FUJ00080037

Document Title:	**HORIZON SUPPORT SERVICES BUSINESS CONTINUITY PLAN**
Document Type:	**CONTINGENCY PLAN**
Release:	Not Applicable
Abstract:	This plan provides a summarised description of the services provided to support the Horizon operational service. The support services consist of IT sub-services, e.g. OCMS, KMS, and operational sub-services, e.g. SOS and SSC. For contractual reasons the Horizon Service Desk is documented in a related plan CS/PLA/015. This document also details the planned actions which can be taken to minimise the risk of one or more of the support services not being available.
Document Status:	APPROVED
Originator & Dept:	Tony Wicks, Royal Mail Group Account, CS, Business Continuity.
Contributors:	Dave Tanner RMGA TDA and Simon Fawkes RMGA TDA
Internal Distribution:	Peter Thompson, Liz Melrose, Brian Pinder, Alex Kemp, Kirsty Gallacher, Mike Stewart, Mike Woolgar, Dave Wilcox, Kevin McKeown, Denise Miller, Nick Crow, Ian Venables, Chris Bourne, Mik Peach, John Simpkins, Tony Wicks, Dave Sackman, Dave Chapman, Dave Tanner, Colin Mills, Nigel Bailey (FSCS), Andrew Gibson (FSCS), Dave Jackson (FSCS)
External Distribution:	Gary Blackburn, Business Continuity Manager Post Office Limited
Approval Authorities:	(*See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Steve Denham	Royal Mail Group Account CS Head of Service Management		
Geof Slocombe	Royal Mail Group Account Infrastructure (Project Manager)		

This business continuity plan is one of three. If the RMGA Duty Manager (or other authorised person) is unable to find the failed infrastructure service or components in this plan they are mandated to refer to CS/PLA/079 The Horizon Services BC plan and CS/PLA/015 The Horizon Service Desk BC plan.

FUJ00080037

Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	04/06/2003	Initial draft registered within PVCS	None
0.2	20/11/2003	Major improvements whilst still draft.	None
0.3	19/01/2004	Further improvements whilst still draft.	None
0.4	13/02/2004	Further improvements whilst still draft.	None
0.5	15/11/04	Changes to reflect infrastructure changes up to and including S75	None
1.0	21/12/04	Issued for formal approval.	None
1.1	10/11/05	Incorporated changes for support infrastructure changes up to and including S92.	None
2.0	13/01/06	Incorporated changes for comments from Dave Tanner, Ian Daniel and Colin Mills.	None
2.1	21/03/06	Incorporated changes for comments from Simon Fawkes and for the introduction of IP Stream network.	None
3.0	07/04/06	Incorporated comments for Mike Woolgar and published for approval.	None
3.1	27/12/06	General update. Figure One amended to include the MoneyGram service	None
4.0	24/01/07	Incorporates minor corrections for Kirsty Walmsley and Pete Thompson	None
4.1	21/09/07	Amended for CP4330, CP4319, CP4037, CP4317, 4344 and CP4412.	None
5.0	24/10/07	Revised trigger tables to reflect that Cable & Wireless NMC disaster recovery site remained in Watford and to remove the entries for Zergo units in Belfast. Updated triggers 105, 106 and 107.	None

0.2 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks

Mandatory Review Authority	Name
Royal Mail Group Account, CS Head of	Steve Denham

FUJ00080037

Service Management	
Royal Mail Group Account Infrastructure (Project Manager)	Dave Sackman
Royal Mail Group Account, CS Service Support Manager	Peter Thompson
Royal Mail Group Account Networks Technical Design Authority	Dave Tanner
Royal Mail Group Account Resilience Technical Design Authority	Dave Chapman
Optional Review / Issued for Information	
Core Services Business Continuity Manager	Nigel Bailey
Royal Mail Group Account, CS Networks Service Delivery Manager	Alex Kemp
Royal Mail Group Account, CS Service Delivery Manager	Liz Melrose
Royal Mail Group Account On-line Services Manager	Mike Stewart
Royal Mail Group Account On-line Services Manager	Mike Woolgar
Royal Mail Group Account Client Interface Manager	Kirsty Gallacher
Royal Mail Group Account Business Security Manager	Brian Pinder

