FUJ00001680

Document Title: **BUSINESS CONTINUITY FRAMEWORK**

Document Type: **SERVICE PROVISION PLAN**

Release: Not Applicable

Abstract: This document provides a Service Continuity Framework in response to Horizon Requirement 830 of schedule A15 and schedule N09 (the Network Banking Contingency Services).

Document Status: APPROVED

Originator & Dept: Tony Wicks, Pathway Customer Service Business Continuity.

Contributors:

Reviewed By:
(Internal Distribution:) Martin Riddell, Peter Jeram, Peter Burden, Bill Reynolds, Richard Brunskill, Pat Lywood, Mike Stewart, Graham Hooper, Mik Peach, David Wilcox, John Wright, Mike Woolgar, Simon Fawkes, James Stinchcombe, Dave Tanner, Pathway Library

External Distribution: Dave Hulbert - Post Office Limited, Post Office Limited Library

Approval Authorities: (*See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Martin Riddell	Director, Pathway Customer Service		
Dave Hulbert	Post Office Limited, Business Continuity Manager		

FUJ00001680

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	13/9/98	Initial draft	None
0.2	5/10/98	Incorporation of comments from Phil Preece(Horizon) and David Jones(Pathway)	None
0.3	11/11/98	Incorporation of further comments.	None
0.4	1/12/98	Incorporation of comments from P Preece.	None
0.5	20/1/99	Format revision. Introduction of test strategy	None
0.6	5/3/99	Incorporation of further comments from P. Preece (Horizon) and B Booth (Horizon)	None
0.7	15/4/99	Incorporation of further comments from P. Preece(Horizon), Paul Martin (Horizon), Andrew Parsonage (Horizon) and B Booth (Horizon)	None
0.8	30/04/99	Incorporated changes that addressed comments raised by P. Preece (Horizon).	None
1.0	02/05/99	Incorporated changes that address comments raised by P. Preece (Horizon).	None
1.1	02/06/99	Removed all references to DSS, BA and any services that were specifically documented in previous versions for the DSS.	None
2.0	18/06/99	Removed For NR2 from title and formalise version 1.1 changes.	None
3.0	02/08/99	Incorporates minor comments from Paul Martin (PON). Issued for approval.	None
3.1	19/10/99	Incorporates changes relating to comments received from Graham White (PON).	None
4.0	29/10/99	No changes made since V3.1, issued at whole integer for approval. (CCN 486c)	None
4.1	03/02/00	Amendments required which reflect the changes implemented in CSR2+ releases during 2000.	None
4.2	03/08/00	Additional changes for CI4 introduction. Specifically in the area of KMS and OCMS.	None
4.3	06/10/00	Incorporates comments on V4.2 and the AP and MBS services.	None

FUJ00001680

5.0	31/10/00	Document formally re-issued for approval	None
5.1	02/07/02	Major rewrite for the introduction of Network Banking and to document all applicable Horizon service changes since version 5.0 was approved.	None
5.2	24/07/02	Incorporates comments from an internal Pathway Customer Service comment cycle.	None
5.3	07/08/02	Incorporates comments from Dave Hulbert, Peter Burden and Mik Peach and is intended to be the final draft of this version.	None
5.4	29/08/02	Incorporates comments from Dave Hulbert and Bob Booth Post Office Limited	None
6.0	08/10/02	Document formally issued for approval after review by Post Office Limited and Pathway.	None

0.2 Review Details

Review Comments by :	*Date*
Review Comments to :	*Originator*

Mandatory Review Authority	Name
Director, Pathway Customer Service	Martin Riddell
Post Office Limited, Business Continuity Manager	Dave Hulbert *
Operations and Support Manager Pathway Customer Service	Peter Burden *
Pathway Technical Design Authority for Availability and Service Management	Simon Fawkes
Optional Review / Issued for Information	

(*) = Reviewers that returned comments

FUJ00001680

0.3 Associated Documents

REF	Reference	Version	Date	Title	Source
1.	CS/PLA/005			OBCS Business Continuity Plan	PVCS
2.	CS/PLA/006			APS Business Continuity Plan	PVCS
3.	CS/PLA/007			TPS and LFS Business Continuity Plan	PVCS
4.	CS/PLA/008			RDMC and MBS Business Continuity Plan	PVCS
5.	CS/PLA/011			Business Continuity Test Plan	PVCS
6.	CS/PLA/012			Systems Operate Business Continuity Plan	PVCS
7.	CS/PLA/013			Energis Network Business Continuity Plan	PVCS
8.	CS/PLA/014			DW and MIS Business Continuity Plan	PVCS
9.	CS/PLA/015			Horizon System Helpdesk Business Continuity Plan	PVCS
10.	CS/PLA/016			Systems Management Infrastructure Business Continuity Plan	PVCS
11.	CS/PLA/017			Fujitsu Services Bracknell Business Continuity Plan	PVCS
12.	CS/PLA/061			NBS and DRS Business Continuity Plan	PVCS
13.	CS/PLA/020			Loss of Campus Business Continuity Plan	PVCS
14.	CS/PLA/041			ACS Business Continuity Plan	PVCS
15.	CS/PLA/047			OCMS Business Continuity Plan	PVCS
16.	CS/PLA/048			KMS Business Continuity Plan	PVCS
17.	CS/PRD/021			Fujitsu Services (Pathway) Problem Management Process	PVCS
18.	CS/PRD/031			Fujitsu Services (Pathway) Customer Service Business Continuity Management Process	PVCS
19.	SU/MAN/018			Operations Procedures Manual Index	PVCS

