NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

29 SEPTEMBER 2016

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 2016 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 IT audit plan for 2016/17 were presented to the Committee in June 2016.

2.2 This report considers the work carried out by Veritau and Audit North during the period to 31 August 2016. 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 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 2016. 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 2016**

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**

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 the mobile device encryption project and ICT project and programme management;

- 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 development of the NYCC 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;

- 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 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 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 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:

(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

11 September 2016

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 2016

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	In House System Development Controls	Substantial Assurance	The audit reviewed the adequacy and effectiveness of controls at the inception of the system development lifecycle.	October 2015	Good controls were found to be in place. The main issues identified were: • Testing plans were not available for the developments examined and the testing process for system development was not always followed. • Technical specification documents were not available, at the time of the audit fieldwork, for both Oracle BAFS Project and the Car Pool Project.	**Two P3 and One P2 actions were agreed.** **Responsible Officers:** Head of Technology Solutions, Development Team Lead It is recognised that services need to improve business process documentation to allow them to create more robust test scripts. The requirements for test scripts are however dependent on the size of the development. This will be reviewed as part of project management. A functional specification now needs to be completed and signed off by the service before any new development commences. Regarding training materials, this is an area under review as to who is responsible and in what form it should be undertaken in. For large development this will be included in project plans.
B	Programme Management	High Assurance	A programme management framework should exist for all IT projects which ensures that	October 2015	Significant progress had been made in addressing the actions raised in the previous audit report:	**No further actions required.**

System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
		they are subject to formal identification, approval, prioritisation and co-ordination. The audit reviewed the progress made in completing the actions raised in the previous IT Programme Management audit.		• A standard approach to benefits management has been introduced. • An approach to risk management for projects and programmes has been agreed with corporate risk management and is being introduced for all projects. • A project management handbook has been developed in Sharepoint providing clear guidance for project managers on not only the stages of the project lifecycle, but the documentation to be used at each stage. • A comprehensive two day Business Case training course was delivered by an external organisation (CIPFA) to senior project mangers to aid their understanding of the purposes and content of a Business Case, and; • The Business Partners presented a session to the Technology and Change senior management team setting out their role and responsibilities together with their expectations of how Technology and Change will support and similarly, how the Business Partner role interfaces with Technology and Change.	

