


# SHARED SERVICES TEAM

**Document Name: HR Advance Disaster Recovery Business Continuity Plan**

**Usage Guidance**

Toolkit materials should only be used with due consideration to the context and requirements of the programme in question. Materials should not be directly applied ‘off the shelf.’

**CATEGORY DESCRIPTION**

<p>1. <i>Example material</i> –The tool has been provided by a single public or private sector organisation, or an external forum that has not been moderated by the Shared Services Team. It represents one possible approach to a given shared service activity, and can be used by Toolkit users as an example / reference aid.</p>	<div style="text-align: center;">  </div> <p>NB. This document was correct as per initial implementation however it was reviewed as part of the Land Registry continuous improvement approach to management of the HR system for Land Registry and may not be the final version.</p>
<p>2. <i>Co-developed material</i> – The tool has been produced through the collaboration of the Shared Services Team and one or more public sector organisations and / or private sector organisations. This tool Provides a jointly developed approach to a given shared services activity, and can be used by Toolkit users as an example / reference aid.</p>	
<p>3. <i>Output Templates</i> – These set out what is typically included in an output of this name. They have been created as part of the development of the toolkit based on experience and best practice from other programmes and project methodologies. However, your organisation may already have a set format and template for you to use.</p>	

*The following information is provided for convenience as part of the service we offer at this website. However, the Cabinet Office cannot accept any liability for its accuracy or content. Visitors who rely on this information do so at their own risk. If the material has been provided by a Private Sector organisation please refer to their Company website for further information.*

**Land Registry**  
**DR and BC Plan**  
**HR Advance (HRA) Project**

**Version 0.4 March 2005**

**Detailed contents**

- 1 Introduction.....4
  - 1.1 Document Purpose .....4
  - 1.2 Status of Document .....4
  - 1.3 Scope .....5
- 2 Part A – General Obligations .....7
  - 2.1 Contractors Procedures .....7
  - 2.2 Business Impact Assessment .....7
  - 2.3 Risk Assessment .....7
  - 2.4 Contractors Solution .....8
  - 2.5 Disaster Recovery Facilities.....9
  - 2.6 Disaster Recovery Scenarios.....9
  - 2.7 Disaster Recovery Solution.....9
  - 2.8 DR Testing ..... 13
  - 2.9 Invocation..... 15
- 3 Part B – Disaster Recovery ..... 16
  - 3.1 Introduction ..... 16
  - 3.2 Backup Methodology ..... 16
  - 3.3 Data Verification Procedures ..... 16
  - 3.4 Tape Management..... 17
  - 3.5 Hardware Maintenance and spares..... 17
  - 3.6 Subcontractors Responsibilities..... 17
  - 3.7 Hardware Configuration Details ..... 17
  - 3.8 Data Centre Site Audits ..... 18
  - 3.9 Disaster Recovery Service Levels ..... 18
  - 3.10 Authority’s Obligations ..... 18
- 4 Part C Business Continuity ..... 20
  - 4.1 Introduction ..... 20
  - 4.2 Disaster Recovery Scenarios..... 20
  - 4.3 Authority Obligations..... 21

# **1 Introduction**

## **1.1 Document Purpose**

The purpose of this document is to define the Disaster Recovery and Business Continuity procedures for the Land Registry HRA system.

For the purpose of this document the following definitions apply:

‘The System’: the hardware and software used to deliver the service as defined in Section 2.4

‘Data Centre’: where the system is hosted.

‘ Disaster’: Either an event or circumstances which cause the complete or partial loss or unavailability of the System or which prevents the normal operation of the System or the performance of any substantial task or function of the system for a period of 8 contiguous hours within Service Hours or more in the event that the Data Centre is destroyed or inoperable.

‘Disaster Recovery’: Recovery of the system to meet the Disaster Recovery Service Levels.

‘Disaster recovery service’: means the part of the Services that will be provided to the Authority in the event a Disaster is declared

‘Business Continuity’: Continuation of the service in a Disaster Recovery situation or a disruption to an element of the service

‘The Authority’: Land Registry

‘The Contractor’: XXXX

## **1.2 Status of Document**

The status of this document is ‘Draft’. The document will require review and update during the course of the HRA Implementation Project after which the Plan will be ‘Issued’.

