NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

29 SEPTEMBER 2011

INTERNAL AUDIT WORK ON COMPUTER AUDIT

**Joint Report of the Head of Internal Audit
and the Assistant Director – 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 2011 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 Ltd. Veritau engages an external contractor for 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 covers a period of three years with the option to extend for a further two years. Veritau exercised the option to extend the contract for a further two years to the end of 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 2010. 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 service directorates depending on the system under review. 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 2011**

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 2010, 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.

1

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

- monitoring of the IT Audit Plan as provided by the external contractor. This involves periodic meetings with PwC to establish progress to date and to discuss audit findings and emerging risks, which may affect the content of the Plan.

- 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 may also attend meetings on a periodic basis to understand key issues as they emerge.

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. As all planned computer audit work for 2009/10 was undertaken by PwC, each of the audit assignments has been assessed according to their own assurance ratings. The details of PwC's opinions and associated definitions are provided for the benefit of members below:

Level of Assurance	Definition
High	Our work found some low impact control weaknesses which, if addressed would improve overall control. However, these weaknesses do not affect key controls and are unlikely to impair the achievement of the objectives of the system. Therefore we can conclude that the key controls have been adequately designed and are operating effectively to deliver the objectives of the system, function or process.
Moderate	There are some weaknesses in the design and/or operation of controls, which could impair the achievement of the objectives of the system, function or process. However, either their impact would be less than critical; or they would be unlikely to occur.
Limited	There are some weaknesses in the design and / or operation of controls which could have a significant impact on the achievement of key system, function or process objectives but should not have a significant impact on the achievement of organisational objectives. However, there are discrete

2

elements of the key system, function or process where we have not identified any significant weaknesses in the design and / or operation of controls, which could impair the achievement of the objectives of the system, function or process. We are therefore able to give limited assurance over certain discrete aspects of the system, function or process.

No   There are weaknesses in the design and/or operation of controls which [in aggregate] have a significant impact on the achievement of key system, function or process objectives and may put at risk the achievement of organisation objectives.

3.5   In addition to the overall assurance given for each audit, PwC also apply a priority to each individual recommendation. The four categories used by PwC are Critical, High, Medium and Low.

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 Council's risk register is continually updated throughout the year to reflect the changes in the 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."

3

4.2   The overall opinion of the Head of Internal Audit on the County Council's computer related controls is that they provide **moderate assurance**. This opinion is based on the individual opinions given by PwC as detailed 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. Moderate assurance is defined by Veritau as:

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.

4.3   Whilst audit work undertaken by PwC during 2010/11 resulted in a number of reports with an overall opinion of either moderate or limited (as per PwC ranking), it should be noted that PwC's IT audit work is focussed on areas of high risk to the County Council. There are many other IT functions/systems, not covered in this report, which continue to operate in an effective control environment.

4.4   A number of the audit reports detailed in **Appendix 1** where opinion given by PwC was limited relate to computer systems operated by service directorates. A common issue which has been highlighted during the year relates to the need for these service administered applications to comply with corporate IT policies and standards, for example change management processes and access controls. It is proposed that this issue will be addressed in the revised Corporate ICT Strategy which is scheduled for completion later this year.

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   DAVID SADLER
Head of Internal Audit   Assistant Director and 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 David Sadler, Assistant Director and Head of ICT and Jen Duck, PwC.
Report presented by Max Thomas, Head of Internal Audit.

County Hall
Northallerton
16 September 2011

4

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

System/Area	Date of Audit	Areas Reviewed	Audit Opinion	Comments	Management Actions Agreed
ISO27001 readiness (Managed by ICT Services)	September 2010	ISO27001 is widely recognised as the de facto good practice information security standard. The audit included a review of control objectives, controls, processes and procedures within ICT's information security management system (ISMS) and assessed the extent to which there were appropriate plans in place to develop, implement, maintain, and continually improve the ISMS. This review was carried out as a readiness assessment to the external ISO27001 inspection from the British Standards Institute.	Moderate	ICT Services has taken a comprehensive approach to implementing information security within its own service and had implemented a management system which will support and maintain information security. Some recommendations were raised to optimise the Council's overall performance. Since the date of the audit, ICT Services has now achieved ISO27001 certification.	All recommendations were agreed by management, and actions developed to investigate and address the points raised. **Responsible Officer: Assistant Director and Head of ICT (F&CS)**
Intranet (Administered by Chief Executive's Group)	November 2010	The objective of this audit was to review the Council's processes for managing and developing the corporate Intranet.	Moderate	The Council has invested significant time and effort in developing the intranet for its employees. Management has considered further intranet development, accessibility, consultation with stakeholders, and technical support. However, areas for improvement were identified including resolving ownership issues in relation to the intranet code, patching intranet servers and improving user administration procedures.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised. **Responsible Officer: Head of Communications (CEG)**

