Perth & Kinross Council

Review of Data Management

AUDIT SCOTLAND

Prepared for Perth & Kinross Council
August 2013

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. It provides services to the Auditor General for Scotland and the Accounts Commission. Together they ensure that the Scottish Government and public sector bodies in Scotland are held to account for the proper, efficient and effective use of public funds.

Contents

Key messages

Introduction and audit approach

1. As part of our planned work for this year, we carried out a review of Data Management. Data management impacts on all functions within an organisation where effective service delivery is based on accurate information. Among the most important aspects of such practices are the existence of information asset registers, risk management procedures and defined data sharing arrangements. The objective of the review was to examine data management procedures and processes within the Council and assess where good practice exists or whether the council is subject to risk.

2. Our review covered the following areas:
   - **Information asset register** – the Council knows what information it holds and how sensitive and critical this information is.
   - **Risk management** – the risks relating to the information held are known and are related to the criticality of the information. Risk management is embedded in the overall management process.
   - **Sharing data** – where data is shared between systems or with third parties, this is done lawfully and with appropriate safeguards in place.
   - **Information awareness** – staff, including information owners and those charged with the day to day management of the information, are clear about their roles and responsibilities in safeguarding the Council's information.
   - **Data protection** – data protection requirements such as preparing information sharing protocols for sharing information with third parties and carrying out privacy impact assessments when use of information changes significantly are taken into account.

3. The findings of the review are set out below and an action plan detailing the risks identified during the review and the actions agreed with management to mitigate the risks can be found in the Appendix.

Key findings

4. Information management, data protection and information security responsibilities are delegated to a team within Legal Services. The team has started setting up the information asset register, has developed a survey assessing the information security awareness of staff and assists staff and managers in dealing with information security issues.

5. There are a number of areas, however, where additional work is required for the Council to increase its awareness about the information it owns and the risks it is exposed to:
   - The information asset register is in a preliminary stage, and further data about information assets should be considered to help assess and mitigate the risks associated with the assets.

- The system risk assessments that are periodically carried out have not fed into an overall corporate assessment of the risks relating to information assets.
- Data sharing agreements are not subject to regular periodic review to identify any changes required.
- Training for staff on information security and data protection available on the Council's intranet has only been taken up by around 30% of staff.
- Privacy impact assessments are not always carried out when significant changes are made to systems.

Risk exposure and planned management action

6. This report summarises the findings from our review and identifies the areas where the council may be exposed to significant risk. Although this report identifies certain risk areas, it is the responsibility of management to decide the extent of the internal control system appropriate to the Council. We would stress, however, that an effective control system is an essential part of the efficient management of any organisation. The risk areas highlighted in this report are only those that have come to our attention during our normal audit work in accordance with our Code of Audit Practice and therefore are not necessarily all of the risk areas that may exist.

7. Risk exists in all organisations which are committed to continuous improvement and, inevitably, will be higher in those undergoing significant change. The objective is to be risk aware with sound processes of risk management, rather than risk averse. Indeed, organisations that seek to avoid risk entirely are unlikely to achieve best value. Risk can be either inherent (because of the environment an organisation operates in or the nature of the operation) or due to the absence of effective controls. Risks take a number of forms including financial, reputational, environmental or physical risks.

8. The action plan included as an appendix to this report details the areas where continued risk exposure requires management action.

9. We have discussed a number of less significant audit points with management. These were lower risk issues and management have agreed to consider taking action on them. These have been excluded from this report so that management can focus on the significant and higher risk points.

Conclusion

10. Our overall conclusion is that the Council's data management processes are off to a good start. However, more work is required and officers have advised that, with competing priorities and ongoing savings requirements, ensuring that safeguarding information is adequately resourced is challenging.

Acknowledgements

11. The contents of this report have been discussed with senior officers within the Legal Service to confirm factual accuracy. The assistance and co-operation we received during the course of our audit is gratefully acknowledged.

Main findings

Introduction

12. Data management impacts on all functions within an organisation where effective service delivery is based on accurate information. Among the most important aspects of such practices are the existence of information asset registers, risk management procedures and defined data sharing arrangements. The objective of this review was to examine data management procedures and processes within the Council and assess where good practice exists or whether the Council is subject to risk.

13. Information management, data protection and information security responsibilities are delegated to a section within Legal Services. The section deals with queries from all services. Information sharing protocols have been put in place for those instances where information is shared with organisations outside the Council. Recently, a staff survey has been developed which assesses staff awareness about various information security related topics. This survey has been used in one service area and will over time be rolled out to all Council departments. The results from the surveys will provide useful focal points for improving information management and security.

Information asset register

14. The information asset register is a tool for the organisation to identify information assets and record each asset's responsible owner. The information asset register can also be used to collect additional information about the information assets that would help the organisation establish whether they are critical for its continued operations. This, in turn, would inform the implementation of security controls for the asset.

