Cheltenham Borough Council
Audit Committee – 26 March 2014
ICT Business Continuity Assurance Report

Accountable member	**Cabinet Member Corporate Services, Councillor Jon Walklett**
Accountable officer	**Director of Resources, Mark Sheldon**
Ward(s) affected	**None**
Key Decision	**No**
Executive summary	At the Audit Committee meeting on 15 January 2014 Members received a mid-year review of progress against the Significant Issues Action Plan and requested a further report on ICT business continuity arrangements and testing. Robust ICT disaster recovery and business continuity arrangements are essential to meet the business needs of this Council and this report identifies the progress made and the actions proposed to give further assurance on ICT disaster recovery.
Recommendations	**The Audit Committee considers the report and the audit findings and makes comment on its content as necessary.** **Priorities for business application recovery are reviewed on an annual basis to reflect any changing business priorities.**

Financial implications	There are no direct financial implications arising form this report. **Contact officer: Mark Sheldon, Director of Resources** **mark.sheldon@cheltenham.gov.uk** **01242 264123**
Legal implications	**Contact officer: , @tewkesbury.gov.uk, 01242**
HR implications (including learning and organisational development)	There are no additional HR implications arising from this report. **Contact officer: Julie McCarthy, HR Manager** **julie.mccarthy@cheltenham.gov.uk** **01242 264355**
Key risks	None arising from this report
Corporate and community plan Implications	Good governance helps to deliver the Councils aspirations to be an excellent, efficient and sustainable Council.

Environmental and climate change implications	None
Property/Asset Implications	**Contact officer: David Roberts@cheltenham.gov.uk**

1. Background

1.1 Cheltenham Borough Council provides a range of services to a large number of people, some of whom are the most vulnerable in our community. Any sustained disruption to these services could have serious consequences to individuals or groups of people, so robust plans need to be in place to cope with unexpected events that cause disruption to normal service delivery.

1.2 The Council's Annual Governance Statement (AGS) for 2012/13 identified Business Continuity Testing as an area for focus during 2013/14 in its Significant Issues Action Plan.

1.3 Audit Committee received a progress update from the Corporate Governance, Risk and Compliance Officer in January 2014 and as a result asked for further assurance on ICT business continuity and testing of business critical applications.

2. ICT business continuity assurance

2.1 Infrastructure

2.1.1 The ICT infrastructure is summarised as building availability, the data centre, ICT staff, networks, telephony and power supply. Appendix 1 details current mitigations and planned actions in these areas. In addition a fully revised, written disaster recovery plan is being produced and will be completed by the end of June 2014.

2.2 Applications

2.2.1 In May 2012, Senior Leadership team agreed four tiers of recovery and the business applications that would be prioritised within each tier. In the event of a major disaster recovery situation a number of infrastructure systems/applications would first have to be recovered before starting the recovery of business applications. This could take some time to complete therefore ***'immediate'*** in reality has to mean ***'as soon as possible'*** and may take days in some scenarios.

Tier	Target Recovery Period
0	Immediate recovery
1	Within 5 days
2	Within 6 – 15 days
3	Greater than 15 days

2.2.2 As part of the Infrastructure Upgrade Strategy and server virtualisation strand of work, a migration programme has been implemented for all business applications that can operate in this environment. All Tier 0 and Tier 1 business applications that can be virtualised have been.

2.2.3 Virtualised applications can be recovered much quicker than conventional tape back-up. In addition, data replication takes place every hour or so as opposed to running an overnight process.

2.2.4 The status of Tier 0 and Tier 1 is summarised at Appendix 2. To undertake full business continuity

assurance testing will require full cooperation from each relevant service area and two working days per service would be required and the impact on public access appreciated.

3. ICT disaster recovery

3.1 For the purposes of this report, ICT disaster recovery is defined as the ability to recover back to business as usual after a major incident that disrupts or stops the data centre and access to systems for more than 24 hours.

3.2 Service business continuity plans should allow for continuation of each business area while the ICT disaster recovery plan is put in to operation and applications brought back up in a priority order which has been informed by business impact assessments. These assessments need to focus on the impact of a service not operating at that point in time.

3.3 South West Audit Partnership (SWAP) are carrying out a comprehensive review of the current disaster recovery arrangements in place and the findings that need to be addressed to provide the critical systems and services required to meet the business continuity requirements of the ICT shared service partners and clients. The findings of this report will be discussed at JMLG and an action plan will be reported to Audit Committee in June.

4. Consultation and feedback

4.1 ICT JMLG and the senior leadership team at each partner organisation will be consulted.

5. Performance management – monitoring and review

5.1 ICT JMLG.

Report author	**Contact officer: Andy Barge, Group Manager – Customer Services** **andy.barge@fdean.gov.uk, 01594 812383**
Appendices	1. **ICT infrastructure assurance** 2. **ICT Application assurance**