Aberdeen City Council

IT Disaster Recovery

Internal Audit Report 2014/2015 for Aberdeen City Council

January 2015

	Target Dates per agreed Internal Audit Charter	**Actual Dates**	**Red/Amber/Green and commentary where applicable**
Terms or reference agreed 4 weeks prior to fieldwork	3 November 2014	25 September 2014	Green
Planned fieldwork start date	1 December 2014	1 December 2014	Green
Fieldwork completion date	12 December 2014	11 December 2014	Green
Draft report issued for Management comment	9 January 2015	8 January 2014	Green
Management Comments received	23 January 2015	29 January 2015	Amber. Note: most comments provided on 21 January.
Report finalised	4 February 2015	30 January 2015	Green
Submitted to Audit and Risk Committee	February 2014	February 2015	Green

pwc

Contents

1. Executive Summary

Report classification	Total number of findings ← Section 3 →				
	Critical	**High**	**Medium**	**Low**	**Advisory**
Low					
Control design	-	-	-	2	-
Operating effectiveness	-	-	-	2	-
Total	**-**	**-**	**-**	**4**	**-**

Summary of findings

1.01 We have conducted a review of IT Disaster Recovery (IT DR) at Aberdeen City Council, with a focus on the policies and plans in place across ICT to address a disaster recovery incident. This has included a review of the planning across all systems that have been identified as critical; these are the ATOS data centre, the Getronics telephony system and the email servers.

1.02 The plans for Disaster Recovery have two layers; at high level there is the overarching ICT Disaster Recovery Plan, which covers the Council's responses to a Disaster Recovery (DR) incident; and the outsourced plans that cover the recovery of the data centre and the telephony system. The outsourced services provide the primary DR solutions for the Council's key systems.

1.03 Overall we found the controls to be largely satisfactory in addressing the risks around disaster recovery. In the course of our review we have noted four low-risk control findings for management's consideration:

- There has been no formal review, of the ICT Disaster Recovery Plan, to ensure that plans are an accurate representation of current practice and considers all critical systems;
- Staff involved in disaster recovery are not provided with any specific training;
- Disaster recovery testing is not as robust for the Getronics contract as it is with the ATOS data centre; and

- Not all departments provide staff to assist with the data centre DR testing.

1.04 We have identified a number of areas of good practice, including:

- There is a strong process in place for identifying and tracking risks around DR for the ATOS data centre. These are all tracked centrally in a joint ATOS/ACC risk register, which is reviewed on a monthly basis;
- There is an annual test of the transfer of operations from the primary to the secondary data centre. This has been carried out with only minor issues in the last two years and provides management with further comfort of the reliability of ATOS's DR procedures;
- There has been a process over the last couple of years of the ICT accounts managers engaging with the different service sectors Business Continuity Planning (BCP) process to ensure that these address issues around an IT DR incident. This process ensures that IT DR is understood to be the responsibility of the business as a whole and that appropriate plans are in place for the users to continue their operations in the absence of IT systems. ICT is seeking to communicate and raise awareness of what the service users can expect from ICT in an incident and the need to have plans to work for a prolonged period in the absence of IT systems; and
- ICT has recently implemented a process to review the criticality of all IT systems to assess any risks around key connections and hardware.

Management comments

We are pleased that the audit highlights the areas of good practice that are already in place regarding IT Disaster Recovery, and will continue to maintain and develop this going forward, incorporating the findings identified in this report

2. Detailed findings and recommendations

2.01 There is a need for a periodic rebasing of the ICT Disaster Recovery plans – Control design deficiency

Finding

We have reviewed the ICT Disaster Recovery Plan and found that, although the plan has been reviewed annually by the information security officer, the plan has not been re-baselined since 2008. As a result we have identified the following inaccuracies within the plan:

- The plan does not reflect the DR responsibilities within major service contracts, e.g. Atos managed data centre and Getronics telephony contracts;
- The plan refers to a DR vendors list which is now superseded by ICT Contracts Register.

Additionally ICT has begun a process to update the assessment of the criticality of systems. This has identified a number of previously critical systems that are non-critical. It is believed that once this process is extended to the systems previously not defined as critical some of these systems will be redefined as critical. This all means that there are potentially gaps in the current planning, however management are aware of these and are working through them. The lack of rebasing means that this change in the assessment of the criticality of systems has not been reflected in the ICT DR plan.

Risks

If there is no rebasing of the plans on a regular basis then this may lead to gaps in the plan including the failure to address critical risks that have developed since the previous version was written. This may impact the ability to restore systems in a timely manner in a DR situation.

