Central Bedfordshire Council
www.centralbedfordshire.gov.uk

APPENDIX A

Disaster Recovery

Statement Plan

Security classification:

Document Control

Owner

Name	Title
Stephan Conaway	Chief Information Officer

Author

Name	Date
Bob Bates, Bernard Sykes and Clive Dilley	November 2012

Reviewed

Name	Date
Matt Scott	November 2012
Bernard Sykes	November 2012
Bernard Sykes	August 2016

Distribution

Recipient	Organisation

Amendment History

Version	Date	Description
0.1	October 2012	First draft
0.2	October 2012	Initial Internal Review
0.3	October 2012	Updated following review
1.0	November 2012	Initial Final Draft
1.1	November 2012	Updates following reviews
1.2	December 2012	Update due to DataCentre move
1.3	December 2012	Utilise CBC document template. Include DR technology overview; 2013 DR plan; update assumptions
1.4	December 2013	DataCentre updates
1.5	April 2015	Personnel and contract updates
1.6	August 2016	Personnel and Application updates

Confidentiality

Glossary of Terms

RTO – Recovery Time Objective - Period of time within which minimum levels of service and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred and a decision has been make to invoke disaster recovery.

RPO - Recovery Point Objective - Point in time to which data must be recovered after a disruption has occurred

ATOD – At Time of Disaster

IRBC – ICT Readiness for Business Continuity

CBC – Central Bedfordshire Council

Primary DC – a datacentre facility that hosts production services

Secondary DC – a datacentre facility that provides standby services

Co-Lo – External 3rd facility where space and power is procured for the hosting of CBC ICT equipment

Table of Contents

1. Background & Scope

This DR Statement and Plan covers the Central Bedfordshire Council (CBC) IT services that are located at the CBC Luton and Hoddesdon facilities and incorporates systems where data and applications are supported from the same infrastructure.

The term “Disaster Recovery” requires a brief explanation, as it is sometimes confused with either high availability/local resilience and/or business continuity. Disaster Recover is a component of CBC service protection, but is not the sole element and although DR will be managed by IT, the key decisions on service restoration must be led by the CBC divisions and sanctioned by the CMT.

High Availability

High Availability is a strategy to prevent potentially full service failure following a local (and typically isolated) event; for example an internal component failure of a server. Without HA, should a component fail, the server will fail and access to the CBC service may be lost or impaired.

The ICT infrastructure has a degree of inbuilt resilience to mitigate the risk of impact associated with “local” failure scenarios, thus already offering a high level of protection against incidents relating to power and network connectivity.

Disaster Recovery

Disaster Recovery covers the loss of an entire data centre/computer room that would result in multiple CBC service failure. The purpose of the disaster recovery strategy is to ensure the timely resumption of ICT services and maintain the integrity of data, focussing on critical services first, should there be a total failure of either of the production environments.

Business Continuity

Business Continuity incorporates the above two scenarios, however the scope is considerably wider than just IT managed systems and provided services, as it includes processes and procedures to continue business operations across all CBC divisions. This may include the adoption of manual processes to temporarily replace ICT services or provision of facilities and staff to perform required functions

Scope

The scope of this strategy document covers Disaster Recovery is defined as a site-wide failure at the Luton or Hoddesdon locations. It will form a key part of CBC Business Continuity Planning (BCP), however the overall responsibility for BCP is outside the remit for IT.

This DR strategy document is structured to include the following elements in alignment with BS ISO/IEC FDIS 27031 – ‘Guideline for Information and Communications Technology Readiness for Business Continuity’:

- Facilities
- Technology
- Data
- Processes

- People
- Suppliers

This document is a working document and is subject to regular updates following component and full DR tests and any subsequent change to the ICT infrastructure or DR provision.

2. Management Summary

CBC's objective is to provide a reasonably balanced DR strategy that takes account of the increasing importance of ICT systems to front line service delivery, whilst recognising that maintaining DR capability will require on-going investment and resource.

The long term goal is to provide hot standby facilities that would enable seamless transfer of ICT service provision from a main data centre (potentially a Co-Lo facility) to a DR facility (potentially Dunstable) in the event of a disaster, so that the current planned provision allows for a period of down-time while the DR service is invoked and made operational.

