Falkirk Council

ICT service review

2012/13

AUDIT SCOTLAND

Prepared for Falkirk Council
August 2013

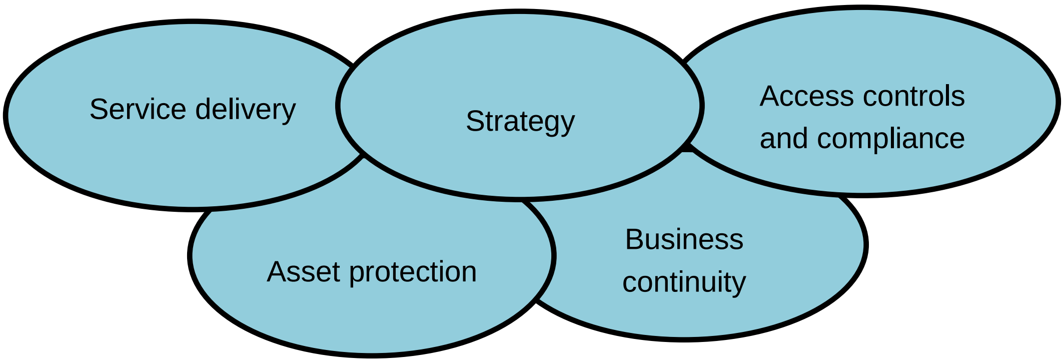
Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively.

Contents

Summary

Introduction and audit approach

1. As part of our risked based assessment carried out during the initial planning stage of Falkirk Council audit, we identified Information and Communication Technology (ICT) as a priority area for review in 2012/13. The audit work was based on an established computer services review methodology developed by Audit Scotland. It provides a high-level risk based assessment of ICT services in five key areas as outlined below.



2. Our audit was carried out using a Computer Services Review (CSR) Client Questionnaire (CQ). The questionnaire was completed in consultation with ICT management who also provided supporting documentation as evidence. In addition, a number of the ICT service functions were previously tested by us to confirm their operational effectiveness.

Key findings

3. The council's ICT section deals with the management of ICT resources, requests for services and business continuity, as well as managing ICT projects and information security.

4. A number of good practices were identified and include the following:
   - effective work practices are in place to manage the council's ICT infrastructure and data centres
   - a service desk process is in place to ensure effective control over support calls
   - sound practices are in place for managing user access to council controlled systems
   - business continuity arrangements have been developed for the back-up and recovery of data although they remain under review
   - effective arrangements are in place for managing the council's ICT hardware and software assets
   - the public sector standard project management methodology (Prince2) is used to control ICT projects.

5. At the same time there are a number of challenges facing the council:

- Investment in ICT provision has to be balanced between priority areas and increasing user and government demands.
- The ICT service is part of a programme of continuous service improvement within the council and is being progressed through service and skill re-alignment.
- Continuous changes in the ICT environment and the sharing of data through collaborative partnerships places new demands on information security policy and arrangements.
- The maintenance of business continuity / disaster recovery arrangements is part of an on-going process which involves completing formal business impact analysis worksheets for all systems.
- The Scottish Government are looking for councils to help develop and deliver plans for superfast broadband as part of the shared services agenda.

Risk exposure and planned management action

6. This report summarises the findings from our review and identifies 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. Also, it should be noted that risk areas highlighted in this report are only those that have come to our attention during our normal audit work 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, is 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 or due to the absence of effective controls. Risks take a number of forms including financial, reputational, environmental or physical.

8. The action plan included as Appendix A of this report details the areas where we have identified exposure to risk and which require management action.

Conclusion

9. Our overall conclusion is that the controls surrounding the management of the ICT service within the council are sound. There are, however, challenges in terms of costs as investment is targeted to the priority needs of the council, and the Scottish Government, while trying to deliver improvements in overall service delivery.

Acknowledgements

10. The contents of this report have to be agreed with senior officers within the ICT service to confirm factual accuracy. The assistance and co-operation we received during the course of our audit is gratefully acknowledged.

Main Findings

Introduction

11. There is an increasing reliance upon ICT initiatives to provide improved service to the public at both a national and local level. In addition organisations such as local authorities must continuously strive to achieve value for money from their ICT investment while ensuring the promised benefits from the technology are fully realised.