### **1.2.1 Plan Review Procedures**

A number of events will trigger a review of the Disaster Recovery and Business Continuity Plan; they include

- Changes to the XXXX policy and procedures
- Changes to the Land Registry policy and procedures
- Legislative changes as defined in the contract.
- Actions arising from recommendations or ‘lessons learned’ at formal test or review of the plan.

- Any changes to the Service provided by XXXX, initiated through Change Control procedures

### 1.2.2 Plan Maintenance

This document will be reviewed at defined points during the course of the HRA Implementation Project. Specifically at the following points:

- Following completion of the Technical Design Document
- Following a Business Impact Analysis undertaken between the Contractor and the Authority
- Following a risk assessment exercise undertaken between the Contractor and Authority
- Following agreement of the Disaster Recovery Management Process (see section 2.7.1)
- When the Disaster Recovery Service supplier has been decided
- Before the service commences

After Service has commenced any updates identified as a result of the trigger events defined in 1.2.1 will be identified as a change, impact assessed and incorporated into the plan as agreed between XXXX and Land Registry.

When amendments are made to the plan, a new version will be created and issued.

## 1.3 Scope

This document outlines the Disaster Recovery and Business Continuity procedures for the Land Registry HRA system. The document covers a Disaster Recovery situation affecting the technical infrastructure for the HRA system, which is hosted at the following locations:

- Pod A, Bridgend Data Centre
- Pod C, Waterton (Contractors new hosting facilities 5km from Pod A)

DR is limited to the current technical landscape. Any requirement for DR for future changes in the landscape will be address through Change Control Procedures.

The document is structured into three sections:

### Part A – General Obligations

This section defines how the Plan will be implemented and the procedures that will be followed to ensure that the Land Registry's requirements for Business Continuity and Disaster Recovery are met.

## Part B – Disaster Recovery

This section will define how the Plan will ensure recovery within the Disaster Recovery Service Levels.

## Part C – Business Continuity

This section defines how the service will be continued in a Disaster Recovery situation or during a disruption of an element of the service.

## 2 Part A – General Obligations

*Part A of the Disaster Recovery and Business Continuity Plan shall specify how the Contractor shall implement the Disaster Recovery and Business Continuity Plan and the procedures which the Contractor shall follow to ensure that the Authority's requirements in respect of business continuity and disaster recovery are met in relation to the services.*

### 2.1 Contractors Procedures

The Contractor has processes and procedures in place for recovery of the system in the event of a disaster situation.

These procedures will be followed if a disaster situation occurs that affects the service provided to the authority.

There are site specific Disaster Recovery Plans maintained by XXXX. Invocation will be notified to the Authority by the Contractors Service Delivery Manager.

### 2.2 Business Impact Assessment

At the end of the Blueprint Phase the Contractor will arrange a workshop with the Authority to discuss the Business Impact of a Disaster involving the HRA system.

The aim will be to break down the service into components at both functional and technical levels, to identify the business critical processes and assess the impact of losing those processes. It will then be possible to prioritise the recovery of the components with the aim of minimising the effect of a disaster on the Authority.

### 2.3 Risk Assessment

<b>Risk</b>	<b>Actions should risk occur</b>
Component Failure:	This risk is counteracted through the design of the hardware and communications solution. This is defined in Section 2.4
Total loss of site: fire, contamination, water damage etc	Contractor will invoke DR Supplier within 8 hours
Loss of services: Power Failure; Generator failure	The Contractor will assess depending on the severity and resolution of the Incident and advise the Authority accordingly
Telecommunications	This risk is counteracted through the design of the hardware and communications solution. This is

Risk	Actions should risk occur
	defined in Section 2.4
Exclusion from building	<p>Contractor will invoke Remote Management initially.</p> <p>The Contractor will assess further action depending on the anticipated resolution and advise the Authority accordingly</p>

## 2.4 Contractors Solution

The contractors' hardware and communications solution is defined in detail in the Technical Design Document.

