Audit Detailed Report

February 2006

audit commission

Masterpiece IT Controls

District of Easington

Audit 2004-2005

External audit is an essential element in the process of accountability for public money and makes an important contribution to the stewardship of public resources and the corporate governance of public services.

Audit in the public sector is underpinned by three fundamental principles:

- auditors are appointed independently from the bodies being audited;
- the scope of auditors' work is extended to cover not only the audit of financial statements but also value for money and the conduct of public business; and
- auditors may report aspects of their work widely to the public and other key stakeholders.

The duties and powers of auditors appointed by the Audit Commission are set out in the Audit Commission Act 1998 and the Local Government Act 1999 and the Commission's statutory Code of Audit Practice. Under the Code of Audit Practice, appointed auditors are also required to comply with the current professional standards issued by the independent Auditing Practices Board.

Appointed auditors act quite separately from the Commission and in meeting their statutory responsibilities are required to exercise their professional judgement independently of both the Commission and the audited body.

Status of our reports to the Council

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to non-executive directors/members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any director/member or officer in their individual capacity; or
- any third party.

Copies of this report

If you require further copies of this report, or a copy in large print, in Braille, on tape, or in a language other than English, please call 0845 056 0566.

For further information on the work of the Commission please contact:
Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ
Tel: 020 7828 1212 Fax: 020 7976 6187 Textphone (minicom): 020 7630 0421
www.audit-commission.gov.uk

Contents

Summary report **4**

Introduction and background 4

Scope and objectives 4

Audit approach 5

Main conclusions 5

Detailed report **7**

Feeder update to and from Masterpiece 7

Data integrity 8

User access arrangements 8

User access security 9

Backup and disaster recovery 11

Appendix 1 – Action plan **13**

Summary report

Introduction and background

1 The main accounting system forms the basis for the Council's annual accounts which are reviewed to form our opinion. It is the most fundamental system the Audit Commission presently audits and we are required to undertake sufficient work to ensure compliance with the International Auditing Standards (ISA).

2 One of the objectives of management in respect of the main accounting system is to ensure that the application controls perform properly the business activity for which they are designed. The purpose of application controls is to ensure the completeness, accuracy, security and effectiveness of processing. Controls may be provided by either programming within the application system or by manual controls exercised by the users.

3 Easington District Council utilise the Masterpiece Financials application residing on the centralised AS400 platform. Most users of this application continue to use the 'green screen' access via the AS400. 'Green screen' access being the traditional method of viewing applications via such a platform.

Scope and objectives

4 The review was designed to address both the opinion and corporate governance elements of our code of practice responsibilities. The main areas included and how we completed this review were as follows.

- Document the flow of information into the main accounting system in order to identify the key IT controls.
- Review and assess the operation of IT controls that relate to the update of the main accounting system (ie interfaces from feeder systems).
- Review and assess the operation of IT controls that relate to ensuring the integrity of data within the main accounting system (ie input validation, error identification, review and resolution and control over master data).
- Review main accounting system user access controls.
- Review main accounting system disaster recovery controls.

5 This review focused primarily on systems and processes that applied to 2004/05 financial year and, therefore, reviewed and assessed a payroll interface that was being replaced due to the replacement of the AS400 based Prolog/Northgate application with a server based version of Northgate ResourceLink. However, we plan to review the new payroll system during 2005/06 and the new interface will be reviewed during this planned review.

Audit approach

6 The audit has been completed through a combination of interviews, document reviews, and testing financial system data using computer audit interrogation software. In addition, review of Internal Audit work on key systems was completed and their IDEA skills were utilised to test some more technical areas such as AS400 user security. We would like to thank Internal Audit for their input to our review.

7 In order to evaluate the integrity of the data managed on the application, we also used IDEA to test Creditors data from Masterpiece. The outcomes of this particular testing will be reported separately at a later date once discussed further with Council management.

Main conclusions

8 The IT environment supporting the Masterpiece Financials application is focused around the AS400 platform the Council continues to operate and support. Indications from ICT suggest that due to the priority of the e-government agenda at present, the likely migration from this to server based solutions in the future and the lack of resource within ICT for development on the platform, a number of weaknesses that are evident are unlikely to be resolved unless they are applied to replacement systems and infrastructures.

