Deloitte.

Dacorum Borough Council – Final Internal Audit Report

IT Business Continuity and Disaster Recovery

Distribution list:

Chris Gordon – Group Manager Performance, Policy and Projects

John Worts – ICT Team Leader

Key dates:

Date of fieldwork: June/July 2011

Date of draft report: September 2011

Receipt of responses January 2012

Date of final report: January 2012

This report has been prepared on the basis of the limitations set out in Appendix C.

This report and the work connected therewith are subject to the Terms and Conditions of the Contract between Dacorum Borough Council and Deloitte & Touche Public Sector Internal Audit Limited. The report is produced solely for the use of Dacorum Borough Council. Its contents should not be quoted or referred to in whole or in part without our prior written consent except as required by law. Deloitte & Touche Public Sector Internal Audit Limited will accept no responsibility to any third party, as the report has not been prepared, and is not intended for any other purpose.

Contents

1. Executive summary

1.1. Background

This audit forms part of the agreed 2011/12 Internal Audit Plan with Dacorum Borough Council.

Dacorum Borough Council established a Business Continuity Plan in March 2008 and a Systems Continuity Plan for ICT Systems (Disaster Recovery Plan) in 2008. The Civil Contingencies Act (2004) places a statutory duty on local authorities, and all Category 1 responders, to maintain Business Continuity Plans to ensure that they can continue to perform their functions in the event of an emergency, so far as is reasonably practical.

The Council's Business Continuity Plan objective is to help ensure that disruption to business services is kept to a minimum and to allow for the phased continuation of key Council services in line with the established plan.

The Council has a contract with ICM Ltd. Who are specialists in recovery services. Depending on the type of disaster experienced, DBC can invoke the Disaster Recovery Plan in one of the following ways:

- Relocation to ICM recovery centre.

  In the event that the Civic Centre becomes unusable, the minimum operations required can be re-located to the ICM site, located in Uxbridge, Middlesex. This site will be available for the use of the Authority within 2 hours of invocation.

- Provision of hardware to the Authority.

  In the event of failure of one or more of the specified servers within an otherwise still functioning server room, ICM can supply servers, to be delivered to the Civic Centre.

- Provision of mobile units.

  In the event of a large scale failure of the Civic Centre computer suite, while the remainder of the building is unaffected, ICM will provide a mobile unit, sited at the Civic Centre. The mobile unit has built-in generators, but preferably should take power from the Civic Centre.

1.2. Objectives and Scope

The overall objective of this audit was to provide the Members, the Chief Executive and other officers with reasonable, but not absolute, assurance on the adequacy and effectiveness of the key controls relating to the following areas:

- A Disaster Recovery Plan (IT Business Continuity Plan) exists with the exact steps to be covered if a disaster event occurs.
- Critical systems required to be recovered following a disaster event have been identified.
- Single points of failure have been identified.
- Council service Business Continuity Plans are fully linked with IT disaster recovery arrangements.
- Server infrastructure includes testing of the ability to recover systems; and
- Tape backups are completed and taken off-site.

1.3. Summary assessment

Based on the work undertaken, as detailed in the 'Audit Objective and Scope', we found that whilst there is a basically sound system of internal control there are weaknesses in the links between IT Disaster recovery arrangements and Council Service Business Continuity Plans. Recovery Time Objectives for critical services and key IT systems need to be identified to allow appropriate strategies to be put in place.

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below.

Evaluation Assessment	Testing Assessment
Substantial	Limited

Management should be aware that our internal audit work was performed according to UK Government Internal Audit Standards which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board.

Similarly, the assessment gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board. The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the control environment for IT Disaster Recovery is shown in Section 3.

1.4. Key findings

We have raised seven priority 2 recommendations, where we believe there is scope for improvement within the control environment and one priority 3 recommendation which is considered to be of a minor nature, but needs to be addressed.

These are summarised below:

- Third party agreements/arrangements where the Council rely on key suppliers and services with respect to disaster recovery for all the critical IT systems have not been included within the IT System Continuity Plan;

- The ICT Systems Continuity Plan does not have clear escalation procedures and details of tasks that need to be carried out during the course of a disaster event;

- There are no salvage and relocation procedures in place for the recovery of Council systems in a disaster situation;

- The current ICT Business Continuity Plan needs to be revised to meet the Dacorum template standards. The role of ICT in other Service Business Continuity Plans needs to be further co-ordinated;

- Recovery Time Objectives (RTO) have not been identified for the recovery of critical services and key IT systems. RTO's assigned to critical activities allow management to recover key systems in a way that minimises the impact on the Council and that is in line with the expectations for recovery from Council services;

- While Dacorum have identified points of failure regarding business system knowledge, the SOCITM review in November 2010 noted a potential weakness regarding the Dacorum Internet site;

- The output from Disaster Recovery tests is not formally presented to management. Management should have the opportunity to comment or make recommendations based on test outcomes; and

- Backup hardware is eight years old and is becoming unreliable. We note that replacement solutions are currently being investigated.

