Audit Committee Agenda

7.30pm, Tuesday 30 September 2014

Bulbourne Room, Civic Centre, Hemel Hempstead

The Councillors listed below are requested to attend the above meeting, on the day and at the time and place stated, to consider the business set out in this agenda.

Adshead
Doole
Douris
Elliot
Harris
Taylor (Chairman)
W Wyatt-Lowe

Substitute Members: Councillors Anderson, N Hollinghurst, Marshall, McKay and Townsend.

For further information, please contact Jim Doyle on Tel: 01442 228222, Email: jim.doyle@dacorum.gov.uk Information about the Council can be found on our website: www.dacorum.gov.uk

PART I

PART II

1. APOLOGIES FOR ABSENCE

To receive any apologies for absence

2. DECLARATIONS OF INTEREST

To receive any declarations of interest

A member with a disclosable pecuniary interest or a personal interest in a matter who attends a meeting of the authority at which the matter is considered -

(i) must disclose the interest at the start of the meeting or when the interest becomes apparent

and, if the interest is a disclosable pecuniary interest, or a personal interest which is also prejudicial

(ii) may not participate in any discussion or vote on the matter (and must withdraw to the public seating area) unless they have been granted a dispensation.

A member who discloses at a meeting a disclosable pecuniary interest which is not registered in the Members' Register of Interests, or is not the subject of a pending notification, must notify the Monitoring Officer of the interest within 28 days of the disclosure.

Disclosable pecuniary interests, personal and prejudicial interests are defined in Part 2 of the Code of Conduct For Members

[If a member is in any doubt as to whether they have an interest which should be declared they should seek the advice of the Monitoring Officer before the start of the meeting]

3. MINUTES AND ACTIONS

To confirm the minutes of the meeting held on 30 July 2014 and consider the actions. (Previously circulated).

4. PUBLIC PARTICIPATION

An opportunity for members of the public to make statements and ask questions in accordance with the rules as to Public Participation

5. INTERNAL AUDIT REPORTS

- Risk Management Strategy Review
- Asset management 2014

See accompanying booklet

6. INTERNAL AUDIT PROGRESS REPORT

See accompanying booklet

7. EXCLUSION OF THE PUBLIC

To consider passing a resolution in the following terms:

That, under s.100A (4) of the Local Government Act 1972 Schedule 12A Part 1 as amended by the Local Government (Access to Information) (Variation) Order 2006 the public be excluded during the items in Part 2 of the Agenda for this meeting, because it is likely, in view of the nature of the business to be transacted, that, if members of the public were present during those items, there would be disclosure to them of exempt information relating to details of Information Security and officer contact details.

APPENDIX A

AUDIT COMMITTEE: Work Programme 2014-15

MEETING DATE	DEADLINE TO MONITORING OFFICER	DEADLINE TO MEMBER SUPPORT	ITEMS:	WHO RESPONSIBLE
30 Sept 2014	17 Sept 2014	22 Sept 2014		
17 Dec 2014	3 Dec 2014	8 Dec 2014		
11 Feb 2015	28 Jan 2015	2 Feb 2015		
7 April 2015	16 March 2015	20 March 2015		

PART II

AGENDA ITEM: 8

UPDATE ON THE COUNCIL'S ICT DISASTER RECOVERY POSITION

Report for:	**Audit Committee**
Date of meeting:	**30 September 2014**
Part:	**2**
If Part II, reason:	Includes details of Information Security. Appendix contains officer contact details

Title of report:	**ICT Disaster Recovery**
Contact:	Neil Harden, Portfolio Holder for ICT Ben Trueman, Group Manager – Technology & Digital Transformation
Purpose of report:	1.To respond to the Audit recommendations for DR testing 2.To respond to Committee requests for provision of the DR plan
Recommendations	1.Testing in line with schedule within report
Corporate objectives:	
Implications: 'Value for money' implications	Financial DR testing out of hours will need to be budgeted for in 2014/15 revenue budget. Value for money
Risk implications	
Equalities implications	
Health and safety Implications	
Consultees:	