The Technical Solution has no single points of failure, except the Modular Storage Array (MSA). In all other respects the solution is designed to be resilient.

The hardware solution is split across two of the Contractors separate 'Pods' or Computer Rooms. The production environment will be sited in Pod A and the Development and Test environments will be sited in the other Pod C.

In an emergency situation, affecting only the production environment, components of the test environment could be utilised to restore the Production Environment

The production hardware solution has been sized, and shall meet the availability and response time requirements as specified in the Service Level Agreement (Schedule 1.2 Appendix 2 service level references 1,4 and 5)

The telecommunications solution includes a total of 8MB bandwidth, comprising two, double 2MB load balanced dedicated leased lines, which are, routed separately, one from each pod to each of the Authorities twin data centres in Plymouth. (Note: the location of the second line is to be confirmed by Authority) This provides resilience should a single link fail. If a single link fails the bandwidth capacity will be reduced by 25%.

In addition different communications suppliers have been used for each link to minimise the risk service loss in the event of a single comms supplier failing.

The routers at each end of the leased lines and the firewalls at Bridgend will be configured to automatically failover should a device fail.

## **2.5 Disaster Recovery Facilities**

In the event of a loss of site, a DR third party supplier will be utilised to provide a replacement DR solution.

This service will be in place when the production service commences in April 2006 and this Plan will be updated to include a definition of the service provided, any processes and procedures agreed.

## **2.6 Disaster Recovery Scenarios**

### **2.6.1 Small Disaster Recovery (DR) Scenario**

A small DR scenario would be one which affects the Contractors solution in a relatively minor way, for example:

One of the production servers failing, which would require immediate failover to the secondary node in the cluster.

Failure of one of the primary communications links which would require all traffic to be routed through the other primary link within the contractors solution

Hardware failure that requires the use of the hardware maintenance supplier. Any individual hardware component failure should not make the production environment unavailable with the exception of the shared production external storage, however this is configured under RAID 5 and the only real single point of failure is the Modular Storage Array (MSA) itself.

Small DR scenarios as defined above would be viewed as incidents and should the Authority be affected would be viewed as a severity 1 incident and would be responded to under the normal Service Level Agreement.

### **2.6.2 Large Disaster Recovery (DR) Scenario**

A 'large DR' scenario would be one, which affects the Contractors solution in a major way e.g. one scenario is considered:

The production facility where the Contractor's solution is hosted suffers a serious incident, which makes it inaccessible or unusable.

This scenario would require the invocation of the Disaster Recovery Plan to recover the Contractors Solution at another location.

## **2.7 Disaster Recovery Solution**

The following Disaster Recovery Solution is available to respond to a Large DR scenario, as identified in section 2.6.2

Whichever recovery method is chosen, the Contractor and Disaster Recovery Supplier would use all reasonable endeavours to recover the Contractor's solution for the Authority

### 2.7.1 Disaster Recovery Management Process

The Contractor shall establish a Disaster Recovery Management Process with the Authority that will be included and maintained within this plan. The process will define the roles and responsibilities of the Contractor and the Authority for invoking the Disaster Recovery Plan and managing the Disaster through from invocation through to restoration of normal service.

It is proposed that this process be defined through a series of workshops and this plan will be updated with the process once agreed.

### 2.7.2 Disaster Recovery Services from Third Party DR Supplier

The Contractor will put in place arrangements with a third party supplier to provide a comprehensive range of Disaster Recovery services, which will enable prompt and accurate recovery of the Contractor's services to the Authority from a number of different DR scenarios.

One or more of these services would be activated in consultation with the Authority dependent upon the nature of the DR scenario.

These DR services will provide a choice of recovery methods at the time of the disaster, of which one or more could be deployed:

- Offload Replacement Hardware
- Mobile Recovery Units
- Remote Connection
- Relocation to Business Recovery Centres

The Contractor together with the Authority, and specialist advice from Disaster Recovery Service Supplier, would decide at time of a disaster which of the following recovery methods would provide the quickest and most suitable recovery.