Central Bedfordshire Council has implemented an ICT infrastructure that incorporates the use of virtual servers split across several sites, which reduces the impact of any significant incident..

There are a number of threats that could result disruption to ICT services, and may ultimately require the disaster recovery process to be invoked if severe enough. These include

- Malicious attack - Unauthorised access, virus attack
- Accidental data loss, software failure
- Equipment, link failure
- Uncontrolled changes to infrastructure or systems resulting in failure or corruption
- Building related events (loss of power or other critical services, prevention of access, structural issue etc)
- External incidents (bomb threat, major crash, civil unrest etc)

A range of measures are already in place to mitigate these threats, including:

- Identity management, physical and logical access security, anti-virus protection.
- Resilient central equipment & networks, virtualised servers, off-site backups
- Controlled, managed, monitored and maintained ICT infrastructure and systems.
- ITIL based change control and support services in-house and via 3rd party contracts
- Replicated data storage between two facilities

3. ICT Resilience

The first principle of ICT Readiness for Business Continuity (IRBC) is Incident Protection. CBCs existing ICT infrastructure has a degree of inbuilt resilience to protect ICT services from the threat of hardware failures and therefore the need to invoke the DR plan for many failure scenarios.

The production infrastructure within the two datacentres is a mixture of physical and virtual servers, with all data held on a centralised storage infrastructure, one at each site. For some applications, data is frequently replicated via log shipping to the secondary facility, while others are backed up to disk and tape, thereby providing various levels of data protection and options for recovery.

3.1. Premises

Most of the critical infrastructure is currently located at the following locations:

- Luton ONI . not owned by CBC. Contains 8 racks
- Interroute, Hoddesdon, not owned by CBC. Contrains 6 racks
- Priory House, Shefford. Contains critical telephony systems (which will be hosted by Vodafone by November 2016), GCSX Exchange and a Domain Controller

Production services are hosted from both the Luton and Hoddesdon premises, so a failure at either site would not impact all business services. Data centre resilience is delivered via the following:

- Each computer rack is provided with dual power supplies with each supply being fed from different distribution boards, protecting against the failure of circuit breakers or distribution boards. Most Networking equipment has dual power supplies.

- Luton and Hoddesdon datacentres have multiple, independent, physically isolated systems that provide redundant (fault tolerant) capacity components and multiple, independent, diverse, active distribution paths simultaneously serving the computer equipment

- Luton and Hoddesdon datacentres are rated Tier 3

.

3.2. Storage

The data storage environment is currently based on an HP 3par storage area network (SAN). The array has inbuilt resilience to protect against the failure of: power modules, disk controller and disk drives. Production data is replicated between the two storage arrays located at Luton and Hoddesdon

3.3. Servers

Applications run on a mix of physical and virtual servers. Virtual servers enable CBC to rapidly deploy new server instances, and move application services to an alternate host

server within the same site should one fail, thus minimising the impact of any outage. Virtual machine configuration information is backed up so that recovery of the system images is possible on an alternate host, or at an alternate site where there is hardware available.

Physical servers are backed up for the purposes of disaster recovery.

3.4. Network

The CBC wide area network infrastructure is based on a DUCL MPLS with inbuilt resilience and dual path connectivity. The Internet service is delivered by JANET via 2 virtual machines located at the Co-Lo facility. The resilience is built into the network infrastructure so there are only a few identified single point of failure at the component level i.e. one internet connection. The Network diagram can be found at the following file location:

https://centralbedfordshire.box.com/s/gy4pq0gfjhoch1a160hk1su2btdb4kfa

3.5. Telephony

Telephony Contact Centre is provided form the cloud by Vodafone

3.6. Data Backup

All CBC production servers are backed up using the council's standard backup processes and software to enable a recovery point in the event of unforeseen server / application interruptions or failures.

Backups from one datacentre e.g. Luton are replicated on disk to the other datacentre e.g. Hoddesdon. Virtual servers can be instanced directly from a vmware backup file.

Reports are produced and checked on a daily basis

Failures are then investigated and remediated as appropriate.

3.7. Security and Access Control

User identity, password and access controls are in place to help ensure that users have authority to access business applications and to prevent unauthorised access. Firewall and anti-virus controls are in place to minimise risk from external threats to data and systems.