(*) = Reviewers that returned comments

0.3 Associated Documents

REF	Reference	Vers	Date	Title	Source
1	CS/SIP/002			Business Continuity Framework	PVCS
2	CS/PLA/011			Business Continuity Test Plan	PVCS
3	CS/PLA/079			The Horizon Services Business Continuity Plan	PVCS
4	CS/PLA/015			The Horizon Service Desk Business Continuity Plan	PVCS
5	CS/PRD/031			Fujitsu Services (RMGA) Business Continuity Management	PVCS
6	CON/MGM/005			Post Office Limited and Fujitsu Services Business Continuity Interface Agreement	Post Office Limited
7	SU/MAN/018			Operations Procedures Manual Index	PVCS
8	NB/SDS/007			System Design Specification for Network Banking End-to-End Service	PVCS

FUJ00080037

9	SY/SPG/002			Agent and Correspondence Server Resilience and Recovery Operations Support Guide	PVCS
10	RS/MAN/013			KMS Operations Guide	PVCS
11	CS/PLA/059			Fujitsu Services (RMGA) Bracknell Incident Management Plan.	PVCS
12	EF/SDS/001			System Design Specification for the Debit Card System	PVCS
13	AS/DPR/021			Design Proposal for Branch Network Resilience	PVCS
14	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.

FUJ00080037

0.4 Abbreviations/Definitions

Abbreviation	Definition
[A]	Authorisation
ACS	Auto-Configuration Service
APOP	Automated Payments Out Pay
APS	Automated Payments Service
BCM	Business Continuity Manager
BCMT	Business Continuity Management Team
BCT	Business Continuity Team
BNR	Branch Network Resilience
[C]	Confirmation
CAPO™	Card Account for Post Office
CI	Card Issuer
C&W	Cable & Wireless
DCS	Debit Card System
DCSM	Debit Card System Management (server)
DMZ	De-Militarised Zone
DRS	Data Reconciliation Service
DVLA (POME)	Department of Vehicle Licensing Authority – Post Office MOT Enquiry
EDS	Electronic Data Systems
EoD	End of Day
EPOSS	Electronic Point of Sale Service
[F]	Financial Advice Note
FI	Financial Institution
FDDI	Fibre Optic Distributed Database
FSCS	Fujitsu Services Core Services
FTMS	File Transfer Management Service
GSN	Global Satellite Network
HSD	Horizon Service Desk
KEK	Key Encryption Key
KES	Key Encryption Seed
KM	Key Management
KMA	Key Management Application
KMC	Key Management Controller

FUJ00080037

KMS	Key Management System
LAN	Local Area Network
LFS	Logistics Feeder Service
LNS	L2TP Network Server
MBCI	Major Business Continuity Incident
MBS	Message Broadcast Service
MIS	Management Information Service
NBX	Network Banking Service (Replacement)
NDC	Northern Data Centre (Post Office Limited)
NST	Network Service Type
OBCS	Order Book Control Service
OCMS	Outlet Change Management Service
OPS	Outlet Processing System
O/S	Operating System
PAF	Postal Address File
PES	Personal Earth Station
PFG	Payment File Generator
PIN	Personal Identification Number
RMGA	Royal Mail Group Account
POL	Post Office Limited
POLFS	Post Office Limited Financial Service
POP	Point Of Presence
[R]	Request
RAB	Release Authorisation Board
RAC	Request, Authorisation, Confirmation Model
RACF	Request, Authorisation, Confirmation with Financial Advice Note
RD	Reference Data
RDMC	Reference Data Management Centre
RDS	Reference Data System
SMC	Systems Management Centre
SSC	System Support Centre
SOS	Systems Operate Service
SRDF	Symmetrix Remote Data Facility; EMC technology used to replicate disk array data between two Campuses
TFS	TRIOLE For Service

