

Fujitsu Services **BUSINESS CONTINUITY FRAMEWORK** Ref: CS/SIP/002
Version: 9.0
COMMERCIAL-IN-CONFIDENCE Date: 19-Oct-2004

Document Title: **BUSINESS CONTINUITY FRAMEWORK**

Document Type: **SERVICE PROVISION PLAN**

Release: Not Applicable

Abstract: This document provides a Service Continuity Framework as required by Schedule 21 of the Varied and Restated Codified Agreement

Document Status: APPROVED

Originator & Dept: Tony Wicks, Post Office Account, Customer Service Business Continuity.

Contributors:

Reviewed By: Dave Baldwin, Peter Burden, Carl Marx, Peter Thompson, John
(Internal Distribution:) Holman-Dine, Bill Reynolds, Richard Brunskill, Mike Stewart, Bill Mitchell, Mik Peach, David Wilcox, John Wright, Mike Woolgar, Simon Fawkes, James Stinchcombe, Dave Tanner, Post Office Account Library

External Distribution: Richard Ashcroft- Post Office Limited, Post Office Limited Library

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

Name	Position	Signature	Date
Dave Baldwin	Director Customer Service, Post Office Account		
Richard Ashcroft	Post Office Limited, Service Continuity Manager		

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
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	None

Fujitsu Services

BUSINESS CONTINUITY FRAMEWORK

Ref: CS/SIP/002

Version: 9.0

COMMERCIAL-IN-CONFIDENCE

Date: 19-Oct-2004

		version 5.0 was approved.	
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
6.1	07/11/02	Introduces the Technical Support Desk and the Debit Card System.	None
6.2	27/11/02	Incorporates a recommended improvement from Peter Burden.	None
7.0	17/12/02	Document formally issued for approval after review by Post Office Limited and Pathway.	None
7.1	12/01/04	Major rewrite for the introduction of the Varied and Restated Codified Agreement and to reflect the Horizon contingency documents being condensed into three Business Continuity Plans during 2003.	None
8.0	11/02/04	Document formally issued for approval after review by Post Office Limited and Post Office Account.	None
8.1	04/06/04	Major update for S55, S60, S70 and S75 Horizon infrastructure changes	None
8.2	12/07/04	Incorporates comments from Peter Burden and amendments identified by Tony Wicks	None
8.3	30/10/04	Incorporates comments from Post Office Limited as per QR 3572.	None
9.0	19/10/04	Nil comments returned from comment cycle. Incorporated amendment to reflect recent organisational changes in Post Office Account.	None

0.2 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks

Mandatory Review Authority	Name
Director, Customer Service, Post Office Account	Dave Baldwin
Post Office Limited, Service Continuity Manager	Richard Ashcroft*
Infrastructure and Availability Manager Customer Service, Post Office Account	Carl Marx
Post Office Account Technical Design Authority for Availability and Service Management	Simon Fawkes
Optional Review / Issued for Information	
Post Office Account Technical Design Authority for Networks	Dave Tanner
Post Office Account Customer Services Manager	Peter Burden

(*) = Reviewers that returned comments

0.3 Associated Documents

REF	Reference	Version	Date	Title	Source
1.	CS/PLA/079			The Horizon Services Business Continuity Plan	PVCS
2.	CS/PLA/080			The Horizon Support Services Business Continuity Plan	PVCS
3.	CS/PLA/011			Business Continuity Test Plan	PVCS
4.	CS/PLA/015			Horizon System Helpdesk Business Continuity Plan	PVCS
5.	CS/PRD/021			Fujitsu Services (Post Office Account) Problem Management Process	PVCS
6.	CS/PRD/031			Fujitsu Services (Post Office Account) Customer Service Business Continuity Management Process	PVCS
7.	SU/MAN/018			Operations Procedures Manual Index	PVCS
8.	TD/DES/031			Resilience and Recovery Strategy for Release 2	PVCS
9.	VI/TSC/105			Technical Integrity & Networking Test Plan	PVCS

