NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

26 SEPTEMBER 2013

INTERNAL AUDIT WORK ON COMPUTER AUDIT

Report of the Head of Internal Audit

1.0 **PURPOSE OF THE REPORT**

1.1 To inform Members of the **internal audit work** performed during the year ended 31 August 2013 on computer related risks and to give an opinion on the systems of internal control in respect of this area.

1.2 To inform Members of the new contract arrangements for IT audit work.

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 computer audit the Committee receives assurance through the work of Veritau Limited. Veritau engages an external contractor to support the provision of internal computer audit services. Since 1 April 2008, that service was provided by PriceWaterhouseCoopers LLP (PwC). The contract with PwC however ended on 31 March 2013.

2.2 This report details the computer audit work undertaken by PwC and provides a summary of the audit reports issued since the last report was presented to this Committee in September 2012

3.0 **WORK DONE DURING THE TWELVE MONTHS ENDED 31 AUGUST 2013**

3.1 A summary of the internal audit reports issued in the year since the last report on computer audit was presented to the Audit Committee in September 2012, and is attached at **Appendix 1**.

3.2 Veritau and PwC officers have also been involved in a number of other areas related to computer audit. These have included;

- providing advice on relevant IT related controls;

- where appropriate, commenting on IT security related policies and strategies, which contribute to the overall information governance framework for the County Council.

3.3 As with previous audit reports, an overall opinion / risk rating has been given for each of the specific systems or areas under review. The opinion / rating given has been based on an assessment of the risks associated with any weaknesses in

control identified. As all the computer audit related work was undertaken by PwC, each of the audit assignments has been assessed according to PwC's own risk ratings. The details of PwC's risk rating and associated definitions are provided in **Appendix 2**.

3.4   In addition to the overall risk rating given for each audit, PwC also apply the same ratings for each individual recommendation.

3.5   It is important that agreed actions are formally followed up to ensure that they have been implemented. PwC IT auditors will follow up all agreed actions on an annual basis. **Based on the follow up audit work undertaken by PwC to date, the Head of Internal Audit is satisfied that management are taking steps to implement the agreed actions necessary to address identified control weaknesses.**

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 (ie 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 County Council's computer related controls is that they provide **substantial assurance.** This opinion is based on the individual opinions / risk ratings given by PwC as detailed in 3.3 of this report. In reaching his opinion, the Head of Internal Audit has placed reliance on the work of PwC and has aligned PwC's overall opinions with Veritau's own assurance ratings. Substantial assurance is defined by Veritau as:

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.

5.0   **NEW IT AUDIT CONTRACT ARRANGEMENTS**

---

[1] The PSIAS refers to the Chief Audit Executive. This is taken to be the Head of Internal Audit.
[2] The PSIAS refers to the board. This is taken to be the Audit Committee.

5.1   As noted in paragraph 2.1 above, the contract with PwC ended on 31 March 2013. Following a tender exercise, Veritau has now awarded a new contract to Audit North for the provision this service. Audit North is an NHS audit consortium based in Durham. The consortium has a dedicated IT audit team and serves a number of NHS and other public sector bodies across the North of England. As part of the new contract arrangements, Audit North will help to build IT audit capacity within Veritau as well as supporting the work of the company's existing in house IT auditor.

5.2   Representatives from Audit North are currently completing an IT audit risk assessment and preparing a strategic audit plan. Details of the risk assessment and strategic plan will be reported to the next meeting of this Committee.

6.0   **RECOMMENDATIONS**

6.1   That Members consider the information provided in this report and determine whether they are satisfied that the control environment operating in respect of IT systems is both adequate and effective.

