Perth & Kinross Council

Computer Services Review

AUDIT SCOTLAND

Prepared for Perth & Kinross Council
August 2012

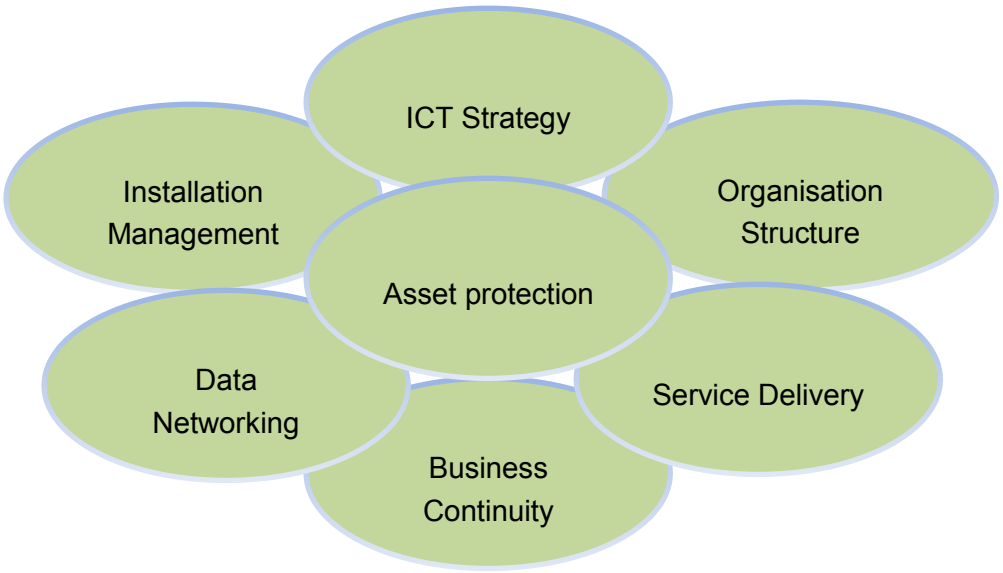
Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. It provides services to the Auditor General for Scotland and the Accounts Commission. Together they ensure that the Scottish Government and public sector bodies in Scotland are held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

Contents

Key messages

Introduction and audit approach

1. As part of our 2011/12 annual audit plan we highlighted that as ICT services at Perth & Kinross Council (the council) were being reviewed that we would undertake a computer services review (CSR) based on an established methodology providing a high-level risk based assessment of ICT services in seven key areas as outlined below.



2. This aspect of our 2011/12 plan was carried out using a CSR Client Questionnaire (CQ) which was completed by ICT management. We also received supporting documentation, as appropriate and held meetings with the relevant IT managers to discuss and clarify any points contained within the CSR CQ.

Key findings

3. The IT Service which is part of Education and Children's Services (ECS) provides information and communication technology services to the council.

4. A number of areas of good practice were identified, including the following:

- The council has an IT strategy which provides the framework for IT investment. Work is underway to assess the implications of the McClelland review on ICT services in the public sector for the strategy.
- The council has a well developed business continuity management framework consisting of corporate and local plans, and includes an IT disaster recovery plan.

- The IT Service has prepared partnership agreements with the user departments to clarify the services it provides and the expectations against which those services will be delivered.

5. At the same time there are a number of challenges facing the council:
   - Information security is an area of continuing challenges and competing demands. One of the key challenges is in raising staff awareness about good information handling practices. Others relate to monitoring of information security standards and gaining knowledge about information resources that are critical to the council in executing its functions.
   - Within the user departments there are staff who support IT systems. The roles and responsibilities of these officers, and where there are possible gaps or overlaps with the responsibilities of the IT Service staff, need to be clarified.
   - Carpenter House computer rooms are not presently fit for purpose. The refurbishment of the building would be an opportunity to address the deficiencies noted.

