NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

7 SEPTEMBER 2017

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 year to 31 August 2017 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.

2.2 This report considers the work carried out by Veritau and Audit North during the period to 31 August 2017. It should be noted the internal audit work referred to in this report tends to be cross cutting in nature and therefore there are no corresponding directorate risk registers to consider.

2.3 The Corporate Risk Register (CRR) is fully reviewed every year and updated by the Chief Executive and Management Board in September / October. A six monthly review is then carried out in April / May. The latest updated Corporate Risk Register was presented to the Committee in June 2017. There have been no significant changes in the County Council's risk profile since that date.

3.0 **WORK CARRIED OUT DURING THE YEAR TO 31 AUGUST 2017**

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 has also been involved in a number of related areas, including:

- providing advice on corporate governance arrangements and IT related controls;

- providing advice and support to assist various project groups;

- 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);

- contributing to the development and roll-out of the procurement strategic action plan, including participation in a number of delivery areas;

- contributing to the annual review and update of the County Council's Financial, Contract and Property Procedure Rules;

- carrying out a number of investigations into data security incidents and corporate or contract related matters that have either been communicated via the whistleblowers' hotline or have arisen from issues and concerns reported to 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 tend to be 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:

---

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

(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 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.

Max Thomas
Head of Internal Audit

Veritau Ltd
County Hall
Northallerton

7 September 2017

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).

INFORMATION TECHNOLOGY - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2017

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	North Yorkshire 2020 – benefits management	Reasonable Assurance	The audit reviewed the project management arrangements adopted by the Council to enable the tracking and realisation of potential benefits arising from technology related projects in the 2020 Programme.	November 2016	There was clear evidence that the structured approach to programme management adopted by the Council had resulted in the delivery of successful projects. However, benefit realisation management arrangements for both cashable and non-cashable benefits were not always being applied consistently or with sufficient rigour. It was recognised that there is a cost involved in measuring benefits and it might therefore be necessary to prioritise key benefits for active monitoring.	**Ten P2 and seven P3 actions were agreed.** **Responsible Officers:** Assistant Director, Technology and Change Head of Projects and Programme Project sponsors and project managers will be asked to ensure that governance arrangements are stated clearly in the project brief and project initiation documents and that these are simplified where possible. The portfolio level governance arrangements will be reviewed to ensure that these are streamlined and that there is clarity about approval processes. There will also be greater clarity regarding who signs off from a finance perspective. The process for initiating new projects will also be reviewed to ensure that this is streamlined and proportionate. Further advice has been given to project sponsors and project

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
						managers on how to treat non cashable benefits for making sure on-going benefits realisation is covered in project closure reports.
B	Synergy	High Assurance	The Synergy system holds records of children and pupils relating to school admissions, school placements, early years', children's centres, troubled families and specialist educational services. The audit reviewed the controls in place to maintain the confidentiality, integrity and availability of information stored and processed using the Synergy system.	May 2017	Good controls were found to be in place. The operational management of the Synergy system included comprehensive system administration and user documentation; a robust user management and access controls process and a training programme for new users. However, some weaknesses were identified with audit trails. For example the system did not log access to client profiles by users. The application also did not have the functionality to restrict access to specific client profiles (for example if a client was known to a user).	**One P3 action was agreed.** **Responsible Officer:** Assistant Director, Technology and Change The audit report was discussed at the Synergy Steering group meeting held on 22 May 2017. The software supplier, Servelec has confirmed that an audit trail is not currently provided for the back office modules (Synergy Modules), although one is available for areas accessed via Gateway. The Steering group will take ownership of the risk and work closely with the Corporate Systems Team in case there is ever the need to request an access report from Servelec.
C	Liquid Logic	Substantial Assurance	The Liquid Logic system holds client records for adults and children including referrals, assessments, care and intervention plans, and contracts. There are approximately 14,000 live	May 2017	Robust user management and access controls were in place with comprehensive system documentation. There was also a fully embedded training programme, including competency assessments for new users.	**Four P4 actions were agreed.** **Responsible Officers:** Service Manager – Infrastructure Team Senior Systems Officer Head of Business Support CYPS & CS

