NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

25 SEPTEMBER 2014

INTERNAL AUDIT REPORT ON INFORMATION TECHNOLOGY, CORPORATE THEMES AND CONTRACTS

Report of the Head of Internal Audit

1.0 PURPOSE OF THE REPORT

1.1 To inform Members of the **internal audit work** completed during the period to 31 August 2014 in respect of information technology (IT), corporate themes and contracts and to give an opinion on the systems of internal control in respect of these areas.

2.0 BACKGROUND

2.1 The Audit Committee is required to assess the quality and effectiveness of the corporate governance arrangements operating within the County Council. In relation to IT, corporate themes and contracts, the Committee receives assurance through the work of internal audit (provided by Veritau) as well as receiving copies of relevant corporate and directorate risk registers. Veritau engages a specialist contractor to support the provision of IT audit services. Since 1 April 2013, that service has been provided by Audit North. Details of the 3 year strategic IT audit plan (to March 2016) prepared by Audit North, were presented to the Committee in December 2013.

2.2 This report considers the work carried out by Veritau and Audit North during the period to 31 August 2014. It should be noted that the internal audit work referred to in this report tends to be cross cutting in nature and therefore there are no corresponding Statements of Assurance (SoA) or directorate risk registers.

2.3 The Corporate Risk Register (CRR) is fully reviewed every year and updated by the Chief Executive and Management Board in August / September. A six monthly review is then carried out in February / March. Details of the Corporate Risk Register were presented to the Committee in June 2014. There have been no significant changes in the County Council's risk profile since that date. A copy of the updated Corporate Risk Register will be presented to the committee once the current review is completed.

.

3.0 WORK CARRIED OUT DURING THE PERIOD TO 31 AUGUST 2014

3.1 Summaries of the internal audit work undertaken and the reports issued in the period are attached as follows:

IT audit assurance and related work	**Appendix 1**
Corporate assurance	**Appendix 2**
Contracts and procurement	**Appendix 3**

3.2 Internal Audit have also been involved in a number of related areas, including:

- providing advice on corporate governance arrangements and IT related controls;
- providing advice and guidance to directorates and schools on ad hoc contract queries and on matters of compliance with the County Council's Contract and LMS Procedure Rules;
- attending meetings of the Corporate Information Governance Group (CIGG), the Corporate Procurement Group (CPG) and various project groups relating to 2020 North Yorkshire;
- contributing to the annual review and update of the County Council's Financial, Contract and Property Procedure Rules;
- completion of the audit certificate for the Carbon Reduction Commitment (CRC) Energy Efficiency return prior to its submission to the Environment Agency in July 2014;
- reviewing the final accounts for capital projects. Using a risk based process, Veritau auditors identify those projects which need to be reviewed in more detail and request the relevant documentation;
- carrying out a number of special investigations into corporate or contract related matters that have either been communicated via the whistleblowers' hotline or have arisen from issues and concerns raised with Veritau by management.

3.3 As with previous audit reports an overall opinion has been given for each of the specific systems or areas under review. The opinion given has been based on an assessment of the risks associated with any weaknesses in control identified. Where weaknesses are identified then remedial actions will be agreed with management. Each agreed action has been given a priority ranking. The opinions and priority rankings used by Veritau are detailed in **appendix 4**.

3.4 It is important that agreed actions are formally followed up to ensure that they have been implemented. Veritau formally follow up all agreed actions on a quarterly basis, taking account of the timescales previously agreed with management for implementation. **On the basis of the follow up work undertaken during the year, the Head of Internal Audit is satisfied with the progress that has been made by management to implement previously agreed actions necessary to address identified control weaknesses.**

3.5 All internal audit work undertaken by Veritau is based on an Audit Risk Assessment. Areas that are assessed as well controlled or low risk are reviewed less often with audit work instead focused on the areas of highest risk. Veritau's auditors work closely with directorate senior managers to address any areas of concern.