Full details of the audit findings and recommendations are shown in Section 4 of the report.

1.5. Management Response

We have included a summary of the management responses in our Final report.

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this audit.

2. Scope of assignment

2.1 Objective

The objective of the internal audit is to identify the controls the Council has in place over the IT Business Continuity and Disaster Recovery and to provide assurance over the recovery options for IT Systems to ensure they are in line with Council service recovery objectives.

2.2 Approach and methodology

The following procedures were adopted to identify and assess risks and controls and thus enable us to recommend control improvements:

- Identification of the role and objectives of each area;
- Identification of risks within the systems, and controls in existence to allow the control objectives to be achieved; and
- Evaluation and testing of controls within the systems.

2.3 Areas covered

In accordance with our agreed terms of reference, our work was undertaken to cover the following audit areas:

- A Disaster Recovery Plan (IT Business Continuity Plan) exists which details the processes to be followed in the event of a disaster, is updated following major system and personnel changes and the accountability for updating the plan has been assigned to a nominated officer. The Disaster Recovery Plan includes the latest system configurations and provides information regarding the exact steps to be followed in the event of a disaster event.
- The Council through agreement with individual service departments have agreed the critical systems required to be recovered in the event of a disaster event.
- Single Points of Failure have been identified and an assessment has been completed of the level of risk. This also looks to identify where a resilient environment is in place.
- Council service Business Continuity Plans are fully linked with IT Disaster Recovery arrangements.
- The Server infrastructure includes testing of the ability to recover systems.
- Tape back ups are completed and are taken to an off-site location to provide additional resilience in the event of a disaster event.

3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

Control Objectives Assessed	Design of Controls	Operation of Controls	Recommendations Raised
Disaster Recovery Plan	✓	≈	**Recommendations1,2, 3 &4**
Critical systems to be recovered	✓	≈	**Recommendation 5**
Single points of failure	✓	≈	**Recommendation 6**
BCP plans linked to IT Disaster recovery arrangements	✓	✓	**None**
Server Infrastructure Recovery	✓	≈	**Recommendation 7**
Tape Backups	✓	≈	**Recommendation 8**

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

4. Observations and Recommendations

Recommendation 1: Third party agreements (Priority 2)

Recommendation

Management should ensure that, where systems are supported by third party suppliers, the reliance on the third party to provide support during incidents should be clearly defined within the ICT Systems Continuity Procedure including details of support hours and key supplier contacts.

Observation

Including third party agreements and their involvement with respect to business continuity and disaster recovery within the ICT Continuity Procedures helps to ensure that the Council has identified where reliance is based on third parties to supply and support systems to the Council. This also helps to ensure that third party responsibilities with regards to the recovery of Council IT systems are defined.

It was determined that third party agreements with respect to business continuity and disaster recovery for all the critical systems have not been included in the IT Systems Continuity Plan.

Review of the Business Continuity Plan confirmed that contact details for some third parties as well as the recovery site have been included in the plan, though this could be strengthened by including any arrangements with regards to the support provided during an incident by third parties for all the business critical systems within the Systems Continuity Procedure.

Where third party responsibilities in relation to disaster recovery are not clear or agreed with the Council, there is a risk that reliance may be placed on a third party without the requirement being understood or without them being made aware of their responsibilities in assisting in the recovery of Council services. This may lead to delays during recovery of the Council's systems.

Responsibility

John Worts - ICT Team Leader

Management response

Agreed.

There will be a review of ICT BCP 3rd Party contact details and responsibilities. We will also review the ICM setup, and plan an off-site invocation.

Completion: 31/3/12

Recommendation 2: Disaster Escalation Procedure (Priority 2)

Recommendation

The ICT System Continuity Plan should have clear escalation procedures that build on the flowcharts in the current version. Tasks that need to be carried out such as off-site storage procedures and server shutdown tasks should be more explicitly defined.

Observation

Documenting the processes that should be followed in the event of a disaster assists in providing clarity in what the expected steps of escalation would be required to be followed during the course of a disaster event. Clarifying specific procedures that need to be followed helps to identify where processes should be followed in a disaster event.

