Audit Summary Report

October 2006

PAPER D

audit commission

IT Assurance - Business Continuity and Disaster Recovery

Isle of Wight Council

Audit 2006/2007

External audit is an essential element in the process of accountability for public money and makes an important contribution to the stewardship of public resources and the corporate governance of public services.

Audit in the public sector is underpinned by three fundamental principles:

- auditors are appointed independently from the bodies being audited;
- the scope of auditors' work is extended to cover not only the audit of financial statements but also value for money and the conduct of public business; and
- auditors may report aspects of their work widely to the public and other key stakeholders.

The duties and powers of auditors appointed by the Audit Commission are set out in the Audit Commission Act 1998 and the Local Government Act 1999 and the Commission's statutory Code of Audit Practice. Under the Code of Audit Practice, appointed auditors are also required to comply with the current professional standards issued by the independent Auditing Practices Board.

Appointed auditors act quite separately from the Commission and in meeting their statutory responsibilities are required to exercise their professional judgement independently of both the Commission and the audited body.

Status of our reports

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to non-executive directors/members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any director/member or officer in their individual capacity; or
- any third party.

Copies of this report

If you require further copies of this report, or a copy in large print, in Braille, on tape, or in a language other than English, please call 0845 056 0566.

For further information on the work of the Commission please contact:
Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ
Tel: 020 7828 1212 Fax: 020 7976 6187 Textphone (minicom): 020 7630 0421
www.audit-commission.gov.uk

Contents

Introduction

1 This review was undertaken to gain assurance that the Council had effective arrangements for:

- backing up and recovering the information in IT systems (which relates to the availability of financial and other information supporting its financial statements); and
- restoring IT services in the event of a disaster, such as a fire (which relates to the efficiency and effectiveness of the Council's service delivery).

Background

2 We issued a report on the Council's ICT arrangements in May 2005 that made three recommendations to address shortcomings in business continuity planning and disaster recovery arrangements identified as part of our 2004/05 audit. This review also followed up the Council's progress in implementing these recommendations.

Audit approach

3 Our method was to compare the Council's arrangements against a best practice checklist. Information was gathered through several interviews with staff in the council's IT department and through the review of relevant documents. The field work for the assessment was carried out on 29 June 2006.

4 We did not consider arrangements for systems outside of the central ICT department (for instance, Revenues and Benefits system based at Sandown; social services; education). Although these are now operationally under the control of the central ICT department the back up function may still be outside the direct control of the management of this department.

Main conclusions

5 The Council needs to take immediate action to improve important aspects of IT security, particularly around disaster recovery planning. Previous efforts to prepare plans have failed to deliver outcomes and as a consequence the Council currently lacks a coherent response plan to safeguard its position in the event of a disaster. Ideally an initial plan should be put in place with immediate effect and arrangements introduced to ensure that this is revisited and improved on a cyclical basis.

ICT disaster recovery

6 There is no disaster recovery plan. In the event of a loss of IT equipment/ services due to an incident, such as a fire, arrangements to recover services will be devised reactively at the point in time that the event occurs. These arrangements are likely to be less effective and efficient than would be the case if a documented disaster recovery plan was in place.

7 We understand that there is a project to create a plan but this has been suspended at the present time due to resource constraints. We are concerned that failure to act quickly in this respect will continue to expose the Council to unnecessary risk.

Backups of data

8 The backup arrangements are sufficient to provide the Council with assurances that it is capable of retrieving key financial information in the event of a system's failure. In practice the backup system will provide a good deal of security of data for the Council on particular systems, including most of the more significant systems.

9 However, backup procedures are uncoordinated and the Council could not demonstrate that these provided fully, the minimum level of cover for all the Council's significant systems. Our review identified weaknesses in terms of documentation; test restores; configuration records of equipment (needed for restores) and the absence of management checks to confirm on a regular basis that the backup system is operating as designed and described. Prompt action is needed to address these issues and reduce the risk being carried by the Council.

Business continuity planning

10 There is a business continuity planning process that is developing plans across all Council services.

11 These have not been linked to ICT disaster recovery but the Council expects that the business continuity plans when developed will help shape the wider ICT disaster recovery requirements.

Detailed findings

Service resilience - diagnostic score

12 We have scored the Council's arrangement against a diagnostic of best practice. This contained 38 questions covering expected arrangements. We scored each question as 0 for no arrangements; 1 for partial achievement; and 2 for complete arrangements or compensating arrangements that covered the same function.

13 The Council scored 35 out of a possible 76 (46 per cent) which represents a low score overall. However, 20 of the Council’s points came from 24 points on preventative measures (83 per cent) which demonstrate an adequate level of practical, day to day, security.

14 However, it also means that the Council’s score for risk assessment and the adequacy of basic procedures was very poor; 9 out 38 points (23 per cent).

IT organisation

15 The IT department is currently being restructured. IT services which previously have been devolved to departments (like education and revenues and benefits) are now being centralised. New staffing structures have been defined but business processes are still being developed.

