Falkirk Council

ICT service review follow-up 2013/14

AUDIT SCOTLAND

Prepared for Falkirk Council
July 2014

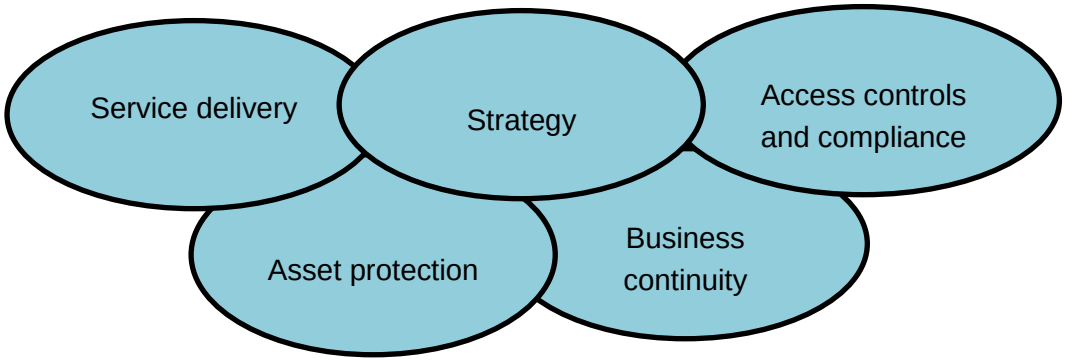
Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively**.**

Contents

Summary

Introduction and audit approach

1. As part of our risked based assessment carried out during the initial planning stage of the Falkirk Council audit, we identified the need to carry out a follow-up audit in 2013/14 to assess progress in implementing the action plan agreed with management as part of out ICT service review audit undertaken in 2012/13. Our 2012/13 audit was based on an established computer services review methodology developed by Audit Scotland. It provided a high-level risk based assessment of ICT services in five key areas as outlined below.



2. Our follow up review was carried out to assess the extent to which the audit recommendations had been implemented. The review was completed in consultation with ICT management who also provided supporting documentation as evidence. In addition, a number of the ICT service functions were considered by us to confirm their operational effectiveness, were appropriate.

3. Any identified revision to actions or proposed timescales where also taken into consideration as well as their impact on the implementation of audit recommendations.

Key findings

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

5. In our 2012/13 report we noted some areas of good practice such as project management. In addition we noted areas of challenge such as information management and agreed some areas where management agreed to improve controls.

6. The council's ICT section has made satisfactory progress with the agreed action plan that accompanied our 2012/13 ICT service review report. Although not all matters were or have been fully concluded to the timescales agreed in the action plan we have noted and accept the reasons for slippage. Unforeseen issues impacted on planned ICT work; in particular, work associated with the new UK Public Services Network (PSN) security accreditation

process caused delays. The process has also resulted in the need for additional policy actions, now being developed, for approval by management, to provide further controls.

7. Our 2012/13 ICT service review included a total of eleven agreed action points of which two were completed at the time of reporting in 2012/13 while seven other seven others are now considered to have been completed. Of the seven, three, which included business continuity and training were adjudged to be ongoing developments, but are now processes that can be considered to be part of business as usual.

8. The two actions that are not complete relate to the development of an Information Management Strategy, to support Data Sharing policies and the Scottish Accord for the Sharing of Personal Information (SASPI), and a review of the council's Information Security Policy (ISP). The first which also supports the introduction of an Information Asset Register (IAR) is still progressing to target with workshops planned to engage and communicate with staff. The delay in reviewing and re-drafting the ISP, prior to seeking approval, is due in part to work on the new security requirements being imposed by the changed PSN accreditation process.

Risk exposure and planned management action

9. This report summarises the findings from our review and identifies areas where the council may continue to 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.

10. The updated risk identification and action plan at Appendix A of this report provides an overall summary of progress in implementing audit recommendations. Appendix B describes any outstanding recommendations and the revised agreed date for implementation while noting any new or amended actions.

Conclusion

11. Our overall conclusion is that satisfactory progress is being made with the previously agreed risk identification and action plan and that the controls surrounding the management of the ICT service within the council remain sound.

Acknowledgements

12. 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.