12. Falkirk Council has a strategically driven approach to provide the services it needs. The council also recognises that the Scottish Government in conjunction with the Improvement Service has a programme of services designed to encourage online access to council and other public services. Management advised us that it will adopt on-line access to services where it considers it appropriate to meet local and service demand.

13. Moreover, management are responsible for ensuring that sound operational controls are in place covering such matters as information security, hardware and software management, and disaster recovery and business continuity processes.

Strategy

14. The council has a strategic ICT vision to meet the needs of local service delivery and the requirements of the Scottish Government in its wider demands for efficiency in the use of technology. The ability of the council to deal with changing information needs and technological innovation to improve service delivery is of key importance to stakeholders.

15. The council's vision for the use of ICT in service provision and improvement should be taking cognisance of national strategies such as the Local Government ICT Strategy, issued in January 2013, and Scotland’s Digital Future: Delivery of Public Services which includes the Scottish Wide Area Network programme (SWAN). SWAN is the first major action launched by Scottish Ministers to achieve the goals set out in Scotland’s Digital Future: Delivery of Public Services. The SWAN programme aims to deliver a single, public services network available for the use of any, and potentially all, public service organisations within Scotland; delivering both cost and performance advantages.

16. The existing 2007 ICT strategy is currently being refreshed to cover the five year period from 2013. In line with other strategies it will align with the council's overall corporate plan. The ICT function is seen as an enabling function which supports the Council in its delivery of services. The targets and goals for the planning and delivery of ICT services are included under the Head of Policy Technology & Improvement (PT&I) in the Corporate & Neighbourhood Services (C&NS) three year Service Performance Plan 2013 - 2016.

Refer risk no. 1

17. The council's new ICT Strategy will cover the strategic priorities for the council and the necessary technical solutions needed to deliver them. In addition, the council is developing a

wireless network strategy. The council aims to deliver wireless networking solutions which will both meet the requirements of the users in a particular setting and protect the integrity and security of the existing council network. At the time of our audit review, the wireless network strategy was in draft and had yet to be finalised and approved.

Refer risk no. 2

18. To replace the current governance arrangements it is proposed that a new Improvement Board has responsibility for ensuring the implementation and delivery of ICT related strategies. The development and maintenance of such strategies remains the responsibility of the Head of Policy, Technology and Improvement.

19. The IT service's Improvement and Technology & Infrastructure Units function is to deliver a range of complex services. This requires a systematic and planned approach to initiate, develop and implement new systems. To address this requirement they have adopted a robust project planning methodology.

Service delivery

Organisational structure

20. The ICT function has been structured and organised into two distinct service areas:

- Technology & Infrastructure, and
- Improvement.

21. Technology & Infrastructure covers hardware support and maintenance including network connections and security. It also includes the provision of first and second line support for corporate applications and the installation and testing of software upgrades / new releases.

22. Improvement includes the provision of business analysis, capital planning, business continuity planning & management and IT training. It also covers IT procurement and contract management.

23. One of the main requirements for effective service delivery is a sound management environment with a staffing structure that focuses on, and identifies, the needs of the council's service priorities. The ICT function has a well defined structure having recently come through a programme of workforce re-structuring. Part of the re-structure was to ensure all posts were filled and supported by current job descriptions. We noted that job descriptions are in place for the new structure although a few positions are still described as vacant.

Refer risk no.3

24. Staff are the key to successful service delivery and in recognition Corporate Services which includes Policy, Technology and Improvement was recently re-awarded Investors in People (IIP). It is also important that the council employ the right staff with the right skills and maintain these through training and development. We noted that the council continues to invest in staff training with the aim of ensuring they have sufficient skills to enable them to make the most effective use of the facilities provided. The commitment to training and

development is outlined in the council's Corporate Training & Development Policy which is supported by an Achievement & Personal Development Scheme (APDS). Individual APDS plans are prepared annually with review meetings taking place 6 months following agreement of the APDS Plan. While managers are aware of their staff's ability and skills there is no overall skill matrix available to assess service training needs.

Refer risk no. 4

Installation management

25. The council's main computer suite is located in the Municipal Buildings (Falkirk) and is secured by a swipe card entry door system. The room housing the main corporate servers is accessed by key fob and is alarmed out of hours. In addition the computer suite is protected by an automatic fire suppression system using a widely accepted HFC227 gas based extinguishing system.

