Internal Audit Report
2010-2011

Records Management & Data Quality

Ann Kirk
Assistant Auditor
30th June 2011

INVESTOR IN PEOPLE

Contents

Audit: Records Management & Data Quality
Auditor: Ann Kirk

If viewing on-screen, please click on the links below or use the scrolling arrows

1 Introduction

1.1 In order for the Council to carry out their responsibilities it is necessary that data and information be collected from members of the public and various other sources.

1.2 Records Management is the practice of maintaining the records of an organisation from the time they are created up to their eventual disposal. This may include classifying, storing, securing and destruction or in some cases archival preservation of records.

1.3 Data makes up records of information and is an asset to the organisation, but only if it is accurate and fit for purpose. Organisations risk adverse publicity or loss of revenue if the data is inaccurate and poor decisions are made as a consequence.

2 Scope

2.1 The audit focused on the high level procedures in place for a sample of five systems used by the Council, including the process for collecting information and data, securing of data, how the Council uses this data and how we manage it ensuring destruction in accordance with the Council's Retention Policy.

2.2 As a result this audit looked at the following areas: -

- Project Control
- Adverse Publicity
- Data Protection Act Compliance

3 Findings

3.1 Each of the five systems, Lagan, Oracle, Northgate, Trent and Uniform all rely on accurate information to be processed onto them. Internal Audit was informed that each Service undertakes training with new employees usually on a one-to-one basis and there are procedures available for each system to ensure uniformity in entering data. The unique sign-on ensures that any errors can be identified back to the processor and additional training provided if necessary.

3.2 All Services have targets for entering data onto the system. These targets ensure that data is not delayed and the information is available to the reader when required. All but one Service reviewed had achieved their target, which was due to lack of staff and sickness.

3.3 Information processed onto the systems is not duplicated. To ensure all data is correct at entry all Services undertook a verification process. This could be by an exception report, for example on duplicate entries or missing data or a system control such as drop down menus. Internal Audit tested a sample of entries onto each system and found them to be accurate.

3.4 There are two types of updates, an upgrade and a patch. An upgrade is where the software has been improved and a patch corrects a fault or updates the data infrastructure. The installation of these updates is the responsibility of the relevant individual working within the Information and Communication Technology (ICT) Applications Team or the Software Provider.

3.5 As part of the Code of Connectivity all changes to the Council's operational systems are to be formally documented. Testing found that this was occurring currently on paper. The IT Applications Manager is looking at ways in the future to record this electronically.

3.6 On receipt of an upgrade or patch they are uploaded into the test environment, this enables all aspects of the system to be tested before going live reducing the possibility of loss or manipulation of data already recorded. To be effective it is best practice to ensure that the test environment mirrors the live environment as much as possible. Internal Audit were informed that the test environment mirrors the live environment for any significant upgrades or patches.

3.7 Internal Audit were informed that the Service using the system undertakes testing of upgrades and patches and that release notes provided by the Software Company are used to ensure the correct areas are tested. Once testing is complete the Service informs the ICT Applications Team.

3.8 Internal Audit reviewed the complaints from members of the public with regards to the information supplied to them and found that there had been no complaints made against the Council in this matter.

3.9 All paper based data entered onto the system is stored within the Service for the required time before being taken down to the depot for storage. There is controlled access to each Service so no members of the public can access the department without the correct identity badge. All electronic data is backed up daily and on a weekly basis stored off site

3.10 The Council's Retention Policy states the timescale that hardcopy data is to be kept; this is sometimes predetermined by legislation. The audit found that not all services were complying with the policy. It is recommended that all Service's ensure that they comply with the Council's retention policy and destroy any data outside of the designated timescales.

3.11 The Council's Retention Policy is also used for electronic information, and therefore all data held on the Council's computer systems should also be destroyed in accordance with the policy. Internal Audit found that this was not the case and recommends that staff investigate archiving on the software systems used by their Services and ensure all data held on removable media devices such as memory sticks are deleted when they are no longer required.

3.12 All hardcopy data destroyed is done so using an industrial shredder.

4 Conclusion

4.1 Internal Audit is satisfied with the way that information is entered onto the systems tested. However there are areas of improvement that have been outlined below in the recommendation.

5 Action Plan

Recommendation		Officer	Priority	Agreed?	Comments	Implementation Date
3.11 & 3.12	That a reminder is sent to all Services to destroy all data as per the Council's Retention Policy. In addition to investigating archiving data held on software systems.	Jane Dodsworth	Medium	Yes		August 2011

High = Fundamental System Weakness – Action is Essential

Medium = Potential Control Weakness – Action Required

Low = Advised for Best Practice