9 The interfaces developed between systems are generally reliant on manual intervention by end users and ICT to transfer data between source and destination systems, usually resulting in a journal by Financial Services onto Masterpiece. Comparisons with other district councils and larger unitary councils highlight a low level of interface automation at Easington (see paragraph 13 for detailed findings and conclusions). Although there was no evidence of unauthorised updates or amendments, the Council is reliant on manual controls to ensure the integrity of the interfaces. Manual intervention can increase the likelihood of errors and is generally a more inefficient use of systems.

10 Inherent issues with a lack of resources in ICT to address the security agenda and ongoing discussions between Internal Audit and personnel over more effective processes for starter and leaver administration are exacerbated by weak security on the network and the AS400. It is acknowledged that although the AS400 does provide some level of security comparable to best practice, some of the issues raised by our review are perhaps not beneficially implemented at this stage of the platform's life cycle. However, weaker controls applied to the network only contribute to weak overall arrangements for user access (see paragraphs 17 to 26 for detailed findings and conclusions).

11 The Council's Masterpiece application is supported by long-established and effective back-up arrangements and disaster recovery for the AS400 and some servers provided by a third party provider. However, the IT DR plan has not been updated for four years and the Council has recently replaced the AS400 based version of their payroll system with a server based version of Northgate ResourceLink. The IT DR plan should reflect current arrangements and also ensure a strategy for including new systems and associated platforms specified during system implementations (see paragraphs 27 to 29 for detailed findings and conclusions).

Detailed report

Feeder update to and from Masterpiece

12 All updates of the General Ledger, Accounts Payable and Accounts Receivable modules of Masterpiece can be categorised as either direct or in-direct feeders. Direct feeders generally relate to system to system interfaces and in-direct feeders tend to be either electronic or manual journals of data from one system updated to another. The Council has a number of key interfaces as follows.

- Payroll data processed by the Prolog/Northgate system is summarised and journalled into Masterpiece GL by Financial Services using assigned access privileges on the application.
- Housing benefit payments are made to citizens via cheque from the open revenues application and the total of cheques paid is journalled into Masterpiece GL by Financial Services.
- Income received via the four cash offices across the district is transferred to the AS400 based Cash Collection system, interfaced with the respective systems for particular funds (ie open revenues for council tax and NNDR, Orchard housing for rent) and journalled into Masterpiece GL by Financial Services.
- Creditor payments are made to suppliers via BACS from the Masterpiece AP module.

13 Many of the interfaces are dependent on manual intervention both on the part of the end users and the ICT department and most interfaces feed through the AS400 as this is the primary platform for the Council systems (eg Masterpiece, cash collection, open revenues etc) including:

- the payroll data from Prolog/Northgate is downloaded into a spreadsheet and ICT then transfer the spreadsheet into a journal file for Financial Services to review before upload to Masterpiece - no direct interface in place;
- Financial Services are responsible for the enveloping of the housing benefit cheques sent to citizens and as a result journal the file of cheques paid into Masterpiece - no direct interface in place; and
- Easington cash office is responsible for uploading cash income from this particular site and the other three cash office sites onto the AS400 based cash collection system. A control sheet is supplied to Financial Services and they are responsible for review, control and upload via journal to Masterpiece - no direct interface in place.

14 In comparison with other district councils, the interfaces are heavily reliant on manual intervention on the part of end users and ICT. There are indications that the AS400 is being 'run down' by the Council and is likely to be completely replaced within the next couple of years. This should provide the Council with the opportunity to automate/integrate system interfaces as and when systems are migrated from the AS400 to server based solutions. Most councils have developed a strategy or migration plan for the AS400 decommissioning that includes the development of more automated interfaces.

Recommendation	
R1	*The Council should ensure that a strategy for the decommissioning of the AS400 is developed and this is shared with end user AS400 users. As a result, the Council has the opportunity to develop more automated interfaces between systems with user input.*

Data integrity

15 The Masterpiece application is operated by the Council with centralised control over updates. Financial Services constitute the majority of the users and this way the Council closely manages the users with access to update or input to Masterpiece. No interface from a source system to Masterpiece is automatic and is reliant on review of the source system output before journal input to Masterpiece. Although the interfaces are generally manual, the process does afford some level of control over update and input to the main accounting system.

16 Internal Audit have completed regular reviews of accounts payable data as part of their standard creditors audits and this has included data interrogation using IDEA. Data integrity issues such as duplicate suppliers and incorrect VAT have been highlighted to management during such audits and action taken to remedy the issues highlighted. This again provides some level of assurance over the quality of data maintained on Masterpiece.