Background papers:	Draft ICT DR Procedures
Historical background *(please give a brief background to this report to enable it to be considered in the right context).*	The Committee asked that a DR plan be presented to this meeting.
Glossary of acronyms and any other abbreviations used in this report:	DR – Disaster Recovery DMZ – Demilitarized Zone RPO – Recovery Point Objective RTO – Recovery Time Objective

Background

The Audit recommendation was that ICT test and provide evidence of testing "all elements of the system recovery." Furthermore, discussion at the previous Committee meeting requested the Group Manager for Technology & Transformation provide a DR plan for this meeting.

This document represents a statement of the Council's current ICT DR position, a brief description of plans to enhance its capabilities and details of planned work to test DR procedures.

Scenarios

In understanding the Council's ICT DR requirements it is useful to review potential scenarios and understand when DBC ICT would expect to invoke DR:

Scenario 1 - Loss of access to the Civic Centre
Response: Users continue to be able to work remotely using Dacorum Anywhere. DR is not invoked.

Scenario 2 – Loss of ICT Services within Civic Centre
Response: Users continue to be able to work remotely using Dacorum Anywhere. DR is not invoked.

(This was proven following a break in the fibre connection between the Civic Centre and our primary data centre in August. As of 9th September, we also have a second connection to the primary data centre running via the secondary data centre. If the first connection fails, then services fail over to this second connection.)

Scenario 3 – Limited physical failure within primary data centre
Response: DBC runs a virtual environment, hosted on multiple physical servers and so are able to move virtual servers to different physical servers in the case of hardware failure. DR is not invoked.
(This was proven on 15th September this year when one of our physical servers failed. Affected services were restored within 30 minutes.)

Scenario 4 – Disaster (fire, flood, etc) affecting or total physical failure of our primary datacentre
Response: First response will always be to concentrate efforts on diagnosis and recovery of the primary data centre. Only if it becomes clear that this will not be feasible in reasonable time, and only after substantive consultation with senior management would we make the decision to invoke Disaster Recovery.
(NB: DBC's primary data centre is hosted within a nuclear bunker in Buckinghamshire CC's Amersham offices.)

Recent Work

In the time since the initial audit was completed, the ICT DR position has changed significantly. In line with plans for decant, the primary data centre has been moved out of the Civic Centre to be hosted by a 3rd party in a different location. In most of the scenarios described above, it is resilience rather than DR that is required. Lack of this resilience has represented the greatest risk to ICT services and so resources have been concentrated on ensuring it is now in place.

This work has included completion of the migration of systems from the Civic Centre to our primary data centre, virtualisation of physical servers and the introduction of a secondary link to that data centre.

DBC ICT has also had to undertake remedial work to address technical issues which compromised our stated DR position. Both back-up (data copied as a daily job) and replication (data copied at regular intervals throughout the day) have proved problematic, with intermittent faults, following their deployment by 3rd party consultants. These are essential elements of the disaster recovery solution and both have required major infrastructure work. Issues with both have now been resolved.

The fundamental method behind the ICT DR Plan sees DBC ICT restoring critical services to its secondary data centre using the latest available data. Unlike many businesses DBC does not rely on rely on back-up for DR purposes. Replication allows us to use a more reliably recent copy of the data and to restore from it more quickly. Back-ups are used primarily for data retrieval and only as a secondary layer of DR assurance.

In mid-July we undertook a small scale test of our DR procedure, successfully proving the concept that services can be restored within the secondary data centre using replicated data.