Fujitsu Services

BUSINESS CONTINUITY FRAMEWORK

Ref: CS/SIP/002

Version: 9.0

COMMERCIAL-IN-CONFIDENCE

Date: 19-Oct-2004

10.	SU/TRP/005			Technical Integrity & Networking Test Results	PVCS
11.	RS/ACS/002			Security Acceptance test Specification	PVCS
12.	SU/TRP/003			Release 2 Final Security Test Report	PVCS
13.	RS/POL/003			Access Control Policy	PVCS
14.	BP/PRO/003			Post Office Site Failure Contingency Procedure	PVCS
15.	CS/PRO/21			Release 2 Electronic Point of Sale Service	PVCS
16.	CS/PRO/25			Release 2 Access Control and User Administration Process & Procedures	PVCS
17.	CS/PRO/45			Release 2 Automated Payment Service	PVCS
18.	CS/PRO/48			Horizon System Help desk Processes & procedures Description	PVCS
19.	CS/PRO/24			Release 2 Operating Environment	PVCS
20.	CS/PRO/22			Order Book Control Service	PVCS
21.	CR/FSP/004			Service Architecture and Design Document	PVCS
22.	CS/QMS/007			Operations Manual for the Customer Service Directorate	PVCS
23.	TD/STR/001			Host Systems Storage Strategy	PVCS
24.	TD/DES/059			High-level Network Design for Release 2	PVCS
25.	TD/DES/033			Agent and Correspondence Server Resilience and Recovery for Release 2	PVCS
26.	TD/DES/086			Correspondence Server back-up Strategy	PVCS
27.	TD/DES/057			Auto-config and Rollout Resilience and Recovery Strategy	PVCS
28.	TD/DES/093			DYNIX/ptx Configuration for Main Host Site Fail-over and Fallback	PVCS
29.	TD/DES/034			High Level Design for Application Recovery after Fail-over using Maestro	PVCS
30.	TD/DES/092			Audit Server Resilience and Recovery for Release 2	PVCS
31.	SD/STR/002			FTMS Resilience and Recovery Strategy for Release 2	PVCS

32.	SD/STR/005			Data Warehouse Disaster Recovery Strategy	PVCS
33.	CON/MGM/005			Post Office Limited and Fujitsu Services Business Continuity Interface Agreement	Post Office Limited
34.	CR/PRP/004			Post Office Limited Disaster Recovery Interface Service (TIP DR)	PVCS
35.	CS/REP/046			Business Continuity Operational Test Report (1999)	PVCS
36.	NB/SDS/007			System Design Specification for Network Banking End-to-End Service	PVCS
37.	NB/SPE/001			Network Banking Statement of Requirements	PVCS
38.	SY/SPG/002			Agent and Correspondence Server Resilience and Recovery Operations Support Guide	PVCS
39.	EF/SDS/001			System Design Specification for the Debit Card System	PVCS
40.	EF/SER/001			Debit Card MoP Functional Description	PVCS
41.	DV/HLD/003			DVLA and PAF Network Infrastructure High Level Design	PVCS
42.	SD/HLD/003			PAF Network Infrastructure High Level Design	PVCS
43.	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.

0.4 Abbreviations/Definitions

Abbreviation	Definition
ACS	Auto Configuration Service
ADSL	Asymmetric Digital Subscriber Line
AP	Automated Payments
AP-ADC	Automated Payments-Advanced Data Capture
APS	Automated Payments System
BCF	Business Continuity Framework
CSR	Core System Release