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			client records (adults and children). The audit reviewed the key controls in place to maintain the confidentiality, integrity and availability of information stored and processed using the Liquid Logic system.		However, there were some inconsistencies in relation to the management of the different modules in the system. Server and server back up configurations differ between the Adults (LLA) and Children's (LCS) modules, and neither module uses the latest build available. Default passwords and security settings were also different. Business Continuity Plans (BCPs) detailing how individual teams within the services would operate in the event of system unavailability had also not been developed.	A server update has taken place, and a project initiated to upgrade the infrastructure to SQL2012. LCS and LLA password parameters and policies have been reviewed and aligned to the Council's corporate policies. Backup configuration across both LCS & LLA environments will be reviewed and standardised. Service teams have been requested to provide details of how they would operate in the event of the system being unavailable. Business continuity is also being considered by the continuous improvement groups (LCS and LLA).
D	IT Security Incident Management	Reasonable Assurance	The audit reviewed the policies and processes in place to mitigate the risks in relation to accidental or malicious IT security incidents.	March 2017	An Incident Management policy has been developed and arrangements and procedures for the detection and resolution of ICT security incidents are in place. However, there was no clearly defined network security strategy or security incident response plan outlining the various co-ordinated actions required to identify and / or address ICT security incidents.	**Four P2 and one P3 actions were agreed.** **Responsible Officer:** Senior Information Security and Compliance Officer. Head of Technology Solutions. The cyber security strategy and recovery plans will be reviewed. A technical network security policy

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					An ICT risk analysis has been carried out but did not evaluate some cyber security risks in sufficient detail to enable the identification of appropriate mitigating actions. There was no clearly defined incident management response plan. Recording and response by service centre staff to security incidents was also inconsistent.	will be created and additional processes added to incident response plan. The Service desk management process will also be reviewed.
E	IT Network and Server Operational Management	Substantial Assurance	The audit reviewed the key controls designed to secure the provision and management of network services. Due to the increasing threat from cyber security attacks the Council needs to ensure that it has appropriate controls in place to provide secure network services and to protect infrastructure and data stored on the network.	May 2017	The controls were generally effective. However, there was no formal policy in place to assess network security vulnerabilities highlighted in new software releases. AAA (Authentication, Authorization and Accounting) security had not been implemented and a generic account was used to facilitate administration access to network switches. Standard operating procedures (SOPs) had not been developed to support day-to-day operational and maintenance tasks. Responsibilities for performing those tasks had also not been identified.	**Three P2 and one P3 actions were agreed.** **Responsible Officer:** Service Manager Unified Comms and Security Technical Lead All switch products are now registered with HP so updates are received when new software versions are released. Where possible, the implementation of RADIUS or TACACS+ for authentication will be considered for those switches that can be configured successfully. AAA security will be applied to all replacement switches as part of the LAN replacement programme

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
						Additional SOPs will be developed to outline the schedule for automated operational tasks and checks such as configuration updates, backups and monitoring.
F	Business Intelligence and Data Warehouse Security Management	Reasonable Assurance	The Business Intelligence (BI) and Data Warehouse systems act as reporting repositories which collate data from a number of systems and provide users with information and reports to support decision making across a number of Council priorities. The integrity and security of the information is therefore critical to ensure the accuracy of reports. The audit reviewed the key controls in place to maintain the confidentiality, integrity and availability of information stored and processed using the Business Intelligence and Data Warehouse systems.	May 2017	There is evidence that the structured approach to Business Intelligence reporting is improving the delivery of quality information to support decision making processes.

Management information and dashboards are being developed using MS Power BI. The control environment for report development was evolving as systems and processes were refined and matured.

However, no formal process was in place for accepting BI reporting development requests into the BI Team development portfolio. An approved project methodology had not been adopted for the implementation of BI Projects.