#### 2.7.2.1 Offload Replacement Hardware

In the event of a disaster, replacement equipment would be off loaded and installed either within one of the Contractor's Bridgend Data Centres, one of the Authority's own twin Data Centres or the Authority's Disaster Recovery facility, and then linked to the Authority's IT infrastructure with specialist support from the Contractor and Disaster Recovery supplier. The Contractor would assume full responsibility for the entire restoration from arrival; rebuilding the systems, restoring data from off site tapes and rolling forward HR and Payroll data to as close as possible to the point of disaster, through to final hand over.

### 2.7.2.2 Mobile Recovery Units

The Disaster Recovery Service supplier could alternatively deliver a Mobile Recovery Unit from a modern fleet of air-conditioned fully equipped computer units. This would be configured with a replica of the Contractor's solution in a mobile computer room and delivered either to the Contractor's site or to the Authority's site. The Mobile Recovery Unit & recovery equipment will be available for a period of between 11 & 16 weeks. During which time, XXXX would be looking to replace the hardware and find alternate premises from which to host it.

It is the Authorities responsibility to ensure suitable plug in points for the mobile unit at its premises

### 2.7.2.3 Remote Connection

Hardware or software failure that falls within the definition within paragraph 2.6.2, could also be viewed by the Authority as a disaster. In this instance, the easiest route to recovery may be to establish ISDN links to the Disaster Recovery Service supplier's Business Recovery Centre to Land Registry and resuming processing on one of their recovery systems rather than initiating a Mobile Recovery Unit. The availability of ISDN links to be used will be discussed and agreed with the Authority. If this service is invoked, the Authority will accept the use of ISDN links for the period of time it takes for a more stable recovery option to be deployed. The service levels defined in section 3.9 will be apply in such circumstances

At the point at which DR was invoked, the Contractor would arrange for a communications specialist to visit the Authority's site and install the necessary remote controllers required to enable this DR service. Meanwhile, the Authority's back-up tapes would be sent to the Business Recovery Centre where the Contractor's support staff would perform a system restore.

### 2.7.2.4 Relocation to longer term facility

The Contractor also has an established relationship with a 3<sup>rd</sup> Party Business Continuity specialist supplier for the provision of a long-term Computer Equipment Room (CER) to be erected in the Visitor's or Staff car parks or any other suitable site at Bridgend Science Park, together with a Mobile long-term Work-area Recovery Facility (MWRC) providing the Contractor with 100 staff positions.

The CER could be erected within eight days of invocation of a disaster, with partial completion in five days. If this solution were required, the Contractor would commit to making the CER fully operational within 8 weeks of invocation.

No of Units	Internal Area		Internal Dimensions		Max Power Distribution	Max Cooling	Installed Capacity
	Sq. Feet	Sq. Mtrs	Feet	Meters	KVA	KW	BTU('000)
20	5280	490	63 x 84	19 x 26	300	308	1,052

(All measurements are shown to the nearest foot or metre)

Both the CER and MWRC are of the dimensions listed above with the MWRC having capacity to provide the Contractor 100 positions for its support staff. The MWRC would be supplied, erected and installed within 14 days of invocation. N.B. This contract does not provide for any computer hardware, since this will be provided under the Disaster Recovery Service supplier contract. Following the invocation of the longer-term relocation solution, the Cold Room Recovery Plan would be invoked. Any member of the Contractor's operational staff can place the supplier on stand-by.

A diesel generator would initially provide the power supply to the CER. The generator would be commissioned within 24 hours of the CER being completed and would remain in service until mains power was restored or for a period of up to one month.

The air conditioning for the CER requires a water supply; initially a bowser would be delivered along with the building. Long-term mains water supply could then be connected by Dwr Cymru (Welsh Water), and the Contractor's Property Manager would make arrangements for this.

The Contractor's onsite Teleprocessing Network consists of BT leased lines and ancillary equipment necessary to connect and control the lines.

Mobile phones will be used initially for verbal communication and BT have given a verbal undertaking that they would make every possible effort to re-route lines from the nearest point to the temporary computer suite in the shortest possible time. The line termination for the re-routed lines is provided as standard equipment in the temporary suite.