FUJ00080037

TIP	Transaction Information Processing
TMR	Tivoli Managed Region
TMS	Transaction Management Service
TPS	Transaction Processing Service
VPN	Virtual Private Network
WAN	Wide Area Network

0.5 Changes in this Version

Version	Changes
4.1	Removed the trigger table entry for the Softek reporting server. Updated for CP4319, the replacement of Hughes satellite service with BT VSAT Amended for CP4037, to reflect the infrastructure changes implemented at the POL NDC disaster recover site at Hounslow. Revised for CP4317, the consolidation of ISDN routers at the Bootle and Wigan Data-centres. The Powerhelp service has been replaced with TRIOLE For Service. POA was replaced with RMGA – Royal Mail Group Account. The plan was revised to reflect that teams, e.g., the HSD and SMC were moving from STE09, which is closing, to STE04
5.0	Revised trigger tables to reflect that Cable & Wireless NMC disaster recovery site remained in Watford and to remove the entries for Zergo units in Belfast which are to be removed in the near future. Updated Post Office Limited contact and escalation details and triggers 105, 106 and 107.

0.6 Changes Expected

Changes
This is an operational document, which will be amended for numerous reasons including: 1, new risks are identified; 2, improved or new contingency actions are identified; 3, there are operational changes to the Horizon Supporting Services Infrastructure.

FUJ00080037

0.7 Table of Contents

FUJ00080037

FUJ00080037

1.0 Introduction

During 2003 Fujitsu Services Royal Mail Group Account (RMGA) introduced a 'streamlined' set of Business Continuity plans comprising of three documents.

1, the Horizon Services Business Continuity Plan (CS/PLA/079);

2, the Horizon Support Services Business Continuity Plan (this document);

3, the Horizon Service Desk Business Continuity Plan

(CS/PLA/015 a CCD therefore kept separate.)

This Contingency Plan provides a summarised description of the overall Operational Horizon Support Service provided by Fujitsu Services. This includes the following sub-services:

- Key Management Service;
- Auto-Configuration Service;
- Outlet Change Management Service;
- SAP (POLFS) Development and QA-Test Systems
- System Management Centre software and operational Services;
- System Support Centre Services;
- System Operate Services;
- Reference Data Management Service (BRA01 based);
- Management Information Services, including the Data Warehouse and the Data Reconciliation Service.
- Cable & Wireless (Network supplier);
- Transaction Network Services (Network Supplier).
- RMGA Programme and Development Operational Support

This document describes the measures taken by Fujitsu Services to minimise the risk of RMGA being unable to provide these services and it explains the actions the Problem, Service, or Business Continuity Manager will take to instigate service recovery.

FUJ00080037

2.0 Scope

This plan covers the following key areas.

- A summary of the individual Horizon support services
- A summary of the testing activities undertaken to validate those services.
- The measures taken to anticipate and plan for business continuity incidents
- A risk and impact assessment
- Agreed trigger points for plan activation
- References to relevant operational recovery processes
- Problem management contacts and escalation points

This plan does not provide detailed operational procedures with regard to recovery. Further details on the procedures for recovery can be found in the Fujitsu Services Core Services Operations Procedures Manual Index (REF7).

3.0 Ownership And Operation

The Fujitsu Services, Royal Mail Group Account, Infrastructure and Availability Manager, who is also responsible for its maintenance and operational verification, owns this plan. The Fujitsu Services Core Services Service Manager operates this plan. Contact details are shown below.