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
C	IT Risk Management	Substantial Assurance	The audit reviewed the efficiency and effectives of the IT risk management process, supporting framework and policies to ensure that IT risks are identified and assessed in accordance with the organisation's overall risk management process.	November 2015	The risk management arrangements were found to be effective with few weaknesses identified. The main issues were: • Operational IT risks within Technology & Change were monitored in isolation as part of the ISO 27001:2013 accreditation process. The risks had not been reviewed since April 2015. • The progress of risk reduction actions is only reviewed as part of the six monthly corporate risk management review. As such, the County Council does not document when risk reduction actions have been completed if they are achieved after the six month review.	**Two P2 and One P3 actions were agreed.** **Responsible Officers:** Head of Technology Solutions, Technology & Change Managing Assistant Director An update of the Action Improvement Register (AIR) will be discussed at the Leadership Team every 6 months. A regular meeting to discuss security issues effecting T&C will be held with members of the leadership team, security officer and operations staff that will be responsible for ensuring the AIR is update and risk mediation is prioritised. Both the Action Improvement Register and Corporate Risk Register will be reviewed at regular T&C Leadership Team Meetings and updates noted. Discussions will be held with the Corporate Risk Management officers with regard to maintaining a record of completed actions, if this is not already available.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
D	North Yorkshire 2020 Customer Portal Project	Reasonable Assurance	The audit reviewed the project management arrangements to ensure that they were proportionate to the size and complexity of the project, and provided effective governance and control to ensure delivery of the project.	November 2015	The arrangements were found to be satisfactory although a number of areas for improvement were noted: • Several documents had not been developed for the customer portal project in line with the Project Management Lifecycle. • Some key decisions for the project were not documented. While decisions are documented for the Customer Theme Board in an action log, we noted that the log for meetings in July and August 2015 did not contain any reference to the customer portal project.	**Two P2 and One P3 Actions were agreed.** **Responsible Officer:** Head of Programme and Projects. A new project will be raised for each business that will utilise the portal functionality and the required project documentation will be produced and will go through a Customer Journey Mapping exercise. Tolerances are to be introduced for time, cost and quality within project plans. Project reporting and governance continues to be improved and key project decisions will be recorded in the relevant Project Governance Board minutes and project action log.
E	Lagan CRM Follow-up	Substantial Assurance	Controls should exist to manage key risks relating to the confidentiality, integrity and availability of information stored and processed by the Lagan CRM system. The audit reviewed the progress made in completing the actions raised in the previous Lagan CRM General Controls audit report.	December 2015	Good progress had been made in addressing the actions raised in the previous audit report. Out of the 11 agreed actions, nine had been implemented, and the remaining two had been partially implemented. • A review of the Lagan access groups had not yet been performed. • The latest version of Lagan (V14R2) did have some improved password functionality	**Two P2 actions were agreed** **Responsible Officer:** Senior Systems Officer, These remaining actions will be completed once resources permit.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					However, the improved functionality did not reference any change to the forced password expiry setting.	
F	Wireless Networking Security	Reasonable Assurance	The audit reviewed the controls in place for managing the wireless network infrastructure to ensure they are adequate to maintain the confidentiality, integrity and availability of network services and information.	January 2016	The controls were found to be satisfactory although a number issues were noted: • Security of the NYCC guest wi-fi could be improved. • Documentation had not been developed detailing the configuration of the wireless network, or to support the day-to-day operational management and maintenance of the wireless network. Relevant responsibilities had also not been defined. • Security monitoring procedures had not been developed for the Aruba wireless network and the Intrusion Detection System (IDS) events are not subject to regular monitoring or review. .	**Two P2 and Two P3 actions were agreed.** **Responsible Officers:** Technical Lead Service Manager - Communications and Security Technology & Change have introduced a more robust project methodology which should address these access issues. More robust test plans have also been introduced. More effective daily checks are being carried out to identify failed Access Points. A VIP Alert queue is being created to ensure alerts that absolutely need attention are given priority. Documentation for this is currently being reviewed and improved. A recent audit of our Security Infrastructure has taken place. In line with the findings of this audit we will look to further refine the alert process.
G	Microsoft Exchange (e-mail system)	Substantial Assurance	The audit reviewed the controls in place to maintain	February 2016	Good controls were found to be in place.	**Two P2 and Two P3 actions were agreed.**

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			the confidentiality, integrity and availability of information stored and processed by the MS Exchange 2010 email system.		The main issues identified were: • The latest MS Exchange 2010 updates had not been applied to the environment. • Documentation had not been developed detailing the implemented settings and configuration of the MS Exchange 2010 installation. • Failover testing to the MS Exchange disaster recovery environment had not been performed since the solution went live in 2011. • Email alerting had not been configured within the Microsoft Systems Centre Operations Manager (SCOM) monitoring software to proactively alert support staff of issues with the Exchange 2010 environment	**Responsible Officer:** Technical Lead The latest MS Exchange 2010 update was applied at the time of the audit. We will add a task as part of our Daily Checks process to check whether there are any updates to Microsoft Exchange 2010. This will be performed weekly or monthly (to be agreed). We are currently improving our system documentation as a team – including the Exchange documentation. Once this has been created, we can use this as a baseline for all future configuration changes to the system. Technology and Change are currently undergoing an audit on DR and Service Continuity. As part of this it is planned to include a managed DR failover of certain servers and systems. As Exchange is a critical system for the council, this should be included in this test. Work will be carried out to understand and develop email-based alerting from SCOM for the exchange system.
H	NYCC 2020 – Oracle Financials	Substantial Assurance	The audit reviewed the controls in place to maintain the confidentiality, integrity and	April 2016	Good controls were found to be in place.	**Two P2 actions and Four P3 actions were agreed.**