Appendix A

Updated risk identification and action plan

Action point	Risk identified	Planned management action	Target date	Current position
1	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.	October 2013	**Completed** The technology strategy was approved at the Executive meeting on 18 March 2014. The PSN accreditation process led to a delay in finalising the strategy and aspects of the strategy have changed fundamentally – specifically issues of Bring Your Own Device. ***No further action required.***
2	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.	December 2013	**Completed** The council's strategic network response is referenced in the approved technology strategy. The tactical requirements are being developed in line with a number of actions needed to maintain PSN compliance and requirements to deliver wider options for using mobile technology in service delivery. ***No further action required***.

Action point	Risk identified	Planned management action	Target date	Current position
3	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.	Initial issues completed	***No further action required.***
4	The Achievement & Personal Development Plan 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).	APDS - ongoing Mar 2014	**Completed** While core training requirements are considered and specific requirements identified during the APDS process further training up-skilling is also identified as new projects are progressed with ICT support requirements. ***No further action required.***
5	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.	Completed	***No further action required.***

Action point	Risk identified	Planned management action	Target date	Current position
6	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.	Mar 2014	**Completed** While planned changes have now been introduced it is recognised that further changes may be needed going forward with the greater use of mobile working. ***No further action required.***
7	The ISP should, where appropriate, reflect best industry practices and reference the most current standards. ***Risk: if policies do not reflect current standards the council may not be able to respond to security incidents effectively.***	The ISP will be reviewed in early 2014 - changes to the document will be made to reflect technology changes, the introduction of Public Records (Scotland) Act PRSA, changes to industry standard, the SASPI and changes coming from the national IT strategies.	June 2014	The PSN accreditation process and the PRSA have resulted in the need for additional policy actions. The policy changes are being developed for approval by management to provide the basis for providing a compliant security control environment. ***Further action required - refer. Appendix B point 1.***
8	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***	Once the pilot in C&NS has been completed, other services will be encouraged to participate.	December 2013	**Completed** With the pilot completed successfully it is intended to encourage other services to participate in the process. ***No further action required.***

Action point	Risk identified	Planned management action	Target date	Current position
	council could suffer loss of both hardware and data.			
9	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 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.	Jan 2015 Ongoing	The overall information and records management response required for identifying and securing all council records and data is progressing to target. The records management plan developed in response to the Public Records (Scotland) Act 2011, covering both paper and electronic forms was approved by the Executive in January 2014, is part of the response. Workshops to inform staff of their and the council's responsibilities for managing information are planned. ***Further action required - refer. Appendix B point 2.***
10	Part of the Disaster Recovery / Business Continuity Planning	We will ensure that tests continue to take place with ICT	Ongoing	**Completed** There are now two members of staff

Action point	Risk identified	Planned management action	Target date	Current position
	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.***	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.		dedicated to managing and updating service BCPs to ensure they remain current and relevant. Limited desk testing is carried out to as part of the process to confirm planned responses to service disruption are practical and achievable. The process is now in effect part of business as usual. ***No further action required.***
11	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.	Ongoing	**Completed** The Executive approved a risk management policy in October 2013 designed to set out a framework for embedding risk management across the council. In this context all services must understand and plan to reduce the risks they face in order to deliver the commitments with in business as usual. ***No further action required.***

Appendix B

Follow on risk identification and action plan

Action point	Original Action	Original risk identified	Planned follow on management action	Responsible officer	Revised target date
1	7	The ISP should, where appropriate, reflect best industry practices and reference the most current standards. ***Risk: if policies do not reflect current standards the council may not be able to respond to security incidents effectively.***	The policy changes addressing the requirements of ongoing compliance with the PSN accreditation process and the PRSA will be developed and approval obtained from the Executive.	Head of P, T & I.	November / December 2014
2	9	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***	Workshops to inform staff of their and the council's responsibilities for managing information will be conducted, as planned. This is part of ensuring the required processes for identifying and ensuring information assets are used and held securely are embedded across the	Head of P, T& I. and Service Improvement Governance Board Chief Governance Officer, Services	January 2015

Action point	Original Action	Original risk identified	Planned follow on management action	Responsible officer	Revised target date
		an IAR then security measures may be inadequate or inappropriate.	council.		

Note - Head of P, T&I refers to Head of Policy, Technology & Improvement.