The ancillary equipment, modems, sharing devices and line splitting devices are mainly stock items and could be obtained immediately from manufacturers. Non-stock items would be provided within four weeks.

The Contractor's Telecoms Manager would be responsible for acquiring this equipment for installation in the CER.

#### 2.7.2.5 Enhanced Emergency Rescue Service

This service is intended to provide temporary back-up for loss of, or damage to essential equipment, cabling or services which place the Contractor's normal computer or business operations at risk.

The following equipment is available on a "supply of equipment only" basis within 24 hours for installation by the Contractor's own staff or by specialist third party contractor. The equipment is available on loan for a period not exceeding 1 month.

EQUIPMENT	CAPACITY
Mobile diesel generator	Up to 1,000 kVA
Frequency converter (400 Hz)	75 kVA
Chilled water	Up to 2 x 35 kW
UPS	400 kVA
Power Distribution units	Up to 2 x 180 kVA
Air-conditioning units	Up to 176 kW
Mobile air-conditioning units	2 x 10W
Temporary office cabins (24ft x 8ft)	6
CableEase RJ45 cabling system	375 x RJ45

## 2.8 DR Testing

During the implementation project and once a year the Contractor would undertake a Disaster Recovery Test. This test would recover the Contractor's solution to DR equipment housed at a Disaster Recovery Service supplier's recovery centre.

This test would be fully documented and all DR procedures would be updated following every test. The Authority would be invited to test the recovered HR and Payroll system at the Service Delivery Suppliers Recovery Centre.

The test during the implementation project will be completed prior to April 2006.

### 2.8.1 DR Test Planning

Tests will be scheduled in agreement of both the Contractor and the Authority.

Both the Authority and the Contractor will be involved in planning the nature and extent of the test.

Before each test, Terms of reference for the test will be agreed between the Contractor and the Authority.

### 2.8.2 DR Test Obligations

The Contractor will provide:

A DR specialist to project manage the test including: planning the test, administering the test and manage post test activities

Technical and support personnel to assist with the planning, participate in the test, identify issues and recommend improvements and assist with post test activities.

The Authority will:

Assist in the planning of the test, participate in the test, assist in the recovery of the applications, data and assist in post test activities and managing notification and communication to the users involved.

### 2.8.3 DR Test Frequency

The Contractor will undertake a one standard test, annually, with duration of two days in a rolling twelve month period.

The Contractor may wish to conduct additional tests during a calendar year to ensure that the Disaster Recovery Service is maintained in a ready state.

The Authority may request additional tests during a calendar year through the Change Control process and will incur additional service charges.

Any testing must be done in contiguous periods of 24 hours or part thereof and will be scheduled in agreement of both the Contractor and the Authority.

### 2.8.4 Standard Test

A standard test will include one Test Manager, one Technical Support resource and one Network support resource, provided by the Contractor

### 2.8.5 Non Standard Testing

A non-standard test i.e. a test conducted outside of the definition of a normal test that has been requested by the Authority will be subject to additional charges.

If the Contractor is requested to take part in any test of the Authorities Disaster Recovery and Business Continuity either as an integrated test of this plan and other plans of the Authority or to support a test of the other plans of the Authority, it will be subject to additional charges.

### 2.8.6 Success Criteria

The effectiveness of all testing will be measured against agreed DR Test Success Criteria.

The success criteria for each test will be defined in the Test Plan for each test. Measurement of this criteria will be conducted during the post test review and a test will not be considered successful until approved by the Authority.

The Contractor will provide test reports to the Authority from all tests.

### 2.8.7 Testing Notice Period

The Authority understands that any scheduled tests may be postponed by the Contractor with or without notice if the system becomes unavailable. The Contractor will also postpone a test involving their Disaster Recovery Supplier, should the supplier ask the Contractor to vacate following the

invocation by another of their clients. Under these circumstances the Contractor will be asked to vacate from the suppliers premises within two hours.

Tests / rehearsals may also be postponed by the Authority. If the postponement is within 30 days of the scheduled date for the test / rehearsal the Authority is aware that there may be a loss of test days or additional charges.

If the test is postponed by either the Contractor or the Authority a retest will be scheduled at the earliest convenience.

