. However, current reporting tools require users to generate reports rather than automatically generating, posting and alerting designated users of exceptions/anomalies. A new business reporting and analytics solution (contract awarded w/c 24/04/2017) has the potential to provide the same reports but in a proactive fashion and without reliance on end users.	There is currently no facility in Discoverer or the Ash system that eliminates the requirement for users to generate reports. If set up to do so the Ash system can generate prompts to users when a report is due to be run but users still have to access the system to run the report. The Ash system will also generate reminders to users if they have not run reports on the scheduled processing date. Implementation of a business reporting and analytics solution in 2017 increases potential for Internal Audit's approach to audits of key financial systems to change from 2017/18 onwards. However, at this point there is no clear indication of the resources required and available to develop reports in the eventual solution and no target date for specifying and developing enhanced MI/BI requirements beyond the development of standard finance and human resources reports.

6 Evidence Checking

6.1 Internal Audit reports issued during the period October 2016 to March 2017 included one high priority and 25 medium priority recommendations. In respect of these 26 recommendations, eight medium priority recommendations have been self-certified by management as fully implemented and revised target dates are being considered for the remaining recommendations. All medium priority recommendations self-certified as implemented were selected for evidence checking.

6.2 Details of those recommendations subject to evidence checking by Internal Audit are detailed in section 5 of this report, above. Summary information regarding the sample of evidence checking undertaken is provided in the table below.

Summary of results of evidence checking by Internal Audit, of medium priority recommendations self certified as implemented by management as at May 2017.

Priority	Total Number of Recommendations Evidence Checked	Number confirmed as Implemented		Number Requiring Additional Action	
		No.	%	No.	%
Critical	0	N/A	N/A	N/A	N/A
High	0	0	0%	0	N/A
Medium	8	8	100%	0	0%
Total	8	8	100%	0	0%