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			availability of information stored and processed by Oracle eBS.		The main issues identified were: • The Finance System Support Team had not developed a business continuity plan detailing how the team would manage and communicate Oracle eBS downtime. • A formal scheduled patch management process had not been established for the Oracle eBS environments (UNIX operating system Oracle RDBMS or Oracle eBS) • Default Oracle RDBMS account configurations had not been changed during the implementation of Oracle eBS R12	**Responsible Officer:** Systems Manager Service Manager Infrastructure An Oracle eBS business continuity plan covering both Finance Systems and the Integrated Finance teams will be prepared. The Finance Systems team and the Server team will have quarterly patch update meetings and schedule six monthly patching. The Finance Systems team is working with DBA and Oracle Support staff to investigate and change any default passwords that were identified, whilst monitoring the effect upon the system any changes will produce.
I	NYCC Disaster Recovery	Substantial Assurance	The audit reviewed the arrangements in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failure or disasters.	May 2016	Good controls were found to be in place. Audit testing also identified some weaknesses in controls, as follows: • The IT Disaster Recovery Plan was still in draft format at the time of audit. • The IT Critical Systems list was being reviewed and had not been ratified. • Third party hosted system providers had not been	**Two P2 actions and Four P3 actions were agreed.** **Responsible officers:** Head of Technology Services Technology & Change Managing Assistant Director Business Impact Analysis (BIA) has been carried out as part of individual services business continuity plans. Technology & Change recognise that the quality of the BIA data would benefit from

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					contacted to determine disaster recovery arrangements in place for each system. • The IT Out of Hours Manual had not been reviewed since 2010 and did not reflect current operational processes or systems.	validation and sign-off from individual services before being presented to the Corporate Information Governance Group (CIGG). An action plan will be implemented to achieve this. For all externally hosted systems managed by Technology & Change, the Corporate Systems Team will contact the company and establish their DR provision in writing. The ICT Out of Hours Manual has been updated with the up to date critical systems and a 6 monthly review cycle has been scheduled.
J	IT Access by Non-NYCC Staff	Limited Assurance	The audit was carried out following a request by Technology & Change. The audit reviewed the framework for governing access to systems for non-NYCC staff to ensure use is appropriately authorised and controlled. The audit also examined whether access was removed when it was no longer required and users received suitable training.	June 2016	The council has clearly recognised the need to manage access to data and systems by users who are not its employees, and has taken a number of positive steps. However, the policy framework lacks sufficient clarity. • The wording of the confidentiality agreement is not user-friendly. Users are not required to sign to confirm that they understand their obligations. • Managers are not enforcing the requirement for users to complete information security	**Six P2 actions and Two P3 actions were agreed.** **Responsible Officer:** Head of Technology Solutions The findings of the audit were reported to the Corporate Information Governance Group (CIGG). The Policy will be reviewed and rewritten, taking account of the ongoing work to extend the use of volunteers across the County Council. A review of the training requirements for roles will also be

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					training. • Individual users are sometimes being granted excessive access rights, and their accounts are not always being disabled and deleted when they leave.	undertaken. The use of an end date for a System Access Request is to be reviewed; however the accounts are regularly reviewed and suspended if no activity has been recorded for 12 months.
K	Schools ICT Data Centre Security	Limited Assurance	The audit reviewed the physical and environmental controls operating within the computer room for schools ICT, to ensure the availability, confidentiality and integrity of the network and server infrastructure.	August 2016	A number of weaknesses were found, including: • There is no automated fire suppression system installed within the computer room. • With the exception of smoke detectors, there is no other environmental monitoring equipment installed (for example, monitoring water, heat or humidity). • Highfield House did not have a backup generator to provide power in the event of a power outage which exceeded the short term cover provided by UPS devices. • The floor of the computer room was carpeted with no anti-static mats or wristbands to provide additional protection to either equipment or staff.	**Three P2 actions and One P3 actions were agreed** **Responsible Officer:** Service Manager - Schools ICT Work is now underway to re-locate all relevant IT hardware to dedicated computer room facilities at County Hall. Anti-static wrist band are being purchased.