## **2.9 Invocation**

The decision to invoke the Disaster Recovery and Business Continuity Plan will be reached via agreement between the Authority and nominated Duty Director who are the only individuals who are authorised to invoke any third party contracts. The Authority should also nominate individuals with the Authority to invoke the plan.

Any employee of either the Authority or the Contractor will have the right to put the Contractor on 'Standby' i.e. a state of readiness to invoke the plan. This will alert the relevant persons and third parties of a potential invocation.

### **3 Part B – Disaster Recovery**

*Part B of the Disaster Recovery and Business Continuity Plan will focus on ensuring that in the event of a disaster, recovery of the services occurs within the timeframes and in accordance with the disaster recovery service levels specified in the initial Disaster Recovery and Business Continuity Plan (“Disaster Recovery Service Levels”)*

#### **3.1 Introduction**

This part of the Disaster Recovery and Business Continuity Plan focuses on the normal service management processes and procedures that the contractor employees in the provision of the service to minimise risk and facility recovery either from a service failure or Disaster Recovery situation. Specifically:

- back-up policy and procedures;
- hardware maintenance;
- sub-contractors responsibilities; and
- Configuration Management

This section also defines the how it would approach recovery from each of the scenarios identified in Part A. It details the infrastructure available, the sub-contractor arrangements in place, the Authorities obligations and the testing and audit arrangements.

#### **3.2 Backup Methodology**

The back-up policy and procedure will be documented in detail in the Technical Design Plan Document. In summary:

- Daily on-line back-ups are taken of all servers and databases using Back-up Exec.
- Transaction logs are copied between pods on an hourly basis during service hours.
- The back-up will include the operating system environment, the application software and the application data.

#### **3.3 Data Verification Procedures**

The back-up schedule is monitored on a daily basis via Back-up Exec. If there is a failure it is reported by telephone, e-mail or fax to the Outsourcing Services service desk and the call is allocated to the relevant support team for resolution.

### **3.4 Tape Management**

After each daily on-line back up the tapes will be securely stored in a separate pod from the production environment in fire proof, locked carry cases. Each week all tapes are taken off site by a third party supplier and securely stored. All tapes are on a four-week tape cycle.

Back-up devices are cleaned when the back-up device indicates cleaning is required.

Before tapes are loaded into the back-up device an assessment is made of their condition. If appearance is substandard, the tape will be replaced.

If in the event of a disaster the latest back-up tape cannot be retrieved from the separate Pod, the latest off site tape will be requested from the third party supplier.

### **3.5 Hardware Maintenance and spares**

All hardware including servers and telecommunications components are covered by third party hardware maintenance. For servers, the maintenance arrangements in place are for 24 x 7 cover with a 4-hour engineer response to site. For firewalls, routers and switches the maintenance arrangements in place are for Monday to Friday, 09:00 – 17:00 with a 4-hour engineer response to site. The third parties will maintain spares sufficient to fulfil their obligations and service level and spares will be delivered under the four-hour response agreements.

### **3.6 Subcontractors Responsibilities**

The Contractor shall ultimately be responsible for all suppliers and subcontractors involved in the provision of the service to the Authority; including those engaged in the resolution of Disaster Recovery conditions.

Off site Tape Storage: Back-up tapes will be stored off site and can be retrieved within 2 hours.

Hardware Maintenance Suppliers would be responsible for carrying out any hardware repairs and supplying spares.

Disaster Recovery Suppliers would be responsible for mobilising hardware and making available a production environment for the Contractors technical consultants to restore the application

Telecommunications suppliers would be responsible for rectifying any communications failures.

### **3.7 Hardware Configuration Details**

Each support team involved in the provision of the service will maintain the configuration records for the hardware supported. This will include;

- Server Build Documents: For each server a build document is created and maintained following a change. Historical build documents are maintained to provide a change history.
- Switch Configuration: Current and historical configuration files are copied and maintained following a change.
- Router Configuration: Current and historical configuration files are copied and maintained following a change
- Firewall configuration and rule set: Current and historical configuration files and rule sets are copied and maintained following a change
- Asset Register: A register of the hardware and software assets is maintained.