4.0 AUDIT OPINION

4.1 Veritau performs its work in accordance with the Public Sector Internal Audit Standards (PSIAS). In connection with reporting, the relevant standard (2450) states that the chief audit executive (CAE)[1] should provide an annual report to the board[2]. The report should include:

(a) details of the scope of the work undertaken and the time period to which the opinion refers (together with disclosure of any restrictions in the scope of that work)

(b) a summary of the audit work from which the opinion is derived (including details of the reliance placed on the work of other assurance bodies)

(c) an opinion on the overall adequacy and effectiveness of the organisation's governance, risk and control framework (i.e. the control environment)

(d) disclosure of any qualifications to that opinion, together with the reasons for that qualification

(e) details of any issues which the CAE judges are of particular relevance to the preparation of the Annual Governance Statement

(f) a statement on conformance with the PSIAS and the results of the internal audit Quality Assurance and Improvement Programme.

4.2 The overall opinion of the Head of Internal Audit on the framework of governance, risk management and control operating across the three functional areas is that it provides **Substantial Assurance**. There are no qualifications to this opinion. With the exception of IT audit, no reliance has been placed on the work of other assurance bodies in reaching this opinion. As noted above, the Head of Internal Audit commissioned specialist IT audit services during the period from Audit North to support the delivery of this aspect of the Audit Plan. The Head of Internal Audit is satisfied with the quality of this work and has therefore placed reliance upon it in reaching his opinion.

5.0 RECOMMENDATION

5.1 That Members consider the information provided in this report and determine whether they are satisfied that the overall control environment operating in respect of information technology, corporate and contract arrangements is both adequate and effective.

[1] For the County Council this is the Head of Internal Audit.
[2] For the County Council this is the Audit Committee.

Max Thomas
Head of Internal Audit

Veritau Ltd
County Hall
Northallerton

27 August 2014

BACKGROUND DOCUMENTS

Relevant audit reports kept by Veritau Ltd at 50 South Parade, Northallerton.

Report prepared and presented by Max Thomas, Head of Internal Audit (Veritau).

Appendix 1

INFORMATION TECHNOLOGY - FINAL AUDIT REPORTS ISSUED IN THE PERIOD TO 31 AUGUST 2014

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	County Hall Data Centre – physical and environmental controls	Substantial Assurance	The audit examined the physical and environmental controls which exist to maintain the security and integrity of the data centre at County Hall.	December 2013	An effective control environment was found to exist, including swipe card access controls and CCTV to restrict and monitor access into both the ICT suite and the data centre. Environmental monitoring software and equipment also exist to provide warning of temperature, water or humidity issues that could have an impact on the delivery and availability of services. The following issues were noted: • a periodic review of those staff with access permissions to both the ICT department and the data centre is not performed; • a report of failed access attempts to the data centre was not regularly generated for review; and • a schedule had not been agreed, to periodically test run the generators.	**Two P2 and one P3 action were agreed** **Responsible Officer:** Head of ICT Operations A review of current access permissions was carried out in January 2014. A quarterly review of failed access attempts will be carried out and documented using SharePoint. A visitor log will also be created. A schedule for generator testing will be established.
B	Server administration and security	Substantial Assurance	The audit reviewed the controls in place to manage the server	December 2013	Good controls were found to be in place. A small number of minor issues were identified.	**Three P3 actions were agreed**

