APPENDIX A

Internal Audit Service

Key Outcomes from Internal Audit Reports Issued Between April 2017 and March 2018

May 2018

North Tyneside Council

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 twelve month period April 2017 to March 2018. 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 2018)

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 May 2017, and work performed from the approved Strategic Audit Plan for 2017/18, 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 six audit opinions are presented. Of these, three (50%) were 'significant assurance', one (17%) was 'moderate assurance' and two (33%) were 'limited assurance' opinion classification. No 'critical priority' recommendations were made. In addition to the six formal audit reports issued in the period, Internal Audit prepared a briefing note for the Head of Law and Governance in her capacity as the Authority's Senior Information Risk Owner (SIRO) to provide her with a summary of Internal Audit findings in relation to a review of the annual code of connection submission to the Public Services Network Authority as prepared by ICT Engie.

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	The system of internal control is designed to meet the organisation's objectives and controls are consistently applied in all the areas reviewed.
Significant Assurance	There is a generally sound system of control designed to meet the organisation's objectives. However, some weakness in the design or inconsistent application of controls put the achievement of particular objectives at risk in some of the areas reviewed.
Limited Assurance	Weaknesses in the design of, or regular non-compliance with, key controls put the achievement of the organisation's objectives at risk in some or all of the areas reviewed.
No Assurance	Significant weaknesses in the design of, or consistent non-compliance with, key controls could result (or have resulted) in failure to achieve the organisation's objectives in the areas reviewed.

Note: Use of the Moderate Assurance opinion classification was discontinued from April 2017 but was allowed for one of the audits included within this report as the assurance level had been agreed with the audit client in advance of April 2017.

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 Working 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)
- Oracle iSupplier

4.6 Internal Audit has also supported 23 special investigations and management requests in this time period. Key themes arising from this work will be included in Internal Audit's annual report.

IA/AHM/KM/SC
May 2018

5 Main Outcomes – Audit Reports Issued During the Period April 2017 to March 2018

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
1	Housing Benefit (HB) and Council Tax Support (CTS)	To provide assurance to the Authority on the following key areas: • Arrangements in place to manage the introduction of Universal Credit (UC); • The procedures in place to ensure HB BACS payments are correct and paid at the right time; • Key Performance Indicator (KPIs), including monitoring and assessment of their effectiveness, with particular reference to reconsiderations and appeals; • Quality Assurance (QA) arrangements; • The current CTS scheme; and • The processes and procedures involved in the recovery of HB overpayments.	**Significant**	0	0	3	0

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• The client management team and ENGIE are effectively managing the phased introduction of UC, which was originally scheduled to replace HB in North Tyneside by February 2018, and following the recent budget is now scheduled for May 2018. Claim levels are regularly monitored along with the impact on resources.	• The current Quality Assurance Key Performance Indicator requires ENGIE to check 5% of all claims processed on a daily basis, with sanctions for poor performance. It would be beneficial to the Authority to examine the current process to determine if the resources could be more effectively utilised to target higher risk areas. • HB debt levels were approximately £7.3m and have increased since responsibility was transferred externally. The client management team believe there has been a lack of resources for HB overpayment recovery and there is no formal KPI in place to provide a mechanism for the Authority to influence performance in this area.	• This was raised with the Client Manager who requested no change. The Benefits Service decided to undertake additional checks, however, these are yet to commence as resource has been required on other areas, for example, introduction of UC and the Information@Work application. • An extra resource has been employed on HB debt recovery and a new KPI introduced in April 2018 for overpayment recovery levels. HB debt levels have not reduced but this is because more debt is being raised following initiatives between the Benefits Service, DWP and HMRC to data match HB debt that identifies more debt and enhances recovery.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
2	Business Rates (NNDR)	To examine and evaluate whether the systems and procedures in operation for the business rates system are fit for purpose and support the delivery of business goals. Key risks relating to this high value/volume area and the impacts on strategic goals such as growing the economy and attracting new businesses will be examined.	**Significant**	0	0	0	4

