ITEM 11

NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

27 SEPTEMBER 2012

INTERNAL AUDIT WORK ON COMPUTER AUDIT

Joint Report of the Head of Internal Audit and the Interim Head of ICT Services

1.0 PURPOSE OF THE REPORT

To inform Members of the internal audit work performed during the year ended 31 August 2012 on computer audit and to give an opinion on the systems of internal control in respect of this area.

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 has been provided by PriceWaterhouseCoopers LLP (PwC). The contract for this service ends in March 2013.

2.2 This report details the computer audit work undertaken and provides a summary of the audit reports issued since the last report was presented to this Committee in September 2011. It should be noted that not all of the audit reports detailed in **Appendix 1** relate specifically to ICT Services but may fall within the responsibility of other directorates depending on the system under review.

2.3 Because this report addresses a functional theme rather than the activity of one directorate, there is no corresponding Statement of Assurance or Directorate Risk Register. ICT Services is part of the Finance and Central Services Directorate and the relevant Statement of Assurance and Risk Register for that directorate will be considered later in the Audit Committee cycle.

3.0 WORK DONE DURING THE TWELVE MONTHS ENDED 31 AUGUST 2012

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 2011, is attached at **Appendix 1**. Specific attention is drawn to any recommendations that management have chosen not to implement. A copy of the 3 year strategic computer audit plan 2011-14 is attached as **Appendix 2** for information. The plan was approved at the April meeting of this Committee.

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

- attending the Technology Implementation Group (TWIG) to present IT audit reports as applicable;
- assisting in the investigation of reported IT security or suspected IT misuse issues as reported to Veritau;
- 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 All internal audit reports relating to computer matters are submitted to TWIG, which is chaired by the Corporate Director – Finance and Central Services. TWIG then considers the management response provided and monitors progress on implementing any agreed actions. A member of PwC attends TWIG for these discussions. Follow-up audit work is also reported to TWIG. A Veritau representative will also attend TWIG meetings on a periodic basis to understand key issues as they emerge.

3.4 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 planned computer audit work for 2011/12 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 for the benefit of members below:

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.

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

3.6 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.**

3.7 All internal audit work undertaken by PwC is based on a comprehensive risk based approach which complies with CIPFA's code of audit practice and internal audit standards. Risk management is a dynamic process and as such, the County Council's risk register is continually updated throughout the year to reflect the changes in the County Council's risk profile. It is essential that the audit plan is mapped to the risk register on an annual basis. If a new risk arises during the year, which requires audit attention, it will be considered on a timely basis.

4.0 AUDIT OPINION

4.1 Veritau works to the CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom. In connection with reporting to Audit Committees, that guidance states that:

"The Head of Internal Audit's formal annual report to the organisation should:

(a) include an opinion on the overall adequacy and effectiveness of the organisation's internal control environment

(b) disclose any qualifications to that opinion

(c) present a summary of the audit work undertaken to formulate the opinion, including reliance placed on work by other assurance bodies

(d) draw attention to any issues the Head of Internal Audit judges particularly relevant to the preparation of the Annual Governance Statement

(e) compare work actually undertaken with the work that was planned and summarise the performance of the Internal Audit function against its performance measures and criteria

(f) comment on compliance with these standards and communicate the results of the Internal Audit quality assurance 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 explained in **paragraph 3.4** of this report. PwC work to the standards laid down by ICAEW and ISACA and their computer audit files are subject to quality assurance review by Veritau. 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 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 IT systems is both adequate and effective.

MAX THOMAS
Head of Internal Audit

JON LEAROYD
Interim Head of ICT

BACKGROUND DOCUMENTS

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

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

County Hall
Northallerton

7 September 2012

APPENDIX 1

COMPUTER AUDIT – FINAL AUDIT REPORTS ISSUED IN THE YEAR ENDED 31 AUGUST 2011

	System/Area	*Opinion / Risk Rating*	*Area Reviewed*	*Date of Audit*	*Comments*	*Management Actions Agreed*
A	Novell to Windows Migration - Group Policy Review	None given	The County Council is in the process of migrating from its legacy Novell and GroupWise platforms to a Microsoft aligned solution as part of its IT strategic vision. The objective of this review was to assess the County Council's Model Office Active Directory (AD) Group Policies to ensure that these protect the confidentiality, integrity and availability of the County Council's information assets. In addition, we reviewed the Group Policies against industry good practice to ensure that security controls were implemented in order to help protect against known threats.	August 2011	The importance of Information Assurance is recognised within the County Council and our review determined that the County Council had taken a risk measured approach to configuring Group Policies. We did not provide an overall opinion or report classification for this review as the scope was limited, however we identified a number of high, medium and low risk findings in some configuration settings of the Group Policies.	Most recommendations were agreed by management, and actions have been developed to investigate and address the points raised. Where recommendations were not accepted the reasons for this were documented and agreed.
B	Novell to Windows Migration – ICT change programme	Medium	The County Council is in the process of migrating from its legacy Novell and GroupWise platforms to a Microsoft aligned solution as part of its IT strategic vision. This audit specifically focussed on the change management procedures used for the recent	February 2012	It was clear from this review that the challenges associated with such an organisation-wide change had been recognised by the County Council. Recommendations were raised in respect of the following areas: • Further development of	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised.