The replacement hardware provided by the Disaster Recovery Supplier would be selected to provide an appropriate and similar infrastructure, which would allow the production environment to be restored. Whilst the hardware specification may differ slightly, the configuration of the application would remain the same.

### **3.8 Data Centre Site Audits**

Once a year the Contractor will complete a Disaster Recovery test over a specified week.

At the end of the week the Authority will be invited to test the recovered system. The Authority would also be given a copy of the Disaster Recovery Test Report. Any subsequent changes required to this plan as a result of the test will be agreed with the Authority before the Plan is updated.

### **3.9 Disaster Recovery Service Levels**

Once the production environment has been made available following invocation of a disaster; either through the Contractor's measures or through provision of replacement hardware from the chosen Disaster Recovery supplier, there may be a reduced response time performance. This is due to the replacement hardware being a logical representation of the solution. Disaster Recovery Service Levels will be discussed at the Business Impact Workshop and agreed thereafter.

### **3.10 Authority's Obligations**

The principle Authority obligations in respect of this Disaster Recovery Plan are as follows:

- To define the business priorities through Business Impact Assessment
- To participate in Risk Assessment
- To participate in the decision making process

- Approve the chosen Disaster Recovery Solution
- Test the Disaster Recovery Solution
- Advise the Contractor of any changes to its' internal Disaster Recovery and Business Continuity arrangements that would require the Disaster Recovery solution to be amended and updated. These changes shall be notified through Change Control procedures set out in Schedule 7.2.

## **4 Part C Business Continuity**

*Part C of the DR&BC Plan will focus on ensuring continuance of the Service in circumstance of the occurrence of a Disaster or a failure of disruption of an element of the Service.*

### **4.1 Introduction**

Once a DR scenario (small or large) was invoked the Contractor would use reasonable endeavours to ensure that normal service could be provided once the system(s) have been recovered, and plan for returning the service to its original infrastructure (where possible) whilst limiting any disturbance to the Authority's day to day access to the Production environment.

### **4.2 Disaster Recovery Scenarios**

As mentioned above a 'small DR' scenario would not normally cause any down time to the Production systems noticeable by the Authority with the exception of hardware faults to the Production shared storage.

#### **4.2.1 Invocation Procedures**

After a small DR scenario had been detected and appropriate remedial action taken, the Authority and the Contractor would arrange a meeting as soon as possible after the event, to discuss how critical business services could be maintained without further business disruption.

#### **4.2.2 Risk Analysis**

The Authority would assess the risks to its internal business processes and would request the Contractor to make an assessment of the resilience of the DR solution. This information would then be utilised to determine future courses of action to protect the DR solution from further degradation.

#### **4.2.3 Single Points of Failure**

The Contractor would take actions to eliminate where possible single points of failure in the DR solution. If any of these actions had new costs associated with them, then the costs would be presented to the Authority for approval before any action was taken.

#### **4.2.4 Business Continuity Maintenance**

The Authority and Contractor would review the DR solution periodically to ensure that it remained capable of delivering the required services to the Authority.

#### **4.2.5 Documentation of Business Processes**

Any changes to the DR configuration of the Contractor's solution and the procedures used to operate it would be recorded.

#### 4.2.6 Communication Strategy

The communication mechanisms to be utilised between the Contractor and the Authority would be agreed with the Authority, and incorporated into this document along with other detailed DR procedures once they are agreed.

Any updates to the DR & BC procedures would be discussed at the initial monthly and subsequent service review meetings.

#### 4.2.7 Reverting to Normal Service

The Contractor would look to restore the Production system to normal service as soon as possible. The Contractor would discuss with the Authority how to limit any additional down time during normal service hours whilst restoring Normal Service e.g. this may mean delaying the change until a maintenance window.

### 4.3 Authority Obligations

The principal Authority obligations in Business Continuity would be

- Participate in the decision making process
- Approve modified procedures to maintain Business Continuity
- Approve the process to revert to Normal Service
- Test the restored Production environment once implemented
- Approve release of the restored Production environment to the Authority's employees.