Documented operating procedures had not been developed to support the day to day BI processes and administration. | **Four P2 and one P3 actions were agreed.**

Responsible Officer: Data and Intelligence Manager

The process for requesting work will be documented as part of the service offer for BI projects.

Following the planned service restructure all new development work will be carried out as either part of a formal project work package or service request recorded in the service management system.

Operational procedures will be documented during the transition process following the restructure. |
| G | Wireless Network Follow-up | Substantial Assurance | The audit reviewed the progress in completing the | May 2017 | Three of the four agreed actions had been fully implemented. Changes | **One P2 action was agreed.**

Responsible Officer: |

System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
		actions agreed with management following the 2015/16 Wireless Network Security audit. The previous audit had identified a number of control weaknesses and had been classified as only providing reasonable assurance.		had been made to the configuration for guest Wi-Fi, and testing confirmed that access was now only possible through registration. Procedural documentation had been updated and further documentation produced to support the purpose and configuration of each Service Set Identifier (SSID). However, wireless Intrusion Detection System (IDS) events were still not being pro-actively monitored or subject to regular review. IDS events could not be exported to provide meaningful information.	Technical Lead A method to better correlate alerts from multiple systems is to be investigated as part of a wider security review. A team structure review will consider more dedicated security roles to improve proactive management of identified events. The software provider has been contacted to obtain advice on the import and analysis of data.

CORPORATE THEMES - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2017

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Payroll / HR	Reasonable Assurance	The audit reviewed the procedures and controls within the ResourceLink payroll system which ensure that: • key payroll information is present and accurate. • high value payments are reasonable. • compulsory unpaid leave is calculated correctly for in-year starters and existing staff Testing was carried out using data analysis software which allowed 100% of the population to be checked (approximately 18,000 records).	June 2017	A small number of errors were identified in relation to National Insurance numbers and multiple payroll numbers. The details were shared with Employment Support Services for them to verify and correct (where necessary). A number of claims for additional hours had not been submitted on a regular basis. All employees are subject to a salary adjustment for compulsory unpaid leave (CUP). However, the corresponding flexitime adjustment for employees who work for only part of the year was not always being made by managers.	**Two P2 and two P3 actions were agreed.** **Responsible Officer:** Business Support Officer Senior HR Advisor Senior HR Advisor, Policy Lead for HR All records will be checked (apart from a small minority that contain specific differences) to ensure the identified data is complete and accurate. Late claiming of additional hours will be raised with the appropriate Senior HR Advisors / managers. Further guidance will be issued to managers to explain the CUP deduction.
B	Employment Documentation	Reasonable Assurance	The Council uses the Wisdom Electronic Data Records Management System (EDRMS) to store and process employment related documentation. The audit reviewed the controls in place	February 2017	The audit found the Wisdom EDRMS system is an intuitive and well-structured software package. Clear guidance and reference material had been circulated to managers. Monitoring of managers' use of	**Two P2 and one P3 actions were agreed.** **Responsible Officer:** Corporate Directors (S151, HAS, BSS, CYPS)

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			to maintain the confidentiality, integrity and availability of information stored and processed using the EDRMS system. .		Wisdom was good. Separate reviews had been conducted in October 2015 and March 2016 that focused on which managers had not yet accessed Wisdom and the relationship between the number of employee files uploaded and the number of reporting staff. Testing found that the uploading of documentation for disciplinary cases was good with all expected documents saved in the correct areas. However, some expected documents were not present for sickness, paternity and maternity cases and for retired employees.	An email was sent to the Corporate Directors with a request made that Service Managers are reminded that employment documentation should be uploaded to Wisdom in a timely manner, and saved in the correct location.
C	Insight Performance Dashboard	Substantial Assurance	The audit reviewed the operation of the insight performance tool to review how effectively it is used by managers, and how it contributes to the management of team performance.	May 2017	Data within Insight is fed directly from ResourceLink and the Learning Zone. It is therefore reliant on the accuracy and completeness of the information that is input into these systems. Most service managers who use Insight were employing the system effectively as a management tool, although no clear correlation could be seen between use of the system and improvement in performance. Some managers were using alternative management tools despite Insight being available and cited technical difficulties or a lack of	**Two P3 actions were agreed.** **Responsible officer:** Assistant Chief Executive (Business Support) The Insight Performance Dashboard will be re-launched with training provided to all managers who request it. An upgrade of MyView will be completed which should reduce structure issues. The possibility of updating training completed through the Nexus