The current ICT systems continuity plan contains flowcharts setting out the procedure for start, standby, invoke and Stand-down. The plan is in the process of being revised to fit the Borough Council template and needs to have clear escalation procedures that build on the flowcharts in the current ICT systems continuity procedure.

Failure to identify the processes that require following in the event of a disaster could mean that there is no clear guidance for staff on the process to be followed. This could mean that key tasks are not followed in a disaster event.

Responsibility

John Worts - ICT Team Leader / Jennifer Young – Civil Contingencies Co-Ordinator

Management response

Agreed. We will review and amend the ICT BCP, for escalation procedures. This will be tested with BCP Officer

31/3/12

Recommendation 3: Salvage Procedures (Priority 3)

Recommendation

A salvage and relocation plan should be clearly documented and included in the Disaster Recovery Plan on the procedures to retrieve items from the affected site/system.

Once established, the documented procedure should be distributed to the relevant disaster recovery team members and training organised to ensure that they understand their responsibility for managing the process.

Observation

Documented salvage processes help to establish the method for obtaining IT data and hardware from an affected disaster site and helps to identify where such hardware is located.

There are currently no salvage and relocation procedures in place. Salvage procedures would set out the procedure to retrieve items from the effected site/system which are not fully affected by the disaster and could be recovered.

Failure to identify salvage arrangements could mean that there is not a process currently in place to recover unaffected equipment from the disaster site.

Responsibility

John Worts - ICT Team Leader

Management response

Agreed. We will evaluate the requirement for a salvage policy / procedure.

31/3/12

Recommendation 4: Disaster Recovery Procedures (Priority 2)

Recommendation

A Business Continuity Plan for ICT, that meets the Dacorum template standards, should be completed and distributed to key staff. All elements of the Disaster Recovery Plan needs to be tested periodically to help ensure that any gaps in the plan or issues resulting from the test can be identified and corrected in a timely manner.

Observation

The provision of IT systems underpins other service area plans and the ICT Recovery Plan should support the assumptions and requirements of these plans and the Corporate Business Continuity Plan.

The updating of Service area business continuity service plans is currently underway and a spreadsheet is utilised to manage responses and shows progress to date. ICT had not responded at the time of the audit fieldwork. The spreadsheet also highlights the checking progress with ICT with regards to the IT systems that each service has in their Business Continuity plans. The Business Continuity plans are not "complete" until this is completed. The current ICT Systems Continuity Procedure does not fit the Dacorum template and the Service Support Manager has had a meeting with the Civil Contingencies Co-ordinator to enhance the current plan in order that it meets the Corporate standard. Currently, there is no clear link between ICT and the service business continuity plans.

Unless an element of co-ordination is developed between ICT and departments to which they supply IT systems, with regard to the recovery of systems, there is a risk that IT systems will not be recovered on a timely basis.

Responsibility

John Worts - ICT Team Leader

Management response –

Agreed. We will complete a Gap Analysis of ICT BCP requirements – 31/3/12

Recommendation 5: Disaster Risk Assessment (Priority 2)

Recommendation

The Recovery Time Objectives (RTO) should be identified for the recovery of critical services and key IT systems. This should ensure that recovery options are put in place to help ensure that IT systems can be recovered in line with the expectations of recovery established within the Council Services Business Continuity Plans.

Based on this information, appropriate strategies (e.g. outsourcing, relocation, considerations, resilience capabilities and re-engineering processes) should be evaluated and included in within the Disaster Recovery Plan to achieve the required RTO.

Observation

The development of approved Recovery Time Objectives helps to set out the requirements for system recovery for Council systems. This helps to ensure that the expectations for the recovery of systems has been established and communicated to relevant Council services.

Recovery Time Objectives have not been identified for the recovery of critical services.

Where the Council has not implemented appropriate RTOs that are in line with the expectations for system recovery that are set out in Council service BCPs, there is a risk that Council services that rely heavily on IT may not be able to restore systems in the expected timeframe.

Responsibility

John Worts - ICT Team Leader

Management response –

Agreed, Recovery Time Objectives' to be set after establishing a test invocation – currently on hold due to lack of staff resources. (Test Invocation to be reviewed by 31/3/12.

Recommendation 6: Single Points of Failure (Priority 2)

Recommendation

Management should ensure that any known or identified Single Points of Failure in the Council's network or IT Infrastructure should be formally logged and subjected to a periodic review. This should include a strategy to remove all single points of failure and a process to log the risk of each point of failure to help ensure that appropriate risk mitigation strategies can be put in place.

