ITEM 10

NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

25 OCTOBER 2019

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 2019 in respect of information technology (IT), corporate themes and contracts.

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.

2.2 This report considers the work carried out by Veritau during the period to 31 August 2019. 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 reviewed every year and updated by the Chief Executive and Management Board in September / October. A six monthly review is then carried out in March / May. The latest updated Corporate Risk Register was presented to the Committee in December 2018. 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 2019

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;
- contributing to the development and roll-out of the procurement strategic action plan, including participation in a number of delivery areas;
- reviewing processes and procedures in place within property services for managing the responsive repairs contract;
- carrying out a number of investigations into 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 In addition to the specific IT audits detailed in Appendix 1, there has been an increased coverage of IT related controls and activities as part of general audits where key IT systems are in operation.

3.4 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**.

3.5 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 regular 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.**

3.6 The programme of audit work is risk based. 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.

5.0 RECOMMENDATION

5.1 That Members consider the information provided in this report and determine whether they are satisfied that the internal 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

10 October 2019

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 2019

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Concerto system audit	Reasonable Assurance	The Concerto system is the County Council's property management system. It is used to manage activities such as repairs and maintenance, servicing of equipment, and building projects. The purpose of the audit was to provide assurance that: • Data held within the Concerto system is only available to authorised individuals (Section 9 [Access Control] of ISO 27001). • the Concerto system is secure (Section 12 [Operations Security] of ISO 27001). • Use of the system complies with legal and contractual requirements (including information governance) (Section 18.1 of ISO 27001).	August 2019	The management of the Concerto system generally conforms to the requirements of the areas of the standards reviewed. All changes to the Concerto system are authorised, tested, logged and completed within a reasonable timescale. The audit also noted recent improvements in control in areas such as authorisation of access to the system for new users and regular review of user accounts. Work is underway to ensure that contracts with third parties who access the system on behalf of the council (e.g. works contractors) include provisions to ensure their use of the system is secure and in line with data protection requirements. However, a number of system weaknesses were identified. These included the following: • A lack of comprehensive audit logs for actions other than financial transactions, and no logging of activity for some users with a high level of access to the system.	**Two P2 & Eight P3 actions was agreed.** **Responsible Officer: Technology & Change Assistant Director** All user action will be logged. A review of all users access will be completed, with a focus on those with heightened and shared access first. Work will start in June following contractor changes. The password parameters for Concerto have now been updated to reflect the corporate policy. Current password reset options will be reviewed with a view to removing the less secure reset type if possible. The implications of this change will need to be discussed with Property Services. The contract with Concerto has been updated to include relevant data protection clauses. The Current G-cloud contract will be reviewed to assess whether NYCC requirements for backup are

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					• A number of users within Property Services retain system administration privileges despite this role having transferred to Technology and Change. • A large number of shared user accounts exist (as opposed to unique usernames for everyone accessing the system), in contravention of corporate policy.	adequately reflected. A variation to the contract will be considered if current arrangements do not meet the requirements.
B	Information Security Management	Reasonable assurance	Information security is the practice of preventing unauthorised access, use, disclosure, disruption or destruction of information. The Council has a number of policies in place that define the desired behaviour of staff with respect to data, IT systems and other assets. The purpose of the audit was to provide assurance that: • The council's Information Security Policies meet ISO 20000 and 27001 standards and • The policies are being followed by Technology and Change staff.	April 2018	Overall we found that the Council has a range of concise information security policies in place. In most cases the policies match the working practices within Technology and Change. However, we identified some differences, as follows; • When external contractors are required to enter the data centre they are escorted at all times. However, no log of visitors is kept. • The Council carries out internal vulnerability scans of the network on a weekly basis. A large number of vulnerabilities including vulnerabilities classed as critical are detected. There is no evidence of any risk	**One P2 & Six P3 actions was agreed.** **Responsible Officer: Technology & Change Assistant Director** A log of all contractors entering the data centre has been implemented. A risk assessment for the critical vulnerabilities will be carried out. A server log will be implemented. An investigations procedure has been implemented but requires further work to align with HR processes. The IT Monitoring Policy will be updated to reflect changes in monitoring of internet usage.