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			environment and prevent unauthorised access and / or changes to applications and data.			**Responsible Officer:** Head of ICT Operations Action was taken immediately to address the issues highlighted in the audit.
C	Schools ICT Data Centre – physical and environmental controls	Limited Assurance	The audit examined the physical and environmental controls which exist to maintain the security and integrity of the data centre at Highfield House, Ripon.	February 2014	Schools ICT (SICT) provides support to approximately 400 schools in North Yorkshire. Highfield House is also used as a training centre and office base for the team. The computer room is a converted office located on the first floor of the building. The audit recognised that significant investment would be required in order to ensure a satisfactory level of physical and environmental protection for the hardware located in the computer room. However, Highfield House is a Grade 2 listed building, built around 1853, and as such there are restrictions on any adaptations that can be made. The following specific control weaknesses were identified: • there are no automated fire suppression systems and, with the exception of smoke detectors, a lack of environmental monitoring equipment (e.g. water, heat	**Six P2 and one P3 action were agreed** **Responsible Officer:** Head of ICT – CYPS The Service Desk solution, the primary solution housed on the servers located in the computer room will move to a hosted solution, therefore making a large part of the server farm, and that hosting customer data, redundant. This will reduce the risk of key equipment and data being damaged or lost. The service will also review the affordability of physical and environmental controls based on the future service provision. A plan to test Disaster Recovery arrangements has been put in place and this will be carried out on a 6-monthly basis.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					and humidity) in the computer room; • live equipment (servers and UPS devices) are stacked on desks within the computer room rather than being housed in cabinets. The computer room was also used as a storage area for new equipment; • there is no backup generator to provide power in the event of a power outage which exceeded the short term cover provided by UPS devices; and • scheduled failover testing was not performed, which would ensure that live services could be manually transferred to run from the disaster recovery server. Additionally, documentation detailing the process to be followed in order to transfer the services had not been developed.	
D	Network security controls	Substantial Assurance	The network infrastructure underpins the provision of systems and services across the County Council. The need to maintain the integrity, availability and confidentiality of information and protect	February 2014	The County Council operates a resilient, high capacity, private data network, which carries voice as well as data traffic. The network design follows a recognised hierarchical model to support high speed central switching, wide area access and security, and the provision of end user devices (for example	**Two P2 and one P3 action were agreed** **Responsible Officer:** Head of ICT Operations Implementation of UPS at County Hall is being evaluated and costs are

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			IT assets requires a security management process. This process includes the use of security techniques and related management procedures (eg network segmentation, device configuration and management controls) to authorise access and control information flows. The audit reviewed the controls in place to ensure that network security remained effective.		computers and telephones). Within the Country Hall campus, a resilient fibre optic ring exists between each of the buildings, making up the Local Area Network component (LAN). The LAN is managed internally by ICT Services. The Wide Area Network (WAN) is managed and monitored by NYnet Limited. Some areas of improvement were noted, as follows: • Uninterruptable Power Supply (UPS) devices were not always present; • one potentially unprotected legacy connection was found; • two Intrusion Prevention System (IPS) sensors protecting part of the network were not active at the time of the audit; and • older, insecure Simple Network Management Protocol (SNMP) versions were found to be in use.	being obtained. This will enable telephones and the Wireless Network to remain active for telephony, laptop PCs and other devices. It is important to note that during a power failure all other office equipment and lighting will be affected until the generators are started. The additional benefit of having the communication cabinets powered by UPS is to ensure the equipment survives the switch between mains and generator power. The need for the legacy network connection will be investigated and appropriate alternative arrangements put in place. The upgrade of the IPS has been completed and sensor segments have now been restored to provide full protection. The use of SNMP versions will be reviewed and, where possible, these will be replaced with the most secure version available. However, some switches are relatively old and may only support v1. If that is the case then consideration will be given to restricting SNMP access to those servers that require it.
E	Firewall security	Substantial Assurance	The firewall allows or blocks incoming and	February 2014	The County Council uses firewall equipment supplied by its chosen	**One P2 and two P3 actions were agreed**