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• An established process is in place to ensure year end billing is run in an effective and timely manner. Officers adhere to the Northgate manual and a reconciliation is completed. • There is a well established process for the reconciliation of business rates income. Daily cash reconciliations are carried out by Business Rates Team, and the Revenues and Benefits Development and Support Team reconcile business rates income on a monthly basis to the general ledger.	• The Business Rates Clerk aims to review a ward file per month to identify potential visits, however, it was confirmed that some reviews were outstanding by approximately one year. • Users were identified with access permissions to Northgate in excess of their business need, which had the potential to enable incorrectly coded transactions within the Business Rates suspense account to be transferred to another account. • Revenues and Benefits Team Officers are responsible for monitoring the Business Rates suspense account but also have access permissions to make transfers resulting in a lack of separation of duties.	• Empty property inspections are still undertaken but the Revenues Service use a more target based approach. This ensures they inspect properties identified using the six week occupation rule to qualify again for exemptions, which are sent for inspection when actioned on the system. The Revenues Service also target companies and rates advisors known for using rates avoidance strategies. • A review of the user base and access permissions was undertaken September 2017. The ability of officers to transfer out of suspense is accepted to be a part of normal duties and monies can only be transferred within NNDR, however, the potential to transfer monies from suspense into, for example, an associate's account is recognised by the Revenues Service and this risk is being managed by management monitoring of suspense account transactions.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
3	Hardware and Software Management	To determine whether controls and procedures in operation over the acquisition, management, reconciliation and disposal of the Authority's computer hardware and software assets are appropriate and operating effectively.	**Significant**	0	0	2	15

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• ICT has formal change control procedures in place for installed software that are documented within the ICT Change Management document. All change requests are logged within the Authority's IT Service Management system (ITSM). Each change request is provided with a unique reference number, applied by the system. Once logged, requests are risk assessed and authorised prior to being actioned, following which testing is completed to ensure systems are operating correctly. Where possible, which applies to the majority of systems, changes are applied and tested within a test system environment prior to being applied to the live system.	• CISCO NetApp hard drives, covered under 3-year warranty, are sent back to the manufacturer if a disk failure occurs. CISCO Netapp disks are not encrypted and may contain sensitive data which would be accessible by a third party when sent away for repair. • There were a number of third parties that accessed systems for which Information Security Assessments were not available. Additionally, Confidentiality Agreements and signed Acceptable Use Policies / Codes of Connection requested by Internal Audit were not available.	• ICT contacted ProAct (supplier of NetApp drives) who confirmed that there are established procedures for the management of hard disks returned through the returns merchandising authorisation process i.e. from the point of shipment through testing, overwriting, and final disposition. At no point in this process do any NetApp or NetApp-contracted personnel access customer data residing on a returned drive. • ICT has developed a task list for all new projects managed by ICT that includes a requirement for project managers to consider whether information sharing agreements are required. This is supported by an increased awareness of the circumstances under which a Privacy Impact Assessment (or Data Protection Impact Assessment as it is referred to in the General Data Protection Regulation) should be undertaken, by whom and whether the ICO needs to be consulted. This does not address existing contracts where there is no assurance that information sharing/data processing agreements are in place. The issue is further complicated as ICT is not responsible for all contracts, for example, responsibility for the Northgate contract still resides with the Authority.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
4	Access Approvals	To determine whether the controls and procedures in place to authorise access to information held electronically provide the Authority with assurance that access to information is correctly restricted and, where appropriate, segregated between the Authority and its business partners.	**Moderate**	0	1	2	5