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					understanding of how to use the system as reasons for low uptake. In some cases managers' highlighted issues with the completeness of data contained within Insight. Other than a failure of managers to enter data the main reasons identified were training via Nexus which can take up to 4 weeks to appear on the system, and issues where structure charts did not reflect teams managed.	external training portal more frequently by the Training and Learning Team will be reviewed. If this is practical, it will be introduced to prevent management from manually compiling statistics.
D	Risk Management	High Assurance	The audit reviewed the frequency with which risk registers are reviewed and updated. The audit also reviewed how risks are managed in relation to commercial activities, and in particular reviewed the management of risk during the creation of the new NY Property Services company.	May 2017	The audit found the corporate arrangements for risk management to be effective. The corporate and directorate risk registers are being updated in line with policy requirements (at least annually). The 2016 risk registers were also compared to previous risk registers. This showed that new and emerging risk are being identified and evaluated at both a corporate and directorate level. A risk register/log and high level project team were created for establishing the new property services company. A 'lessons learnt' document was also produced following the completion of the project to help capture key challenges, processes and	**One P3 action was agreed** **Responsible Officer:** Corporate Director - Strategic Resources The lessons learnt document will be shared widely to support future projects.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					opportunities. However, this document had not been widely shared. In the future, a monthly report will be prepared for the company board summarising the current operational risks and associated risk appetite.	
E	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. Two reports were finalised during the period covering separate areas of County Hall.	Various	Following each visit, a detailed report was sent to the Senior Information Risk Owner (SIRO), as well as to relevant directorate managers. Findings have also been discussed by the Corporate Information Governance Group (CIGG). Working practices were found to be poor in a number of instances. Two visits were classified as Limited Assurance and one was Reasonable Assurance.	**Six P2 actions were agreed** **Responsible Officer:** Corporate Director - Strategic Resources (and others) Responses have been obtained from relevant directorate managers following each audit. Management have viewed the findings extremely seriously and have taken immediate action where issues have been discovered. Follow up visits have been arranged where significant information risks have been identified. A programme of further visits is currently being prepared.

CONTRACTS - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2017

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Best Value Forms - Compliance with Contract Procedure Rules	No opinion given	A change to the Councils Contract Procedure Rules in February 2016 provided some extra freedoms for low value purchases. For contracts valued at under £25,000 competitive quotes are no longer mandatory. If quotations are not sought a Best Value Form must be completed. The audit reviewed the application of the new procedures and sought to establish whether: • Forms are being completed to the required standard • Opportunities offered by the new CPRs for purchasing decisions under £25000 are being taken We completed and reported four separate audits in this area during the period.	August 2017	The majority of forms reviewed had been completed in line with expected practice. We identified weaknesses which reflect the 'bedding in' of the new process. For example, some forms were not fully or properly completed. Some had quotations supporting the form (when both are not required). Some small items should have been sourced from existing Council contracts. However, there was a general improvement in the standard of completed forms over time. Some variability in the number and nature of forms being completed was noted. For example, one directorate (BES) completed seven times the number of forms compared to HAS. We also found some inconsistency in what was being recorded on the Forward Procurement Plan (FPP).	**Eight areas for improvement were highlighted to address control weaknesses.** **Responsible Officer:** **Head of Procurement and Contract Management** The findings were in line with managements observations of the new arrangements. The Procurement Board has received regular information on the use of the new procedures. Internal Audit has been asked to further review the use of Best Value forms in 2017/18. This will also help review the progress being made to embed the new arrangements. The completion and use of the FPP is an area which we are regularly reviewing. The findings from the audit will be considered as part of our usual work with directorate procurement champions.

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.
Reasonable 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.