Name	Position	Office Contact No.	Out of hours No.
Steve Denham	Fujitsu Services, Royal Mail Group Account, Head of Service Management.	GRO	GRO
Tony Wicks Royal Mail Group Account (Deputy)	Fujitsu Services, Royal Mail Group Account, Business Continuity Manager.	GRO	GRO

The Fujitsu Services RMGA Business Continuity Manager and the Service Managers within Fujitsu Services RMGA Customer Service Operations, responsible for service availability, hold copies of this plan.

FUJ00080037

4.0 Service Functionality

4.1 Services Overview

For the purposes of Business Continuity planning this contingency plan has been produced to document the Royal Mail Group Account responsibilities for the end to end Horizon Services. From an operational perspective it is impracticable for the 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 are documented in the risk table within section 10.

Figure One provides an overview of all the Horizon Services for which RMGA has partial or full responsibility. The diagram also provides details of the support applications and services covered within REF 3 and 4.

It is emphasised that hardware components such as the Database Server, Generic Agents, Correspondence Servers, LAN Switches and Network Routers in the Data-centre deliver service to all the sub-services detailed in this plan. For some sub-services, for example Network Banking, there are hardware and software components specifically dedicated to that sub-service, e.g. the NBX Authorisation Agent servers and NBX De-militarised Zone.

4.1.1 Infrastructure Sub-Services

A number of IT sub-services are used to support the Horizon services, however for the purposes of this plan they can be categorised into the following seven infrastructure support sub-services:

The Key Management Service;

The Auto-Configuration Service;

The Outlet Change Management Service;

Management Information Systems (Data Warehouse and Data Reconciliation Service TES);

SAP - Post Office Limited Financial Service (Development and QATest servers)

System Management Service (primarily consisting of Tivoli eventing);

Network Services (C&W and Transaction Network Services).

For the purposes of this continuity plan these sub-services can be considered to be running from the infrastructure contained in the campuses (see REF3 for Campus details.)

4.1.2 Operational Support Sub-services

Additionally there are a number of Horizon operational support sub-services:

These consist of a number of support teams:

1) The Horizon Service Desk who provide first line support.
2) The System Management Centre who, in addition to system management, provide second line technical support.

FUJ00080037

3) The System Support Centre (SSC) who primarily provides third line support services.

4) Fourth line support is provided either by the Royal Mail Group Account Development team or by external suppliers, e.g. Esher or Microsoft.

The Horizon service is also supported by number of operational units

1) The Core Services System Operate Service team who provide Unix, NT and database operational expertise.

2) The System Management Centre operational event management team and MSS staff based at Wigan and Stevenage.

3) The RMGA Customer Service operational teams, i.e. providing Reference Data operational service, and the Horizon Service Delivery Management functions.

4) The RMGA Programme and Development operational support teams.