16 This means that although the IT staff are now within a centralised management structure, for all practical purposes ICT operations are still being controlled at department level.

IT security and resilience – recent improvements

17 The previous IT security manager left around December 2005. A new security manager and team were put in place in June 2006 as part of the departmental reorganisation.

18 There have been upgrades to backup arrangements (introduction of a central back up server for office applications servers); improvements to the environment of the servers (air conditioning and power supplies). Identified needs which are outstanding are a disaster recovery contract; network connections and the telephone system.

Disaster recovery

19 ICT disaster recovery is not developed. This means that the efficiency and effectiveness of the ICT service which could be provided to customer facing departments following loss of IT equipment is unknown and may not meet the needs of those departments.

20 There is no ICT disaster recovery plan. Activities would be decided there and then if there was a disaster affecting the ICT service.

21 There is a project to create a disaster recovery plan but this has not progressed due to the lack of an ICT security manager.

Backups

22 Backup arrangements appear adequate to meet the Council's requirements for the retrieval of financial information in support of the financial statements. However, arrangements are not robust and do not provide the Council with the full range of assurances over its wider efficiency and effectiveness requirements.

23 The ICT department oversees at least four approaches to backups.

- Windows and Netware servers providing email and other office type applications are backed up to a dedicated server located 1.5 miles from the main offices. This is a newly installed automatic system and can be expected to be reliable although the arrangements were not specifically tested during this review. There is documentation describing this arrangement.
- Major financial and other systems reside on UNIX and Linux servers in the ICT server farm at County Hall. These are backed up manually using tape drives attached to the machines. Tapes are stored in a safe in the ICT department across the road from the County Hall. It should be noted that in the event of a chemical spillage or similar happening it is possible that both County Hall and the tape safe will be inaccessible. There is documentation describing this arrangement and the safe containing backup was viewed during this review.
- There are a number of significant systems which are backed up by other methods. These include Education, Social Services and Revenues and Benefits. A document describing the arrangements for backing up Revenues and Benefits has been supplied hence we are unable to comment on the robustness of these arrangements.
- Some back up tapes are also stored off site in banks.

24 There is no overall documentation describing all systems that are backed up; the various backup methods; the locations of backups; and the management checks to confirm whether arrangements are operating correctly.

25 Management does not check that arrangements are operating correctly.

26 There is no configuration management system that holds details of the hardware, operating systems and applications systems that are being backed up. However, configuration details are held informally in spreadsheets residing on office systems; and some backups include application and operating systems as well as data files. There is an intention to introduce ITIL standards for configuration management.

27 There are no test restores of backups; although some tapes are verified after being taken; and there have been some partial restores for live operational reasons.

Business Continuity Planning

28 There is a business continuity manager and a project in hand to put in place business continuity plans for each of the departments of the council. This is not linked to the ICT disaster recovery plan. It will however help the ICT department prioritise which services should be recovered first; in which order; and in what timescale. This will be useful in helping the ICT department draw up an effective and business orientated disaster recovery plan.

Recommendations
Improvements to backup regime
R1 Create one document on all significant information systems and how they are backed up.
R2 Review this information to ensure backups and storage arrangements are sufficient.
R3 Maintain configuration details of systems that are backed.
R4 Perform test restores of backups as part of a quality control system.
R5 Monitor backup arrangements to ensure they are working.
Disaster recovery
R6 Create a basic disaster recovery system and document it.
R7 Revisit this system and documentation iteratively to create further improved versions of disaster recovery plans.
R8 Link disaster recovery plans to organisation wide business continuity planning.

Appendix 1 – Action Plan

Page no.	Recommendation	Priority 1 = Low 2 = Med 3 = High	Responsibility	Agreed	Comments	Date
	Improvement to backup regime					
8	R1 Create one document on all significant information systems and how they are backed up.	3	Dave Booth	Yes		October 2006
8	R2 Review this information to ensure backups and storage arrangements are sufficient.	3	Dave Booth	Yes		December 2006
8	R3 Maintain configuration details of systems that are backed.	2	Jason Fuller	Yes		November 2006
8	R4 Perform test restores of backups as part of a quality control system.	2	Jason Fuller	No	We currently do not have spare capacity in terms of test equipment. However we are reviewing and updating a Business Case on 'Server Recovery' and will include that here.	September 2007
8	R5 Monitor backup arrangements to ensure they are working.	2	Dave Booth	Yes	To be transferred to Service Desk as part of their responsibilities.	February 2007
	Disaster recovery					
8	R6 Create a basic disaster recovery system and document it.	3	Dave Booth	Yes	Create the basis of Disaster Recovery plan as per advice from this report, by date shown.	December 2006
8	R7 Revisit this system and documentation iteratively to create further improved versions of disaster recovery plans.	2	Dave Booth	Yes	This will to enhance the Disaster Recovery plan to meet Council's D/R Plans.	July 2007
8	R8 Link disaster recovery plans to organisation wide business continuity planning.	3	Dave Booth	Yes		August 2007