External users connect using 2 factor authentication i.e. Google Authenticator

3.8. Management and Monitoring Systems

Server, storage and network performance and capacity are managed to ensure that business applications operate effectively.

Certain parts of the infrastructure are monitored. E.g., HP 3par storage.

The alerts are emailed to an ICTAlerts mailbox which is monitored on a daily basis and alerts highlighted in the morning daily checks report to relevant team members.

3.9. ICT Support Services

CBC have support arrangements with external suppliers to support the ICT team in the areas of backup software, voice communication, server hardware break/fix and applications.

Details can be found on Box:

https://centralbedfordshire.box.com/s/85rjgp3nhn0lm4g20lcyobfrfcpm6ytd

On LanDesk (servicedesk system)

3.10. Change Control Processes

ICT processes and procedures are in place to challenge and control changes to the ICT environment so that the risk of introducing a change that causes an incident is minimised.

Details can be found at the following file

https://centralbedfordshire.box.com/s/0a4pr60vh9fb20qkpm5jp4h1nc8ju6us

4. DR Foundations and Concepts

4.1. Objective

To support the Council's critical services to maintain a service in line with the Council's business continuity plans and objectives, as defined within the document produced by the Emergency Planning Team:

"Business System Requirements, Version 1.0, 27th May 20120"

The DR strategy, and following sections of this document, assumes the complete failure of a primary datacentre.

Recovery priority will be determined at the time of the incident, based on available hardware, and in a priority order agreed with the Incident Management Team, dependent upon factors such as:

Time of incident (critical business activities)
Nature and scale of incident
Likely period of disruption

4.2. Datacentre Strategy

On the loss of a data centre. (DC)

Test and Dev services at the surviving data centre will be closed down

Production servers from the stricken DC will be recreated from the replicated 3par data.

#	Component	Comment
1	SAN Asynchronous Replication	Data is replicated from SAN to SAN over the MPLS network on a period basis (every 5 minutes) to ensure integrity across sites and a consistent RPO point. Recovered virtual servers will access the data to enable service to continue.
2	Application Recovery (e.g. Log Shipping)	A small number of services utilise application driven data protection techniques (e.g. Log Shipping) as well as SAN based replication. This is typically used for data roll-back/forward following data corruption. Where practical, these systems will utilise SAN based replication for DR purposes in preference to application driven.
3	Backup	Backup used to provide temporary DR capability to in-scope locations that have local servers that are not attached to the SAN (Note: Future strategy will be to relocate these servers into main data centres).
4	Telephony fail-over process	DR recovery currently requires re-routing of telephony using a Hunt Group and re-direct of specific 0300 numbers into Watling House Will be hosted by Vodafone come November 2016 which has dual site resiliency

4.3. Concepts

The DR strategy is based on the following:

The failover of ICT services to the secondary datacentre is a manual process

The RTO commences from the point of decision to invoke DR

This strategy is for resumption of ICT services. The business is to address business resumption and Incident Management.

All critical application data, files and folders are held on the Storage Area Network

4.4. Change Control

Any change to the ICT Services that may affect DR capability will only be implemented once the business continuity implications have been assessed and agreed.

4.5. Assumptions

When running in disaster recovery mode, the following assumptions apply:

In agreement with the business some services delivered may be reduced in capacity

All non-essential systems maintenance will be suspended

All system upgrades will be suspended

Break/fix calls will take priority

There will be a change freeze for application deployment or modification

5. DR ICT Components

5.1. Technology

5.1.1. Servers

On datacentre failure to Luton or Hoddesdon, IT will recreate the production servers at the surviving DataCentre from the replicated data

The recovery priority will be based on the circumstances and nature of the event at the time, the storage tiering system and input from the emergency planning team..

5.1.2. Data

Dual Enterprise class storage arrays (3Par) replicate production data between DCs.. Each array has inbuilt resilience against power and single component failure. All production SAN data is replicated via the storage hardware from the primary site to the secondary.

Recovery of data will be prioritised by application recovery priority.