FUJ00080037

Horizon Support Services Overview

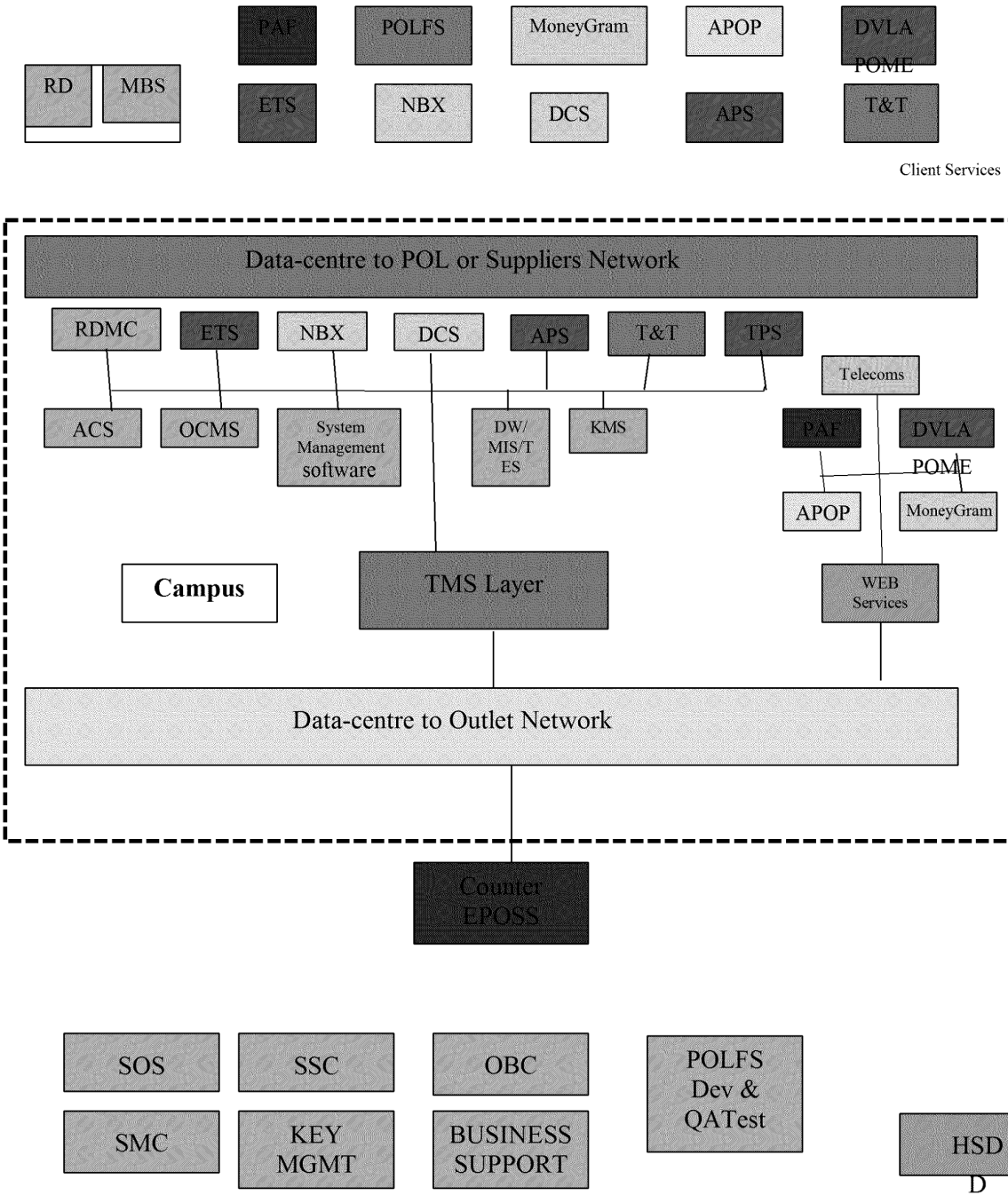


Figure One

FUJ00080037

4.2 Infrastructure Support Services

This section provides descriptions of the functionality of the seven infrastructure supporting sub-services documented within this plan.

4.2.1 The Key Management Service

4.2.1.1 Introduction to Cryptography in RMGA

The Security Functional Specification identifies a number of uses for cryptography in securing the RMGA business services. Subsequent agreements have identified further requirements for cryptography to protect third-party software. With one exception, the complete list of cryptographic protections at the time of writing is:

- APS Smart Acknowledgement
- Audit Server
- Software Issue
- Client services Automated Payment service
- Post Office Filestore Encryption Key
- Post Office Counters Ltd, Transaction Information Processing
- POL Reference Data
- Automated Payment service bulk Client transaction records
- Landis & Gyr 3rd party code and data protection
- Landis & Gyr transaction-enabling functions
- Utimaco Virtual Private Network
- Rambutan encryption of data links
- Pinpads

The exception is the Escher Riposte application software authentication. Keys for this cryptographic function are not managed within the RMGA run-time system and so are excluded from the scope of this document.