FUJ00001680

20.	TD/DES/031			Resilience and Recovery Strategy for Release 2	PVCS
21.	VI/TSC/105			Technical Integrity & Networking Test Plan	PVCS
22.	SU/TRP/005			Technical Integrity & Networking Test Results	PVCS
23.	RS/ACS/002			Security Acceptance test Specification	PVCS
24.	SU/TRP/003			Release 2 Final Security Test Report	PVCS
25.	RS/POL/003			Access Control Policy	PVCS
26.	BP/PRO/003			Post Office Site Failure Contingency Procedure	PVCS
27.	CS/PRO/21			Release 2 Electronic Point of Sale Service	PVCS
28.	CS/PRO/25			Release 2 Access Control and User Administration Process & Procedures	PVCS
29.	CS/PRO/45			Release 2 Automated Payment Service	PVCS
30.	CS/PRO/48			Horizon System Help desk Processes & procedures Description	PVCS
31.	CS/PRO/24			Release 2 Operating Environment	PVCS
32.	CS/PRO/22			Order Book Control Service	PVCS
33.	CR/FSP/004			Service Architecture and Design Document	PVCS
34.	CS/QMS/007			Operations Manual for the Customer Service Directorate	PVCS
35.	TD/STR/001			Host Systems Storage Strategy	PVCS
36.	TD/DES/059			High-level Network Design for Release 2	PVCS
37.	TD/DES/033			Agent and Correspondence Server Resilience and Recovery for Release 2	PVCS
38.	TD/DES/086			Correspondence Server back-up Strategy	PVCS

FUJ00001680

39.	TD/DES/057			Auto-config and Rollout Resilience and Recovery Strategy	PVCS
40.	TD/DES/093			DYNIX/ptx Configuration for Main Host Site Fail-over and Fallback	PVCS
41.	TD/DES/034			High Level Design for Application Recovery after Fail-over using Maestro	PVCS
42.	TD/DES/092			Audit Server Resilience and Recovery for Release 2	PVCS
43.	SD/STR/002			FTMS Resilience and Recovery Strategy for Release 2	PVCS
44.	SD/STR/005			Data Warehouse Disaster Recovery Strategy	PVCS
45.	CON/MGM/005			Post Office Limited and Fujitsu Services Business Continuity Interface Agreement	Post Office Limited
46.	CR/PRP/004			Post Office Limited Disaster Recovery Interface Service (TIP DR)	PVCS
47.	CS/REP/046			Business Continuity Operational Test Report (1999)	PVCS
48.	NB/SDS/007			System Design Specification for Network Banking End-to-End Service	PVCS
49.	NB/SPE/001			Network Banking Statement of Requirements	PVCS
50.	SY/SPG/002			Agent and Correspondence Server Resilience and Recovery Operations Support Guide	PVCS
51.	PA/TEM/001			Fujitsu Services Document Template	PVCS

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

FUJ00001680

0.4 Abbreviations/Definitions

Abbreviation	Definition
ACS	Auto Configuration Service
AP	Automated Payments
APS	Automated Payments System
BCF	Business Continuity Framework
CSR	Core System Release
DRS	Data Reconciliation Service
DW	Data Warehouse
EPOS	Electronic Point of Sale
HAPS	Host Automated Payments Service
HSHD	Horizon System Help Desk
KMS	Key Management Service
LFS	Logistics Feeder Service
LNS	L2TP Network Server
MBCI	Major Business Continuity Incident
MBS	Message Broadcast Service
MIS	Management Information Service
NB	Network Banking
NBE	Network Banking Engine
NBR	Network Banking Requirement
NBS	Network Banking Service
NRO	National Roll Out
OBCS	Order Book Control Service
OCMS	Outlet Change Management System
POL	Post Office Limited
RAB	Release Authorisation Board
RD	Reference Data
RDMC	Reference Data Management Centre
SIAM	Service Impact Assessment Module
SMC	Systems Management Centre

FUJ00001680

SSC	System Support Centre
SOS	Systems Operate Service
TIP	Transaction Information Processing
TMS	Transaction Management Service
TPS	Transaction Processing Service

0.5 Changes in this Version

Version	Changes
5.1	Major rewrite for the introduction of Network Banking and to document all applicable Horizon service changes since version 5.0 was approved.
5.2	Incorporates amendments to address comments raised by Peter Burden on an internal Pathway Customer Service comment cycle.
5.3	Incorporates comments from Dave Hulbert (Post Office Limited BCM), Peter Burden and Mik Peach
5.4	Incorporates amendments for comments detailed in Quality Review Comment Sheet QR2156from Bob Booth and Dave Hulbert Post Office Limited

0.6 Changes Expected

Changes
It is expected that this document will be revised when the Debit Card Service is introduced.

FUJ00001680

0.7 Table of Contents

FUJ00001680

FUJ00001680

1.0 Introduction

A key requirement in the Pathway solution is that of business continuity i.e. ensuring there are operational processes and procedures in place to ensure that any component failure has minimal effect on the service provided.

This will cover failures in the core Fujitsu Services (Pathway) services e.g. NBS, TPS, APS etc, support services and client services where appropriate.

