Argyll & Bute Council

ICT service review 2011/12

AUDIT SCOTLAND

Prepared for Argyll & Bute Council
October 2012

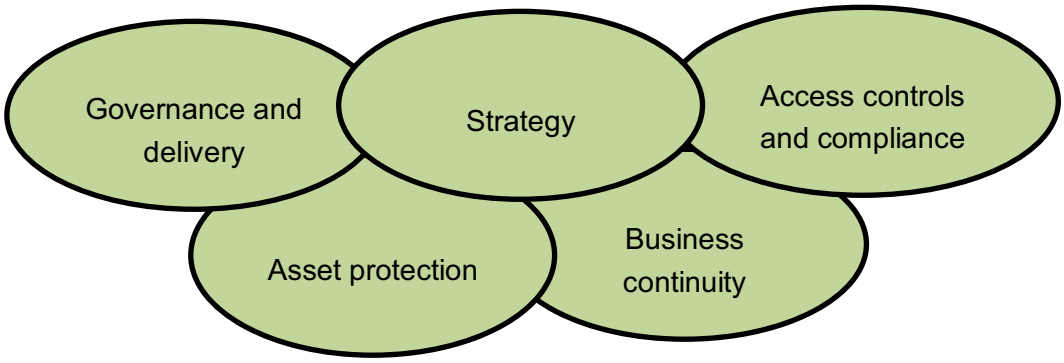
Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. It provides services to the Auditor General for Scotland and the Accounts Commission. Together they ensure that the Scottish Government and public sector bodies in Scotland are held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

Contents

Summary

Introduction and audit approach

1. As part of our risked based assessment carried out during the initial planning stage of Argyll & Bute Council audit, we identified Information and Communication Technology (ICT) as a priority area for review in 2011/12. 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 Preliminary Service Evaluation (PSE) and elements of the Computer Services Review (CSR) Client Questionnaire (CQ) which were completed in consultation with ICT management and from supporting documentation, as appropriate, as back-up evidence. In addition a number of the IT service functions were tested in detail to confirm operational effectiveness.

Key findings

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

4. A number of good practices were identified and include the following:
   - there are sound practices in place for managing user access to systems controlled by the council.
   - there is a service desk process to ensure effective control is exercised over support calls through a service tool.
   - business continuity arrangements have been developed for the back-up and recovery of data although under review.
   - there are arrangements in place for managing the council's ICT 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:

   - Information and Communication Technology (ICT) is an integral part of the council's service delivery activities. Investment in ICT provision is being provided and infrastructure and facilities are being re-configured with a project to close and transfer the Campbeltown server room to a new upgraded data centre at Kilmory.
   - the ICT service is part of a programme of continuous service improvement. The implementation of the Information Technology Infrastructure Library (ITIL) will be used to manage this process.
   - the continuous changes and usage of data through collaborative partnerships places new demands on information security policy and arrangements.
   - the Scottish Government are looking to the council to help develop and deliver plans for superfast broadband and invest further in the standardisation of networks and services to ensure compliance with the public service network (PSN).
   - the maintenance of business continuity / disaster recovery arrangements is part of an on-going process. The requirements needed to support the arrangements at the new data centre will need to be incorporated into the current plans.

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 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, 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 (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 Appendix A of this report details the areas where continued risk exposure requires 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 investments

are 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 been 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 Information Communications Technology (ICT) in the delivery of government and locally driven initiatives to provide improved service to the public. 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. To provide the needed services Argyll & Bute Council have a strategically driven approach. The council also recognises that the Scottish Government in conjunction with the Improvement Service has a programme of services to encourage online access to council and other public services. The council advise that it will align with this approach where it considers it appropriate.

13. In addition to the strategic approach being adopted for the provision of ICT services, there is a requirement to provide sound operational control over matters like, information security, hardware and software management and the ability to provide adequate disaster recovery and business continuity.

Strategy

14. The council's strategic ICT vision is designed 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.

15. The council's vision for the use of ICT in service provision and improvement is seen by the adoption new technology and work practices, for example the council encourages the use of voice and video conferencing to avoid unnecessary travel. This has seen the installation of visual and audio equipment in meeting rooms across key offices of the council. In addition the Scottish Government are looking to the council's strategy to help develop and deliver plans for superfast broadband and invest further in the standardisation of networks and services to ensure compliance with the PSN.

16. The current ICT strategy dated October 2008 and covering the period to 2011 was developed in line with the council's overall corporate plans, with the ICT service seen as an ‘enabling’ function which supports the Council in its delivery of services. The ICT planning process continues to follow corporate requirements and an ICT service review has been conducted to identify the council's ICT infrastructure and ICT applications needs going forward. The ICT strategy should, however, be refreshed to provide a "roadmap" and benchmark for monitoring service delivery.