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			outgoing network traffic to provide protection from intrusion attempts / malicious code from the internet or outbound traffic from the County Council's network to other organisations. The audit reviewed the configuration of the firewalls in place to ensure that they adequately maintain the confidentiality, integrity and availability of networked services.		vendor, Juniper Networks. The firewalls are configured so as to provide a degree of resilience in respect of a hardware failure. Whilst the audit noted a number of good practices in operation, such as change control management, there were some minor control weaknesses which, if addressed, would enhance the existing security environment. The areas for improvement included: • a recent review of the rule set had not been performed in the context of current business requirements; • the operating software version present on the nexus and N3 Juniper firewall devices was not current; and • a firewall log retention period had not been defined.	**Responsible Officer:** Head of ICT Operations A Firewall Security Management tool with the capability for automating the process of rule management will be evaluated. The evaluation will determine whether the product can provide an efficient means of identifying those rules that present a risk or are no longer in use. A business case will be presented for approval following the evaluation. The firewall software has been upgraded to the latest version. In addition, the main firewalls were upgraded in February 2014. The previous firewall monitoring software has been replaced with the McAfee Enterprise Security Management (ESM) solution and a log retention period of 9 months has been set. 6 monthly reports are also now required for PSN compliance.
F	VMWare security controls	Substantial Assurance	Virtualisation allows computing resources to be used remotely. For example, applications operating on one device	May 2014	The audit found good arrangements were in place, including access controls, change management controls and a high level of resilience. A small number of areas	**One P2 and two P3 actions were agreed** **Responsible Officer:** Head of ICT Operations

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			can be used by other devices. In addition, virtualisation can be performed on many other computing resources, including operating systems, networks, memory and storage. Eighty percent of the County Council's server estate is virtualised and this arrangement helps to underpin service provision and business continuity. The audit examined the design of the controls in respect of the security and configuration of the VMWare Server Virtualisation solution.		for improvement were identified, including: • a procedure had not been developed for the re-provision of user access to systems from the VMware Disaster Recovery (DR) environment, in the event of a failure of the live VMware environment; • A patch management policy had not been defined (including VMWare) and a control was not in place to initiate the review of patches on a periodic basis. Additionally, there was no control to check the application of critical patches, which may require action sooner than the planned review period.	VMWare Site Recovery Manager (SRM) has been successfully implemented. This will facilitate a quicker recovery of servers / systems to the DR environment. Access to the DR environment has also been restricted to specific roles to ensure a more controlled recovery. A formal VMware patching policy will be adopted with six monthly updates of all ESX servers and patches deemed as critical being reviewed monthly. VMware update alerts will also be sent to a common email account to enable easier access.
G	Software licensing – follow up	Moderate Assurance	The audit was a follow up review to assess the progress made to address the control weaknesses previously identified by internal audit in 2013.	May 2014	Four of the eight recommendations contained in the original report were found to have been implemented. Progress had also been made to address the remaining four recommendations, as follows: • Software Asset Management (SAM) discoverer and management tools are now being used; • a software audit had been	**Responsible Officer:** Head of ICT Operations The software asset management tool included in the Microsoft licence contract will be installed and used as a baseline process to evaluate the overall software licence position. It will also allow the other software asset management tools which are available to be tested. This is due to be completed by September 2014.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					performed in conjunction with Microsoft; and • regular meetings had been held with software providers to confirm the accuracy of the County Council's software licensing arrangements. At the time of the audit, work was also ongoing to upgrade to the latest version of Microsoft System Centre Configuration Manager (SCCM), which incorporates new functionality enabling it to be used for broader SAM tasks.	Following evaluation, the knowledge gained will be used to inform the on-going strategy for software asset management. This will be completed by December 2014. A proposal will then be presented to the Technology and Change Leadership Team by January 2015
H	Liquid Logic – general IT controls	Substantial Assurance	The Liquid Logic Children's Social Care system (LCS) holds information relating to children and social care, including assessments, care plans and child protection information. The system security controls are essential to maintaining the confidentiality, integrity and availability of information stored and processed by the system. The audit examined the effectiveness of those controls.	June 2014	The audit found robust user management and access controls in place; satisfactory system documentation and a training programme for new users. A small number of areas for improvement were identified, including: • the lack of a dedicated server to host LCS despite the system being categorised as 'gold' (business critical); • the current SQL Server database software (2005 Service Pack 4) is still supported by Microsoft. However, no further development work is planned	**Two P2 and four P3 actions were agreed** **Responsible Officer:** Head of ICT – CYPS A plan to upgrade the whole infrastructure for LCS will be developed. This will include upgrading the front end servers which are currently Windows 2003 to Windows 2008, and the SQL version from 2005 to 2008. Access by the LCS supplier will be reviewed. A BCP will be developed, in