A principle requirement specified within Requirement 830 of schedule A15, is the provision of contingency plans which conform to an overall 'Service Continuity Framework'.

It is the objective of this document and associated contingency plans to satisfy that requirement and Fujitsu Services (Pathway) and Post Office Limited have agreed that the title of this document should be 'Business Continuity Framework'.

Specifically this document will cover the following areas.

a) Provide a baseline definition of the Business Continuity Framework and contingency plans as specified in Requirement 830.

b) Provide a detailed definition of Fujitsu Services (Pathway) deliverables associated with business continuity and the methods of review and assurance.

c) Define the contents and format of the contingency plans.

d) Define the overall test strategy adopted for testing of the contingency plans.

e) Define the management processes for the management of Major Business Continuity Incidents.

2.0 Scope

The scope of this document is targeted towards the Acceptance Review process associated with Requirement 830. It also includes acceptance of other contingency-related requirements as specified at 2.1. The method of acceptance will be specified as appropriate.

The general framework defined in this document is release-independent.

This document does not include any details in respect of the technical testing of the recovery processes, however REF22 does.

2.1 Related Requirements

For completeness, the following list identifies the other requirements related to Business Continuity for:

Core System Release: 699, 803, 816, 820, 828, 831, 834, 891, 894, 911, 913, and 914

Network Banking Release: NBR276, NBR472 and NBR513 as defined in REF 49.

FUJ00001680

3.0 Definitions

Business Continuity Framework is this document, which has been generated to satisfy the requirement for a Service Continuity Framework.

At a working level, Post Office Limited and Fujitsu Services (Pathway) generally recognise the term Business Continuity as having three closely related components:

Resilience may be defined as the steps taken to avert a loss of service or disaster or reduce the likelihood of a disaster or loss of service.

Contingency may be defined as the interim processes and procedures adopted during the loss of service.

Recovery may be defined as the business and technical arrangements to restore a lost system or service and manage the process of reversion to normal processing and full resumption of service.

FUJ00001680

4.0 Framework Overview

4.1 Introduction

The Business Continuity Framework defines the methodology agreed between Fujitsu Services (Pathway) and Post Office Limited for handling all aspects of Business Continuity. This section defines the elements of the Business Continuity Framework for the Horizon (CSR) and Network Banking releases.

The constituent elements of the Business Continuity Framework may be represented as follows. Each element will be looked at in more detail below.

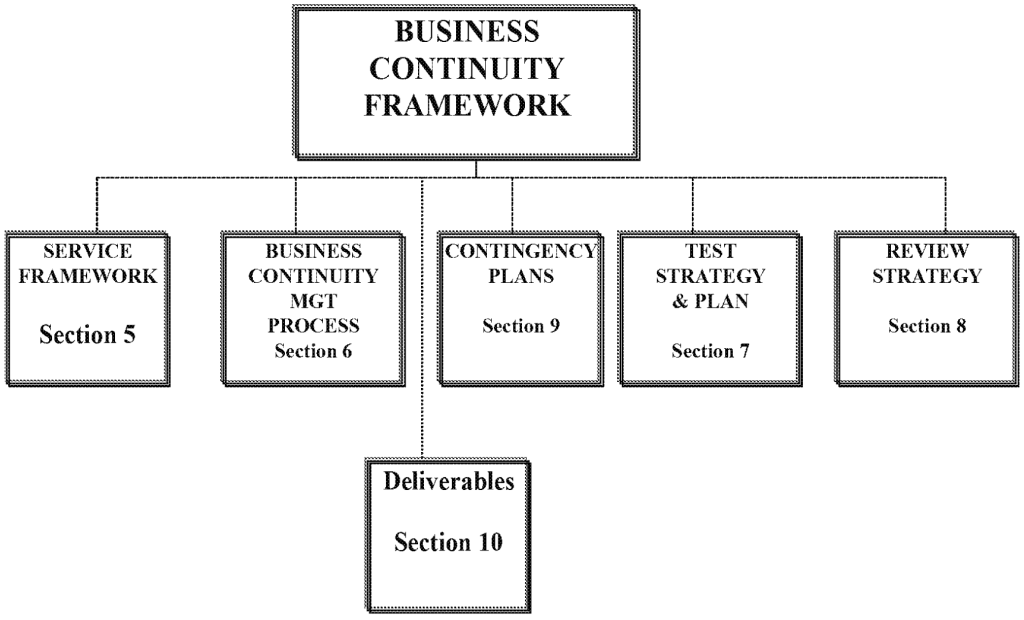

Figure 4.1 Service Elements

FUJ00001680

4.1.1 Contingency Plans

Although Requirement 830 defines the provision of a Contingency Plan, in practice there are a number of contingency plans. There is a plan for each major service element. The contents of the contingency plans are specified within Requirement 830. All plans must be of the document type Contingency Plan and shall contain Continuity Plan within the title. Each plan shall have a specified owner. (Further details in section 9)

Whilst a number of Fujitsu Services (Pathway) business continuity plans already exist, having been created for the CSR release, this document has been written to define the contents of Business Continuity plans and therefore generally uses future phraseology.

Major elements of the plan follow.

4.1.1.1 Service Definition

The BCF shall be defined in terms of services rather than components of infrastructure. The definitions of the services that are a subject of the BCF are defined in this document. This is looked at in more detail in section 5.

