

**REPORT NO. 5**

**REPORT TO THE GOVERNANCE AND AUDIT COMMITTEE  
MEETING ON 10<sup>TH</sup> DECEMBER 2019**

---

**Meeting:** Governance and Audit Committee  
**Date:** 10<sup>th</sup> December 2019  
**Subject:** ICT Business Continuity and Disaster Recovery Provisions  
**Report of:** Service Manager ICT  
**Portfolio Holder:** Councillor Dann – Corporate Portfolio  
**Status:** For comment and noting  
**Relevant Ward(s):** All

---

1 Purpose Report

1.1 To provide an update on the status of the testing of Business Continuity and Disaster Recovery arrangements.

2 **Recommendations:**

2.1 **To comment on and note the action update.**

3 Summary of Reasons for the Recommendations

3.1 Not applicable as this is an action update.

4 Impact on Communities

4.1 Not applicable as this is an action update.

5 Key Facts

5.1 Not applicable as this is an action update.

6 Legal Issues

6.1 Not applicable as this is an action update.

7 Resource Issues

7.1 Not applicable as this is an action update.

- 8 Equality Implications
  - 8.1 Not applicable as this is an action update.
  - 9 Impact on the Organisation
  - 9.1 Not applicable as this is an action update.
  - 10 Community Safety Implications
  - 10.1 Not applicable as this is an action update.
  - 11. Carbon Management Implications
  - 11.1 Not applicable as this is an action update.
  - 12. Risk Management Implications
  - 12.1 Not applicable as this is an action update.
  - 13 Consultation
  - 13.1 Not applicable as this is an action update.
  - 14 Options Considered
  - 14.1 Not applicable as this is an action update.
  - 15 Background Papers
  - 15.1 *Not applicable as this is an action update.*
- 

**Previous report(s):**

**Information Issued Under Sensitive Issue Procedure:**

**Ward Members Notified:**

**Appendices:**

- A. Appendix 1 – Disaster Recovery Testing Actions (Appendix A - Business Continuity and Disaster Recovery Testing.docx)**

### Overview

ICT have two separate arrangements for Business Continuity and Disaster Recovery which are as follows:

- Business Continuity – nightly backups both on-site and to a remote location that allow for individual systems on data items to be recovered to the main ICT infrastructure in the event of a loss.
- Disaster Recovery – A Microsoft cloud hosted environment that contains offline replicas of key systems, such as Uniform, that can be brought online in the event that the Symington building is lost.

Both solutions are subject to testing by the ICT team, and by service areas as appropriate.

### Business Continuity Recovery and Testing Procedures

Nightly backups are taken of all on-premise servers overnight, which are then immediately copied off-site. Retaining an on-site copy means items can be recovered quickly, whilst the off-site copy means we can restore the entire environment should the Symington Building be lost and have to be re-built. During the rebuild the Disaster Recovery arrangements would be used.

Recovery of backed up data is regularly undertaken as a matter of day-to-day business as users often accidentally delete or change things they did not mean to. Following the backup of a system, our backup solution performs an automated validation process to ensure that the backup is successful. Any failure in the backup process is immediately reported to the IT helpdesk for resolution by ICT staff members.

As well as regularly recovering data for staff, ICT also periodically recover entire environments into a test state in order to facilitate upgrades and updates. Test recovery procedures are also run through before any major event, such as a local or general election.

### Disaster Recovery Setup and Testing Procedures

Business critical servers are automatically replicated to a Microsoft datacentre in the west of the UK, and depending on the amount of data that changes during any given day, the replicated servers are between 15 and 90 minutes behind those of the live server – i.e. the data on the replicated server will generally be up to 90 minutes old. As well as replicating line-of-business applications such as Uniform – which is used by many service areas – all key infrastructure servers that support them are also replicated.

There are two ways in which replicated servers can be brought online:

1. As a direct replacement for servers in the Symington building, which would be turned off as part of the recovery process – if not already inaccessible.
2. In a sandboxed test environment, allowing staff the opportunity to test the DR arrangements without affecting live services.

The approach for testing the DR environment is as follows:

1. IT launch the chosen server, and all supporting servers, in the test environment.
2. IT then run through all the standard tests that IT normal undertake when commissioning a new live server, such as user logons, launching applications, accessing files etc.
3. When IT are satisfied the server and the applications on it are working as far as they can test the server is handed over to the service area staff to test business processes.

During the 2019/20 financial year IT have been undertaking steps one and two and have undertaken 33 distinct disaster recovery tests, with 4 more remaining to do. In Q4 of 2019/20 the Uniform and Elections servers will be tested with service area staff from the Corporate Services team. (this is in addition to the normal pre-election tests that will take place in November 2019).

Following testing of the Uniform system by Corporate Services a follow-up test schedule will be created for 2020/21 to ensure that all affected service teams have the opportunity to run through their full BC/DR procedures, including testing the DR environment.

Appendix 1 lists what tests have been undertaken by the ICT team and which are left to undertake.

### **Symington Building Loss – continued operation of other services.**

The following offices/services rely on communications with the Symington building:

- Harborough Market
- Police Station (Lifeline)
- Hinckley and Bosworth Borough Council (Revs and Bens)
- Charnwood (Contact Centre and onwards connection to HBBC for Revs and Bens)
- Innovation Centre.

In order to mitigate the impact on the above services should the building be lost a new wide-area network (the mechanism by which all the sites talk to each other) has been procured and is currently being implemented. This new network will ensure:

- HBBC and CBC can continue to communicate.
- The Police Station, Market and Innovation Centre will continue to have emails and internet services, as well as direct access to the Disaster Recovery environment.

It is anticipated that the new connections will go live in early January 2020.

### **Wider Disaster Recovery Considerations**

IT will facilitate connection to the DR environment from all un-affected offices – i.e. those not affected by the event that took down the Symington building – as well as any other non-HDC managed building that we may need to use. The new arrangements allows secure remote access to the Disaster Recovery environment from any location with an internet connection, affording flexibility to cope with

different scales of incident, from loss of a single building to regional infrastructure failures.