Current work

We are currently undertaking significant work to improve our DR position:

Description	Benefit	Delivery
Split Netscaler Devices across primary & secondary data centres	This will greatly simplify the job of enabling Dacorum Anywhere within our DR environment	Mid November
Implement VMWare Clustering, High Availability and Distributed Resource Scheduler	This will enable automatic failover of partial hardware failure (see Scenario 3) and improve operational performance	End November
Deploy new firewall at secondary data centre to enable connection to BPSN	This will enable data to be shared with central government in the event of DR invocation	End November
Enable DMZ (“Demilitarized Zone”) within DR environment	This will allow key internet based services (web self-service/e-forms & smartphones) to work in the event of DR invocation	Mid December

Long terms plans will consider a re-design of the fundamental principles of the Council’s ICT DR position, specifically looking at sharing services across both data centres so that if one fails critical services can be maintained without significant interruption.

High Level Recovery Plan

Throughout this work, the ‘High Level Recovery Plan’ (which is included within the Corporate Business Continuity Plan) has been our baseline plan in the event of a disaster. The High Level Recovery Plan features two key elements which define planned timescales around the resumption of services.

These elements are:

Recovery Point Objectives (RPOs) - these indicate the maximum age of data that should be restored in the event of disaster

Recovery Time Objectives (RTOs) - these indicate how long it is acceptable to wait for a given service to be restored.

These values are applied across tiers of systems depending on the Council’s view of their criticality. Timescales for RTOs and RPOs had previously been provided for the Business Continuity Plan by 3rd party contractors and it was essential that DBC ICT review these values, particularly in the context of issues around replication. This review process had been indicated both through DBC line management and directly to the Resilience Coordinator within Environmental Services, who is responsible for maintaining the Business Continuity Plan.

The Team Leader for ICT Operations is currently working with the Resilience Coordinator to ensure that achievable timescales for RTOs and RPOs are provided and that services are given the correct level of priority. While this is under review, an interim view of achievable RPOs and RTOs based on the existing priority of services is included within the draft ICT DR Procedures, appended to this report.

These would see Core Infrastructure restored within 3 hours with 1 hour's maximum data loss and Critical Servers restored within 6 hours with 1 hour's maximum data loss.

Testing

Until the RPOs and RTOs were reliably established, there was no baseline against which to conduct testing. We do, however, now have the following plans for DR testing in place:

Test	Description	Date
1st Desktop Test	This will be a walkthrough exercise with ICT staff ensuring familiarity and assuring the practicality of operational and technical processes	Mid-October
2nd Desktop Test	Following forthcoming work detailed above, the walkthrough exercise will be repeated to reflect the changed state of infrastructure	Late December
Core Infrastructure Testing – Network/Intranet	Out of hours work to test the fundamental network/internet functions within the DR environment	December
Core Infrastructure Testing – Exchange	Out of hours work to test our capacity to enable email within the DR environment	January
Core Infrastructure Testing – Dacorum Anywhere	Out of hours work to test our capacity to bring up Dacorum Anywhere in the DR environment	January
Full test of Core Infrastructure and Critical Servers	Full weekend testing our capacity to enable all core and critical servers within the DR environment. *NB: This is not expected to include DMZ functionality which would see a significant disruption to live web-based services (e-forms etc.)*	April *Date under review for organisational / operational requirements. Consultation with Senior Officers and Members will be undertaken nearer the date.*

Any testing beyond desktop exercises will mean the suspension of critical services. For this reason testing will only be undertaken at the weekend. The Committee should be aware, however, that a full test of all elements of the ICT DR Procedures would take more than a weekend to undertake as moving all services to DR is estimated to take 48 hours, with a further 48 to restore to the production environment. For this reason, a test of all elements within a single event is not planned.

Assuming the full test of Core Infrastructure and Critical Servers is successful then further tests of component elements will be undertaken.
All of these tests will use invocation processes as detailed in the latest version of the ICT DR Procedures. The output of all these tests (pass, fail, lessons learned etc.) will be provided as a report to DBC senior management

For completeness, the latest draft of the ICT DR procedures is appended to this report. A first live version of this document will be produced following the 1st Desktop Test in October.