CTF	Critical Time Factor
DCS	Debit Card System
DRS	Data Reconciliation Service
DVLA POME	Department of Vehicle Licensing Authority – Post Office MOT Enquiry
DW	Data Warehouse
EPOS	Electronic Point of Sale
ETS	Electronic Top-ups 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
NBS	Network Banking Service
NBX	Network Banking Service (Release S75 replacement service)
NRO	National Roll Out
OBCS	Order Book Control Service
OCMS	Outlet Change Management System
PAF	Postal Address File
POL	Post Office Limited
POLFS	Post Office Limited Financial Service
RAB	Release Authorisation Board
RD	Reference Data
RDMC	Reference Data Management Centre
SIAM	Service Impact Assessment Module
SMC	Systems Management Centre
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
8.1	Major update for new Horizon release, i.e. S55 – the introduction of ADSL S60 – the introduction of DVLA (POME), PAF and POLFS (SAP) services. S70 – the introduction of ‘Chip and PIN’ EMV S75 – the introduction of the NBX Network Banking Service (revised test 16 and 22).
8.2	Incorporates comments from Peter Burden Amendments made to Figure 5.1 and Table 2.
8.3	Incorporates comments from Post Office Limited as per QR 3572. Changed Post Office Limited approval authority to Richard Ashcroft and removed references to the Technical Support Desk.
9.0	Nil comments returned from comment cycle. Incorporated amendment to reflect recent organisational changes in Post Office Account.

0.6 Changes Expected

Changes
It is expected that this framework will be amended to reflect the introduction of new services.

0.7 Table of Contents

1.0	INTRODUCTION.....	11
2.0	SCOPE.....	11
3.0	DEFINITIONS.....	11
4.0	FRAMEWORK OVERVIEW.....	13
4.1	INTRODUCTION.....	13
4.1.1	Contingency Plans.....	14
4.1.1.1	Service Definition.....	14
4.1.1.2	Risk Analysis And Service Impact.....	14
4.1.1.3	Escalation Contacts.....	14
4.1.1.4	Resilience Strategy documents.....	14
4.1.1.5	Contingency Procedures.....	14
4.1.2	Service Framework.....	15
4.1.3	Business Continuity Management Process.....	15
4.1.4	Test strategy and plans.....	15
4.1.5	Review strategy.....	15
4.1.6	Deliverables and Acceptance Methods.....	15
5.0	SERVICE FRAMEWORK.....	16
5.1	INTRODUCTION.....	16
5.2	SERVICE TO PLAN RELATIONSHIP TABLE.....	18
6.0	BUSINESS CONTINUITY MANAGEMENT PROCESS.....	20
7.0	TEST STRATEGY AND PLANS.....	21
7.1	REQUIREMENT.....	21
7.2	INITIAL TESTING.....	21
7.2.1	Existing Services.....	21
7.2.2	New Services.....	21
7.3	ONGOING TESTING.....	21
8.0	REVIEW STRATEGY.....	24
9.0	CONTINGENCY PLANS.....	25
9.1	OWNERSHIP OF PLANS.....	25
9.2	PLAN ACTIVATION.....	25
9.3	IMPACT AND RISK ASSESSMENT.....	25
9.4	OTHER REQUIREMENTS.....	26
9.4.1	Preventative Measures.....	26
9.4.1.1	Technical Design.....	26
9.4.1.2	Security.....	27
9.4.2	Preparedness Measures.....	27
9.4.3	Contingency Measures.....	27
9.4.4	Recovery of Normal Service.....	27
9.4.5	Contact List.....	27
10.0	DELIVERABLES AND ACCEPTANCE METHODS.....	28

Fujitsu Services

BUSINESS CONTINUITY FRAMEWORK

Ref: CS/SIP/002

Version: 9.0

COMMERCIAL-IN-CONFIDENCE

Date: 19-Oct-2004

10.1	INTRODUCTION.....	28
10.1.1	Joint Review.....	28
10.1.2	Document Inspection.....	28
10.1.3	Procedural Walkthrough.....	28
10.1.4	Operational Test.....	28
10.2	CONTRACT CONTROLLED DOCUMENTS.....	29
10.2.1	Summary.....	29
10.2.2	Deliverables List.....	29
10.3	BCF REFERENCED DOCUMENTS.....	30
10.3.1	Summary.....	30
10.3.2	Deliverables List.....	30
10.4	TECHNICAL DESIGN DOCUMENTATION.....	30
10.4.1	Summary.....	30
10.4.2	Deliverables List.....	31
10.4.3	Review Method.....	32
10.5	CUSTOMER CONTINGENCY PLANS AND PATHWAY DELIVERABLES IN SUPPORT OF PLANS...	
	32	
10.5.1	Summary.....	32
10.5.2	Deliverables List.....	32

1.0 Introduction

A key requirement in the Post Office Account 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 (Post Office Account) services e.g. NBS, TPS, APS etc, support services and client services where appropriate.