Action plan

Finding rating	Agreed action	Responsible person / title	Target date:
Low	Future updates of the ICT Disaster Recovery Plan will be scheduled annually and after any significant changes to systems, and will incorporate changes to current practice, levels of system criticality and lessons learned from any Disaster Recovery exercises.	Sandra Massey, IT Manager	30 April 2015

2.02 There is a need to have regular table top reviews to both test plans and to raise awareness of DR among participants– Control operating deficiency

Finding

The council produce a ICT Disaster Recovery Plan. This sits above the main ATOS plan to recover the data centre and covers management's response to a DR incident. This overarching plan has not been tested during the year. Management are aware of this issue, and in the past they performed monthly tests to test this plan. However, these where stopped due to time constraints

Additionally in discussion with staff it has been identified that there is a low level of awareness of the plans in place. For example, staff who are referenced in the plan were not able to identify what level of authority is needed to activate it. The root cause of this is a lack of training with no training in DR currently taking place.

Risks

There is a risk that if the plans are not tested then there may be unidentified gaps in planning and these may not be discovered until a disaster.

Additionally if this testing does not involve training and awareness building of those that could be called upon to enact the plan then the plan may not be able to be enacted in an emergency.

Action plan

Finding rating	Agreed action	Responsible person / title
Low	ICT will undertake an annual walkthrough of the plans by those involved in their operation to try and identify any weaknesses and to ensure that key people are aware of their responsibilities and actions in a disaster recovery situation. (a table top review)	Sandra Massey (ICT Manager)
		Target date:
		30 June 2015

2.03 Getronics DR responsibilities need to be more actively controlled– Control operating deficiency

Finding

Getronics manage the telephony systems and have a maintenance provision in the contract that covers the recovery of the system in a DR situation. This however needs to be more firmly managed with the ATOS contract being held up as good practice to be followed. In our review of the current DR arrangement with Getronics we identified the following issues:

- The current plan supplied by Getronics is out of date:
- The last test performed on the DR plan has not yet been documented: and
- There have been a number of changes to the placement of the switch gear and the plans have not been updated to reflect these changes.

Risks

The Council may not be able to recover the telephony system in a timely manner without proper DR processes in place.

Action plan

Finding rating	Agreed action	Responsible person / title
Low	Telephony DR processes will be updated and tested, with the support of Getronics, as per their contractual arrangements	Sandra Massey, IT Manager
		Target date:
		31 May 2015

2.04 Service users are not always made available for testing of ATOS DR– Control operating deficiency

Finding

The annual test of the ATOS DR plan for the data centre requires testing of the operation of the critical systems to be effective. Ideally this should be done by the users to ensure that testing actively reflects the needs of users.

ICT have had difficulties getting some of the smaller departments to provide staff to do this, due to budgetary impacts around overtime, which has resulted in these service units not participating in the DR tests.

For example, Cremations and Burials did not participate in the 2014 test, which resulted in an issue not being identified until Monday morning, after the test was completed.

Risks

There is a risk that if service units do not support with this testing, specific business issues may not be identified prior to a DR incident.

Action plan

Finding rating	Agreed action	Responsible person / title
Low	System Owners should consider and document the risk of not testing their systems during disaster recovery testing of the data centre. IT will ensure that they request and retain copies of risk assessments prior to all future IT Disaster Recovery exercises	Sandra Massey, IT Manager
		Target date:
		30 November 2015

Appendix 1 – Background and Scope

Background

AP1.01 IT Disaster Recovery (IT DR) planning is an important component of business continuity planning. Where organisations rely on IT systems for their operations it is critical that IT disaster recovery is appropriately planned for, and considered within the context of the organisation's wider business continuity management strategy.

AP1.02 Aberdeen City Council's operations are reliant on several critical IT systems across a broad range of Council services. The failure of any of these systems could have a significant impact on the Council's ability to deliver services across the city. Effective IT disaster recovery planning is therefore essential to ensuring that the Council is able to respond to system failures in the event of a major disaster incident, in order to maintain operations of all critical systems.

Governance and Management

AP1.03 The starting point of planning for IT DR is the identification of the criticality of systems and the timeline for recovery of those systems to minimise disruption to operations. This was originally performed, when the plans were first designed, by the service departments identifying those systems they considered to be critical to their operations. This drove the original creation and operation of the DR plans. There has not been a full review since that plan was developed in 2004, as a consequence ICT believe there may exist several systems, implemented since the last full review, that are critical to Council services but not included in the DR plans.

AP1.04 ICT uses seven criteria to define the criticality of the system: user base, financial impact, reputational impact, contractual impact, customer impact, inter-connections and survivability. This has been performed for all those systems identified as critical when the DR plans were originally written. However, this has yet to be done for systems previously defined as non-critical. ICT believe that some of these non-critical systems will be redefined as critical once this review takes place.

AP1.05 The assessment of criticality performed in 2004 drove the creation of a high level plan for Disaster Recovery, called the ICT Disaster Recovery Plan. This plan has been updated several times in the intervening period. This update consists of the reviewer emailing the team leaders and asking them if there are any changes that need to be made and if the phone numbers on the list are complete. This update is performed annually and was last done in December 2013.

AP1.06 Additional plans are maintained at a more practical level to restore access to the critical IT systems in the event of a failure. The main way this would be done is to transfer from the primary data centre in Livingston to a Secondary data centre in Edinburgh. These connect in to the Aberdeen City Council Network through a

different set of connections thereby allowing the entire IT system to be switched to a second operating environment. Responsible for both these data centres is maintained by ATOS a subcontractor.