4.1.1.2 Risk Analysis And Service Impact

Each contingency plan will identify all potential risks in terms of likelihood and service impact.

Once an incident occurs which has a service continuity impact, there must be a mechanism in place to assess the impact of the incident and the possible effect(s) it will have on the end to end service. This is fairly complex and will be dependant upon time of day and therefore will be a real-time process i.e. the impact of the service failure at 2am will be different from the impact at 8pm. However, a high-level impact statement will be included in the relevant contingency plan.

4.1.1.3 Escalation Contacts

Each contingency plan will contain escalation routes in conformance to Cross-Domain Business Continuity management processes.

4.1.1.4 Resilience Strategy documents

Each contingency plan will contain, where appropriate, references to the underlying resilience strategy document and/or technical design documents.

4.1.1.5 Contingency Procedures

Each contingency plan will contain a section defining contingency actions.

From an operational perspective contingency actions are documented in a number of places, depending upon the severity of the service element failure.

1, Within operational procedures, subordinate to REF19. Where appropriate the contingency plan will make reference to the relevant operations manual.

FUJ00001680

2, Where appropriate, contingency actions are documented within the Action column of the Risk Analysis (and service impact) section of each plan.

3, Where appropriate, for potential MBCIs and MBCI contingency actions are documented in the contingency section of each plan.

4.1.2 Service Framework

Section 5 contains details of the service elements and components together with their relationship to each of the contingency plans.

4.1.3 Business Continuity Management Process

The resolution of incidents will be dealt with through the standard Help Desk Incident Management process.

In the event of a Major Business Continuity Incident there will be a need for controlled and co-ordinated activity across Pathway and Post Office Limited. (See section 6)

4.1.4 Test strategy and plans

The test schedule and method will be defined as a separate document (REF 5) and will be referred to within the contingency plans. The overall high-level strategy will be defined in this document for agreement. (See section 7)

4.1.5 Review strategy

A review strategy defines the joint review mechanism prior to acceptance and also the review mechanism of the processes following acceptance. This is defined in a later section for agreement. (See section 8)

4.1.6 Deliverables and Acceptance Methods

Section 10 defines the deliverables required to satisfy the Business Continuity requirements of Fujitsu Services (Pathway).

Also included in that section is the method of acceptance planned for each deliverable.

FUJ00001680

5.0 Service Framework

5.1 Introduction

Although Requirement 830 makes reference to a single contingency plan, this is impractical in terms of contingency planning as the impact and effects of any failure will vary for each service.

Having identified the requirement for a number of contingency plans there is an option of making each plan based upon major system components, for example produce a contingency plan for host hardware failure.

The disadvantage in this methodology is that in the case of a major host hardware failure, although there may be a generic recovery process to recover the databases, there will be totally different contingency actions in terms of service impact and escalation for each of the services on the host e.g. the business impact on APS. It is for this reason that the chosen framework is principally service based. The end-to-end solution is split into a number of constituent services as defined in the following section. These services are split into areas:

a) Pathway Core Services. These are services directly within the Pathway contractual boundary and for which Pathway have full responsibility for operations and maintenance. These services are directly involved in the receipt, processing and delivery of business data

b) Pathway Support and Supplier Services. These are services that provide support functionality but are not involved in business data traffic as above. Examples of these services would include the Horizon Systems Helpdesk and Energis.

c) Client Services. These are services that are beyond the Pathway contractual boundary but are part of the end-to-end business data traffic flow.

Additionally there are Service Components. These represent a part of the system infrastructure and can be an individual component such as a Correspondence Server, or a major component such as a Pathway Campus.

5.2 Service Breakdown

For the purposes of Business Continuity planning the contingency plans will be produced for the end to end service. From an operational perspective it is impracticable for these plans to cover every element or component in the end-to-end service, e.g. an unserviceable power lead in a single counter outlet, however major components will be documented.

The core service elements and support services are show in Figure 5.2 below.