CORPORATE THEMES - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2016

	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. Five 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. Findings have also been discussed by the Corporate Information Governance Group (CIGG). Working practices were found to be weak in a number of instances. Four visits were classified as Limited Assurance and one visit was classified as High Assurance.	**Five P2 and one P3 action 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.
B	Reorganisation, restructure and redundancy	High Assurance	The audit reviewed the procedures and controls in place to enable the effective management of service reorganisations and restructures. Redundancy payments were also reviewed	April 2016	We found there are clear policies and procedures in place to effectively manage reorganisations, redeployments and redundancies. We found one settlement agreement which had been incorrectly coded as	**Two P3 actions were agreed.** **Responsible Officer:** Assistant Chief Executive (Business Support) HR & Organisational

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			to ensure they were being calculated correctly and paid in a timely manner.		a redundancy payment.	Updated guidance has been issued to staff within ESS to ensure future payments are correctly coded.
C	Risk Management	Substantial Assurance	The audit examined whether: • risks were being appropriately identified • risk mitigation was adequate with evidence of improvements • the defined process for North Yorkshire 2020 projects had been followed.	May 2016	We found the arrangements for managing risk were good with few weaknesses identified. Appropriate risks for the projects chosen were identified through consultations with a variety of different stakeholders.	**No actions were agreed.**

CONTRACTS - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 31 AUGUST 2016

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Revenue Contracts; Action for Children – (follow up)	No opinion	The audit reviewed the progress made in respect of the arrangements in place with Action for Children at May Lodge, Scarborough. The previous audit in 2014 had highlighted a number of contractual and operational issues. The report included a number of recommendations for future action.	November 2015	Progress has been in a number of areas. There have been some initiatives implemented to improve arrangements and contract monitoring and so far these seem to be working well. The new Registered Manager had developed an action plan to address a number of operational matters. We also noted signed contracts were now in place for all service users. The Council still has work to complete to ensure future contractual decision making maximises the outcomes for the Council and service users.	Officers in HAS are to seek legal and procurement advice prior to commencing the forthcoming procurement exercise. Any future agreements will include appropriate contract and performance management arrangements.
B	Allerton Waste Recovery Park – Contract Management Healthcheck	No opinion	The County Council signed an agreement with AmeyCespa for the Allerton Waste Recovery Park (AWRP) project in October 2014. Whilst the facility is not due to become operational until 2018 there is a need for robust contract management to be in place well in advance of the operational commencement of	March 2016	The Council has made good progress in developing the contract management arrangements and managing the risks associated with the AWRP scheme. The AWRP key risks are well known by officers and have also been highlighted through the risk management processes. Officers were aware of the need for a number of areas to progress in the	Officers have integrated the agreed areas into forthcoming planning and work on the AWRP scheme.

	System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			the contract. The purpose of this review was to provide an initial 'healthcheck' on some of the immediate key contract management risk areas facing the Council with the AWRP contract.		forthcoming months. We provided a summary of findings and recommended actions. We also agreed with officers that the key areas to focus on were: • The development of a high level strategy document for the AWRP contract. • Finalising the construction and commissioning sections of the Contract Management Manual. • Preparing a resource plan for the contract with a particular focus on the requirements for the operational phase • Developing the requirements for the Management Information System for the project which will include performance, reporting and financial elements.	
C	Contracts with the Dalewood Trust	No opinion	Dalewood Trust (Dalewood) is a charitable trust based in Whitby, North Yorkshire. The County Council has two block contracts with Dalewood. The largest contract is for the provision of a day service These contracts have been in place since 1 April 2005. Based upon the current extension period both contracts will expire on 31	August 2016	We found a number of weaknesses in the arrangements being operated covering areas such as procurement, contract management and the level and quality of service delivery. A number of recommendations to address these matters were contained in the report.	Senior officers in HAS have agreed an action plan to ensure all of the matters identified in the review are addressed.

System/Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
		March 2018. We were asked by management to perform a detailed review of the contract, including contract approval, contract monitoring, approval of additional payments and value for money.			

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.