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 IT Service is generally well run and provides generally good services to the user departments. The recent service restructure has, however, resulted in some uncertainty for staff and it may take some time for the new structure to bed in and any difficulties arising to be resolved. In addition, budget cuts may impact the ability of the service to keep up to date with technological innovations.

Acknowledgements

11. The contents of this report have been discussed with senior officers within the IT 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. Information and communication technology is at the heart of many of the services the council provides. Although there are still paper files and archives in place, much of the information that council staff require to do their job is stored in computer systems. The purpose of this review was to provide a high level overview of the way these computer systems are managed and the information stored in them is protected.

ICT strategy

13. An organisation should have an ICT strategy endorsed by senior management to enable it to plan formally for the introduction of information systems that meet corporate business objectives.

14. The council's ICT strategy was prepared in 2011 and approved at the Policy and Resources Committee on 15 June 2011. This was just before the publication of the McClelland *Review of ICT Infrastructure in the Public Sector in Scotland* and the full implications of this review for the council had not been assessed as part of the 2011 strategy. Work has been done since to assess the impact of the McClelland recommendations for the council and as a result the strategy will be reviewed during 2012 to include the outcomes.

15. The council's officer led Corporate Resource Group (CRG) has a remit that includes considering both strategic and operational IT issues and acts as the key stakeholder forum for the Corporate IT Manager. The CRG oversees the integration of IT strategic planning with finance, asset and workforce planning and recently agreed a reporting framework to ensure it received regular reports on progress towards delivery of the strategy.

Organisation structure

16. There should be an organisational structure that ensures sufficient staffing resources are in place to meet departmental and local information needs. The structure should clearly highlight who is delegated the authority for the provision of services and also set out defined roles and responsibilities for the delivery of services.

17. The council has merged corporate and education IT services into one department within Education & Children's Services (ECS). The Head of IT retired in June 2011 and at that stage the three managers in the IT Service reported to the Head of Corporate Business Change and Information Technology (IT) within ECS. In the Spring of 2012, a Corporate IT Manager was appointed and a restructure of the IT Service was completed in June 2012.

18. As a result of the service restructuring exercise, the responsibilities of staff within the IT Service have been reviewed, clarified and reallocated as appropriate. As a result of the restructuring it has been recognised that there are staff within other council services who also carry out a role in supporting local IT systems. The way responsibilities are split between the

IT Service and departmental system support staff can differ depending on the type of system and competences required. However, any IT support should follow good practice. A consistent approach to managing systems (for example, dealing with upgrades and changes, user management, suppliers and projects) across all application platforms should improve the management of complex systems. A first step would be to clarify where departmental responsibilities end and IT Service responsibilities take over, in addition to implementing consistent procedures.

Risk area 1

19. The IT Service has adopted the ITIL (Information Technology Infrastructure Library) service management framework which promotes a best practice approach to IT service management and aligns with business objectives. One of the pillars of this approach is the implementation of good change management practices. Change management can mean different things to different people, so a consistent approach which is documented and applies to all staff who work with IT systems is important. Changes in the IT environment can range from system upgrades, both small and large, to setting up users, replacing hardware and acquiring new systems.

20. The IT Service developed its change management procedures in 2011 and has since been working to implement and embed the procedures in their daily working practices. We will keep this area under review going forward.

21. One of the other key elements of ITIL best practice is the requirement to document procedures so they can be applied consistently across all IT platforms (application systems and hardware). At present the IT Service's documented procedures are not fully complete. Procedures for managing user access to information resources - including remote access by staff and access by suppliers - are currently being developed. Back-up and recovery procedures mainly consist of a sequence of tasks on the Net Backup system which manages the back-up process. Further procedure documents were not available at the time of the review.

22. Documenting processes and procedures are not only relevant for the implementation of ITIL but also form a baseline of activities that need to be carried out competently in the event of the usual staff being absent. Identifying such processes and documenting them would help improve the effectiveness and efficiency of the IT Service and help meet resource pressures.

Risk area 2

Installation management

23. Installation management should ensure that there are acceptable levels of environmental, physical and logical access controls over system operators, software and data at both central and remote sites.