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• Areas of good practice were identified in relation to the ICT Service Desk's management of telephone requests and also the controls in place to manage password resets for business applications.	• e-Forms were developed using Oracle Portal. The installed version of Oracle Portal is 9.0.4 which was de-supported by Oracle in 2008. The server hosting the software is ten years old and therefore sourcing spare parts in the event of failure has become increasingly difficult. The operating system installed on the server is Solaris 9, for which extended support ended in October 2014, and supporting databases operate using Oracle 9i, which was de-supported in July 2010. Hardware and software infrastructure hosting e-Forms is unsupported and its continued use poses a risk to the Authority's connection to the Public Services Network (PSN).	• A project to develop a new e-Forms process has been passed to the Customer Journey application team with a target date of August 2018 for completion. All applications on the de-supported Oracle Portal have been reviewed by ICT in association with business areas and have either been deleted or are being migrated to a supported platform with a target date of August 2018. A replacement for the Authority's flexible time recording system is being considered and, if a replacement system is not in place by August 2018, the de-supported Oracle Portal will be firewalled off from the rest of the network.
	• Requests for access to data volumes on the Storage Area Network (SAN) are not subject to effective challenge and may lead to inappropriate access. Access is controlled by including users in File Access Groups (FAGs), however, users are not aware of the FAGs to which they have been assigned and each user can be assigned to multiple FAGs of which there are approximately 2,500. Membership of FAGs is not subject to periodic review.	• This issue is being addressed as part of the implementation of SharePoint which includes a review and update of Active Directory. However, unless the Storage Area Network is decommissioned there will still be a requirement to review and rationalise FAGs. The target date for addressing this issue has passed but that is mainly due to delays in the SharePoint project which is currently scheduled to be implemented by the end of 2018.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
5	Information Governance – Preparation for General Data Protection Regulation (GDPR)	To review arrangements in place to prepare for the European Union's GDPR. GDPR replaces Data Protection Directive 95/46/EC and will be enforced across all EU member states by 25 May 2018 at which point penalties associated with non-compliance increase in comparison to the Data Protection Act (DPA).	**Limited**	0	0	5	0

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• Key decision makers within the organisation have been made aware that the law is changing to the GDPR and of the likely impact and have identified areas that could cause compliance problems under GDPR. • The organisation's privacy notices (corporate and service specific) have been reviewed and arrangements are under consideration/in place to make any necessary changes in order to include the increased requirements of GDPR. • The organisation has developed effective policies and procedures to detect, report and investigate any potential personal data breach. • The Authority has designated the Information and Records Manager as its Data Protection Officer (DPO).	• A number of the organisation's systems and applications that record personal data would not facilitate portability of that data electronically and in a commonly used format. • Data controllers must have an authentication procedure in place to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by GDPR. It was unclear whether an authentication procedure would be in place to verify the identity of the person making the SAR. • It was unclear whether a cost/benefit analysis of providing data subjects with on-line access to their data had been undertaken or considered and whether, as a result, a system would be developed. • The organisation had not formally assessed the types of data it holds or documented which types would fall within the notification requirement if there was a breach. • The Authority had not reviewed the terms of its partnership and data processing agreements to consider GDPR implications.	• This issue has not been progressed but will be examined on a case by case basis if requests for data portability are received. • There remains a lack of clarity in relation to what is considered to be the required level of identity assurance. The process currently in place provides reasonable assurance and exceptions, for example, homeless persons or persons just out of prison are subject to additional checks. • Development of an application to provide data subjects with secure and authenticated on-line access to their data would be a considerable undertaking that will not be progressed until the Information Commissioners Office (ICO) defines the required level of identity assurance. • Completion of a data audit has provided the organisation with a clear understanding of what data breaches would need to be reported to the ICO. The new breach reporting process includes a risk assessment and scoring mechanism. • A process to review terms of the Authority's partnership and data processing agreements is on-going.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
6	School ICT Thematic Reviews	To assess, on a thematic basis, the application of controls associated with the discharge of responsibilities relating to ICT Assurance, within a sample of schools.	**Limited**	0	1	6	9

