CARLISLE CITY COUNCIL
www.carlisle.gov.uk

AUDIT COMMITTEE

Committee Report

Public

Date of Meeting: **2 August 2006**

Title: **DISASTER RECOVERY AND BUSINESS CONTINUITY**

Report of: **The Director of Corporate Services**

Report reference: **FS36/06**

Summary:

The purpose of this report is to report on the impact of the January 2005 flood on business continuity plans within Financial Services.

A full Internal Audit review has just recently been carried out into the Council's Business Continuity arrangements and a summary of this report and recommendations is also appended for information.

Recommendations:

Members are asked to note the actions being taken within Financial Services to limit the damage in the unfortunate situation of another such loss.

Members are also asked to note and comment on the Internal Audit review into the Council's overall Business Continuity arrangements.

Contact Officer: Angela Brown   **Ext:**   7299

Note: in compliance with section 100d of the Local Government (Access to Information) Act 1985 the report has been prepared in part from the following papers: None

To: The Chairman and Members of the   FS36/06
        Audit Committee
        <u>2 August 2006</u>

<u>DISASTER RECOVERY AND BUSINESS CONTINUITY</u>

1.   <u>Introduction</u>

1.1   Members of the Audit Committee on 17 July 2006 requested an update on business
        continuity arrangements within Financial Services following the impact of the loss of
        paper based records in the January 2005 floods.

1.2   A full Internal Audit review has just recently been carried out into the Council's
        Business Continuity arrangements and a summary of this report and
        recommendations is also appended for information.

2.   <u>Financial Services Business Continuity Arrangements</u>

2.1   Generally speaking, the vast majority of financial records are now kept in an
        electronic format and recovery of these records following the flood was for the most
        part extremely quick and efficient. This was particularly important because the
        disaster happened in the middle of the budget cycle. Although there was an
        inevitable short delay in the meetings process, due to the need to concentrate on
        disaster recovery, on the whole the immediate inconvenience caused by the flood
        was relatively small in that respect. Had the disaster happened some years earlier,
        before the advent of electronic data storage etc, the problems would have been far
        greater.

2.2   However as members are aware, the loss of paper based records going back seven
        or more years has caused some significant problems for the service. For example:

        -   Loss of bank statements. Photocopies of paper statements are provided as
            audit evidence of when a transaction passed through the bank account and the
            Audit Commission had to be convinced that a report from ICON (the Council's
            Income Management system) could be accepted for this purpose. The paper
            statements were annotated as items were identified to isolate queries. This is
            important when an item may refer to a paying in slip for more than one day's
            income.

- Loss of first manual attempt at bank reconciliation. All original coding sheets from April 2004 were being analysed for method of payment then cross checked to the general ledger and the bank statements. Due to the flood all original documents were lost as were papers to support the work undertaken to identify over 10,000 transactions that had been tracked from income systems to the general ledger.

- Loss of system implementation notes. Manual notes were made during implementation of both the general ledger and bank reconciliation systems but due to other priorities these were not converted into an electronic format. The value of this information is that it ensures the logic of decisions is continued. Procedures and manuals are now created electronically wherever possible.

- Creditor invoices. The authority is obliged to keep primary records such as invoices for six years after the end of each financial year. In practice the immediate past year is often referred to for audit and other purposes but thereafter such documents are only rarely revisited. Should a query arise, suppliers would have to be contacted or the information sought by other means. There is an obvious time and inconvenience factor in this process though by its nature, this problem will decrease as time passes.

- Adjustment A records. Kept in the basement were working papers on final accounts and estimates dating back many years. Of necessity these records were all manually based and though only occasionally consulted, they were an irreplaceable source of information. A technical issue has now arisen regarding the audit of the accounts (Adjustment A) which to be properly addressed would require access to working papers dating back to 1990 or even before. These records are lost forever and a note to this effect has been prepared as part of the audit process. A similar caveat would apply to any other query that might arise in relation to an audit issue that required access to old working papers. More formal published financial records dating back over a hundred years were also lost but copies of these are in general also held by the County Library and/or the County Archives so that such information is not irretrievable should it be required.

- Leasing Information. The Council held a considerable amount of manual data relating to leasing agreements which had been entered into over many years. Ironically a major exercise had recently been completed to rationalise and consolidate these records and this data was lost.

2.3   The impact of the loss of these paper based records will be felt for some time as each time a query is received involving these lost records, officers have to spend significant time either reconstructing the files or obtaining the information by other means. For example, virtually all records relating to past insurance claims were lost but in the main the information is replicated in the records of the Council's insurers (St Paul Travelers and Zurich Municipal) and nearly all their own recent data is held electronically. Occasionally queries are received dating back very many years, even prior to the 1974 reorganisation of local government and these can pose greater problems although even they can eventually be overcome in most cases.