FUJ00001680

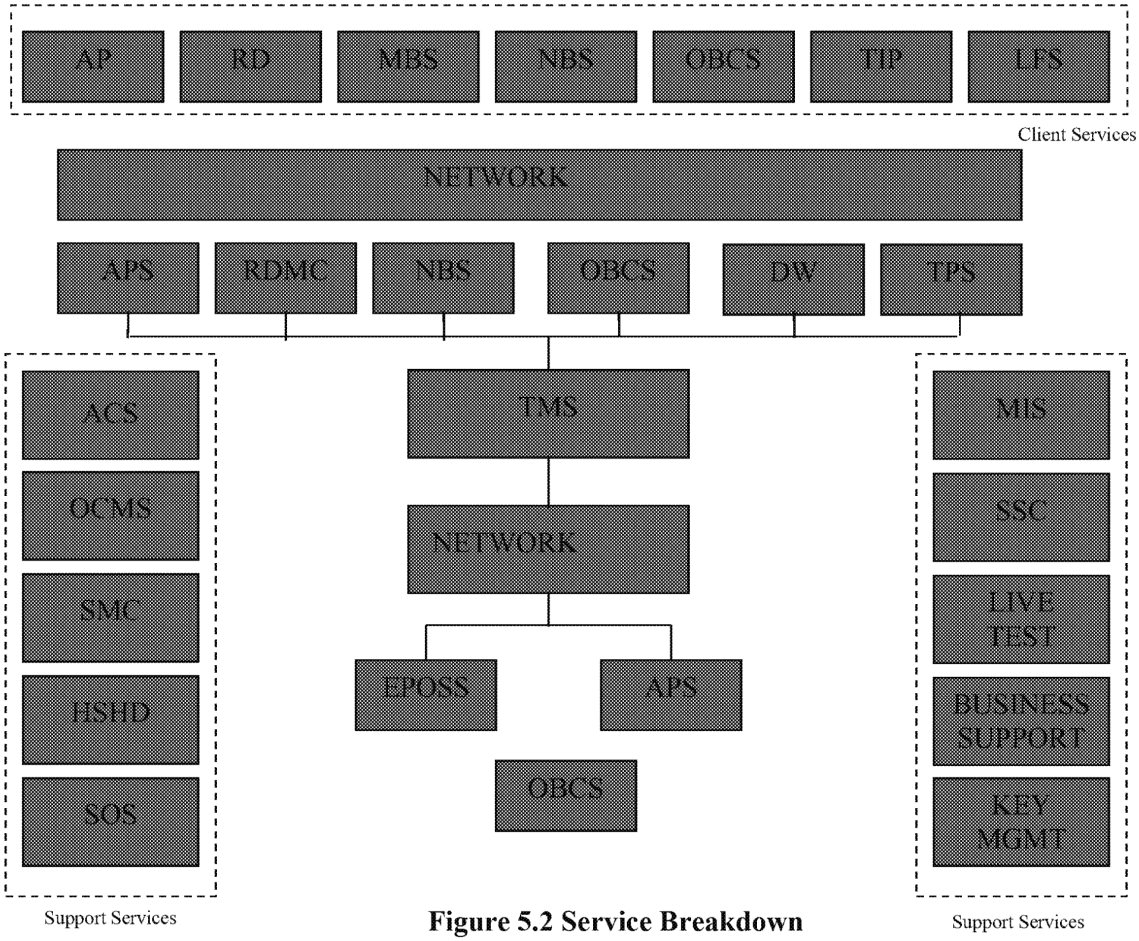

Figure 5.2 Service Breakdown

Notes:

1, the contingency planning for TMS layer and for Networks will be included within the individual service contingency plans.

2, the Data Reconciliation Service, which is responsible for reconciling all NBS transactions reported to the NBE, shall be included within the NBS contingency plan.

5.3 Service to Plan Relationship Table

Table 1 below identifies which contingency plan addresses each of the service elements in Figure 5.2 above:

FUJ00001680

Table 1

Service or Service Element	Expansion of Acronym	Related Contingency Plan(s)	Test Ref. (Table 7.2)
AP	Automated Payments	APS	20
APS	Automated Payment Service	APS	2,3,4,5,6,7
BUSINESS SUPPORT		Fujitsu Services Bracknell	1
DRS	Data Reconciliation Service	NBS/DRS	2,3
DW	Data Warehouse	MIS/DW	13
EPOSS	Electronic Point of Sale System	APS, TPS/LFS	2,3,4,5,6,7
HSHD	Horizon Systems Helpdesk	HSHD	10
KMS	Key Management Service	KMS	19
LIVE TEST		Fujitsu Services Bracknell	1
LFS	Logistics Feeder Service	TPS/LFS	2,3,4,5,6,7
MBS	Message Broadcast Service	RDMC/MBS	1,9
MIS	Management Information Systems	Fujitsu Services Bracknell	13
NETWORK		Energis, APS, OBCS, TPS/LFS, NBS/DRS	2,3,4,5,6,7,15 ,22
NBS	Network Banking Service	NBS/DRS	2,3,5,6,16,22, 23
OBCS	Order Book Control Service	OBCS	2,3,4,5,6,7
OCMS	Outlet Change Management System	OCMS	17
RDMC	Reference Data Management Centre	RDMC/MBS & Fujitsu Services Bracknell	1,9
ACS	Auto Configuration Service	ACS	8
SMC	Systems Management Centre	SMC	12
SOS	Systems Operate Service	SOS	11
SSC	Systems Support Centre	Fujitsu Services Bracknell	1,14
TIP	Transaction Information Processing	TPS/LFS	2,3,4,5,6,7,18
TMS	Transaction Management System	APS, OBCS, TPS/LFS	2,3,4,5,6,7,18
TPS	Transaction Processing Service	TPS/LFS	2,3,4,5,6,7,18

FUJ00001680

6.0 Business Continuity Management Process

An incident is an unplanned occurrence that adversely impacts upon the normal service in some important way. The scale of the event can range from a minor fault to a major outage e.g.:

Minor incident e.g. Horizon terminal failure affecting service at an individual outlet.

Major incident e.g. outage of key back-end system affecting service at 17,500 outlets.

The resolution of minor incidents will be dealt with through the standard Help Desk Incident Management process.

Major Business Continuity Incidents will have a significant impact upon Post Office Limited. In such cases there will be a need for controlled and co-ordinated activity across supplier organisations and Post Office Limited. Consequently all Major Business Continuity Incidents will be managed via the 'Fujitsu Services (Pathway) Customer Service Business Continuity Management' process (REF 18) and the Post Office Limited and Fujitsu Services Business Continuity Interface Agreement (REF 45). These documents support the immediate escalation of major incidents to a Cross Domain Business Continuity Management Team (BCMT). The BCMT consists of operational managers from each organisation.