4.2.1.2 Key Management System Implementation

All the cryptographic functions in the above list require keys. These keys must be securely created, distributed and installed in the cryptographic functions, and each key must be changed periodically. Hence, there are a number of common key management activities to be performed across a diverse spectrum of keys. All of this activity is to be managed by a single officer of RMGA, defined as the Cryptographic Key Manager.

To help to visualise this problem space, and to begin to organise it, the “fan diagram” of Figure Two was evolved.

FUJ00080037

Key Management "Fan Diagram"

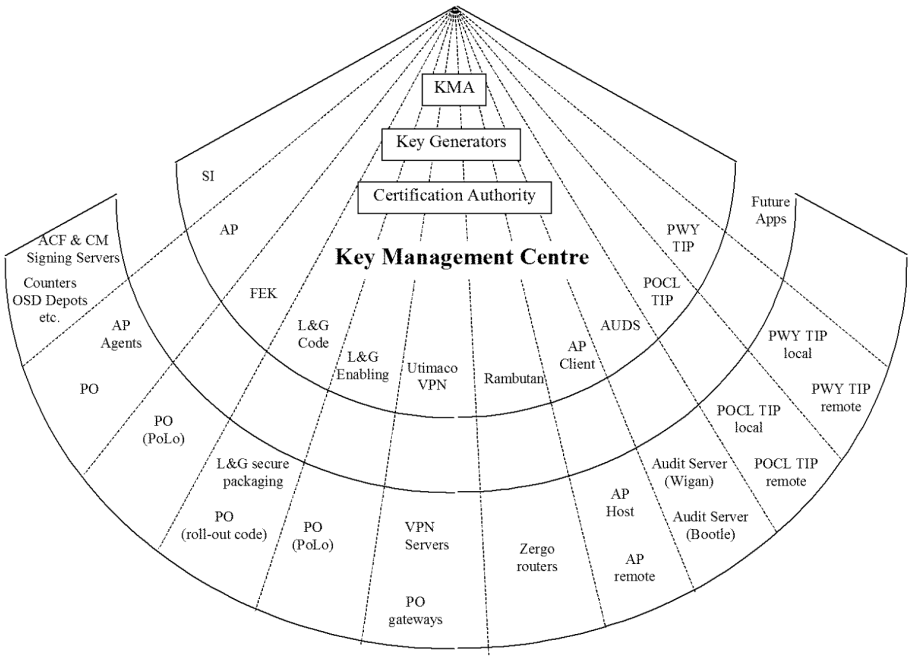


Figure Two.

It represents key management emanating from a single point of control and fanning out along segments which correspond to the various uses of cryptography (as listed above) to the many points at which the keys are used. Note that the TIP and RD cryptographic applications are considered under the protection domains POL TIP and PWY TIP, one corresponding to authentication of POL to RMGA and the other corresponding to authentication of RMGA to POL.

Some key management actions are manual. Representation in the fan diagram does not necessarily imply automation. For example, Rambutan keys, which are supplied by an external agency and installed in special hardware, will be managed entirely by manual procedures. However, the Key Management system will provide the Key Manager with facilities to record and track manual procedures.

Figure Three provides an abstract view of the subsystems and main data flows of the Key Management System.