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					and two later, fully supported, versions are available (SQL Server 2008 and SQL Server 2012). There were no formal plans in place to upgrade the SQL Server to a fully supported version; • there were no controls in place to restrict or monitor remote access by the LCS supplier; • a business continuity plan (BCP) detailing how the Systems Team would manage and communicate a failure of LCS had not been developed; and • a recent test recovery from backup for LCS had not worked properly.	conjunction with the Technology and Change BCP, for use by the Corporate Systems Team, outlining how LCS downtime will be managed. The issues that occurred with the recent test will be addressed in the next Disaster Recovery test planned for July 2014.
I	Lagan Customer Relationship Management System (CRM) – general IT controls	Moderate Assurance	The Lagan CRM System is used to manage contact and interaction with local residents. The system records, tracks and monitors all customer contact, including requests for services. The system was installed approximately six years ago and is managed and administered on a day to day basis by a CRM Support Team.	July 2014	The audit identified a number of weaknesses in control, including: • the lack of a dedicated server to host Lagan despite the system being categorised as 'gold' (business critical); • the current SQL Server database software (2005 Service Pack 4) is still supported by Microsoft. However, no further development work is planned and two later, fully supported, versions are available (SQL	**Four P2 and three P3 actions were agreed** **Responsible Officer:** Head of ICT Operations A new process is currently being developed which will channel all Lagan new / amendments / leaver user requests through to a central point in Technology & Change and enable them to be dealt with directly by the Corporate Systems Team. The form will capture all required

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			The audit examined access, systems maintenance and business continuity controls.		Server 2008 and SQL Server 2012). There were no formal plans in place to upgrade the SQL Server to a fully supported version; • There were limited password settings available within the Lagan CRM system for configuration and those that were available were not set in line with the IT access policy. User passwords were set to 'never to expire' and the password minimum length was only set to four characters; • User management processes for new users, leavers or amendments to existing users had not been formalised or documented. Authorisation from line managers for new user access or user amendments was not recorded; • A business continuity plan (BCP) detailing how the CRM Support Team would respond to a system failure had not been developed.	system access information, including appropriate authorisation. A user review will be undertaken as part of housekeeping tasks scheduled after the Lagan upgrade. This will establish a snapshot of currently active users and users that are no longer require access. User accounts that are no longer required will be disabled. Access groups will also be reviewed and where possible consolidated into a structure that ties in with defined job roles. The SQL Server version will be upgraded as part of the Lagan upgrade project. The server environment hosting Lagan will also be reviewed. Password controls will be discussed as part of the Lagan upgrade project. The intention will be to include Lagan within the existing single sign-on process. The Corporate Systems team will develop a full BCP.
J	Synergy system - general IT controls	Substantial Assurance	At the time of the audit, the County Council was implementing the Synergy Children's	July 2014	The audit found good arrangements were in place, including systems access controls, documentation and new user management	**Two P2 and three P3 actions were agreed**

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			Information Management System suite of products to support and manage education administration. The first module (Admissions) went live in August 2013 and, at the time of the audit, five modules had been implemented with a further two scheduled by October 2014. The audit examined access, systems maintenance and business continuity controls.		procedures. A small number of areas for improvement were identified, including: • the SQL server backup was only run once a day rather than more frequently; • a test recovery from the backup had not been performed; • a detailed business continuity plan (BCP) had not been prepared to manage the service and communicate with members of staff in the event of any system failure.	**Responsible Officer:** Head of ICT – CYPS The frequency of system backups will be explored further with the supplier to determine best practice. The live Synergy SQL database backup has now been restored although further testing is planned to ensure a full recovery of the system is possible. The Corporate Systems team will develop a full BCP.
K	Schools ICT – server administration and security	Moderate Assurance	Schools ICT (SICT) provides server and network management support to a significant number of schools within North Yorkshire. Each school has its own server hardware underpinning the provision of key business systems and operations. The schools sign up to a base Technical Support Services contract, which	July 2014	The schools visited were operating up to date Sophos anti-malware, various back-up management software and automatic Windows updates for patch management. There were no issues in respect of the anti-malware and server patching configurations in operation and controls were generally operating effectively. However, a number of control weaknesses were noted, including: • the physical and environmental controls	**Three P2 and two P3 actions were agreed** **Responsible Officer:** Head of ICT – CYPS Improved advice and guidance will be provided to schools on recommended: • physical and environmental controls to protect servers; • secure password controls; • user management particularly the disabling of accounts