2.4   Following the flood, finance officers have been instructed to ensure all records wherever possible are kept and filed in electronic format though in practice, as has been seen, this is merely the extension and formalisation of an existing process. In particular the Document Image Processing review will in future ensure that all creditor invoices are scanned into the system and paper invoices will not need to be retained. Unfortunately this project has been delayed due to the impact of the delay on the 2004/05 Audit and problems with the bank reconciliation system, but is intended to commence in the current financial year.

3.   Conclusions

3.1   Following the flood, the vast majority of financial systems and information were re-established very quickly and normal service levels resumed.

3.2   Problems were however, and continue to be, experienced regarding the loss of hard copy paper records going back seven or more years.

4.   Recommendations

4.1   Members are asked to note the actions being taken within Financial Services to limit the damage in the unfortunate situation of another such loss.
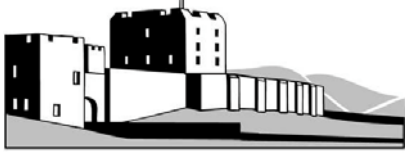
4.2   Members are also asked to note and comment on the Internal Audit review into the Council's overall Business Continuity arrangements.

ANGELA BROWN
Director of Corporate Services

Contact Officer: Angela Brown   Ext: 7299

Internal Audit Services

Audit of Disaster Recovery & Business Continuity (Including IT)

Systems Review

Corporate Services

Final Report

25 July 2006

Document Ref:	C:\DOCUME~1\moragd\LOCALS~1\Temp\FS36-06 (Appendix) Audit Report BCP.doc

Recipient of Report	Action Required	Mgmt Summary	Applicable Section(s) of Matters Arising	Appendix B to note
Director of People, Policy & Performance / Deputy Chief Executive	-Note action required for follow up in approx. 6 months	Full Summary	All Sections	B (i) B (ii) & (iii) (for info only)
Head of IT Services	-Note action required for follow up in approx. 6 months	Full Summary	All Sections	B (ii) B (i) & (iii) (for info only)
Head of Finance, Development & Support Manager	-Note action required for follow up in approx. 6 months	Full Summary	All Sections	B (iii)
Director of Corporate Services	Draft & Final report – for info only	Full Summary	All Sections	All
Audit Committee	Final report – for info only	Full Summary	None	All

1. Reason for the Audit

1.1. The audit was undertaken as part of the agreed Audit Plan for 2006/07.

2. Background Information / Summary of the Audit Area

2.1. Business Continuity Management (BCM) is not just about disaster recovery, crisis management, risk management or IT. It is a business issue, which presents the opportunity to review the way the Authority performs its processes, to improve procedures and practices and increase resilience to interruption and loss.

2.2. BCM can be defined as a process of anticipating incidents which will affect critical functions and activities of the Authority, and ensuring response to any such incident in a planned and rehearsed manner.

2.3. There are 5 main steps to BCM which are:-

   1. **Understanding the Business** – Using business impact and risk assessment, identifying the critical deliverables and enablers in the Authority, evaluating recovery priorities and assessing the risks which could lead to business interruption and/or damage to the Authority's reputation.

   2. **Continuity Strategy** – determining the selection of alternative strategies available to mitigate loss, assessing the relative merits of these against the business environment and their likely effectiveness in maintaining the Authority's critical functions.

   3. **Developing the Response** – Improving the risk profile through improvements to operational procedures and practices, implementing alternative business strategies, using risk financing measures including insurance and building Business Continuity Plans (BCP).

   4. **Establish the Continuity Culture** – Introduction of the BCM / BCP process by education and awareness of all employees, customers and suppliers.

   5. **Exercising & Plan Maintenance** – ongoing plan testing, audit, managing and updating of the BCP and its processes.

2.4. Why the need for a Business Continuity Plan?

   - The Authority's customers expect continuity of supply in all circumstances.
   - The Authority's employees and suppliers expect the Authority to protect their livelihoods.
   - The Authority's reputation is at risk if there is no BCP.
   - It is implicit in good Corporate Governance and demonstrates best practice in business management.
   - Customers and employees expect management to be fully in control, and be seen to be in control, of any crisis.
   - It is now a requirement for the Use Of Resources Assessment.

2.5.   Before implementing a BCP the following should be taken into consideration:

- Involve everyone in the Authority.
- Select a "board level" champion at Senior Management Level – to demonstrate top-level commitment.
- Ensure that the BCM / BCP process mirrors the Authority's changing and developing needs.
- Build on existing management procedures, particularly risk management and contingency activities.
- Audit and maintain the BCP / BCM process continuously to ensure that it becomes an integral part of the Authority's culture.

