Coventry City Council

Briefing note

To
Audit and Procurement Committee

Date
16th February 2015

Subject
IT Systems Back Up, Recovery and Data Centre Update

1 Background

At the Audit and Procurement Committee on the 20th October 2014, the outcome of the follow up audit review of IT Systems Back Up, Recovery and Data Centre was considered. Despite progress being made, Internal Audit determined that only limited assurance could be provided that effective systems were in place to manage the risks associated with the Council's arrangements for system backup and recovery.

The level of assurance primarily reflected the fact that whilst the ICT Service had put in place disaster recovery arrangements for certain key systems, this had not been informed by the views of senior management from across the Council as part of business continuity planning. As such, the risk was that current arrangements may not match the needs of the Council.

After considering these findings, the Audit and Procurement Committee requested an update in early 2015 to ensure action has now been taken in response to this report.

2 Current Position on Disaster Recovery

The wide variety of ICT systems and applications used across the Council are provided from a main data centre located in the Council House, containing over 250 servers, network storage devices, data network devices and a myriad of other equipment used to support the infrastructure. Much of the data network and storage where appropriate, has built in resilience to ensure services can continue. This and the other DR provision already in place is similar to the provision that other Local Authorities have made, and is based on the risk assessment that whilst a major incident poses a high risk to the Council, the likelihood of such an event is very low.

Over the past 5 years, a considerable amount of resource has been invested in:

- Moving the Council to a virtual server environment which a high degree of disaster recovery capability,
- A second data centre located in Nuneaton, which holds a second, test and development virtual server environment. In the event of a problem with the main data centre, the virtual environment can be failed over to this second data centre.

Other developments are also taking place including action to mitigate the impact if an individual server fails as part of our service modernisation plans. This will also involve moving servers to the Nuneaton data centre to improve resilience and in the future making greater use of “cloud based” opportunities which are virtual ways of backing up systems rather than physical locations.

Work is also underway to review and consolidate all of the applications and systems in use across the council to reduce cost and reduce the number of systems that require DR capability.

At present ICT can guarantee the recovery of the main ICT back office functions (email, Internet access, data stored on the network and access to the network). These back office functions are essential for the day to day running of the Council and our work. This therefore provides assurance that the Council does have in place arrangements to recover key data and ability to use these systems in the event of an incident. The following 7 key systems also have recovery arrangements in place:

- Agresso (Finance System)
- Resourcelink (HR/Payroll)
- CareDirector (Adult Social Care)
- Protocol (Children’s Social Care)
- CRM (Contact Centre System)
- Academy (Revenue and Benefits)
- Business Objects (Reporting system – necessary for payroll)

These 7 systems cover off the major priorities for ‘life and limb’, paying our staff, paying benefits, paying suppliers and protecting our citizens.

3 Progress since the October Audit and Procurement Committee

After the October Committee, the Internal Audit and Risk Manager met with the Assistant Director, Communities and Health and the Assistant Director, ICT, Transformation and Customer Services to agree how this matter would be progressed. An exercise co-ordinated by the Internal Audit and Risk Service with support from the Council's Resilience Team was undertaken for all Assistant Directors across the Council to identify their business critical systems. The information from this exercise was then forwarded to ICT for consideration.

The exercise identified a total of 72 systems deemed to be key by the Directorates. Of these systems:

- 8 systems are externally hosted (including the Council’s website), and the hosting organisation provides DR facilities
- 14 systems are outside the control of ICT. For those, it is directorate management responsibility to ensure that appropriate disaster recovery and business continuity plans are in place.
- 7 Systems are identified above as already having DR measures in place
- The remaining 43 systems are covered by daily backups of data and systems as part of normal ICT operations, but recovery of those systems may require additional investment to meet the Recovery Time objectives identified by the Directorates, such as Confirm, Servitor, iLap etc.

4 Next Steps

The following actions (along with timescales) are planned over the coming months in order to ensure that the Council has effective disaster recovery arrangements across its key systems:

- ICT to work with management to ensure that for all the systems identified as business critical, that proportionate disaster recovery requirements are agreed that consider the impact of the loss of systems from an operational perspective and the cost to implement recovery arrangements. (May 2015)
- ICT will develop a full DR testing plan for each critical system, and carry out regular documented tests to recover the system. These tests will be reported back to both the Assistant Director ICT, Transformation and Customer Services and Internal Audit and Risk Manager on a quarterly basis. (June 2015)

A follow up audit to review the revised disaster recovery arrangements will be undertaken in August 2015.

Stephen Mangan, Internal Audit and Risk Manager
Mark Chester, Head of ICT Infrastructure and Operations
5 February 2015