24. The council's IT server hardware is distributed over three locations, which are connected in a triangular grid. Communications hardware which allows remote offices to connect to the corporate systems is located in Carpenter House and 2 High Street. Two storage area

networks which store most of the council's Windows based systems and information are located in 2 High Street and Pullar House, while the Unix systems which hold the information for major transactional systems such as Swift (Social Work) and Northgate (Housing and Revenues & Benefits) are located in Carpenter House.

25. We found that, at present, Carpenter House does not have the benefit of a generator or other alternative power source so if there is a black or brown-out affecting the building, some of the council's major systems will not be available to staff. Carpenter House is due to be refurbished and this would be an ideal opportunity to address this and improve the building as a location for holding communications and server hardware

Risk area 3

Service delivery

26. Efficient and effective delivery of ICT services is fundamental to supporting the delivery of the Council's frontline services. Arrangements should, therefore, be in place to ensure that levels of ICT service provided are to a satisfactory standard.

27. The IT Service has, in conjunction with the other council services, developed partnership agreements. There is one Generic Partnership Agreement which covers most of the generic IT services such as back-up, remote access, warranties, standard hardware (printers) and so on. These are supplemented with service specific agreements to meet the needs of individual services.

28. Service performance is captured in a set of Key Performance Indicators, both in monthly team reports and ECS service indicators. Performance is published on the council's intranet where this information is available for all staff. The partnership agreements are reviewed twice a year.

Asset protection

29. Asset protection in relation to information management and information technology concerns the availability, confidentiality and integrity of:

- hardware assets - the servers, desktop and cabling infrastructure that stores and transports information
- software assets - the applications that enable staff to carry out their work, typically subject to licence agreements
- information assets - collections of data and information stored in application systems, databases, electronic and paper documents.

30. The council has an Information Security Policy Statement in place to ensure the confidentiality, integrity and availability of all the council's information assets and to ensure that they are appropriately protected from all threats, whether internal or external, deliberate or accidental. Further details, which follow the Information Security Management standards (ISO27000 series), are available for all staff on the council's intranet.

31. Monitoring adherence to these standards can be challenging. Each year, a benchmarking exercise is carried out to assess the capability and maturity of the services against the published standards. During our review, we highlighted additional monitoring and supervisory checks that could be implemented to assess compliance within the technical environment and officers have agreed to consider taking these forward.

32. The council does not currently have comprehensive knowledge of all its software and information assets. While the big application systems are well known, it is the more limited software deployments and unstructured information assets which are proving more difficult to categorise. As a result the council may not be aware of all its business critical information resources and therefore may not take the most appropriate measures to protect them against deliberate or accidental loss.

Risk area 4

33. At present, there is no structured approach to increase staff awareness of good information security practices. Good information security practices should be part of the normal working practices, for example, clear screen and clear desk policies should be reinforced as well as good password practices. Guidance on dealing with information - especially when this information is copied or removed from its normal storage space - should be an integral part of team and management meeting discussions when information transfer and processing is discussed.

34. Data loss incidents in Scotland over the last few years have been shown to generate a lot of negative press coverage. Aside from the reputational damage this may cause, the powers of the Information Commissioner's Office which investigates Data Protection breaches have increased and this can result in significant fines of up to £500,000.

Risk area 5

35. Audit Scotland's Your Business @ Risk survey (a free, anonymous survey tool available to all Audit Scotland clients) could also be used to gauge information security awareness and, where appropriate, devise an action plan to address any specific areas where awareness is lacking or current practices do not meet best practice.

Business continuity

36. Organisations that are reliant on ICT services require formal procedures for assessing risk to these services. Risk assessment should be used as the basis for the continuity planning of business critical systems, for operational documentation and for test scenarios to address disaster recovery planning.

37. The council finalised its current Corporate Business Continuity Management - Incident Management Plan in July 2011. The plan covers how business continuity will be invoked, how responsibilities will be allocated and communication will be organised in the event of an incident. The IT Service has prepared an ICT Disaster Recovery Plan listing the business critical systems that are prioritised for recovery in the event of any incident.