AP1.07 The only critical systems that are maintained outside the ATOS data centre are the telephony system and the email servers. The telephony system is maintained by Getronics. They provide ACC with a DR plan to enable recovery of the telephony system in a DR incident. The responsibility for this plan and the updating of this lies with Getronics, as they have a contractual obligation to maintain the system including in the case of a major incident.

AP1.08 The email system is hosted on three different servers; if one of these fails then the other servers maintain the system. No DR plan for the email system is considered necessary; ICT judge the risk of all three servers at three separate sites failing at once is considered too low to consider planning for it.

Disaster Recovery testing

AP1.09 ACC does not have a plan in place to test its overarching ICT Disaster Recovery Plan. ICT instead relies on the testing of the major practical component plans, such as the ATOS and Getronics plans to recover the data centre and telephony system, to ensure its DR plans are up to date.

AP1.10 The ATOS plan is tested on an annual basis. This is led by ATOS who are contractually responsible for this test in partnership with ACC who provide the necessary ICT staff as and when necessary. This is performed over a weekend with a transfer to the DR data centre on the Saturday and a transfer back on the Sunday. The Services are expected to supply staff to perform testing on the Saturday and the Sunday to ensure that the data centres are operating effectively.

AP1.11 All issues identified and unresolved on the day are placed on the ATOS risk register, which is reviewed on a monthly basis at a joint meeting. This meeting is led by ATOS and attended by key staff in ICT at ACC.

Training and awareness

AP1.12 Historically training and awareness of DR within ICT has been covered by 'table top' scenario testing of these plans on a monthly basis. However, this has not been performed recently due to limitations on the time of these individuals required to participate.

Awareness of the IT DR procedures is facilitated through the engagement of the Account Managers in the Business Continuity Planning (BCP) of the service units. This is done to ensure the service units are aware of what they can expect from ICT in the event of a disaster, and to emphasise that service units are expected to have plans in place to operate without the IT systems for a prolonged period of up to 24 hours.

Appendix 2 – Agreed Terms of reference

Background

IT disaster recovery planning is an important component of business continuity planning. Where organisations rely on IT systems for their operations it is critical that IT disaster recovery is appropriately planned for, and considered within the context of the organisation's wider business continuity management strategy.

Aberdeen City Council's operations are reliant on several IT systems across a broad range of Council services. The failure of any of these IT systems could have a significant impact on the Council's ability to deliver services across the City. Effective IT disaster recovery planning is therefore essential to ensuring that the Council is able to respond to system failures in the event of a major disaster incident, in order to maintain operations of all critical systems.

Our review will assess the current effectiveness of IT disaster recovery planning at the Council and whether these plans are aligned to the Council's wider business continuity planning.

Scope

We will review the design and operating effectiveness of the key controls in place to monitor disaster recovery. The sub-processes included in this review are:

Sub-process	Control objectives
Governance and management	• Disaster recovery plans cover end-to-end processes for all critical in-house IT systems. The assessment of the criticality of IT systems is aligned to the Council's business continuity plan. • Disaster recovery plans are in place for the outsourced data centre. These plans are reviewed to ensure they align with the Council's business continuity plan. • Governance arrangements are in place within ICT to ensure disaster recovery plans are regularly reviewed and assessed for appropriateness. A senior responsible owner has been appointed to manage disaster recovery. • IT disaster recovery plans are designed to be aligned with good practice.

Disaster recovery testing	• All IT disaster recovery plans are tested annually to ensure they are operating effectively. • IT disaster recovery test results are reviewed by ICT and Corporate Governance management and where issues are identified during testing these are escalated and resolved with changes made to plans as appropriate. • Sufficient resources are allocated to enable effective execution of IT disaster recovery plans
Training and awareness	• Key staff with responsibility for IT disaster recovery have sufficient training to enable them to perform their roles. • Awareness training is delivered across the organisation to educate staff on how to respond in an IT disaster recovery situation. At a minimum, completion of this training is monitored for key staff.

Limitations of scope

The scope of our review is outlined above. This will be undertaken on a sample basis. Our scope does not include an evaluation of the Council's business continuity planning, or provide assurance over recoverability for any future events.

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the procedures in place through discussion with key personnel, review of documentation and walkthrough tests where appropriate.
- Identify any events that have invoked the disaster recovery procedures within the current financial year, through investigation with management.
- Identify the key risks in respect of IT disaster recovery.
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the key controls on a sample basis.

Key Council Contacts

Name	Title	Role	Contact details
Paul Fleming	Head of Customer Service and Performance	Project Sponsor	pfleming@aberdeencity.gov.uk
Sandra Massey	ICT Manager	Key Contact	smassey@aberdeencity.gov.uk

Appendix 3 - Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken a review of IT Disaster Recovery, subject to the limitations outlined below.

Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls relating to IT Disaster Recovery is as at 11th December 2014. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.