15. The Information Compliance Section has started gathering information on all the systems used by the Council. This register is still in a preliminary stage, recording the name of the system, its owner and custodian. The Council needs to consider what other information is necessary to assess the risks inherent to the system or information repository and which additional controls should be put in place to mitigate these risks. Some additional information which would be useful is: whether the system holds any personal and/or sensitive information, whether third parties have access to the system and if, and by which means, the system exchanges data with other systems.

Risk area 1

Risk management

16. An organisation's risk management methodology is a systematic process to highlight, mitigate and manage the risks the organisation may be exposed to. With regard to information assets, the risks depend on the sensitivity of the information, both in terms of criticality and personal content, and the solutions that can be put in place to protect the information.

17. System owners are required periodically to provide a self-assessment against the ISO27000 (Information Security Management) standard. A corporate assessment would establish where information security controls are lacking and which, if any, mitigating controls are required. In addition, the risk assessment is not routinely prepared for new systems, or systems which undergo a significant change (for example, change from access through council network only to remote or on-line access).

Risk area 2

Sharing data

18. Sharing data of a personal or sensitive personal nature as defined by the Data Protection Act can only be done for legitimate reasons. Data sharing agreements are put in place when data is exchanged with external parties such as other local authorities, the health service, or central government.

19. We found that existing data sharing agreements are not reviewed as a matter of course to ensure that circumstances have not changed that would affect the agreement. This is not in line with good practice.

Risk area 3

Information awareness

20. Staff routinely dealing with information (in a local authority this can be nearly all staff) should be aware of the sensitivity of this information. Additional protective measures may be required to ensure that information is not lost or inadvertently made public.

21. Training packages on data protection, freedom of information and data security are available on the Council's intranet as eLearning modules. The training available is not used frequently. Of the total number of individuals employed (approximately 5,700) only 1,350 staff have successfully completed information security and 1,490 data protection training since the eLearning modules became available. As a result awareness of information and data security issues may not reach the staff it is intended for.

Risk area 4

Data protection

22. An organisation should have processes in place to ensure that personal and sensitive personal data are processed in line with the requirements of the Data Protection Act. Introduction of new processes or systems that involve information covered by the Act should be assessed for the impact of the Act and any additional security controls that may be required to be put in place to meet the obligations.

23. A privacy impact assessment (PIA) helps to assess and identify any privacy concerns and address them at an early stage, rather than privacy protection solutions having to be added retrospectively after a system has been developed. Typically a PIA is required when the use

of a system or process changes considerably, which could be the level of detail of information collected or the means by which data is collected.

24. The Council's internal guidance for the use of PIAs allows an abbreviated assessment to take place where the privacy impact is deemed minimal. During our review we found that this approach was applied, for example, where a change of paper to on-line collection of potentially sensitive information was implemented. The means of collecting personal and sensitive information electronically, however, can bring additional exposure which requires a more detailed PIA.

Risk area 5

Appendix

Risk identification and action plan

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
1	15	The Information Compliance Section has started gathering information on all the systems used by the Council. This register is still in a preliminary stage, recording the name of the system, its owner and custodian. The Council needs to consider what other information is necessary to assess the risks inherent to the system or information repository and which additional controls should be put in place to mitigate these risks. ***Risk: the Council may not be fully aware of the volume of information it holds and how critical this is to its operations. Therefore the controls required to mitigate the risks associated with the information may not be comprehensive.***	The Asset Register will be extended to include additional relevant information.	D Henderson	October 2014

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
2	17	A corporate risk assessment of the Council's information resources is not carried out. In addition risks associated with new information sources are not assessed as a matter of course. ***Risk: the Council is not aware of all the risks relating to the sensitive and business critical information it holds.***	Consideration will be given to undertaking a corporate risk assessment. Asset Owners will be encouraged to comply with the existing Information Security standards and to ensure that a systematic risk assessment is made of all new information sources.	D Henderson D Henderson	March 2014 October 2013
3	19	Data sharing agreements are not reviewed periodically. ***Risk: the data sharing agreements does not reflect the current data sharing procedures.***	A register of data sharing agreements is already planned to be published including the responsible office and the review date. Responsible officers will be given reminders of the need to review agreements.	D Henderson	March 2015
4	21	Training available to staff on information security and data protection is not taken up in the numbers expected and does not appear to be refreshed periodically. ***Risk: staff are not aware of information security and data protection requirements.***	It is already planned to implement revised e-Learning modules for Information Security and Data Protection. These will be refreshed periodically thereafter.	D Henderson	March 2014

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
5	23	Full Privacy Impact Assessments are not always carried out. ***Risk: the existing PIA guidance is not fit for purpose.***	It is already planned to embed privacy Impact Assessments in the committee report process.	D Henderson	March 2014