Refer risk no. 1

17. Due to the complex nature of services delivered by the council it is recognised that there should be a systematic and planned approach taken in the initiation and delivery of projects, to develop the corporate ICT infrastructure and/or for the introduction of new systems. To address this requirement the corporate ICT function has adopted the Prince2 project planning methodology which is the accepted standard for the public sector.

Governance and delivery

18. To ensure the priorities and service targets set by the ICT strategy were achieved the council created an ICT Strategy Group. In accordance with the strategy each Directorate had to nominate a representative for the corporate ICT Strategy Group at Head of Service level who was tasked with identifying ICT implications of their respective departmental service plans. The strategy group are not currently meeting on a regular basis to monitor the ICT strategy. The services do, however, provide input to the capital programme which includes investment in improved ICT infrastructure and new applications to support new or changing business needs.

Refer risk no. 2

19. To support the strategy and to provide the required focus, the ICT function has been structured into two distinct service areas; Infrastructure Services and Application Services. ICT Infrastructure provides hardware support and maintenance including network connections and security while ICT Applications provides first line support for corporate applications and installation and testing of software upgrades and new releases.

20. An integral part of governance beside the provision of a sound control environment and a procedural framework is having adequate key skills and a process of maintenance and training. The council continue to invest in staff training, ensuring they have sufficient skills to enable them to make the most effective use of the facilities provided. In this context performance development reviews are carried out for all staff on an annual cycle and this incorporates annual training plans. Progress is reviewed against these on a 6 monthly basis.

21. As part of providing a sound control environment through service improvement the ICT service has a project in place to implement new work practices through the introduction of ITIL standard V3. ITIL is a widely accepted and recognised approach to IT service management. ITIL provides a cohesive set of best practice, drawn from the public and private sectors designed to improved service delivery.

Refer risk no. 3

22. In addition the council has been following a continuous assessment model through benchmarking and customer satisfaction surveys. The benchmarking measures used are provided by SOCITM the most widely used by Scottish public authorities. The council look closely at areas where results fall below the KPI median or where customers look for specific improvement.

23. The council's delivery plans indicate a number of significant ICT challenges against a backdrop of making financial savings. There are a number of initiatives in place to meet these

challenges, for example ICT will continue to develop the council website to meet the changing requirements and expectations of the customer and at the same time will look to drive down the cost of local printing by developing and implementing a corporate wide print strategy. In addition, the upgrading of the Kilmory data centre allows for the closure of the server room at Campbeltown a further step toward reducing the council's energy consumption.

Refer risk no. 4

Access controls and compliance

24. To ensure compliance with corporate and national standards for the provision of security and confidentiality for the council's customer and other sensitive information, the ICT service has policies and arrangements in place to ensure adequate access and identity management. The arrangements are designed to ensure users are authorised and appropriate system access permissions granted.

25. In the review of overall security arrangements we note an information security policy dated February 2005 and approved by the Strategic Management Team. The policy includes rules for computer use, email use and internet use. It is, however, noted that the security policy is out of date and in need of review and refresh in line with the International Standards Organisation ISO27001 information security standards framework which provides best practice guidance. While a policy update appears to be required some matters such as email and internet access have now been superseded or updated by the issue of an acceptable use policy (AUP) dated January 2010.

Refer risk no. 5

26. We are advised by council representatives that the maintenance and review of the corporate information security policy and related matters such as information management / sharing and encryption practice is now within the remit of Democratic Services.

27. Government and statutory agencies such as the Information Commissioner's Office (ICO) are placing increased demands on council's to have secure practices and policies in place for issues such as information classification and data sharing. The ICO carried out a review of the council's practices in a number of related areas in 2009 and followed up in 2010, in relation to Data Protection Act 1998 compliance, and found a number of areas in need of improvement. Follow up by internal audit has shown some progress in meeting the recommendations made by the ICO. Notwithstanding this and given an increasing demand for sharing services and data the council need to ensure policy and procedures in this area remain current and are monitored.

Refer risk no. 5

28. There is a process in place to authorise the activity of users and users are required to sign up to the acceptable use policy. This process is supported by operating procedures which include the removal of redundant users and the monitoring of internet activity as set out in the AUP.

Asset protection

29. The council's policies such as the information security policy and the corporate asset strategy requires that 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. In order for assets to be protected appropriately they need to be identified and recorded. The ICT section is required to maintain a register of hardware and software assets on behalf of the council. All assets under the responsibility of the ICT service are known having been tagged and physically checked in the last 18 months. Although the ICT service has no formal asset register system software the databases for hardware and software assets are held on spread sheets and linked to the service desk tool 'Heat' to help in the provision of support and overall planning.

31. An important part of the lifecycle of hardware assets is disposal. It must be ensured, in particular, that all data is erased to confirm no sensitive personal data will be placed at risk of disclosure. It was advised that the ICT service currently manage disposal through a Waste Electrical and Electronic Equipment Directive (WEEE) certified 3rd party organisation. The corporate asset strategy identified the need for an asset disposal policy and due to changing circumstances the ICT service is currently reviewing their processes in respect of disposal.