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			provides unlimited telephone, remote and on-site assistance support to resolve faults and also technical advice and support to end users. The schools are also able to enhance the support received by purchasing additional support levels. The audit examined the controls in place to prevent unauthorised access to information, maintain continuity of service and avoid loss of data.		adopted by schools may not provide adequate server protection; • secure password controls had not been enforced by Active Directory group policies; • formal user management process were not in place to ensure that all access to the school network and data was appropriate; • internal backup jobs were not checked for completeness on a daily basis and records were not maintained detailing the reasons for any failed backups; and • automated server monitoring software had not been installed, which could alert SICT of any issues that may impact on server availability.	relating to leavers; • backup arrangements. SICT are also implementing the Sostenuto solution for recording user management requests. This information will then be visible to schools. The new Centrastage solution being implemented will also provide consistent daily backup monitoring. However, there is an opportunity to develop a more formal backup monitoring service that extends beyond simply checking that jobs have ended successfully or not. SICT will develop this further as extending the service to regularly test restore capabilities may be an option some schools would require. The provision of automated server monitoring will be kept under review although there has been little demand from schools for this type of service in the past.

Appendix 2

CORPORATE THEMES - FINAL AUDIT REPORTS ISSUED IN THE PERIOD TO 31 AUGUST 2014

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Information Security compliance audits	Various	Unannounced audit visits are made to offices and establishments across the County Council. The visits are intended to assess the extent to which personal and sensitive data is being held and processed securely. The visits also consider the security of assets, particularly mobile electronic devices and other portable equipment. Seven reports were finalised during the period covering separate areas of County Hall and other buildings.	Various	Following each visit, a detailed report was sent to the Senior Information Risk Owner (SIRO), as well as to relevant directorate managers. Working practices were found to be poor in a number of instances, as follows: • three visits were classified as Limited Assurance; • two as Moderate Assurance; • one as Substantial Assurance. A composite report (Limited Assurance) was also issued covering a number of visits to smaller establishments made in 2013. There has been a general improvement over the period with fewer issues detected in the most recent visits.	**Various P1, P2 and P3 actions were agreed** **Responsible Officer:** Corporate Director - Strategic Resources (and others) Responses have been obtained to each report. Management have viewed the findings extremely seriously and have taken immediate action where issues have been discovered.
B	Corporate Information Governance Group (CIGG), Data Breaches and ICO Investigation	Moderate Assurance	The audit reviewed the effectiveness of the strategic arrangements for information governance, including the operation of the Corporate Information	February 2014	The audit found that the County Council has made good progress in developing its corporate information governance arrangements. However, CIGG needed to adopt a more focused and strategic approach to considering new and	**Three P2 actions were agreed** **Responsible Officer:** Corporate Director - Strategic Resources (and others)