	System/Area	*Opinion / Risk Rating*	*Area Reviewed*	*Date of Audit*	*Comments*	*Management Actions Agreed*
			implementation of Microsoft Outlook, to identify both good practice and areas for further development in advance of the full desktop rollout planned during 2012.		communications and training plan; • Consideration given to implementing a dedicated route to log user calls; and • Further development of risks and issues logs.	
C	IT Contract Management	Medium	The County Council has a number of significant contracts, and ICT services have recently appointed a commercial manager to lead on IT procurement and contract management. This review focussed on the IT contract management processes for the Computacenter and Azzurri contracts.	Septemb er 2011	Although a number of areas of good practice were observed during the review, areas for improvement were identified in relation to: • Policies and procedures to be further developed; • Value for money considerations should be formalised; • The need for a review of post procurement contract management processes; and • Development of performance monitoring and management information activities.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised.
D	IT Security	Low	The County Council achieved ISO27001 certification for its ICT department in 2010, and was due to have a surveillance audit in November 2011 as part of the process for retaining certification. We undertook an	August 2011	The County Council has invested significant time and effort in implementing a secure ISO27001 ISMS. Management has consulted with stakeholders, and considered the assets, risks, compliance framework, resource	All recommendations (all low risk) were agreed by management, and actions have been developed to investigate and address the points raised.

	System/Area	Opinion / Risk Rating	Area Reviewed	Date of Audit	Comments	Management Actions Agreed
			interim review of the Council's ICT Information Security Management System as a precursor to the 27001 surveillance audit (which was successful). In addition, as part of the ongoing focus on IT security, we reviewed the effectiveness and management of the anti-virus controls deployed at the County Council.		requirements and technical facilities.	
E	IT Disaster Recovery	Medium	The County Council has an ongoing project to review and improve its IT Disaster Recovery (ITDR) programme ensuring that its arrangements for the UNIX environment are aligned with its Business Continuity Plan (BCP), and suitable controls, processes and improvements have been implemented. As part of this review we assessed the key controls in place relating to ITDR for the UNIX system to assess whether these were appropriate and would support the UNIX environment in the event of a disaster.	June 2012	Although areas of good practice were identified, we also highlighted weaknesses in the following areas; • The need to develop ITDR documentation • Establishment of a formalised ITDR testing schedule • Review of Internet Protocol (IP) address configuration • Formalisation of third party support arrangements	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised.

	System/Area	***Opinion / Risk Rating***	***Area Reviewed***	***Date of Audit***	***Comments***	***Management Actions Agreed***
F	IT Service Desk and SAR	Medium	The County Council is implementing a SAR solution to improve the administration of new user access to systems and hardware requests by streamlining and automating the request and approval process, to reduce the need for manual requests and e-mail authorisations. This audit focussed on the security and appropriatness of the solution to be deployed.	April 2012	During the review, we identified a number of recommendations relating to: • Project management and the project framework; • Development of the solution and change requests; • Access to the solution including the log in process for users and integration with Windows; and • The process for approval of requests for access or hardware.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised.
G	ICT Change Programme (ICT Workstreams)	Medium	A ‘One Council’ change programme has been established with objectives that include: identifying and maximising savings without impacting on frontline delivery; encouraging an enhanced culture of customer excellence; and ensuring a strong focus on performance. To support this programme a number of workstreams have been initiated across the organisation. This review focused on two of the workstreams within ICT Systems and Data, e-mail and retention and applications.	March 2012	For the two workstreams reviewed as part of this audit, there were clear links between their specific objectives and the achievement of the One Council Vision. We also identified some areas for improvement which included: • Development of elements of the implementation plan; and • Documentation of all interdependent tasks.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised.

APPENDIX 2

3 YEAR STRATEGIC COMPUTER AUDIT PLAN 2011/14

System	2011/12 Days
Novell to Windows migration	25
IT contract management	10
IT change programme	8
IT security	10
IT disaster recovery*	12
IT service desk and SAR	5
Follow up on prior year recommendations	7
Planning, management and attendance at TWIG and Audit Committees	3
Total	**80****

System	2012/13 Days
Novell to Windows migration	10
IT asset management	10
IT change programme	10
IT Governance***	10
IT shared services	10
Software licensing****	5
Follow up on prior year recommendations	2
Planning, management and attendance at TWIG and Audit Committees	3
Total	**60**

System	2013/14 days
IT project management	10
IT change programme	10
Standards for managing IT systems	5
IT resource management	10
IT continuous improvement	5
IT strategy	5
Follow up on prior year recommendations	2
Planning, management and attendance at TWIG and Audit Committees	3
Total	**50**

*Scope extended to include business impact assessment workshop.
**10 days were deferred from the 2010/11 internal audit plan.
*** Change to original ISO27001 ISMS review, which has been deferred until such a time that ISMS is rolled out across the Council.
**** Brought forward from 2013/14