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• Where USB storage devices were identified in use by school staff appropriate encryption standards were applied. • All wireless networks examined were configured with industry standard encryption to minimise the risk of unauthorised access. • Where schools permitted Bring Your Own Devices (BYOD), access to the internet was provided but without the potential to access main school networks. • Specialist software to monitor key words and phrases is in use within some schools, which provides real time email alerts to nominated staff members including screenshots of the access to allow potential safeguarding decisions to be made in a timely manner. • Several schools use a software application (CPOMS) for monitoring child protection, safeguarding and a whole range of welfare issues, replacing the traditional paper based methods to record such information.	• Weaknesses in the protection of devices from malware threats. • The security applied to mobile devices was generally insufficient to minimise unauthorised access to potentially sensitive pupil data. • Weaknesses in the monitoring of access to online content may impact on schools' ability to comply with statutory legislation. • Schools may not have the in-house skills necessary to configure appropriate security when implementing critical systems i.e. email. • Systems hosted internally and externally that hold sensitive personal data were not protected with two-factor authentication. • Data Sharing Agreements were not in place for the majority of instances where schools share personal data with 3rd party organisations. • Disaster recovery/business continuity plans lack documented procedures which would allow an appropriately skilled ICT Technician to restore systems and data.	• Issues arising from the audit were presented at a Head Teachers' forum in January 2018. A briefing note to governors will be circulated before the end of the summer 2018 term. The autonomy of schools means the Authority can advise schools but cannot enforce controls. • Risks to the corporate network associated with weaknesses in schools ICT environments will be addressed by a network segregation project being implemented by ICT that is scheduled to be complete by the middle of 2018. This project will include the deployment of individual firewalls between each school and the corporate network.

	Audit Title	Audit Objectives	Assurance Opinion	Recommendations			
				Critical	High	Medium	Low
7	Public Services Network (PSN) Code of Connection Submission 2017	To determine whether ICT responses in the 2017 Code of Connection (CoCo) are a fair representation of controls and procedures either under development or planned to be implemented across the Authority's ICT network infrastructure and associated devices.	Not Applicable	-	-	-	-

Good Practice Highlighted	Main Issues Identified	Progress Made / Action Taken
• ICT has enabled effective anti-virus and content filtering software. • Mobile device management software has been deployed across tablets and mobile telephones that encrypts data and allows devices to be remotely wiped should they be lost. • Effective physical security is in place to restrict access to the Authority's key infrastructure assets and logical access controls have been applied by ICT to enhance desktop security. • An intrusion detection system (IDS) that monitors the network for malicious activity or policy violations has been supplemented by implementation of a complementary intrusion prevention system (IPS). • IT Health Checks (ITHC) are undertaken by certified suppliers and the most recent ITHC is issued to the PSNA.	• A lack of progress on key issues, including the replacement of unsupported operating systems, that were included in ICT's 2015 and 2016 remedial action plans and reported to the PSN Authority (PSNA) as underway, were likely to result in increased scrutiny of the 2017 submission. • The 2016 submission, issued September 2016, was initially rejected by the PSNA who expressed concern over the time proposed to address several issues and considered some timescales for remedial action to be unacceptable, specifically high priority issues that remained open more than 3 months beyond the date of the external IT Health Check (ITHC). The 2017 submission included timescales for high priority issues that extend over several months. • The presence of a number of issues in the 2017 remedial action plan that had previously been reported in the 2015 and 2016 plans indicated that remedial work was not being completed as planned. In some cases action is deferred until the following CoCo submission increases its urgency. This is an issue that, following the 2016 review, is likely to draw attention from the PSNA.	• The 2017 PSN submission issued December 2017 has not been approved by the PSNA. This is primarily due to the number of outstanding issues still in planning stages and the timescales proposed for addressing weaknesses highlighted in the ITHC. • In April 2018 the PSNA requested an update on issues including the decommissioning of Windows 2003 servers and the network segregation project. The number of Windows 2003 servers still in use has reduced to five (two in libraries, one in leisure and two in schools) and will be resolved initially by implementing network segregation and, for schools, installing firewalls between schools and the corporate network. • Increased resource in the ICT Security team is allowing internal scans of the network to be undertaken as a proactive measure rather than awaiting the results of external scans. • Imminent implementation of Microsoft's System Centre Configuration Manager will automate patch management, software distribution, operating system deployment to the desktop estate further enhancing PSN compliance.

6 Evidence Checking

6.1 Internal Audit reports issued during the period April 2017 to March 2018 included two high priority and eighteen medium priority recommendations. In respect of these twenty recommendations, one high priority and eleven medium priority recommendations have been self-certified by management as fully implemented, five medium priority recommendations have not reached their target dates and revised target dates are being considered for the remaining recommendations. All high and medium priority recommendations in the audits in scope 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 high priority and medium priority recommendations self certified as implemented by management as at May 2018.

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	1	1	100%	0	0%
Medium	11	11	100%	0	0%
Total	12	12	100%	0	0%