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			Governance Group (CIGG), the reporting and investigation of data security breaches and the response to enquiries by the Information Commissioner's Office (ICO).		emerging information governance risks. The information governance policy framework also needed to be updated and streamlined. The audit also reviewed the internal response to an ICO investigation in 2013. The roles and responsibilities of key officers needed to be more clearly defined and understood in such circumstances. There was also no central record maintained of information relating to serious data security breaches. In respect of other data security breaches, good progress had been made to establish reporting arrangements. However, some improvements were still required, as follows: • the information incident investigation procedures needed to be updated; • no monitoring is undertaken to ensure that internal deadlines for completing investigations are met; • it is unclear how or whether the County Council routinely learns the lessons from data breaches.	The Council had already recognised that CIGG could be more effective. A new strategic CIGG group has therefore been established, supported by a virtual group comprising directorate information governance champions. The new strategic CIGG offers clear leadership and focus. LAGAN is to be used to retain a complete record of data security breaches. A lead officer will also be clearly identified at the outset of any future ICO investigation. Revised procedures for data security breaches will be established, including arrangements to share knowledge and any lessons learnt.
C	Payroll	Limited Assurance	Employment Support Services (ESS) are responsible for	February 2014	As previously reported to the Committee, a number of significant control weaknesses were found, as	**One P1, six P2 and two P3 actions were agreed**

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			processing salaries, calculating deductions, processing timesheets and expense claims and ensuring that the service complies with all relevant statutory regulations. ESS provides a payroll service for 45,000 employees and pensioners and incurs employee related expenditure of approximately £26m per annum. They are also responsible for processing the payrolls of 14 external bodies. A major restructure of the service took place in March 2013. The audit was requested by management and involved a review of the procedures and controls within the payroll system to ensure they were working effectively. The audit covered the period when the new operating arrangements were being implemented.		follows: • errors had occurred leading to incorrect amounts being paid to some staff; • all of the errors involved an element of manual intervention following an unexpected occurrence. There was not a sufficiently robust system in place to check these calculations before they were processed; • exception reports were not being used as effectively as they should; • payroll staff did not have access to a central pay element guide. Information is held in a variety of sources which increases the risk that staff do not fully understand the implications of changes; • no information is recorded to enable the reasons for pay advances to be effectively monitored; • whilst individual and service information is collected and targets set, performance information is not routinely reported to all external customers; • errors had occurred with the calculation of VAT on some	**Responsible Officer:** Head of Business Support Services All of the findings included in the report were agreed by management. Manual calculations will now be checked at a 100% level. Variance and deviance reports for net pay will now be produced and checked on a monthly basis. A central pay element guide/booklet will be compiled which will be distributed to all staff and customers. Detailed processing and customer service information will be distributed internally and to external customers. ResourceLink will be updated, and responsibility to senior member of ESS assigned, to help prevent mileage issues such as those found in the audit. A reminder will be issued to staff and managers that timesheets signed by the same person will be rejected. A further audit is due to commence shortly. This will include a review to assess the progress made by management to implement the agreed actions.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					mileage claims; • some timesheets were being processed by ESS when they had been signed and authorised by the same person.	
D	Post implementation reviews (PIR) / Review of salt barn project (BES)	Substantial Assurance	A post implementation review (PIR) is generally conducted after the completion of a project / work programme. The main purposes of a PIR are to evaluate whether the original objectives were met, determine how effectively the project/programme was run, learn lessons for the future and to capture learning points for further improvements. Completing a PIR is therefore an important learning process. The audit consisted of two parts. The first part considered the extent to which the County Council has defined corporate arrangements in place to undertake post implementation reviews. In conjunction with management, the	May 2014	The audit found that the County Council has structures in place to share good practice, for example, the Corporate Procurement Group meets regularly and discusses the outcomes of major projects. However, there is scope to further improve Council wide learning by introducing proportionate and simple mechanisms. The issues which occurred with the salt barn project were shared with the Corporate Procurement Group so as to raise awareness and enable lessons to be learnt.	**Two P3 actions were agreed** **Responsible Officer:** Assistant Director – Strategic Resources Head of Procurement and Contract Management Corporate Performance Group. The Council will work with Internal Audit to gain experience with completing post implementation reviews.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			audit also reviewed one specific project to evaluate the extent to which it had achieved its intended aims and objectives.			
E	Risk Management	Substantial Assurance	The audit examined the Council's arrangements for managing risk. The systems for identifying, evaluating and recording risks were examined. The processes for determining risk appetite, obtaining assurances to support mitigating actions, training and management reporting were also examined.	July 2014	The audit found that the systems and processes for risk management were operating well. A few areas for possible improvement were highlighted, including the need to provide further training for Members.	**One P2 and two P3 actions were agreed.** **Responsible Officer** Corporate Risk and Insurance Manager. Training requirements for Members will be considered by the Corporate Governance Officer Group.