5.2. Applications

The following details the DR strategy for applications:

Application	**DR Strategy**
Email	CBC hosted is a Clustered solution. DR server at Hoddesdon
	Office 365/Email in the Cloud
Office 365 (Word, excel etc.)	Office documents in Box (Cloud)
SWIFT	Data replicated to server at Hoddesdon
CCMS	Data replicated to server at Hoddesdon
Fsa (S: drive files)	Data replicated to server at Hoddesdon
Citrix	With 6.5 a load balanced solution with nodes at Luton and Hoddesdon
Modern.gov	Cloud Hosted
Telephony	To be host by Vodafone in the cloud by Nov 16
MDM/mobile iron SSO OKTA	Cloud hosted
Terms	Cloud solution
All other	Production Disk and Non-production Tape based recovery

5.3. Network

Access to JANET is provided through virtual machines hosted in the DMZ located at the Luton facility. There is currently no DR provision for this service.

6. DR Processes

6.1. Recovery Priority

The recovery priority of applications will be determined at the time of the incident in accordance with the Emergency Planning Team procedures.

ICT have aligned servers and associated datastores to application tiers by criticality. This is documented in the following location:

https://centralbedfordshire.box.com/s/jt7yjjw6k7bo5u40y4lai8yb5pfe0yq7

6.2. Recovery Process

ICT Service Continuity is described in terms of the following incident levels:

- **Single user**
- **Department**
- **Council Wide**

The high level process for recovery is as follows:

6.2.1. Roles and Responsibilities

CBC IT/DR Staff

The CBC Emergency Planning Team (EPT) and/or an appointed Incident Controller (IC) will notify one or more of the IT/DR personnel listed below.

Name	Responsibility	Contact Via
Stephan Conaway	CIO	Stephan.conaway@centralbedfordshire.gov.uk 07816873947
Bernard Sykes	Ops and Networks Manager	Bernard.sykes@centralbedfordshire.gov.uk 07391 411863
Steve Holton	Data Centre Manager	Steve.Holton@centralbedfordshire.gov.uk 07792 129480
Jeremy Wood	Network Services Manager	Jeremy.wood@centralbedfordshire.gov.uk 07795 257448

CBD IT/DR Management

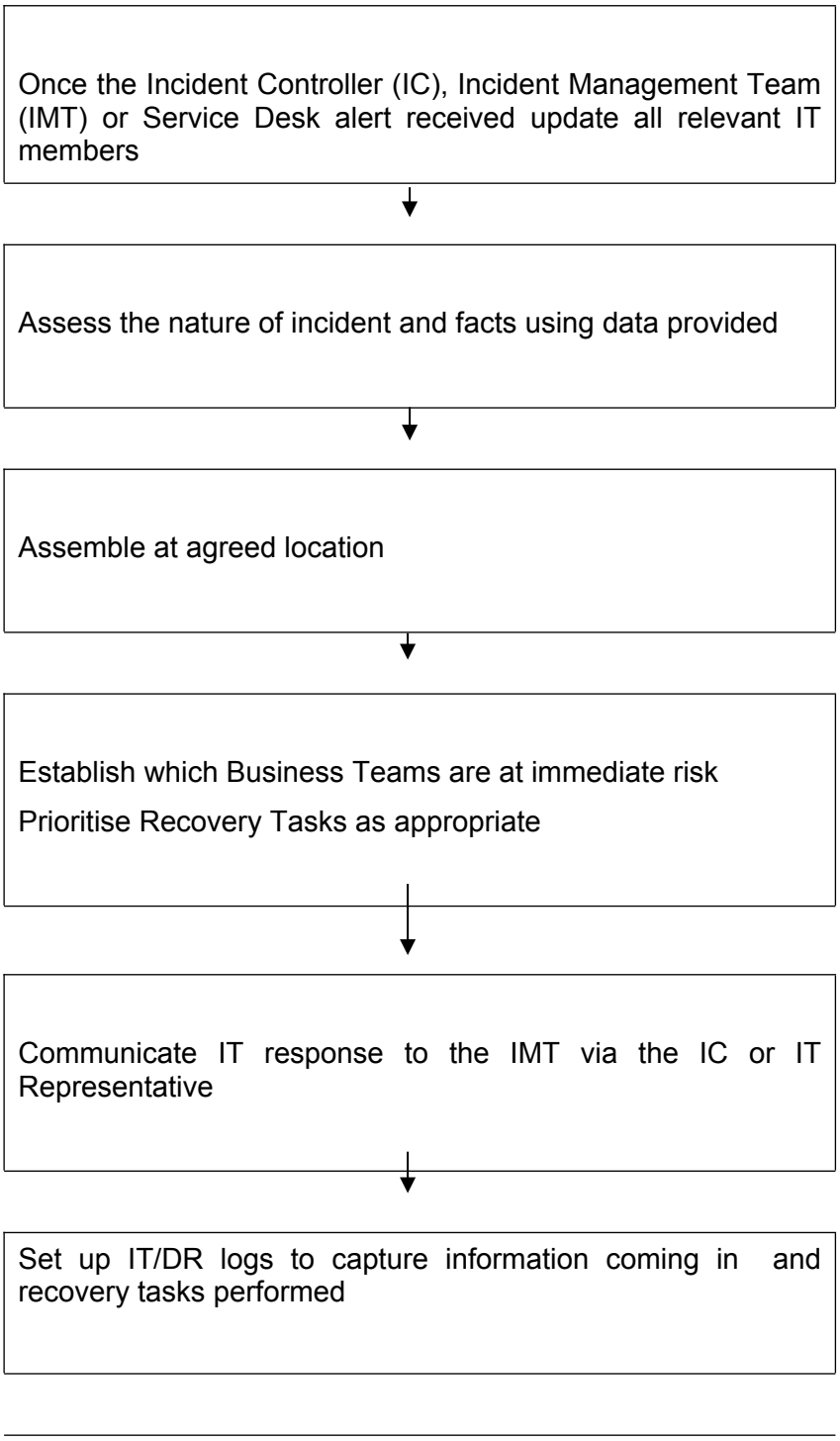
It is the responsibility of CBC IT/DR management to:

- Notify the appointed Incident Controller of the disaster (if ‘first at scene’)
- Evaluate the extent of the problem/incident in relation to underpinning IT Infrastructure and associated services that may lead to an invocation in association with the appointed Incident Controller.
- Review, evaluate and communicate potential consequences of underpinning IT to the Emergency Planning Team, in order for strategy to be agreed (relevant to the time and nature of the disaster.)
- Initiate IT/DR procedures
- Co-ordinate and communicate recovery operations to the EPT.
- Monitor recovery
- Document and update recovery processes
- Liaise with Business Recovery Team leaders on user acceptance and/or handover.
- Support Business Recovery Team as required
- Expedite authorisation where necessary
- Ensure conversion to standby facilities and the final resumption of operations are under sufficient audit control to provide reliability and consistency for auditing.

CBC IT Staff

- Install and configure ESX environment
- Install and configure backup/recover environment – including tape library
- Install and configure physical servers
- Provision and configure storage from supplied pool
- Configure network to accommodate recovery requirements
- Restore data (for tape-based recoveries)
- Apply latest replicated data (for replicated environments)
- Test services and applications in conjunction with business and application owners to ensure services and applications are fully recovered and

6.2.2. Incident Response



6.2.3. Invocation

CBC has personnel within the IT department and the Emergency Planning Team (EPT) who are nominated key invocation personnel. . The IT personnel are:

Bernard Sykes

Stephan Conaway
Steve Holton
Jeremy Wood

6.2.4. Recovery Steps

6.2.4.1. Recovery from Replication (application level replication)

Applications using log shipping for 'failover'-based recovery are:

CCMS (data replicated to server at Watling House)

SWIFT (data replicated to server at Watling House)

CITRIX (load-balanced with nodes at Bedford and Watling House)

Exchange (clustered solution)

As the data will already be at the alternate site, recovery will typically consist of 'failing over' servers, with elements of re-configuration specific to each application.

After 'fail over' Business/Application owners will ensure recovered applications and services are fully functional and read for use (before handover to users)

6.2.4.2. Recovery from Backup disk and (tape for non-production systems if required)

NOTE: Some of the following steps may be implemented in parallel, depending on resource availability.

Steps to recover from backups at the DR site are as follows.