User access arrangements

17 In order to gain access to the Masterpiece application, a user requires:

- physical access to a council building;
- a network user id and logon (administered by ICT);
- an AS400 user id and logon (administered by ICT); and
- a Masterpiece user id and logon (administered by Financial Services).

18 User access arrangements (ie new starters and leavers) are broadly formal on each platform for new starters but recent Internal Audit coverage has identified a lack of formal notification of leavers between end user departments, ICT and personnel. Ongoing discussions between Internal Audit and personnel continue to resolve the areas of concern highlighted. However, best practice does suggest that formal arrangements should be established for new starters and leavers and therefore we support such improvements where feasible.

Recommendation
R2 The Council should establish or re-enforce a corporate process for user access management that encapsulates both corporate infrastructures/ systems (such as network, email, and intranet) and applications (such as Masterpiece). This should also include leaver administration.

User access security

19 A user requires a network user id and password logon to access the network before gaining access to the AS400 or Masterpiece. ICT administer access to the network and govern the security parameters assigned to the users of the network with:

- minimum password length - five characters - therefore, passwords are not required to be strong;
- minimum password age - 0 days - therefore, passwords do not expire;
- enforce password history - five passwords - the system remembers the last five passwords;
- password must meet complexity requirements - disabled - therefore, no strong passwords (supporting minimum password length observation); and
- account lockout threshold - five invalid logon attempts - users can guess five times before lockout - possibly set to five to ensure users can guess their passwords without excessively needing to contact Helpdesk for a password reset.

20 A user requires an AS400 user id and password logon to access the AS400 before gaining access to Masterpiece. ICT administer access to the AS400 and govern the security parameters assigned to the users (commonly known as the system values) with:

- all users requiring a user id and a password to log on;
- passwords expiring at 30 day intervals;
- passwords must be a minimum of six characters;
- the last 32 passwords being remembered by the AS400 when changing these; and
- controls over password strength (ie inclusion of numeric etc) not enforced and, therefore, passwords are not required to be strong.

21 Further detailed review of some of the AS400 users identified some shared user profiles including the following.

- Some users do share user profiles and this can on occasions provide problems when passwords have been reset by one user of the shared profile but not shared with other users.
- The password of the QSYSOPR profile with reasonably high privileges is known to a number of users within ICT.

22 There is a general opinion in ICT that the impact of the e-government agenda has resulted in a lack of resource to address every aspect of the security agenda and therefore a risk-based approach has been adopted given the fact that the AS400 is likely to be replaced within the next few years. Although issues have been raised with ICT in respect of the AS400, these are not assessed by ICT as benefiting from improvement at this stage as there could be an impact on productivity (ie password resets etc), the extra development work required (to redevelop interfaces that require high privileged user access) and the knowledge to date of few security issues on this platform.

23 However, although we acknowledge the Council's approach to the security of this platform, the general security governing users of the Masterpiece application is reduced by the weak controls applied to the network which contributes in part to the user access controls applied to users of the application. The network and associated controls will also support the server based applications that replace AS400 based systems such as Masterpiece, Prolog/Northgate, and cash collection etc.

24 When comparing the security on the network and the AS400, it is likely that the ICT department receive regular requests for password resets and it is usually a reason for reducing the strength of password controls such as password expiry, complexity, minimum length so that users can use easily guessable passwords that they do not forget.

Recommendations	
R3	*The Council should strengthen the security parameters on the network including ensuring users change their passwords every 30 to 60 days, are six characters as a minimum and are required to be reasonably complex.*
R4	*The Council should where possible align the security parameters on the network and AS400 to reduce the risk of excessive password resets and easily guessable passwords.*
R5	*The Council should ensure where practical, that all users are assigned to individually attributable user ids and logons to provide an effective audit trail.*

25 A user requires a user id and a password to gain access to Masterpiece once they have successfully logged onto the network and the AS400. User access security for Masterpiece is governed by the following rules:

- there is no automatic password expiry;
- passwords must be between one to eight characters;
- the system does not hold previous passwords; and
- there is unlimited number of attempts to guess the password.