3.   Scope of the Audit

3.1.   Audit testing and verification has been carried out to form an opinion over the adequacy of systems and controls in place relating to the risks identified. Key areas for review are:

Section of Report (Matters Arising)	Area Examined
1.	Ownership & Management
2.	Planning & Prevention
3.	The Corporate Plan
4.	IT Users' Plan
5.	Resourcing & Training
6.	Testing the Plan

4.   Associated Risks of Providing this Service/Function

4.1.   Examination of the Corporate Risk Register noted the following identified risk:

Ref	Risk Description	Risk Score
11	Failure to have robust Business Continuity Planning arrangements Severe impact on business/provisions of services.	8

5. Overall Conclusion of the Audit Review

5.1. Following the recent re-organisation within Carlisle City Council, maintenance of the Business Continuity Plan now falls under the responsibility of the People, Policy & Performance Directorate, however no resources or budget has been allocated to this. After the flood in January 2005, a BCP Project Co-ordinator was brought in by the Council to review the BCP. This review was going to be conducted in 2 stages. Stage 1 was to review the general format of the Plan and the type of information it contains. It was also to determine whether the BCP has proved to be adequate and effective to anticipate risks and respond to critical business issues, and manage and monitor the recovery process. The conclusion of Stage 1 was reported to the Corporate Management Team (CMT) on 25/07/05. Stage 2 was to review and update (in depth) the BCP itself, drawing upon experience and lessons learned about how to improve recovery strategies and action plans. To date Stage 2 has not been implemented.

5.2. It is of prime importance that this Authority's Disaster Recovery and Business Continuity Plan, including IT, should be reviewed and updated as a matter of urgency, once this has been implemented and agreed by SMT (Senior Management Team) and the Corporate Resources Overview and Scrutiny Committee. Testing, maintaining and updating the Plan in line with current business requirements will be of high importance as will the ongoing training of key officers to ensure that they are able to carry out their individual roles effectively in the event of an emergency.

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (i)

Action Plan for Business Continuity Planning, People, Policy & Performance Directorate

Responsible officer for implementation is the Director of People, Policy & Performance.

This action plan will be followed up in approximately 6 months time. Please note that the outcome of the follow up will be reported to the Audit Committee.

Ref	*Issue*	*Recommendation*	*Grade*	*Action to be Taken (including responsible officer for overseeing the implementation)*	*Level of Risk (H, M or L)*	*Target Date*
1A	The BCP is out of date and not all Service Areas have fed in or are included in the BCP.	It is recommended that all Directors should be responsible for creating and / or updating their BCP for their service areas as a matter of urgency. The plans should be completed using an agreed corporate format to ensure consistency. Once these have been completed, the Director of People, Policy & Performance should ensure that all the plans are amalgamated into one overall BCP for the Authority.	A	In discussion with Marsh to procure support to develop a new BCP that reflects the new structure and corporate priorities. Responsible Officer – Deputy Chief Executive	H	Oct 06
1B	The BCP is out of date.	As soon as the overall BCP has been completed the Plan should go to SMT and the Corporate Resources Overview and Scrutiny Committee to be agreed.	A	Agreed Responsible Officer – Deputy Chief Executive	M	Dec 06

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (i)

1C	The BCP is not currently reviewed or updated.	Once the BCP has been completed and agreed a procedure should be implemented and an Officer made responsible for ensuring that it is regularly reviewed and any relevant updates completed. All major changes/updates should then be reported to SMT and the Corporate Resources Overview and Scrutiny Committee. Key officers should also be advised of any changes.	A	Agreed Responsible Officer – Deputy Chief Executive	M	Mar 07 – every 6 months
1D	The BCP is currently not tested.	An Officer should also be responsible for testing the BCP, these procedures should be implemented and tested on a regular basis and the outcome of the testing should be documented and reported to SMT and the Corporate Resources Overview and Scrutiny Committee.	A	Agreed. Testing arrangements to be advised by Marsh Responsible Officer – Deputy Chief Executive	M	Mar 07 - annually

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (i)

1E	There is currently no master emergency Key Officer contact document for the BCP.	It is recommended that the laminated Emergency Planning and Out of Hours Council Services/Contact Information document be amalgamated so that it can be used as the emergency contact list for the Emergency Planning Response Plan and the BCP.	A	Agreed Responsible Officer – Deputy Chief Executive	M	Sep 06
1F	Not all the individual directorates BCP's clearly state, which Officers are responsible for completing individual tasks.	All the individual directorates BCP's should be updated to clearly state which officers and their individual team members who are responsible for completing individual tasks.	A	Agreed Responsible Officer – Deputy Chief Executive	H	Nov 06
1G	There is currently no applicable links with the BCP and the Emergency Planning Response Plan.	Clear links to the Emergency Planning Response Plan should be transparent with the BCP where applicable.	B	Agreed Responsible Officer – Deputy Chief Executive	M	Dec 06
1H	Key Services / priorities to both the public and the Authority are not identified and prioritised within the BCP.	Key Services/priorities to both the public and the Authority should be identified and prioritised within the BCP.	B	Agreed Responsible Officer – Deputy Chief Executive	M	Oct 06