6.2   That Members note the new contract arrangements for IT audit work.

Max Thomas
Head of Internal Audit
Veritau Limited
County Hall
Northallerton

BACKGROUND DOCUMENTS

Relevant Audit Reports kept at Veritau Limited, County Hall, Northallerton, DL7 8AL. Contact Max Thomas, extension 2143

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

County Hall
Northallerton

9 September 2013

COMPUTER AUDIT – FINAL AUDIT REPORTS ISSUED IN THE YEAR ENDED 31 AUGUST 2013

	System/Area	Opinion / Risk Rating	Area Reviewed	Date of Audit	Comments	Management Actions Agreed
A	Windows Migration – Asset Tracking	Medium	Following the migration from Novell to Windows, Microsoft's System Centre Configuration Manager (SCCM) is now being used to monitor asset utilisation so as to improve deployment and security. The objectives of the audit were to: • Assess the plans in place to monitor IT asset usage • Provide recommendations to improve the efficiency of asset usage and promote effective asset deployment	July 2013	A number of areas of good practice were identified including the completion of a baseline exercise to identify the total asset stock and the adoption of a central ICT budget for asset purchases. A small number of areas for improvement were however identified, including: • The need to undertake an exercise to identify disconnected IT assets • The need to introduce and scope an IT asset audit procedure	The findings of the audit were accepted. A process will be designed to use the SCCM reported data and to track assets not connected each month. In addition, SCCM data will be compared against the known Configuration Management Database (CMDB) records. Exception reporting will then highlight where desktops appear to have changed location and/or laptops where the primary user appears to have changed. Three '**medium**' ranked recommendations were made. **Responsible Officer:** Assistant Director – ICT Services
B	IT Asset Management	Medium	At the time of the audit, the County Council was recording IT assets centrally on a Microsoft Access database. However, a decision had been made to use a Configuration Management Database (CMDB) instead. The CMDB will be linked to the helpdesk system (Landesk) thereby	June 2013	A number of areas of good practice were identified including the County Council's IT asset policy framework. The plans for the new system and associated processes were also considered to be well developed. A small number of areas for improvement were however identified, including:	The findings of the audit were accepted. The System Centre Configuration Manager (SCCM) will be used once the CMDB is available to record and track IT assets. Relevant processes will be developed to ensure regular audit checks are performed. Two '**medium**', one '**low**' and one '**advisory**' recommendations

	System/Area	Opinion / Risk Rating	Area Reviewed	Date of Audit	Comments	Management Actions Agreed
			allowing electronic verification and auditing functions to be undertaken. The objectives of the audit were to: • Review current practices for recording and controlling IT assets • Assess the plans to develop the new IT asset management system • Provide appropriate advice on the implementation of the new system (including consideration of how IT assets deployed outside the County Council estate should be recorded).		• Limitations in the functionality of the existing IT asset database • A lack of periodic reviews / audits of the IT asset database (to verify the completeness and accuracy of the records) • Insufficient integration of IT asset management into wider organisational processes and controls.	were made. **Responsible Officer:** Assistant Director – ICT Services
C	Change Programme – Flexible Working	Not given	The objectives of the audit were to assess: • The technological options available to support flexible working • The extent to which the ICT plans for developing or acquiring new technology linked to other One Council work streams and / or the needs of end users • The possible security implications of the	June 2013	A number of areas of good practice were identified including the fact that ICT was aware of its existing capabilities and the possible security challenges of the new technologies. ICT had also identified or commenced a number of projects which would benefit flexible working. Some areas of improvement were identified, including the need to formalise the flexible working programme, define user needs and technology assessment	The findings of the audit were accepted. A formal and overarching flexible working programme will be developed by October 2013. The existing corporate pilot group (established to test new and different types of devices) will inform the roll out of the new technologies. The potential security risks will be kept under review. One '**high**' and four '**medium**' recommendations were made. **Responsible Officer:**