A principle requirement specified within schedule 21 of the Varied and Restated Codified Agreement 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 (Post Office Account) 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 Schedule 21 of the Varied and Restated Codified Agreement.
- b) Provide a detailed definition of Fujitsu Services (Post Office Account) 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 the Varied and Restated Codified Agreement.

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 REF10 does.

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 (Post Office Account) generally recognise the term Business Continuity as having three closely related components:

Fujitsu Services

BUSINESS CONTINUITY FRAMEWORK

Ref: CS/SIP/002

Version: 9.0

COMMERCIAL-IN-CONFIDENCE

Date: 19-Oct-2004

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.

4.0 Framework Overview

4.1 Introduction

The Business Continuity Framework defines the methodology agreed between Fujitsu Services (Post Office Account) and Post Office Limited for handling all aspects of Business Continuity.

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

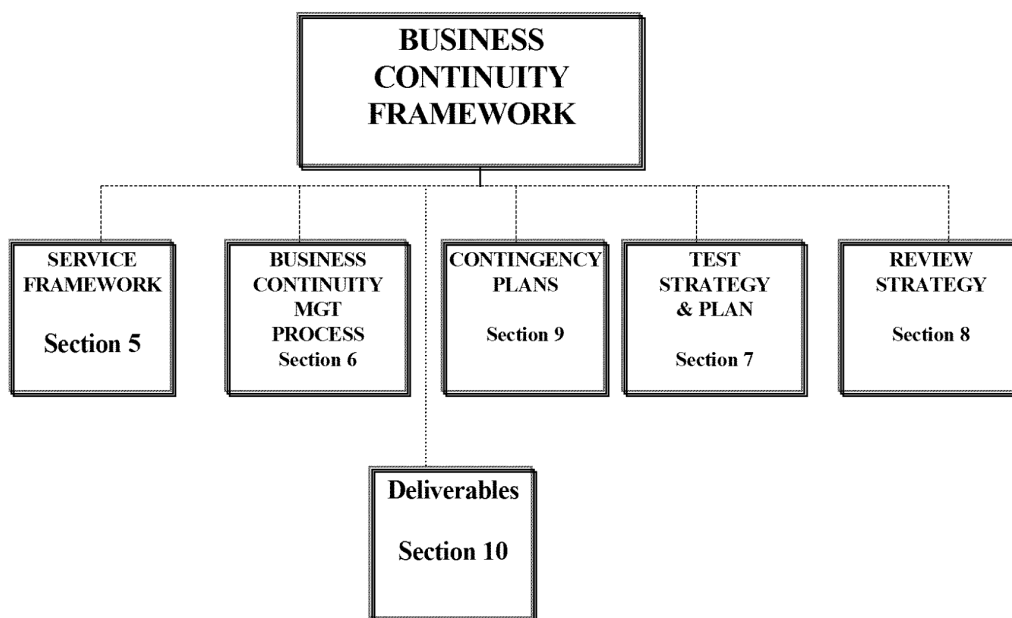


Figure 4.1 Service Elements

4.1.1 Contingency Plans

At the time of writing version 8.0 of this document there are three Continuity Plans:

The Horizon Services Business Continuity Plan

The Horizon Support Services Business Continuity Plan

Horizon System Helpdesk Business Continuity Plan

The contents of these continuity plans are specified within Schedule 21 of the Varied and Restated Codified Agreement. 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)

Major elements of the plans are as follows.