FUJ00001680

7.0 Test Strategy and Plans

7.1 Requirement

Requirement 830 states the requirement as follows

' *The contingency plans shall include a testing strategy with two distinct parts*

a) *Initial testing before commencement of RollOut of Services*

b) *Regular testing'*

The testing requirements for Network Banking are specifically stipulated in Codified Agreement Schedule N09 and are detailed in sections 7.2.2 and 7.3 below.

7.2 Initial Testing

7.2.1 Core System Release

Initial technical testing of technical processes, e.g. database recovery, was conducted as part of the technical testing specified in REF 21 which was covered in Pathways Technical and Security Test Programme and a joint report showing the results of this testing was issued. (see REF 22).

Prior to CSR National Rollout the applicable contingency plans were operationally tested, using the test plans defined in REF5, to validate the integrity of those plans. The results of this testing is reported in REF 47.

7.2.2 Network Banking

Before Network Banking Live Pilot, Fujitsu Services (Pathway) shall carry out initial testing of NBS business continuity plans and facilities through procedural walkthroughs which shall (subject to any agreement to the contrary between the parties) include initial testing of technical processes and the production of test reports.

Before Network Banking Go-Live (Network Banking operating in all outlets) Fujitsu Services (Pathway) shall carry out live operational test(s) of the business continuity plan for the following elements of the NBS:

1, Bootle Data Centre failure

2, Host Central Server failure

3, LNS, ISDN Router failure

4, An NBS Authorisation Agent failure

5, Failure of the NBS/NBE Interface.

These tests are to be incorporated in REF5.

FUJ00001680

7.2.3 New Services

Where services are introduced as part of a new release the Test Plan (REF5) will be revised to include the Business Continuity testing of those services and define when the initial testing will be conducted.

The level and schedule of testing is dependent upon operational constraints and is accomplished by a mix of operational tests and procedural walk-through. Where involvement is required from Post Office Limited the test schedule will be agreed in advance.

In addition customer-initiated test activity may be included, with Pathway agreement, within the Business Continuity Test Plan (REF5).

7.3 Ongoing testing

For ongoing testing, an overall test strategy will be produced defining for each service:

a) name of service

b) ownership of testing plan

c) type of testing i.e. procedural walk-through or operational test

d) frequency of testing and scheduled dates

e) test objectives, conditions, script and expected results

f) other units taking part

g) criteria for success and failure

h) test reports and follow-up

On-going business continuity tests will be conducted, after Network Banking Go-Live, in accordance with the test methodology and frequency agreed in N09 and defined in table 2. These tests may be cancelled or rescheduled and/or the method used for a test may be varied for operational business reasons by agreement in writing between Post Office Limited and Fujitsu Services (Pathway) Business Continuity Managers. Such agreement is not to be unreasonably withheld.

FUJ00001680

Table 2

Test No.	Business Continuity Test	Test Methodology and Frequency	Owner	Ass Doc Ref. Section 0.3
2	Fujitsu Services (Pathway) Campus failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	13
3	Sequent Host Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	1,2,3
4	Correspondence Server Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	1,2,3
5	LNS/ISDN Router Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	1,2,3
6	Datacentre LAN Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	1,2,3
7	Agent Platform Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	1,2,3
9	RDMC failure	Operational Test Environment once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	4
16	Network Banking Authorisation Agent	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	12
22	Network Banking Engine Interface	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (Pathway)	12
23	Network Banking Service Reconciliation Service	Integrated within test 3.	Fujitsu Services (Pathway)	12

All other on-going business continuity test details will be defined on an annual basis and included within the yearly schedule in REF5. The Fujitsu Services (Pathway) Business Continuity Manager will be responsible for the planning of the other on-going tests, i.e. those not defined in table 2, and will co-ordinate and schedule activity as appropriate with the Post Office Limited Business Continuity Manager and suppliers.

FUJ00001680

8.0 Review Strategy

A Business Continuity Steering Group has been established between Post Office Limited and Fujitsu Services (Pathway). This group reviews the progress of each release against the Fujitsu Services (Pathway) delivery and acceptance plans. It also facilitates the co-ordination of joint development review and assurance activities where necessary. This forum also provides an objective feed into the release authorisation process for new releases.

This team, or subset of the team, reviews all aspects of business continuity on an ongoing basis, during Live Trials and beyond. The remit of the team is to continually look at ways of improving cross-domain business continuity processes.

FUJ00001680

9.0 Contingency Plans

Throughout section 9, the use of *Italics* denotes the actual words in requirement 830 of the contract.

The contingency plans shall be based on impact and risk assessments and agreed between the CONTRACTOR and AUTHORITIES by a date consistent with the Project Plan.

9.1 Ownership of Plans

'*Ownership of all contingency actions shall be identified in the contingency plans'*

Each contingency Plan will clearly state the owner of the plan who is responsible for the definition, maintenance, testing and review of the plan.

In addition to this, the Fujitsu Services (Pathway) Business Continuity Manager will have overall responsibility for the development, co-ordination and integration where appropriate of all Contingency Plans and providing Post Office Limited with a single point of contact.

9.2 Plan Activation

'*The contingency plans shall include activation procedures and time periods within which the contingency measures shall be activated'*

Where appropriate Contingency Plans will contain a risk and impact assessment for both the core post office day (08:00 to 20:00) and the non-core post office day (20:00 to 08:00). (See 9.3). For services where the impact of the service element failure is common throughout the day, a single risk and impact assessment will be documented.