Refer risk no. 6

32. In addition to hardware and software registers is a project is in place to develop an information classification scheme for both paper and electronic documents. The scheme should record the information assets owned by the council and could impact on data storage.

33. As part of the process for managing information all relevant data held by the council including customer records and corporate information require to be backed up and stored in a secure manner. The ICT service has operating procedures to cover the backup of data using the 'Tivoli' system, including off-site replication between sites for resilience and ease of recovery and backup to tape. The completeness and accuracy of the process is monitored on a daily basis. The impact of the rationalisation of server rooms at Kilmory and Campbeltown on secure off-site back may need to be reviewed.

Business continuity

34. Argyll & Bute 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.

35. In addition the council recognises 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.

36. 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.

37. 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 council is rationalising processing capacity with the closure and transfer of the server room at Campbeltown to Kilmory. The premise at Kilmory is protected using fire detection and gas suppression systems and uninterruptible power supply (UPS) for power management in the event of failure.

38. It was found that the council has plans in place to address business continuity planning disaster / recovery relating specifically to information technology and ICT services. The ICT business continuity / disaster recovery arrangements are designed to cover various scenarios from environmental risk, for example damage to premise. The plans are currently under review as part of the council's business continuity planning work, and a fully documented ICT recovery plan will be developed following the consolidation of the Campbeltown and Kilmory sites. Detailed test plans should also be developed to ensure appropriate levels of recovery for all areas of the ICT infrastructure is achievable in the timescales required by the business.

Refer risk no. 7

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 strategy it is possible that effective ICT enabled services will not be provided.***	The ICT Strategy will be reviewed and refreshed as part of the IT workstream within the new Corporate Improvement Programme and following publication of the new Local Government IT Strategy for Scotland	IT Infrastructure Manager	31st March 2013
2	18	The ICT strategy group is indicated by the council as the vehicle services can collectively use to provide input to prioritising the implementation and delivery of ICT enabled systems. ***Risk: without regular input from services to the ICT strategy it is possible that effective ICT enabled services will not be provided.***	The new ICT Client Liaison team will work alongside services to ensure regular input into the ICT strategy. In addition the Corporate Improvement Board, with cross -service representation, is expected to take responsibility for overseeing the ICT Strategy refresh	IT Infrastructure Manager	31st March 2013
3	21	Implementing a standard for service management is an important step in delivering process improvement going forward. ***Risk: without the***	Initial ITIL foundation training has been completed and a full ITIL Implementation will occur throughout 2013	Production Manager	31st December 2013

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
		adoption of standards it is possible that an effective service will not be provided.			
4	23	The ICT service faces a set of challenges over the coming years with increasing demand to make savings in line with council targets. ***Risk: if the ICT service does not fulfil the plans in place or being developed it will be difficult to make the anticipated savings.***	The Council's performance management system, Asset Management Board, Transformation Board, Corporate Improvement Board, IT Management Team and Corporate Services Department Management Team all monitor progress of the major ICT projects expected to contribute to the longer term savings plans of the Council. Monitoring processes are already in place however the ICT Service will continue to present further opportunities to the various boards to innovate and generate further savings but will look to the Council to maintain investment in services at current levels to ensure plans can be delivered.	IT Infrastructure Manager Production Manager	On-going
5	25 & 27	There should be a current information security policy in place to provide a framework for the provision of secure ICT service. ***Risk: if the information security policy is not***	The IS Forum will be reconstituted and will meet on a more regular basis. The forum will be responsible for the development of a revised Information Security policy and for the continual	Information Security Forum	31st March 2013

Action point	Refer para no	Risk identified	Planned management action	Responsible officer	Target date
		reviewed and updated on a regular basis it is possible that systems, data and information may be at risk.	review of that policy thereafter.		
6	31	The disposal of ICT assets must be carried out in a secure and cost effective manner to ensure data security and effective use of equipment. ***Risk: process and cost benefits may not reflect the council's strategic objectives and changing needs.***	A formal IT Asset disposal policy will be developed and a contract put in place to ensure all IT assets are disposed of in accordance with all relevant legislation.	Networks Manager Production Manager	31st March 2013
7	38	The council should have plans in place to ensure there is adequate IT business or service continuity arrangements in place. ***Risk: if plans do not reflect current needs the council will not be able to effectively respond to unforeseen events.***	The Council has IT Disaster Recovery and IT Service Business Continuity plans in place. These are currently undergoing refinement to accommodate the on-going refurbishment and re-classification of the Helensburgh server room and the impending closure of the Campbeltown room. The plans will focus on more regular testing to ensure recovery plans are clearly documented.	Networks Manager	31 March 2013