26 Application user access security is assessed as weak, however, it is acknowledged that the majority of users only have 'enquiry' access except for Financial Services who have 'input'. However, the users with 'input' access are adequately segregated by assignment to one of a small number of 'profiles' which have pre-determined roles on the application. Security applied to the levels of the network and the AS400 are also relied upon.

Backup and disaster recovery

27 Arrangements for the backup of key systems are as follows.

- An automated daily backup at 2.00 am onto magnetic tape and is stored in a fire proof safe on-site. The daily Friday tape is taken off-site to a workshop and this is used to store the four Friday tapes as weekly backups. There are seven tapes for the daily backup. Four tapes are used for Monday to Thursday.
- Previous reviews by Internal Audit of the creditors system have reviewed the backup arrangements and concluded that satisfactory arrangements are enforced.

28 Arrangements for disaster recovery are as follows.

- A contract is in place with NDR for the AS400 on which Masterpiece resides - every now and again DR tests are completed and staff are brought on-site - there has not been a test for a couple of years.
- The IT DR Plan was last updated in 2001 - however, ICT indicate that although the plan requires an update this does not indicate that the cover is not in place for the AS400 and some other servers with NDR. Review of the plan indicated cover for both AS400 and some servers.

29 The Council appears to have appropriate backup arrangements established and although the IT DR plan has not been updated recently, DR arrangements are in place for the AS400 on which the Masterpiece application resides.

Recommendations	
R6	*The Council should update the IT DR plan to reflect the arrangements in place and where possible complete annual test restores.*
R7	*The Council should ensure that the requirement for DR is specified as an acceptance criteria for any new system that is migrated from the AS400 to a server solution. This is particularly important during a period where payroll has recently migrated and others are likely to 'follow suit'.*

Appendix 1 – Action plan

Page no.	**Recommendations**	**Priority** **1 = Low** **2 = Med** **3 = High**	**Responsibility**	**Agreed**	**Comments**	**Date**
8	R1 The Council should ensure that a strategy for the decommissioning of the AS400 is developed and this is shared with end user AS400 users. As a result, the Council has the opportunity to develop more automated interfaces between systems with user input.	3	Head of ICT and E-Government	Yes	AS400 de-commissioning strategy needs to be developed. Authority not keen to automate interfaces although this would be possible. The belief is that the current process provides more effective control over data quality.	May 2006

Page no.	**Recommendations**	**Priority** **1 = Low** **2 = Med** **3 = High**	**Responsibility**	**Agreed**	**Comments**	**Date**
9	R2 The Council should establish or re-enforce a corporate process for user access management that encapsulates both corporate infrastructures/ systems and applications. This should also include leaver administration.	2	Head of ICT and E-Government	Yes	This is predominantly an issue for the leaver process and discussions continue to resolve this.	Ongoing.
11	R3 The Council should strengthen the security parameters on the network including ensuring users change their passwords every 30 to 60 days, are six characters as a minimum and are required to be reasonably complex.	3	Head of ICT and E-Government	Yes	Although it is agreed that the recommendation is essentially the adoption of good practice, this will come with a reduction in officer productivity. It is essential that any proposals in relation to the required improvement are discussed at senior management level and that the implications of implementing the recommendation are fully highlighted and considered.	December 2006

Page no.	**Recommendations**	**Priority** **1 = Low** **2 = Med** **3 = High**	**Responsibility**	**Agreed**	**Comments**	**Date**
11	R4 The Council should where possible align the security parameters on the network and AS400 to reduce the risk of excessive password resets and easily guessable passwords.	3	Head of ICT and E-Government	Yes	As for R3.	December 2006
11	R5 The Council should ensure where practical, that all users are assigned to individually attributable user ids and logons to provide an effective audit trail.	3	Head of ICT and E-Government	Yes	The differing examples of generic user accounts needs to be investigated and discussed further but attributable user accounts will be implemented wherever practical.	August 2006

Page no.	Recommendations	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
12	R6 The Council should update the IT DR plan to reflect the arrangements in place and where possible complete annual (as a minimum) test restores.	3	Head of ICT and E-Government	Yes	It is agreed that such arrangements are enforced on an annual basis.	December 2006
12	R7 The Council should ensure that the requirement for DR is specified as an acceptance criteria for any new system that is migrated from the AS400 to a server solution. This is particularly important during a period where payroll has recently migrated and others are likely to 'follow suit'.	3	Head of ICT and E-Government	Yes	Agreed as recommended.	Ongoing.