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (i)

1I	It is understood that there are no emergency packs prepared in the event of an emergency.	Consideration should also be given to preparing an emergency pack for key service areas, for example manual receipts etc for the Customer Contact Centre.	C	Agreed Responsible Officer – Deputy Chief Executive	L	Dec 06
3C	The Business Recovery Management Team detailed in the BCP is out of date.	It is recommended that the Business Recovery Management Team, which is detailed in the BCP, be updated as soon as possible.	A	Agreed Responsible Officer – Deputy Chief Executive	H	Aug 06
5A	Key Officers featured in the BCP have not received any training since the flood in January 2005.	Once the Disaster Recovery and BCP has been updated and agreed it is recommended that the Director of People, Policy & Performance ensures that all key officers fully understand their allocated roles and that they receive adequate training to ensure that they can effectively fulfil that role in the event of a disaster/emergency.	A	Agreed Responsible Officer – Deputy Chief Executive Will require a budget	M	Apr 07

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (ii)

Action Plan for IT Services, Corporate Services Directorate

Responsible officer for implementation is the Head of ICT.

This action plan will be followed up in approximately 6 months time. Please note that the outcome of the follow up will be reported to the Audit Committee.

Ref	Issue	Recommendation	Grade	Action to be Taken (including responsible officer for overseeing the implementation)	Level of Risk (H, M or L)	Timescale
2A	The back up tapes are not tested on a regular and structured basis	It is recommended that the back up tapes should be regularly tested to establish if the data could be read and restored, in accordance with an agreed programme of testing.	A	A comprehensive and auditable plan for testing backup tapes will be created and implemented. Application & Information Manager	H	December 2006
2B	The BCP does not include the priority order that IT systems should be recovered in the event of a disaster.	It is recommended that systems should be completed in order of importance so that the critical systems are clearly identifiable this should be included in the BCP.	B	BCP to Rank the systems to be recovered in a priority order as determined by the Business Systems Inventory. Head of ICT	L	December 2006

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (ii)

3B	An alternative method has not yet been agreed for replenishing the main IT server in the event of a disaster.	It is recommended prior to the main IT server recovery contract expiring later this year that an alternative method is agreed and implemented.	B	Agreed. Head of ICT.	H	November 2006
4A	There is no requirement for IT users (service areas) to create their own IT disaster recovery and BCP.	Consideration should be given to the IT Users (service areas) creating their own IT disaster recovery and BCP to reflect their business areas. Once completed this could form part of the Authority's overall BCP.	B	Head of ICT has considered the issue and concluded that the most effective method of provision of IT Disaster Recovery is through central planning as part of the corporate Disaster Recovery & BCP planning. Head of ICT.	L	Complete

Audit of Disaster Recovery & Business Continuity (Including IT)
Final Report 2006/07
Summary of Agreed Actions

APPENDIX B (iii)

Action Plan for Development & Support Services, Corporate Services Directorate

Responsible officer for implementation is the Head of Financial Services.

This action plan will be followed up in approximately 6 months time. Please note that the outcome of the follow up will be reported to the Audit Committee.

Ref	Issue	Recommendation	Grade	Action to be Taken (including responsible officer for overseeing the implementation)	Level of Risk (H, M or L)	Timescale
3A	There are no agreements in place with suppliers to replenish equipment including IT in the event of an emergency.	It is recommended that agreements with framework suppliers should include the recovery process in the event of a disaster / emergency, this should include IT equipment.	B	Corporate Procurement are currently reviewing the existing supplier arrangement with the Cumbria Procurement Initiative (CPI). Disaster Recovery forms part of this review. Development & Support Manager	M	November 2006
5B	The emergency procurement arrangements / procedures which were drafted for use following the 2005 flood are not included in the BCP and the key "authorising" Officers have not been reviewed and updated.	It is recommended that the emergency procurement arrangements / procedures which were drafted for use following the 2005 flood should be updated and refered to in the BCP. The Corporate Procurement Section should take responsibility for these emergency procedures and this would include activating them and co-ordinating any emergency spending.	A	Corporate Procurement to review existing Emergency Procurement procedures as detailed earlier in 3A. Development & Support Manager	H	November 2006