

REPORT FOR:

GOVERNANCE, AUDIT AND RISK
MANAGEMENT COMMITTEE

Date of Meeting:

23rd January 2012

Subject:

IT Disaster recovery

Responsible Officer:

Carol Cutler
Director of Customer Services and
Business Transformation

Exempt:

No

Enclosures:

None

Section 1 – Summary and Recommendations

This report sets out the current arrangements and position regarding IT disaster recovery.

Recommendations:

None. This report is for information.

Section 2 – Report

Background

Disaster Recovery (DR) is the means by which an organisation secures its IT data enabling it to get up and running in the event that the primary data centre location and systems are unavailable for whatever reason. DR is part of Business Continuity preparations, the process by which an organisation ensures it can continue its business in the event of major disruption.

The foundation of DR (level 1) is to regularly take copies of system data and to store those copies in a different and secure location. This enables those systems to be restored onto alternative equipment. The problem with only having this level of DR is the time it can take to procure, set up and make available the alternative solution and the ability of the organisation to function in the meantime. It is likely to take at least a month to regain access to key systems and it is also likely to be expensive to procure in such an emergency.

The next level (level 2) therefore, is to have access to suitably configured equipment in an alternative data centre available on demand. Depending on risk and urgency there are 3 available options:-

- 1) Hot: an exact copy of the system available immediately with up-to-date data already loaded. i.e. an exact replica but not the same scale.
- 2) Warm: usually available within 24-48 hours with configured hardware but no data. The data would be loaded from the last back up.
- 3) Cold: space and connectivity available and not for our exclusive use – this can take up to 2 weeks to procure, configure and make available.

Current situation

The Council has always had level 1 DR and uses Iron Mountain to store copies securely off site. Capita took over this responsibility in November 2010 and one of the critical PI's is the completion of successful back ups.

Until 2005 the Council had no level 2 DR. As part of the Business Transformation Partnership project to introduce SAP for the major corporate systems hot DR was implemented for SAP. Capita provided a second set of servers in their West Malling data centre with mirroring of data.

Capita have tested that the mirroring is taking place as required and satisfied themselves that the service can be switched to the backup servers. For the full annual DR test required by the contract the Council has to provide a significant number of users to work over a weekend to test that the 'failover' has worked correctly. Due to the magnitude of tasks requiring weekend working by the SAP team this year the full test has not been completed. This is now scheduled to take place in February. It is only when this is completed that we can be fully satisfied that the solution works.

In 2010 when our IT was outsourced to Capita we added other elements of DR to the requirements. The level of DR required was determined following liaison with the business, to determine the speed with which they needed to regain use of their system in the event of a disaster. The contract provides:-

- 1) DR for telephony – this is at a level equivalent to ‘hot’ and the solution distributes our telephony resource over 3 sites for added resilience,.
- 2) Warm DR for Frameworki from contract start (within 48 hours)
- 3) Warm DR for the internet from contract start
- 4) Cold DR for all other key systems once transformed (within 2 weeks)
- 5) Reasonable endeavours for remaining systems

Telephony DR is in place and fully tested including user testing.

Frameworki DR is in place and fully tested including user testing.

The WAN provides multiple access point to the internet so DR is provided and has been fully tested.

Finalising the remaining DR has been delayed due to slippage in completing the transformation programme. However, Capita confirm that both space and connectivity are available and in the event of a disaster we could expect Capita to get the equipment in place as a matter of urgency.

More recently the Council has been considering an option to keep the primary data centre in Harrow in return for a budget saving. This proposal is included in the budget for 2013/4. Implementation of this would mean that the secondary data centre will be in Capita’s West Malling site rather than Laindon.

Financial Implications

None specifically related to disaster recovery.

Risk Management Implications

This report is about risk management.

Equalities implications

None.

Section 3 - Statutory Officer Clearance

Name Julie Alderson



Chief Financial Officer

Date: 9 January 2013

Name: Hugh Peart



Monitoring Officer

Date: 10 January 2013

Section 4 - Contact Details and Background Papers

Contact: Carol Cutler extension 6701

Background Papers: None.