38. The council does not use tape back-ups partly due to the cost of and the difficulties in acquiring off-site storage for tapes. The back-up system in place for council systems mirrors information across two storage sites. As these two sites are within a mile of one another in the centre of Perth, there is the possibility that a major incident would affect both sites. Within a changing technology environment, it would be prudent to revisit this back-up approach periodically to ensure it remains fit for purpose.

39. Testing scenarios have been played out to test the feasibility of parts of the business continuity plans. In addition, where the IT Service has also suffered its own unexpected incidents (power outage, gas leak), there have been "live" tests of the plan. However, from the evidence provided it would appear that testing of council-wide plans was mostly carried out in 2010. It would be advisable to revisit tests periodically, especially after service restructures have taken place and people have either left the council or have been assigned different roles.

40. The council's Business Continuity Strategy Group is responsible for developing, leading and monitoring the business continuity management programme across all Council Services. As of July 2012, a new Chair of the Business Continuity Strategy Group was appointed and this would be a good opportunity to revisit the framework in place.

41. At the moment, the IT Service does not yet have system specific recovery plans in place. Such plans might include, but are not limited to, hardware requirements and where these can be obtained, location of database and application software, details of tasks required to rebuild a server and communication with users.

Risk area 6

Data networking

42. To accord with good practice, an organisation should have a network strategy that enables it to plan for the delivery of facilities to meet local and wide area service requirements. It should also set the standards required to control and secure the network in respect of reliability, resilience and the ability to recover from disaster. Business-as-usual data networking developments are included in the overall IT strategy; for new data networking technologies a separate strategy is developed and submitted for approval.

43. At present, the council does not deploy wireless access outside of school campuses. We were advised that there has been a lot of pressure on the IT Service to enable such access at various locations. A strategy for implementing a wireless network which can be accessed securely by council staff as well as guests has recently been prepared. The strategy will be submitted for approval to the Corporate Resources Group later this year.

Appendix

Risk identification and action plan

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
1	18	Most IT services are provided by IT Service staff; however, some system management tasks are carried out by user departments' staff. ***Risk: there may not be a consistent approach to manage systems across all application systems and platforms.***	A review of IT staffing in Services was approved by the Executive Officer Team in January 2012 as part of the Review of IT Services.	Corporate IT Manager (Ken Wilson)	April 2013
2	22	Not all processes and procedures within the IT Service are fully documented. ***Risk: tasks may not be carried out or may be carried out ineffectively, particularly where new or temporary staff are involved.***	Fully document all key processes and procedures.	IT Service Manager (Dave Adams)	June 2013
3	25	Carpenter House's computer room does not benefit from alternative power sources for the critical systems housed in its server rooms. ***Risk: systems located in the server room may be negatively affected by unexpected power outage.***	Increased protection for the IT Information processing facilities will be included as a key element of the refurbishment of Carpenter House in 2013/14.	IT Service Manager (Lynne Harris)	June 2014

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
4	32	At the moment, the council does not have a comprehensive record of all of its software and information assets. ***Risk: the council may not be aware of all its critical information sources or take the appropriate measures to protect them.***	Develop and implement a system and processes for the recording and management of software and information assets.	IT Team Leader - Customer & Business Services (Susan Cannon)	June 2013
5	34	Raising information security awareness is not currently an integral part of council activity at all levels. ***Risk: there are risks of both reputation loss and monetary fines when good information management practices are not being promoted and adhered to.***	Increasing security awareness is part of our 3 year strategy. Once this has been approved, a more detailed action plan will be developed.	Information Compliance Manager (Donald Henderson)	September 2012 (approval of strategy)
6	41	Individual system recovery plans have not been prepared. ***Risk: in the event of an outage of a major system, the service may not be recovered within satisfactory timescales.***	System recovery plans will be developed for all business critical systems.	IT Team Leader - Server Infrastructure (Cammie Watson)	April 2013