Cheltenham Borough Council
Audit Committee – 17 June 2015
ICT Disaster Recovery Preparation and Testing 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 26 March 2014 Members received an assurance report on ICT Disaster Recovery arrangements. 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 since the previous report and the actions proposed to give further assurance on ICT disaster recovery and testing.
Recommendations	**The Audit Committee considers the report and the audit findings and makes comment on its content as necessary.**

Financial implications	There are no direct financial implications arising from this report. Contact Officer: Mark Sheldon, mark.sheldon@cheltenham.gov.uk, 01242 264123
Legal implications	None
HR implications (including learning and organisational development)	There are no additional HR implications arising from this report.
Key risks	The councils corporate risk register includes the risk (reference CR77) which says if the new reciprocal ICT business continuity arrangements with FODDC are not put in place then there is a risk that key councils services in the event of an emergency or an unplanned event will not be effective. The progress made in delivering improved BCP arrangements has helped significantly towards mitigating this risk.
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	None

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 2013/14 identified Business Continuity Testing as an area for focus during 2014/15 in its Significant Issues Action Plan.

1.3 Audit Committee received a progress update from the ICT Shared Service in March 2014 and requested an annual assurance review on ICT business continuity and testing.

2. ICT Disaster Recovery Framework

2.1 An effective IT Disaster Recovery (DR) Strategy captures all of the necessary plans and processes to support the response to recover IT assets and applications in the event of a major incident that disrupts the critical business processes of the Council and its customers.

2.2 The primary objective of the DR program is to survive an incident and/or disaster and to re-establish normal business operations quickly and efficiently. In order to survive, IT Shared Service must assure that it can react appropriately and in a timely manner if an incident or disaster strikes so critical operations can resume normal processing within a reasonable time frame based upon an objective business impact analysis.

2.3 The DR Framework that is progressing will aim to:

- Balance the protection and recovery cost versus the risk to the business;
- Ensure that Council invests only what is crucial for protection and recovery;
- Identify weaknesses and implement a disaster prevention program;
- Minimise the duration of a serious disruption to operational service delivery;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort.

2.4 The development of a viable recovery strategy needs to be a joint effort between IT Shared Service and the business units who use IT services. Its successful and cost effective completion will need close cooperation and involvement from all areas.

2.5 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 focus on the impact of a service not operating at a given point in time. Whilst the four tiers of recovery described in the previous report are still recognised, the order of recovering applications within a given tier may vary depending on the time of the month e.g. benefit payment run or council tax collection.

3. Annual progress review

3.1 Appendix 1 provides a more detailed overview of progress since the last report and against some of the specific action areas identified at the last review.

3.2 External support was commissioned in October 2014 to provide a robust and objective IT Disaster Recovery review and to help develop a new framework.

3.3 As part of this process and the ongoing governance framework an annual scorecard is completed, using the red/amber/ green summary status. In addition, an assessment is made of the IT Disaster Recovery (ITDR) maturity level, which is summarised in the table below.

3.4 At October 2014 the scorecard status was red and the maturity level assessed as 1 - 2. At March 2015 the status had progressed to amber and the maturity level assessed as 3. On the basis that one of the primary points of our ITDR framework is to balance the protection and recovery cost versus the risk to the business our maximum maturity level target is 4.

0 Vulnerable	The business does not have an understanding of ITDR and how to apply it and any IT disruption will have a business impact
1 Developing	The business is in the process of learning and developing a greater understanding of ITDR and how to effectively apply it within the organisation
2 Reactive	The business has a basic understanding of the requirements for ITDR and processes need to be formalised and embedded
3 Managed	The business has a good understanding of ITDR and has a clear roadmap for applying and managing the various ITDR elements
4 Proactive	All elements of ITDR are in place, are being applied and are integrated with service areas
5 Resilient	The business uses processes and approaches that extend ITDR elements to increase business resilience by developing new concepts and ideas

3.5 The focus areas for the next twelve months will be:

- Complete the final ITDR framework
- Test the ITDR operational plan
- Test ITDR integration with service business continuity plans
- Complete the new storage architecture for the enhanced DR data centre

4. Consultation and feedback

4.1 Joint Security Working Group, ICT JMLG and the senior leadership team at each partner organisation will be consulted.

5. Performance management – monitoring and review

5.1 Joint Security Working Group and ICT JMLG.

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