The risk assessment identifies the critical time periods for activation of contingency measures and identifies the associated contingency actions.

9.3 Impact and Risk Assessment

'*The contingency plans shall be based on impact and risk assessments'*

Contained within each service are a number of critical components, the failure of which would cause a potential service disruption. Consideration shall also be given to the impact arising from the loss of building or staff. Each of these critical components and the associated failure scenarios will be identified and documented within a risk and impact matrix within the Contingency Plan. This matrix is used as a tool to present in a tabular form all risks identified with a service together with the impact of that risk occurring, the time after which that impact becomes critical, and the contingency actions to be taken.

Associated with each of the above elements are impact statements, which will define the likely business impacts of failure of the critical components. To aid in the definition of these, each Contingency Plan, where appropriate, will contain a schematic defining the operational day for that particular service. SLA liabilities will

FUJ00001680

be used as an aid in determining business impact. Where the impact triggers either a Potential MBCI or an MBCI, the appropriate action will be identified from within the matrix.

Associated with the impact statement will be a reference to the specific recovery and contingency procedures required.

Business impact assessment will be reviewed jointly with Post Office Limited and will be subject to ongoing review.

The combination of risk and impact will also determine the level of ongoing testing that will form part of the testing strategy.

9.4 Other Requirements

'*The contingency plan shall include, without limitation, the following*

a) *Prevention measures*

b) *Preparedness measures*

c) *Contingency measures*

d) *Recovery of normal service*

e) *Contacts list'*

In addition to the above the plans shall include details of the individual services, references to the relevant operations manual and references to the underlying resilience strategy document and/or technical design documents, where appropriate.

9.4.1 Preventative Measures

Preventative measures are defined as those measures that are in place to prevent service continuity failures in the first place. There are two aspects that are considered.

9.4.1.1 Technical Design

A key element of the design of the service is the elimination of single points of failure and the ability to Fail-over to a replicated operational facility and/or environment and to recover the service in a timely manner.

This capability is documented in a number of technical design documents, which in turn are referenced within the relevant Contingency Plans.

9.4.1.2 Security

Another preventative measure is the denial of access to the service to anyone who may wish to deliberately cause disruption. Although not mentioned specifically within Contingency Plans, this requirement is met through general conformance to Access Control Policy (REF25) and the Security Functional Specification (REF23).

9.4.2 Preparedness Measures

Preparedness measures are implemented in a number of ways:

FUJ00001680

a) The provision of risk and impact assessments, along with references to appropriate recovery and contingency procedures will allow appropriate actions to be carried out in a pre-prepared manner.

b) Initial technical testing and the operational testing of Contingency Plans will ensure all activation of the Plans will have been carefully rehearsed.

c) Joint process and procedure walk-through will, as above, ensure all Cross-Domain (multi-party) Business Continuity processes are tested thoroughly.

9.4.3 Contingency Measures

Contingency measures may be defined as the actions to be performed in the event of a service break to enable business impact to be minimised during the service outage prior to recovery being completed.

Contingency measures will include the recognition, activation, incident management and initiation of recovery procedures. These will be documented within the contingency plan and also as references to supporting documentation.

An example of contingency measures is failing over the host server in the event of the prime server experiencing a failure.

9.4.4 Recovery of Normal Service

These procedures will be mainly of a technical operational nature and will mainly refer to technical procedures defined within the Fujitsu Services (Core Services) Operational Procedures Manual REF19. There may be references to other activities that may impact across service boundaries. Where appropriate these will be referenced within the plan.

9.4.5 Contact List

Each contingency plan will document the contacts for initial contact and technical liaison where appropriate, together with details of escalation contacts. This will be in accordance with the Business Continuity Management process.

FUJ00001680

10.0 Deliverables and Acceptance Methods

10.1 Introduction

This section defines the deliverables required to satisfy the Business Continuity requirements of Fujitsu Services (Pathway).

Also included within this section is the method of acceptance planned for each deliverable.

Section 7.2.1 of this document defines the technical and initial business continuity testing for the CSR release. The business continuity initial test results for CSR were published in the Business Continuity Operational test Report (1999) REF47.

Section 7.2.2 of this BCF defines the initial business continuity tests that are to be conducted as part of the Network Banking Service Acceptance Process.

Methodologies used in the acceptance process include those identified below:

10.1.1 Joint Review

Joint review is by circulation of, discussion about and agreement upon the structure and content of a document by Fujitsu Services (Pathway) and Post Office Limited.

10.1.2 Document Inspection

Formal inspection of a paper copy, by Post Office Limited, of a commercially sensitive (i.e. technical design) or Service Provider (i.e. Fujitsu Services Core Services) operational document, by the appropriate reviewing authorities, whilst under supervision by the document owner. No paper or electronic copies must be taken. Objective of this process is to verify the existence of the document; no approval rights are associated with this activity.

Inspection to take place at the premises of the document owner.

10.1.3 Procedural Walkthrough

A paper based technique whereby a scenario is selected and the actions and procedures of those Service Delivery Units (SDU) impacted followed through to ensure that both individual service delivery unit procedures, and cross boundary SDU procedures, are both complete and fully integrated. Where appropriate, i.e. affecting Post Office Limited services, Post Office Limited will be invited to procedural walkthroughs.