26. A feature of the business continuity arrangements for the Municipal Buildings (which cover the Computer Suite) is protection from the loss of mains electricity through a back-up generator. In addition, all servers and core network equipment within the computer room are protected by uninterrupted power supplies (UPS). The generator is tested monthly and serviced twice a year. Load testing was carried out at installation while the council successfully used the generator in a 'live' scenario in January 2011. We were also advised that there is to be a review of the requirements for a future test to confirm generator capacity.

Refer risk no. 5

27. User access to corporate systems through the council network needs to be tightly controlled for security purposes. The primary method of controlling user access is through the use of “active directory” user profiles. These are assigned to council employees by ICT staff and provide access to email, internet and corporate data files (based on service management authorisation). In addition, server access allows service administrators to set up users in key areas such as financial systems.

28. As part of the control and management of access to the council's computer systems and networks it is the responsibility of the ICT function to ensure the use of the “super user” level of access is restricted, logged and monitored to ensure that there is no misuse. Super user / administrator access generally provides full unrestricted access to systems. This level of access is controlled by team leaders, with passwords securely stored in fire safes. Usage is regularly reviewed and passwords changed, as required, including where staff turnover has taken place.

29. In terms of capacity management, the ICT function is responsible for ensuring that there is sufficient storage capacity for retaining data. ICT are also responsible for maintaining network capacity and ensuring that there is sufficient bandwidth to provide the required access to data at main and remote sites. For change management there is a requirement to ensure amendments to either infrastructure, or systems, are appropriately tested and authorised prior to implementation. Our review found that sound controls were in place for capacity and change management and these were functioning adequately.

Service monitoring

30. The council has a help desk system in place with specific staff assigned to manage the system. They report to the Technology and Infrastructure Manager. The help desk system has recently undergone some fundamental change with the implementation of new work practices. The main change has been the amalgamation of first line support with the service desk function. This has required a different skill mix with the staff carrying out this function now all working as support engineers. This change has also allowed the introduction of staff rotation and enabled staff to undertake more technically complex second and third level support. The aim is to help resolve more calls at an earlier stage as well as support staff development.

Refer risk no. 6

31. Furthermore, the ICT service has carried out a number of customer satisfaction surveys as part of continuous service improvement. In this context performance figures are produced monthly to show how well targets are being met. These are scrutinised by Services and PT & I management with actions taken to resolve any issues as they occur.

Access controls and compliance

32. The ICT department has a number of policies and arrangements in place to comply with corporate and national standards governing the provision of security and confidentiality of sensitive information. The recent fine of £150,000 imposed on Glasgow City Council, by the Information Commissioner's Office, for the loss of two encrypted laptops containing the personal details of local tax payers only serves to highlight the importance of ICT security.

33. In our review of overall security arrangements we identified an information security policy (ISP) dated May 2011 which was approved by the Corporate Management Team. The policy includes rules for matters such as data sharing and home / remote working. It also cross-refers to the council's Acceptable Use Policy (AUP) dated May 2011. The AUP covers, amongst other things, computer use, email use and internet use. We noted, however, that the security policy makes reference to the British Standard on Information Security BS7799-2. This standard has been superseded by BS ISO/IEC 27001 which is also under revision and planned for re-issue by the end of 2013.

Refer risk no. 7

34. Government and statutory agencies such as the Information Commissioner's Office (ICO) are placing increased demands on councils to have secure practices and policies in place for issues such as information classification and data sharing. The ISP makes reference to both areas of information management and the creation of an Information Management Strategy which will be part of the new ICT Strategy. Falkirk Council engages in sharing data with partner agencies/ organisations and is a member of the Forth Valley Data Sharing Partnership. The objective in all cases is to enable the efficient flow of information without compromising security, integrity and confidentiality. Notwithstanding this and given an increasing demand for sharing services, and data, the council through the Governance section

need to ensure that all services remain fully aware of their responsibilities when granting access to areas where sensitive data is held.