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 REF7. Where appropriate the contingency plan will make reference to the relevant operations manual.

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 Post Office Account 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 3) 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 (Post Office Account).

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

5.0 Service Framework

5.1 Introduction

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

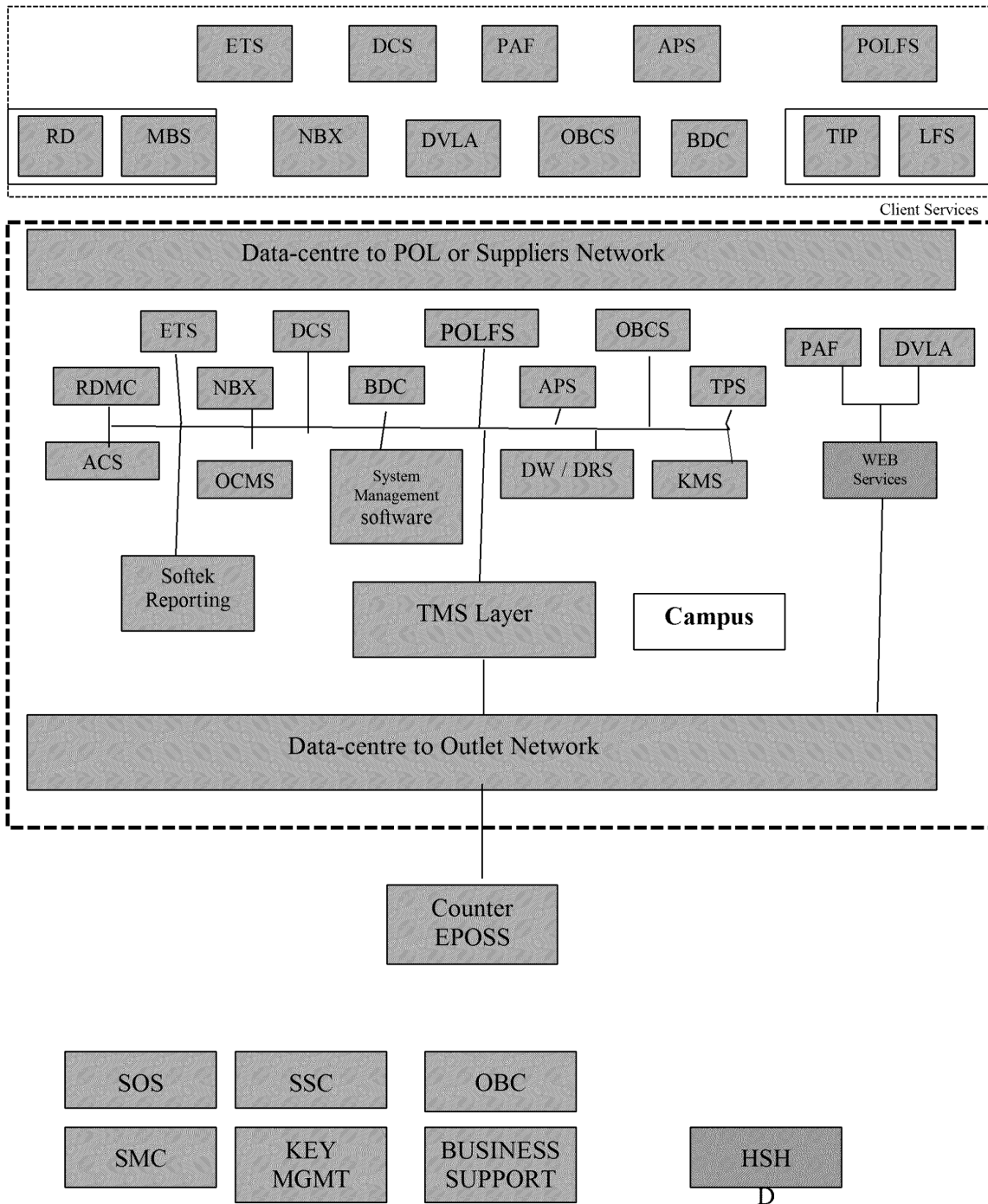
The service framework is show diagrammatically in Figure 5.1 below. During 2003 a simplified set of three Business Continuity Plans were produced, as a significant amount of the Horizon infrastructure is shared by numerous services and therefore was replicated across many of the original continuity plans. The reduced set has several advantages include easier access to the applicable information by POA Duty Managers during incident management and improved documentation maintenance. The three Business Continuity Plans are:

The Horizon Services Business Continuity Plan which documents the contingency measures for the primary Horizon services

The Horizon Support Services Business Continuity Plan which documents, with the exception of the HSH services, the contingency measures for the supporting Horizon services

Horizon System Helpdesk Business Continuity Plan

Services Overview



Horizon Services detailed in
● REF 1

● Support Applications and
Services detailed in REF 2

● Support Services detailed in
REF 4

5.2 Service to Plan Relationship Table

Table 1 below identifies which contingency plan addresses each of the service elements in Figure 5.1 above:

Table 1

Service or Service Element	Expansion of Acronym	Related Contingency Plan(s)	Test Ref. (Table 7.2)
ACS	Auto Configuration Service	Horizon Support Services	8
AP	Automated Payments	Horizon Services	20
APS	Automated Payment Service	Horizon Services	2,3,4,5,6,7
BDC	Bureau de Change	Horizon Services	2,3,4,5,6,7
BUSINESS SUPPORT		Horizon Support Services	1
DATA CENTRE	Data Centre	Horizon Support Services	2
DCS	Debit Card System	Horizon Services	25
DRS	Data Reconciliation Service	Horizon Support Services	2,3
DVLA (POME)	Department of Vehicle Licensing Authority – Post Office MOT Enquiry	Horizon Services	26
DW	Data Warehouse	Horizon Support Services	2,3
EPOSS	Electronic Point of Sale System	Horizon Services	2,3,4,5,6,7
ETS	Electronic Top-ups Service	Horizon Services	25
HSHD	Horizon Systems Helpdesk	HSH	10
KMS	Key Management Service	Horizon Support Services	19
LIVE TEST		Horizon Support Services	1
LFS	Logistics Feeder Service	Horizon Services	2,3,4,5,6,7
MBS	Message Broadcast Service	Horizon Services	1,9
MIS	Management Information Systems	Horizon Support Services	13
NETWORK		Horizon Services and Horizon Support Services	2,3,4,5,6,7,15,22
NBX	Network Banking Service	Horizon Services	2,3,5,6,16,22,24
OBCS	Order Book Control Service	Horizon Services	2,3,4,5,6,7
OCMS	Outlet Change Management	Horizon Support Services	17

Fujitsu Services

BUSINESS CONTINUITY FRAMEWORK

Ref: CS/SIP/002

Version: 9.0

COMMERCIAL-IN-CONFIDENCE

Date: 19-Oct-2004

	System		
PAF	Postal Address File (service)	Horizon Support Services	27
POLFS	Post Office Limited Financial Service	Horizon Services and Horizon Support Services	28
RDMC	Reference Data Management Centre	Horizon Support Services	1,9
SMC	Systems Management Centre	Horizon Support Services	12
SOS	Systems Operate Service	Horizon Support Services	11
SSC	Systems Support Centre	Horizon Support Services	1,14
TIP	Transaction Information Processing	Horizon Services	2,3,4,5,6,7,18
TMS	Transaction Management System	Horizon Services	2,3,4,5,6,7,18
TPS	Transaction Processing Service	Horizon Services	2,3,4,5,6,7,18

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 (Post Office Account) Customer Service Business Continuity Management' process (REF6) and the Post Office Limited and Fujitsu Services Business Continuity Interface Agreement (REF 33). 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.