Appendix 3

CONTRACTS - FINAL AUDIT REPORTS ISSUED IN THE PERIOD TO 31 AUGUST 2014

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Review of the Northallerton College Enhanced Engineering Unit - capital contract	Substantial Assurance	The contract for the building work was awarded to Interserve. The work was completed in December 2011 and the value of the contract was £205k (excluding the cost of furniture and fittings). The audit reviewed the procedures followed to ensure compliance with the Procurement Manual and Contract Procedure Rules.	October 2013	The correct procedures had generally been followed. Management were advised to address the following issues when undertaking similar schemes in the future: • there is a need to follow the published tender requirements throughout the process; • less reliance should be placed on Jacobs to provide an evidential trail; • furniture and fittings costs should be recorded on budget reports and the final account examination form; and • care should be taken to ensure that the original signed contract documentation is submitted to the County Record Office in Malpas Road for safekeeping.	**Two P2 and two P3 actions were agreed** **Responsible officer:** Assistant Director – Strategic Resources and Property (CYPS) The issues highlighted in the report will be addressed through the next review of the Property Procedure Rules and new regular liaison meetings between Property Services and Jacobs which will be in place by February 2014.
B	Review of King James School capital contract – refurbishment of science laboratory and other associated works.	Substantial Assurance	The scheme formed part of the 2012/13 Capital Programme. A feasibility study was undertaken by Jacobs but the anticipated	April 2014	The audit found that appropriate contract management arrangements had been in place to deliver the scheme. Payments had also been checked and made in line with contractual requirements.	**Two P2 and one P3 actions were agreed** **Responsible officers:** Assistant Director – Strategic Resources and Property (CYPS)

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			scheme costs initially exceed the approved budget of £670k. Further changes were then made to the proposed scheme layout to enable the work to begin. The audit reviewed the procedures followed to ensure compliance with the Procurement Manual and Contract Procedure Rules.		Management were advised to address the following issues when undertaking similar schemes in the future: • information on YORtender should be complete and the relevant file should not be archived until the work is completed; • further measures should be considered to ensure that sub-contractors meet the same quality standards expected of the main contractor; • evaluation models involving framework contracts should continue to be sent to Internal Audit.	The issues identified in the audit will be discussed with Jacobs and NYPS and procedures amended accordingly.
C	Revenue contract - Action for Children (May Lodge Scarborough)	Moderate Assurance	The contract with Action for Children (AfC) is to provide a flexible residential short breaks service for disabled children and young people in Scarborough In September 2013, the County Council extended the contract until March 2015. However this extension was only on the basis that AfC implement a number of service	August 2014	The contract had been subject to a Performance Improvement plan, designed to address various concerns initially raised in 2012. The audit noted that: • the current contract ends in March 2015. There are many complex decisions which need to be made to ensure the forthcoming procurement exercise maximises the outcomes for the County Council and service users • any future contract should have	**Three P2 and two P3 actions were agreed** **Responsible officers:** Assistant Director – Strategic Resources, Finance and Management Support (HAS) Officers will seek legal and procurement advice prior to commencing the forthcoming procurement exercise. Any future agreements will also include appropriate contract and performance management

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			improvements, supported by a detailed action plan. In 2012/13, expenditure on this block contract was £640k of which £400k was contributed by the Clinical Commissioning Group's (CCGs) (NHS). The audit reviewed the arrangements in place to monitor the delivery of the service and to ensure payments are correct.		robust monitoring arrangements included and a method of payment linked to obtainng best value; • monitoring of the current contract needs to ensure that Action for Children always have sufficient staff on duty to maintain appropriate levels of care.	arrangements.

Appendix 4

AUDIT OPINIONS AND PRIORITIES FOR ACTIONS

Audit Opinions	
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Moderate assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.