5

System/Area	Date of Audit	Areas Reviewed	Audit Opinion	Comments	Management Actions Agreed
Remote working (Implemented and administered by ICT Services)	February 2011	The Council is implementing new remote working solutions, including a remote access VPN solution and remote access portal which will both be hosted by NYnet. The remote access VPN solution was in the process of being rolled out at the time of our work, and the objective of this audit was to review the implementation and security of this. The remote access portal is not due to be implemented until 2011/12 and was not included in the scope of our review.	Moderate	The new remote access solution is operating well. However, a number of issues were identified with the project management arrangements. Areas for improvement were identified in relation to: • migration and implementation arrangements; • user access administration and security; • monitoring of failed authentications; • clarification on the disaster recovery arrangements at NYnet; and • the need to develop procedural documentation.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised. **Responsible Officer: Assistant Director and Head of ICT (F&CS)**
IT Disaster Recovery (Managed by ICT Services)	March 2011	ICT Services has an ongoing project to improve Disaster Recovery (DR) of IT systems. This review focused on reviewing the current status of the project and the controls / processes which are being implemented. We also reviewed ICT's existing documentation and planning around DR arrangements. We have not provided an opinion or assurance rating as the project is ongoing. Also, IT DR will also be covered as part of the IT audit plan in 2011/12 as this project has not	None Required	The main findings included the following; • ICT is in the process of completing a business assessment to formally define , its critical activities and supporting IT services; • Although significant enhancements in Disaster Recovery facilities have been established through outsourced suppliers there is currently no formalised IT Disaster Recovery (ITDR) implementation programme in place; and formal recovery documentation has yet	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised. **Responsible Officer: Assistant Director and Head of ICT (F&CS)**

System/Area	Date of Audit	Areas Reviewed	Audit Opinion	Comments	Management Actions Agreed
		yet been completed.		to be produced; ICT has produced a roadmap for the development of ITDR and grouped the findings into short term / quick wins and medium to longer term categories.	
Lagan (Implemented and administered by Chief Executive's Group)	November 2010	The Council uses the Lagan CRM system in its Customer Service Centre and there are other business processes which are also built into the system, such as the HR Service Centre and Highways. The objective of the audit was to review the IT controls and processes supporting the system to ensure that data was processed on a complete, accurate and timely basis.	Limited	We identified a number of weaknesses in relation to the security of the system and access controls. These weaknesses potentially expose the Council to a risk of data loss. Additionally, we found areas in relation to change control procedures and governance arrangements where improvements could also be made. In a number of instances, the identified risks could be mitigated by the adoption of corporate IT standards.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised. **Responsible Officer:** **Head of Change and Improvement (CEG)**
Swift Financials (Implemented and administered by Health and Adult Services)	March 2011	The Council is in the process of implementing Swift Financials in the Adult and Community Services Directorate. The objective of this audit was to undertake a pre-implementation review of the Independent Sector Payment (ISP) module to confirm there were appropriate controls in place prior to 'go live'.	Limited	A number of issues were identified with the project implementation arrangements. In particular, we recommended that business processes should be fully documented and user administration procedures formally defined.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised. **Responsible Officer:** **ICT Client manager - HAS**

System/Area	Date of Audit	Areas Reviewed	Audit Opinion	Comments	Management Actions Agreed
Impulse (Implemented by Children and Young People's Services and administration recently transferred to ICT Services)	November 2010	The Council is in the process of implementing an integrated children's system, Impulse. The overall aim of the system is to move towards a single view of a child. A phased approach is being undertaken and modules are being introduced in accordance with an agreed programme. The objective of this audit is to review the Council's processes and controls for managing the implementation of the Impulse System and the ongoing administration.	Limited	The Council has invested significant time and effort in implementing and supporting the Impulse system and management has identified several areas where improvements to current processes could be made. These include the establishment of an Impulse operating schedule, the migration to a centralised fault recording system, and the use of an alternative to the schools data loader system. Other areas where there are opportunities for improvement include Disaster Recover (DR) testing, change management, establishment of SLA's and logical security arrangements.	All recommendations were agreed by management, and actions have been developed to investigate and address the points raised. **Responsible Officer: Assistant Director and Head of ICT (CYPS)**

3 YEAR STRATEGIC COMPUTER AUDIT PLAN 2011/14

Systems	2011/12 Days	Systems	2012/13 Days	Systems	2013/14 Days
Novell to Windows migration	10	Novell to Windows migration	10	Software licensing	5
IT contract management	10	IT asset management	10	IT project management	10
IT change programme	15	IT change programme	10	IT change programme	10
IT security	10	ISO27001 ISMS	10	Standards for managing IT systems	5
IT strategy	8	IT shared services	10	IT resource management	10
IT disaster recovery	7			IT continuous improvement	5
IT service desk and SAR	5			IT strategy	5
IT continuous improvement	5				
Follow up on prior year recommendations	7	Follow up on prior year recommendations	2	Follow up on prior year recommendations	2
Planning, management and attendance at TWIG and Audit Committees	3	Planning, management and attendance at TWIG and Audit Committees	3	Planning, management and attendance at TWIG and Audit Committees	3
Total	**80***	**Total**	**55**	**Total**	**55**

* 10 days were deferred from the 2010/11 internal audit plan.

9