35. A fundamental principle of any security environment is to prevent incidents (e.g. viruses) and to detect them promptly. We noted that the council have antivirus software and firewalls are in place. The effectiveness of the council's measures to prevent and detect problems is monitored and updated on a regular basis. For example, penetration testing takes place for all new systems which span across the firewall while access to download files/executable programmes from the internet is restricted and monitored through internet filtering software.

Asset protection

36. The council's ICT policies require that asset protection (including the availability, confidentiality and integrity of data) meets the following principles:

    – Maintain appropriate protection of corporate assets.

    – Ensure that information assets are recorded

    – Ensure that information assets receive an appropriate level of protection.

37. Assets can only be protected if they are appropriately identified and recorded. The council's ICT section maintains a register of hardware and software assets while all assets have been tagged for physical identification. Also, the council uses the System Centre Configuration Manager (SCCM) to manage its ICT hardware and software inventory. In addition, as part of a proposed programme of physical checking of assets, a pilot is underway within Corporate & Neighbourhood Services to check compliance with the ISP and AUP in relation to mobile devices.

Refer risk no. 8

38. An important part of the lifecycle of hardware assets is disposal. The council must ensure that all data is erased so that no sensitive personal data will be placed at risk of disclosure. We were informed that the ICT service currently manages asset disposals through a Waste Electrical and Electronic Equipment Directive (WEEE) certified 3rd party organisation. This external company deals with the final destruction of equipment and also does a hard drive 'wipe' and disposal service.

39. In addition to its asset registers the council should have an information asset register (IAR) relating to important datasets. These information assets should be managed in line with council policy to ensure that data is appropriately protected. As previously noted an Information Management Strategy will be part of the council's new ICT Strategy and this should include the creation of an IAR. The IAR should record important information such as data ownership, sensitivity and whether the data is shared with partner organisations.

Refer risk no. 9

40. As part of the process for managing information all relevant data held by the council including customer records and corporate information should be backed up and stored in a secure manner. We noted that operating procedures are in place which cover data back-up including

off-site replication for resilience and ease of recovery. The completeness and accuracy of this process is monitored on a daily basis.

Business continuity

41. Falkirk Council recognises that planning for emergencies is an integral part of good business practice. For the ICT service the term disaster recovery is used to refer to the ability to resume essential information technology services (data networking, key application systems and email) in the event of a significant outage.

42. In addition, the council acknowledges the need for business or service continuity planning and management, which is defined as the processes put in place to ensure the delivery of its core services in the event of unforeseen circumstances short of total service outage. It is recognised by the council that the circumstances can be a natural or man-made disaster (adverse weather conditions, flooding, and terrorism), unavailability of key premises for carrying out the services or long term absence of key staff.

43. The main legislative requirement upon the council to ensure continuity of service is based upon the Civil Contingencies Act 2004 and the resultant Contingency Planning (Scotland) Regulations 2005.

44. A significant aspect of business continuity planning and disaster recovery planning is prevention and minimising risk through the provision of resilient systems and a protected physical environment. The measures as noted include a back-up generator and all servers and core network equipment are protected by UPS and back-ups are taken with on and offsite storage of data.

45. We found that the council has plans in place to address business continuity planning (BCP) and disaster recovery (DR) relating specifically to information technology and ICT services. The ICT BCP / DR plan is intended to allow for numerous scenarios allowing part or parts of the plan to be chosen depending on the situation. These plans are reviewed at least annually and tested by the Emergency Planning Team. Specific ICT BCP exercises take place regularly; however there is no test plan within the DR plan and there was no feedback available from the last exercises to allow review of results. It would also be useful if the plan had a document information page to record changes as a result of tests or other amendments.

Refer risk no. 10

46. The council has employed Gallacher Basset to help develop a formal risk analysis methodology and identify business critical systems. As part of this process all services are required to complete formal business impact analysis (BIA) worksheets. The ICT has started to complete this documentation. Once completed all BIA worksheets will form part of the council's IT Business Continuity Planning System - a new web based system which will allow services to view what BCP documentation is held for their systems.