7.0 Test Strategy and Plans

7.1 Requirement

Schedule 21 of the Varied and Restated Codified Agreement states the requirement as follows

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

a) Initial testing before commencement of Roll-Out of Services

b) Regular testing’

7.2 Initial Testing

7.2.1 Existing Services.

Initial Business Continuity testing was conducted prior to the full operational introduction of the Horizon Service (Core System Release) and the subsequent release of major services, e.g. MBS, NBS and ETS services. Test reports have been produced for this testing and are maintained in PVCS within the CS/REP/nnn documentation work-set.

7.2.2 New Services

Where services are introduced as part of a new release the Test Plan (REF3) 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 Post Office Account agreement, within the Business Continuity Test Plan (REF3).

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 in accordance with the test methodology and frequency agreed in Schedule 21 of the Varied and Restated Codified Agreement.

Table 2

Test No.	Business Continuity Test	Test Methodology and Frequency	Owner	Ass Doc Ref. Section 0.3
2	Fujitsu Services (POA) Campus failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
3	Database Server Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
4	Correspondence Server Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
5	Router Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
6	Data-centre LAN Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
7	Agent Platform Failure	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
9	RDMC failure	Operational Test Environment once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	2
16	Network Banking Service	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
22	Network Banking Clients Interface	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
25	Debit Card Service/Electronic Top-ups Service	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
26	DVLA (POME) web service	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
27	PAF web service	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1
28	POLFS	Live operational test once per year and a procedural walk-through once per year.	Fujitsu Services (POA)	1

All other on-going business continuity test details will be defined on an annual basis and included within the yearly schedule in REF3. The Fujitsu Services (POA) 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.

8.0 Review Strategy

A Business Continuity Steering Group has been established between Post Office Limited and Fujitsu Services (Post Office Account). This group reviews the progress of each release against the Fujitsu Services (Post Office Account) 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.

9.0 Contingency Plans

Throughout section 9, the use of *Italics* denotes the actual words in Schedule 21 of the Varied and Restated Codified Agreement.

'The Business Continuity Plans shall be based on impact and risk assessments and agreed by Fujitsu Services and Post Office

9.1 Ownership of Plans

'Ownership of all contingency actions shall be identified in the Business Continuity 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 (POA) 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 Business Continuity 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.

Alternatively, a single risk statement may be documented throughout the day in the risk table. The Critical Time Factors (CTF) here shall be determined by the criticality of the service activity. I.e. for on-line service, e.g. NBS and DCS the CTF is identified against Post Office Core Day processing, whilst for file transfers, e.g. APS and TPS the CTF is identified against Post Office Non-Core Day processing. 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 Business Continuity Plans shall be based on impact and risk assessments by Fujitsu Services and Post Office...'

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 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 (REF13) and the Security Functional Specification (REF11).

9.4.2 Preparedness Measures

Preparedness measures are implemented in a number of ways:

- 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 REF7. 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.

10.0 Deliverables and Acceptance Methods

10.1 Introduction

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

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

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 (Post Office Account) 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 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 Business Continuity Plan	CS/PLA/015	Joint Review and sign-off

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 (POA) Business Continuity Operational Test Plan	CS/PLA/011	Fujitsu Services (POA)	Joint review
Fujitsu Services (POA) Business Continuity Management Process	CS/PRD/031	Fujitsu Services (POA)	Not Applicable
Operations Manual for the Customer Service Directorate	CS/QMS/007	Fujitsu Services (POA)	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
The Horizon Services Business Continuity Plan	CS/PLA/079	Fujitsu Services (POA)	Document inspection to verify compliance with BCF
The Horizon Support Services Business Continuity Plan	CS/PLA/080	Fujitsu Services (POA)	Document inspection to verify compliance with BCF

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

Fujitsu Services

BUSINESS CONTINUITY FRAMEWORK

Ref: CS/SIP/002

Version: 9.0

COMMERCIAL-IN-CONFIDENCE

Date: 19-Oct-2004

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

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 (Post Office Account) 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 (Post Office Account) 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