10.1.4 Operational Test

An exercise using live operational service components, or where more appropriate and agreed by Post Office Limited a test environment, whereby a scenario is selected and the actions and procedures of those Service Delivery Units (SDU) impacted are followed through. This is to ensure that both individual service delivery unit procedures, and cross boundary SDU procedures are both complete and fully

FUJ00001680

integrated, and that the desired outcome on the operational service components is achieved. This is then followed by the total regression of any changes made to the live service components.

An example of live operational functionality testing was the Campus Fail-over test that was conducted during CSR Live Trial. An example of a business continuity operational test in a test environment is the verification of recovery procedures for the Reference Data RDT Host.

10.2 Contract Controlled Documents

10.2.1 Summary

This section includes all references to current Contract Controlled Documents relating to Business Continuity.

10.2.2 Deliverables List

Document	Document Reference	Remarks/Acceptance Method
Business Continuity Framework	CS/SIP/002	Joint Review and sign-off
Horizon Systems Helpdesk Continuity Plan	CS/PLA/015	Joint Review and sign-off

FUJ00001680

10.3 BCF Referenced Documents

10.3.1 Summary

This section summarises all the business continuity deliverables specified within the BCF:

10.3.2 Deliverables List

Plan	Document Reference	Owner	Review method
Fujitsu Services (Pathway) Business Continuity Operational Test Plan	CS/PLA/011	Fujitsu Services (Pathway)	Joint review
Fujitsu Services (Pathway) Business Continuity Management Process	CS/PRD/031	Fujitsu Services (Pathway)	Not Applicable
Operations Manual for the Customer Service Directorate	CS/QMS/007	Fujitsu Services (Pathway)	Document inspection to verify existence of procedures
Operations Procedures Manual Index	SU/MAN/018	Fujitsu Services (Core Services)	Document inspection to verify existence of procedures
OBCS Business Continuity Plan	CS/PLA/005	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
APS Business Continuity Plan	CS/PLA/006	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
TPS and LFS Business Continuity Plan	CS/PLA/007	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
RDMC and MBS Business Continuity Plan	CS/PLA/008	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
Data Warehouse and MIS Business	CS/PLA/014	Fujitsu Services	Document inspection to verify

FUJ00001680

Continuity Plan		(Pathway)	compliance with BCF
Energis Network Business Continuity Plan	CS/PLA/013	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
Systems Operate Service Business Continuity Plan	CS/PLA/012	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
Systems Management Infrastructure Business Continuity Plan	CS/PLA/016	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
Fujitsu Services Bracknell Business Continuity Plan	CS/PLA/017	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
Loss of Campus Business Continuity Plan	CS/PLA/020	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
ACS Business Continuity Plan	CS/PLA/041	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
OCMS Business Continuity Plan	CS/PLA/047	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
KMS Business Continuity Plan	CS/PLA/048	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF
NBS and DRS Business Continuity Plan	CS/PLA/061	Fujitsu Services (Pathway)	Document inspection to verify compliance with BCF

FUJ00001680

10.4 Technical Design Documentation

10.4.1 Summary

This section contains all technical design documentation relating to Business Continuity.

10.4.2 Deliverables List

Document	Document Reference	Owner	Review method
Resilience and Recovery strategy for Release 2	TD/DES/031	Fujitsu Services (Pathway)	Note 2
Host Failover strategy	TD/STR/001	Fujitsu Services (Pathway)	Note 2
High-level Network Design for Release 2	TD/DES/059	Fujitsu Services (Pathway)	Note 2
Agent and Correspondence Server Resilience and Recovery for Release 2	TD/DES/033	Fujitsu Services (Pathway)	Note 2
Correspondence Server back-up Strategy	TD/DES/086	Fujitsu Services (Pathway)	Note 2
Auto-config and Rollout Resilience and Recovery Strategy	TD/DES/057	Fujitsu Services (Pathway)	Note 2
DYNIX/ptx Configuration for Main Host Site Fail-over and Fallback	TD/DES/093	Fujitsu Services (Pathway)	Note 2
High Level Design for Application Recovery after Fail-over using Maestro	TD/DES/034	Fujitsu Services (Pathway)	Note 2
Audit Server Resilience and Recovery Release 2	TD/DES/092	Fujitsu Services (Pathway)	Note 2
FTMS Resilience and Recovery	SD/STR/002	Fujitsu Services (Pathway)	Note 2
Data Warehouse Disaster Recovery Strategy	SD/STR/005	Fujitsu Services (Pathway)	Note 2
Agent and Correspondence Server Resilience and Recovery Operations Support Guide	SY/SPG/002	Fujitsu Services (Pathway)	Note 2

FUJ00001680

10.4.3 Review Method

NOTE	METHOD	SUCCESS CRITERIA
1	Document inspection to verify compliance with BCF if required by customer. Confidentiality Restrictions apply. Inspection on Fujitsu Services (Pathway) site by suitable qualified customer staff with no copying of document	Not applicable
2	A review of the technical design documentation does not form part of the Network Banking acceptance process.	Not applicable

10.5 Customer Contingency Plans and Pathway Deliverables in Support of Plans

10.5.1 Summary

This section summarises the deliverables produced by Fujitsu Services (Pathway) in support of external contingency plans. It also contains reference to the associated external Contingency Plan for completeness

10.5.2 Deliverables List

No documents are required in support of external contingency plans