Refer risk no. 11

Appendix A

Risk identification and action plan

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
1	16	The ICT strategy is an important means of providing a "roadmap" and benchmark for measuring the delivery of ICT enabled service improvement going forward. ***Risk: without a current ICT strategy aligned to service plans it is possible that effective ICT enabled services will not be delivered.***	As of July 2013, the draft strategy has been out for discussion. It is planned to discuss this with services prior to seeking approval from Members.	Head of Performance, Technology & Improvement	October 2013
2	17	The wireless networking strategy is required to provide the council with a flexible approach in the implementation and delivery of ICT enabled systems. ***Risk: without a wireless networking strategy the council could reduce its options for making use of the most appropriate technology for delivering services.***	The policy has been in draft for some time and we will undertake a final review and update of this. This will then require CMT and committee approval.	Technology & Infrastructure Manager	December 2013
3	23	There are a number of vacancies within the ICT staffing structure. ***Risk: ICT lack skilled staff and capacity to deliver services effectively.***	The vacancies noted at the time of the audit have been filled.	Service Unit Managers	Initial issues completed

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
4	24	The APDS requires that employees have individual training and development plans. This should not preclude the development of a departmental skills matrix to inform training provision. ***Risk: if the ICT service does manage its departmental training plans it could be difficult to provide or improve service.***	We will continue to ensure that all employees undertake these. Additionally, we are reviewing options for undertaking skills analysis using the SOCITM Skills Framework for the Information Age (SFIA).	Head of P,T&I, Unit Managers, Team Leaders	APDS - ongoing March 2014
5	26	It is essential that the capacity of the generator providing business continuity to the Municipal Buildings is known. ***Risk: if the generator's capacity is not fully known then system support cannot be guaranteed.***	The known capacity of the generator is 40% greater than the maximum supply to the building which Scottish Power can provide. A further successful 'live test' took place in May 2013.	Technology & Infrastructure Manager	Now completed
6	30	The effective amalgamation of support functions is required to improve service. ***Risk: savings and improvement may not be delivered without effective measurement of outcomes.***	Work is underway to review all areas of T&I to better utilise the staff resources available to the team. Changes have already been made to the Service Desk.	Technology & Infrastructure Manager & Team Leaders	Mar 2014
7	33	The ISP should, where appropriate, reflect best industry practices and reference the most current standards.	The ISP will be reviewed in early 2014 - changes to the document will be made to reflect technology changes,	Head of P,T&I	June 2014

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
		Risk: if policies do not reflect current standards the council may not be able to respond to security incidents effectively.	the introduction of Public Records (Scotland) Act PRSA, changes to industry standard, the SASPI and changes coming from the national IT strategies.		
8	37	The pilot exercise for checking council mobile devices should be able to identify all mobile assets for which the council is responsible. ***Risk: if checks cannot be designed to identify all ICT assets then the council could suffer loss of both hardware and data.***	Once the pilot in C&NS has been completed, other services will be encouraged to participate.	C&NS All Heads of Service	December 2013
9	39	The council should be able to identify all information assets including data ownership, sensitivity and if shared with partner organisations. ***Risk: if information assets are not documented in an IAR then security measures may be inadequate or inappropriate.***	Part of the new Strategy will be to work with Services, the Records Management and Corporate Risk Management Groups to prepare an Information Management Strategy. Additionally, the Scottish Accord for the Sharing of Personal Information (SASPI) and associated framework	Head of P,T&I. Service and Improvement Governance Board Chief Governance Officer, Services	Jan 2015 Ongoing

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
			documentation has superseded the original Data Sharing partnership Framework and should be used in all Data Sharing situations. Governance is the lead Service for this.		
10	45	Part of the Disaster Recovery / Business Continuity Planning process is to carry out testing and to learn lessons which can then be used to update plans. ***Risk: if testing is not planned and results documented lessons learned may not be reflected in plans.***	We will ensure that tests continue to take place with ICT as well as participating in wider Council and Service wide business continuity plans and exercises. We will request feedback from Civil Contingencies staff for future exercises.	Head of P,T&I, Unit Managers	Ongoing
11	46	The effective assessment of service risk is important in identifying business critical systems. ***Risk: if services do not complete and maintain their business impact analysis work sheets then BCP plans may not accurately reflect all business critical systems.***	We will continue to work with Services on the central and Service based BCP plans. We are also participating in the Gallagher Bassett risk analysis exercise. We also maintain a specific ICT risk register.	Head of P,T&I, Unit Managers All Services' Civil Contingencies Officer Corporate Risk Management Group	Ongoing