Close down non-production servers

Build Netbackup environment – including all Catalog metadata, DR configuration, and tape library (may be hosted on physical or virtual server – TBC)

Create servers from replicated backups

Configure applications into running state and test

Business/Application owners will ensure recovered applications and services are fully functional and read for use (before handover to users)

6.3. Recovery Documentation

The recovery documentation is held in a "battlebox" directory at
https://centralbedfordshire.box.com/s/6kiccchnv7a57gmd1s2alkz9t7hqlexq
On Box and on the S: drive

The recovery plan makes an assumption that the following skills/technical specialisms and technical competencies are in place at CBC:

Microsoft servers 2003, 2008, 2012

VMware 5.5

Netbackup 7.6

IP skillsets

7. DR Personnel

7.1. ICT

Members of the ICT team would be assigned to the recovery operation based on the nature of the incident and availability.

Members of the Network Team would be assigned to the recovery as required.

Members of the Application Team will be assigned to the recovery operation once the server environment has been recovered.

7.2. External

The following third party suppliers would be involved in recovery and validation of the products that they support:

SWIFT
CCMS

7.3. Business Users / Business Application Owners

Business users will be involved in testing to ensure that recovered applications are fully functional and ready for use, before wider access is permitted.

7.4. Emergency Planning Team

The Emergency Planning team plays a key role during a disaster situation. For ICT DR, they act as co-ordinators to prioritise recovery with the business and act as a primary communications conduit between ICT and the user base.

7.5. Other ICT Service Users

The Emergency Planning Team will manage communications to impacted officers, members and external parties and agencies outside CBC.

The Emergency Planning team will be notified of all P1 incidents /major incidents which by definition would include DR events. The Emergency Planning Team operate a 24/7 duty system. In the event of a DR event the Duty First Contact Officer would be contacted on the following number **07964 111942**. A voicemail service is available for this number along with instructions on the voicemail about what information should be provided. There is also an emergency email account which is monitored by the Duty First Contact Officer emergency@centralbedfordshire.gov.uk."

8. Return to Normal Operation

At some point restoration will be deemed feasible and desirable and services will be transitioned back to “normal” operations. Depending on the nature and severity of the incident, and the duration of running in disaster recovery mode, the return of services could be to either the original infrastructure, or to a new arrangement, especially where the disruption has forced a permanent change to the business. It is acknowledged that this task will be substantial.

For this reason, return to normal is not prescriptive and must be planned carefully with the business to ensure the transition schedule has minimal business impact.

The return process must:

Ensure that all needed infrastructure services, such as power, cooling, connectivity, and security are operational

Schedule installation of system hardware and software

Establish connectivity between internal and external systems and premises

Reverse or establish data replication from DR site

Test system operations to ensure full functionality

Transition services from the DR facility

Gain business sign off

Terminate contingency operations

When returning services to a new infrastructure, careful consideration must be given to:

Software licensing, especially if hardware dependent

Legacy equipment

Original version of operating system, patches and software compared to what is available at the time of restoration of services

For CBC, the preference is to return to operations in the primary datacentre. However if the incident results in the total failure and destruction of the primary datacentre, then an alternate strategy will be reviewed with the business.

9. DR Testing

As we are in the process of continuous moves to the cloud there will be a full comprehensive DR test on completion of the first datacentre move to the cloud after March 2017

An annual DR testing programme will be agreed subsequently with the business

In most instances testing the whole set of DR elements and processes in one test is impractical and therefore a structured phased approach is recommended, fully aligned to the wider business continuity management scope and complementing the broader exercise programme.

DR testing will require input from the following teams:

- ICT – recovery of core infrastructure, application servers, software and data
- Applications – recovery and validation of applications and databases
- Business – user testing

10. Risks

10.1. Restrictions

- There is no statement from the CMT on the level of impact they are prepared to accept in a Disaster situation. This would validate the recovery objectives as defined by each area of the business.

10.2. Vulnerabilities

The following list itemises known shortfalls within the provision of DR. This document will be updated in accordance with any actions taken to address these items.

- The current recovery objectives or expectations of the business have not been validated
- There is limited formal documentation linking business systems to ICT infrastructure. This means a heavy reliance on key individuals and could impact an efficient large scale recovery.
- Current testing is at an ICT component level and a full test of business system recover will be required to give complete assurance over the recovery capabilities.