Observation

A Review of the Council's infrastructure to identify and log all single points of failure within ICT would help the authority improve resilience in its network. This would also allow appropriate risk mitigation strategies to be put in place over all identified single points of failure.

Dacorum have identified single points of failure that relate to business system knowledge relating to Northgate Revenues and Benefits, Housing – Orchard system and EIS (HR/Payroll system). Some risk mitigation strategies have been identified. Review of the SOCITM ICT Service Review identified some additional single points of failure for which there have not been appropriate risk mitigation strategies put in place. The SOCITM review noted that Dacorum hosts its Internet site using a server in the Civic Centre which has a number of single points of failure including the server and the connection to the Internet.

Failure to review all single points of failure would mean that the Council has not fully logged all areas of its infrastructure where failure of a single component could cause significant disruption to Council IT Systems and services. Failure to put appropriate risk mitigation strategies in place would mean there is no identified plan for how these single points of failure may be removed from the Council infrastructure.

Responsibility

John Worts - ICT Team Leader

Management response –

Transition towards a shared service arrangement with another partner will mitigate the Single Points of failure identified in this report. Review of ICT service delivery and support structure.

December 2012

Recommendation 7: Disaster Recovery Testing (Priority 2)

Recommendation

Disaster Recovery testing should be in place to test all elements of the system recovery as set out in the agreement with ICM. We also recommend that when tests have been carried out there is evidence to show that the results are reported to senior management and that any subsequent recommendations are implemented.

Observation

Testing all elements of the Disaster Recovery Plan and the subsequent reporting to senior management helps to provide assurance that all elements of the plan have been tested and that results are escalated to the appropriate management level.

Disaster recovery tests were carried out at the ICM facility in Uxbridge in February 2009 and April 2010, however, this has not tested the option of a ‘caravan’ being supplied to the Council. The tests documented the staff involved, servers tested, backup procedure and disaster recovery procedure. The tests also documented problems and the lessons learnt. There is no evidence available to show that test results have been reported to senior management.

Failure to test all elements of the DR plan can mean that arrangements on which the Council place reliance have not been fully tested.

Responsibility

John Worts - ICT Team Leader

Management response

Agreed. This needs a test invocation – currently on hold due to lack of staff resources currently (Test Invocation to be reviewed by 31/3/12).

Recommendation 8: Tape Backups (Priority 2)

Recommendation

The Council should continue to develop alternative backup solutions to assist in the recovery of systems as the existing Tivoli back up arrangements become more unreliable.

Observation

Developing new or alternative back up strategies help to ensure that systems can continue to be backed up and that faster methods of restoring data can be implemented.

Dacorum BC use Tivoli storage manager and tape library systems for their backup solution which was installed in 2003. This requires updating as it is becoming unreliable. We understand that replacement solutions are being investigated which is prudent to ensure that a full restoration of data can continue to be carried out.

Failure to develop back up arrangements and solutions could mean that old systems become unreliable. This could increase the likelihood of back up failure.

Responsibility

John Worts - ICT Team Leader

Management response

Agreed. We are currently using a replacement Tivoli storage system and Overland tape library, until an established reliable backup solution is acquired. Implementation by June 2012

Appendix A – Reporting definitions

Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Level	Symbol	Evaluation Assessment	Testing Assessment
Full	✓	There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
Substantial	≈	Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
Limited	?	Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
Nil	✗	Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of ‘Full’ does not imply that there are no risks to the stated control objectives.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
Priority 1	Recommendations which are fundamental to the system and upon which the organisation should take immediate action.
Priority 2	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
Priority 3	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
System Improvement Opportunity	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

Appendix B – Staff interviewed

The following personnel were consulted:

John Worts	Service Support Manager
Jennifer Young	Civil Contingencies Co-ordinator
Linda Dargue	Insurance and Risk Officer
James Deane	Group Manager Financial Services
Mark Parrott	Technical Support officer

We would like to thank the staff involved for their co-operation during the audit.

Appendix C - Statement of responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system. The assurance level awarded in our internal audit report is not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Deloitte & Touche Public Sector Internal Audit Limited

London

January 2012

In this document references to Deloitte are references to Deloitte & Touche Public Sector Internal Audit Limited.

Registered office: Hill House, 1 Little New Street, London EC4A 3TR, United Kingdom. Registered in England and Wales No 4585162.

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte LLP, the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Member of Deloitte Touche Tohmatsu Limited