	System/Area	Opinion / Risk Rating	Area Reviewed	Date of Audit	Comments	Management Actions Agreed
			preferred options		criteria, and undertake a formal security risk assessment.	Assistant Director – ICT Services
D	ICT Governance – ISO20000 readiness	Not given	The review was intended to assess compliance with ISO20000 standards prior to the formal certification audit.	December 2012	The review noted that the County Council had invested significant time and effort to ensure systems and processes were compliant with the required standards. However, a few areas required further improvement, including: • A senior officer should be given 'ownership' of the standard to ensure ongoing adherence • Recognition that change control currently relies too much on a key member of staff • The failure to use data collected by the service desk to identify issues or weaknesses in ICT provision.	The audit recommendations were mostly accepted. Changes and improvements were made as necessary to ensure ISO IEC 20000 certification was achieved. One '**high**' and two '**medium**' recommendations were made. **Responsible Officer:** Assistant Director – ICT Services
E	ICT Shared Services	Medium	The County Council currently provides certain IT related services to the district councils in North Yorkshire. These include telephony services and some network support. The audit reviewed the current processes that are in place to	June 2013	The County Council has a range of services which are available to other partners. Service Level Agreements are in place with the relevant councils and performance is regularly monitored through account management meetings. The	The recommendations were agreed in principle although it was noted that the existing arrangements had been developed as and when opportunities arose. An appropriate shared service framework would be developed

	System/Area	Opinion / Risk Rating	Area Reviewed	Date of Audit	Comments	Management Actions Agreed
			support the shared service model and assessed where there might be gaps and / or opportunities for possible development.		County Council had also recently commissioned an external review (by Castlerigg Consultancy) to assess the appetite for further collaboration. A number of recommendations were made, as follows: • A strategy and objectives for the provision of shared services should be developed • A governance framework should be developed and implemented • A service catalogue and cost model should developed	(including governance and risk management) by October 2013. Four '**medium'** recommendations were made. **Responsible Officer:** Assistant Director – ICT Services
F	Software Licensing	High	The County Council has processes in place to manage software licenses. Enterprise agreements exist for key applications and these are recorded centrally and reviewed annually. However, smaller applications are often managed by the relevant service department. The objective of the audit was to review the current practices for managing software licences.	February 2013	At the time of the audit, the County Council was due to implement the Microsoft System Centre Configuration Manager (SCCM). This will improve the identification of licences and hence overall software management. However, the auditors noted that: • There was no software license database to record	The findings of the audit were accepted. A business case will be developed to asses the costs and benefits of implementing a complaint software asset management database. A review will also be undertaken using existing tools to identify the software already installed on corporate devices. Any identified gaps will be addressed but also feed into the business case. One '**high'**, two '**medium'** and

System/Area	Opinion / Risk Rating	Area Reviewed	Date of Audit	Comments	Management Actions Agreed
				compliance • There were no defined procedures to record or track ongoing license verification • The policy framework needed to be strengthened and the existing procedures needed to be better integrated into the wider organisational processes and controls.	one '**low**' recommendations were made. **Responsible Officer:** Assistant Director – ICT Services

" PWC'S RISK RATINGS"

Risk Rating	Definition

Risk Rating   **Definition**

Critical

A finding that could have a:

- *Critical* impact on operational performance or

- *Critical* monetary or financial statement impact or

- *Critical* breach in laws and regulations that could result in material fines or consequences *or*

- *Critical* impact on the reputation or brand of the organisation which could threaten its future viability

High

A finding that could have a:

- *Significant* impact on operational performance or

- *Significant* monetary or financial statement impact or

- *Significant* breach in laws and regulations resulting in significant fines and consequences *or*

- *Significant* impact on the reputation or brand of the organisation

Medium

A finding that could have a:

- *Moderate* impact on operational performance or

- *Moderate* monetary or financial statement impact or

- *Moderate* breach in laws and regulations resulting in fines and consequences or

- *Moderate* impact on the reputation or brand of the organisation

Low

A finding that could have a:

- **Minor** impact on the organisation's operational performance or

- **Minor** monetary or financial statement impact or

- **Minor** breach in laws and regulations with limited consequences or

- **Minor** impact on the reputation of the organisation

Advisory | A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.