System/Area		Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					assessment for the critical vulnerabilities. - There has been no formal risk assessment carried out to decide why server logging is not activated. - The audit trail for investigations carried out by Technology & Change is not located in a central place. - Privileged user accounts are used to give administrator access to databases, systems and applications. Users with privileged user accounts are not monitored to ensure that the accounts are used appropriately.	Privileged user accounts are due to be reviewed during the next Information Security Meeting.
C	Software Development	Substantial Assurance	An in-house IT development team develops and maintains applications and services used across the Council, such as its website and intranet. The Council also purchases and uses 'off-the-shelf' and customised software solutions provided by third parties. Regardless of its source, information security is a critical part of any software solution.	June 2019	The internally developed Customer Portal and Individual Performance Management systems were reviewed as examples. Good arrangements are in place. There is an established process for identifying security requirements during software acquisition and development, with third party suppliers. For in-house systems, security requirements are included as part of the technical specifications provided to developers.	**One P2 & Six P3 actions was agreed.** **Responsible Officer: Technology & Change Assistant Director** A new Secure Software Development Policy will be created. A definition of security functionality requirements and relevant testing will be created and added into the development team’s procedure library.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			The purpose of the audit was to provide assurance that: • Access to systems is suitably controlled and restricted • Information security and continuity requirements are identified and incorporated during software development • Any software development or changes are done in a secure environment following an appropriate software development lifecycle • The development team receives sufficient assurance that software solutions provided by third parties have been appropriately and securely developed.		The arrangements for access to one of the Development team's primary development tools, were reviewed and found to be appropriate. The Development Team Manager is also preparing a system testing procedure.	Security testing will be added to the checklist. The results of security testing and any changes made as a result of testing will be recorded prior to the release of new software.

Appendix 2

CORPORATE THEMES - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2019

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Compliance with the Transparency Code	High Assurance	The Transparency Code requires local authorities to publish certain sets of data in specific timeframes. Audit work in 2017 concluded only 3 of the relevant sections of the Code had related information published correctly and in accordance with the required timelines. This audit examined the progress made to improve the collation and publication of the required data sets. This included testing to see whether: • the Council complies with all required sections of the Local Transparency Code • appropriate training has been provided to information asset owners and operational employees • individuals have been identified and allocated specific responsibilities	November 2018	The Council now has a strong framework in place and is complying with the Transparency Code regulations. All mandatory fields are now published correctly and within the required timescales. Relevant training is in place and is operating effectively. Training is provided as a combination of 1:2:1, group meetings and through e-learning. Relevant officers understand their responsibilities. There is also overarching oversight and guidance from the Data Governance Team. Checks are made at different stages to ensure all mandatory fields have been published on the Data North Yorkshire website and within the appropriate timescales.	**No actions identified**

System/Area		Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			• sufficient checks are now in place to ensure compliance with the Code.			
B	Payroll-HR	Substantial Assurance	Maternity, Paternity, Adoption and Maternity Support Leave and Pay policies are in place and apply to all Council employees. There are some differences in entitlement depending on the conditions of service that apply. Keep in Touch (KIT) payments may be paid to employees on maternity or adoption leave at the employees' hourly contractual rate for up to ten days or sessions. The purpose of this review was to provide assurance that: • Maternity, Paternity, Adoption, Maternity Support leave and pay were correctly calculated and paid only to employees who qualify; • KIT payments were calculated and paid correctly.	September 2018	A review of payments made for employees on paternity and adoption leave was undertaken. Except for one minor error the calculations were found to be correct. One employee had notified their manager that they were adopting. However, no Matching Certificate could be found on Lagan for this employee. Documentation for maternity cases was also not always available on the Wisdom system. A number of KIT claim forms and managers' records were missing from the Wisdom system.	**Four P3 actions were agreed.** **Responsible Officer: Assistant Chief Executive (Business Support), HR and OD.** Guidance in relation to the adoption leave process has been updated to prompt administrators to request the matching certificate from the line manager/employee and to escalate to their line manager should no response be received within one working week. Regular communications to managers regarding uploading of documents onto Wisdom will be placed on Team Brief. The Payroll team will do spot checks on these cases to ensure the required forms are present on Wisdom.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
C	Risk Management (CYPS and HAS)	Substantial Assurance	The purpose of this audit was to provide assurance that: • There are appropriate tools in place to effectively manage risks at a service level; • Service level risk management is understood consistently throughout the Council; • Service risk registers are effective, complete, and up to date. The focus of the audit was on HAS and CYPS. The audit scope did not include the Council's corporate risk management arrangements.	November 2018	Responsibility is clearly defined within the Corporate Risk Management strategy. Generally the risk registers for both HAS and CYPS appear to be up to date, and include emerging risks. Significant improvements have been made recently to the risk management process within HAS. A directorate strategic risk management group has been created and the risk register has been reviewed and updated to ensure all risks are adequately addressed. There is no similar group within CYPS. It was evident that although there is an understanding of risk management across the directorate, there is little joint review or discussion of service risk registers.	**Two P3 actions were agreed.** **Responsible Officer: CYPS & HAS Assistant Directors.** A directorate risk management group to be recreated for CYPS with agreed terms of reference. An updated directorate risk register to be discussed twice a year at Leadership team.
D	Contractor Due Diligence	Limited Assurance	The Council has a significant number of contracts. Many of these contracts deliver key projects and services which the Council relies on to achieve its objectives. There may therefore be significant and detrimental financial and reputational risks if any of these key contracts fail. The purpose of this audit was to provide assurance that:	May 2019	There is currently no corporate approach to contractor due diligence across the Council. There is also no guidance that outlines the risk of supplier failure, and how to reduce and manage this risk effectively. Arrangements are not in place throughout the Council to review suppliers/contractors on a regular basis, to check financial resilience through the life of the contract.	**Three P2 actions were agreed.** **Responsible Officer: Head of Procurement and Contract Management.** The Council plans to develop and introduce: • The major suppliers/supplier monitoring dashboard.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			• Arrangements were in place throughout the Council to review suppliers/contractors on a regular basis, to check financial resilience through the life of the contract; • Up to date and accurate information was being captured and used effectively by the Council; • All contract managers were being adequately informed in order to deliver effective due diligence.		The Council is aware of these weaknesses and plans are therefore in place to improve contractor due diligence arrangements. For instance a supplier dashboard is currently being designed, which will help to identify the highest risk (based on price and contract) suppliers and monitor them based on live information streams.	• Contract management e-learning (to include contractor due diligence). • A contract management toolkit (to include contractor due diligence) to provide practical help to officers involved in contract management. It is envisaged that these improvements will be completed by December 2019.
E	Information Security compliance audits	Various compliance visits: 2x High Assurance 3x Substantial Assurance 1x Reasonable Assurance	We completed unannounced information security compliance visits to the following offices: • Jesmond House, Harrogate • North Yorkshire House, Scarborough • Legal Services, County Hall Northallerton (two visits) • South Block, County Hall Northallerton • Manor Road, Knaresborough	Various	Following each visit, a detailed report was sent to the Senior Information Risk Owner (SIRO), as well as to relevant directorate managers. Data security practices and compliance with council policies was found to be poor in a number of instances.	**Four P2 and Six P3 actions were agreed.** **Responsible Officers: various** Responses have been obtained from relevant directorate managers following each audit. The findings have been taken seriously and management has taken immediate action where issues have been discovered. Follow up visits have been arranged where significant information risks have been identified.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
		3x Limited Assurance	• Sandpiper House, Selby • North Block, County Hall, Northallerton • MAST, Northallerton			

Appendix 3

CONTRACTS - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2019

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Best Value Forms Compliance	Reasonable Assurance	Where quotations are not sought for low value purchases (below £25k), officers are required to complete Best Value Forms (BVF). The purpose of this audit was to provide assurance that: • The BVF submitted are being completed to the required standard • A consistent approach is followed across all directorates. The audit reviewed forms completed between October 2017 and March 2018.	September 2018	Improvements have been made to the quality and completion of the forms compared to the previous audit in 2017. However, incomplete or inaccurate BVF were still evident. Some forms had no budget manager approval, others were unsigned and some were incomplete. We also found differences in the number of forms being completed by each directorate. For example, the number of forms completed by BES and Central Services was higher than HAS. This disparity may warrant further investigation. The Best Value Form was originally introduced to deliver more simplicity and flexibility to the procurement procedure. It was unclear at this stage whether the envisaged benefits had been realised.	**Two P2 and One P3 actions were agreed.** **Responsible Officer: Head of Procurement & Contract Management.** The role of the Procurement Team in processing BVF to be discussed at the Procurement Board. Communication with regards to appropriate usage, purpose and benefits of the BVF and FPP to be issued to relevant officers. This communication will also be reiterated to managers in the 'Managers Mail'.

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.
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.