FUJ00080037

KM Data Flow - Abstract View

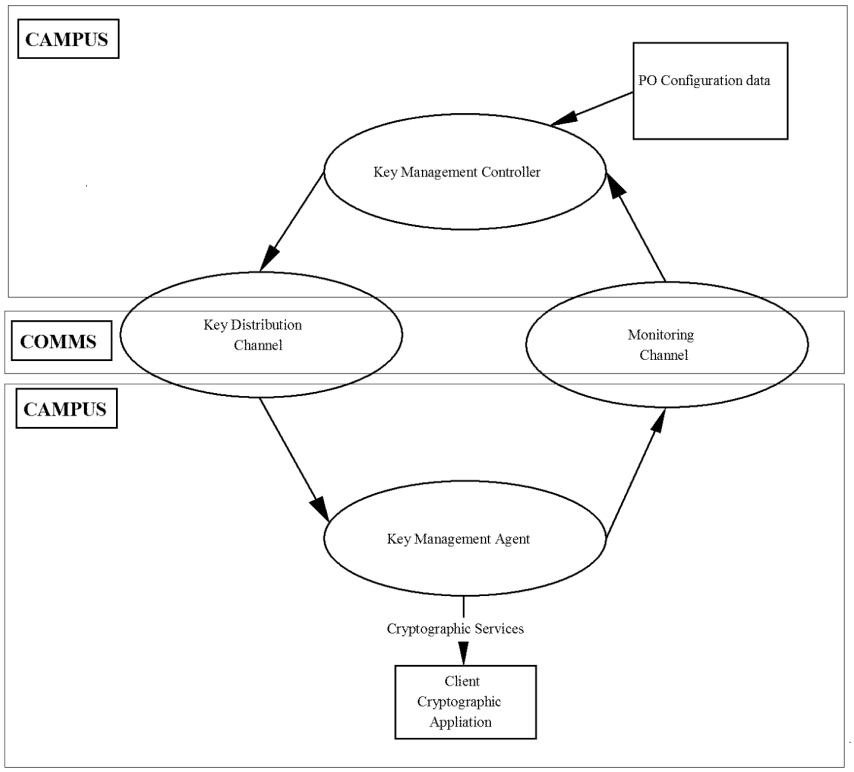


Figure Three

4.2.1.3 The Key Management Controller

The Key Management Controller (KMC) is the software providing the control centre for the key management system. It comprises the Key Management Application (KMA), which is in fact a suite of programs built around a management information database, together with supporting software and hardware for key generation and certification. The database contains a model of the rest of the system and all the managed objects (keys, clients, etc.) within it. The KMA uses this model to give the Key Manager a view of the system status, and to assist the Key Manager in performing management actions, guarding the integrity and coherence of the system as a whole.

The KMA functionality must be available to the Key Manager located at either BRA01 or LEW02. This is achieved via a client-server architecture with KMA workstations being located at BRA01 and LEW02 and a server at each of the RMGA Campuses.

4.2.1.4 The Key Management Application Workstations

KMA workstations are available at BRA01 and at LEW02 (for disaster recovery purposes).

4.2.1.5 The Key Management Server.

Key Management Servers are available at both Data-centres and are connected on KMS LANs via two 1 Gbit inter-campus virtual LAN. One server acts as a standby for the other. The disks containing the KM information base on the standby server

FUJ00080037

mirrors those of the active server via a high speed link. The disks are actually attached to an EMC server which manages the replication. For simplicity it is considered that the EMC server is part of the KM server. A spare client workstation is available in one of the campuses.

4.2.1.6 Key Management Clients

A Key Management client comprises a platform and associated software requiring the services of the Key Management Controller. The client population is numerically dominated by the PCs on PO counters but there are many other client types

On many types of client, a Key Management Client Agent is installed; this is the software primarily responsible for mediating between the Key Management system and the cryptographic support software running on the client during normal operation.

The KMC and its clients communicate by means of distribution and monitoring channels.

4.2.1.7 Certification Authority Workstations

The Certification Authority (CA) is an application which takes public keys as input and packages them in public key certificates (PKC). The certificates are signed with the CA private key. The CA also signs CRLs. The CA is implemented on a dedicated off-line platform, the CA workstation (CAW). Data is transferred between the CAW and the KMA workstation using removable disks. There are two CA workstations, a master and a secondary for disaster recovery purposes, both are maintained in secure off-line facilities.

4.2.1.8 KMS Admin Workstations

KMS Admin workstations are available at:

BRA01 and LEW02 for the use of the Security Manager and Security Auditor;

Trident House (IRE11) and Bridgeview (DR standby site) for System Operation Service security manager, KMS SYSADM and DBA administration;

BRA01 for System Support Centre support use.

4.2.1.9 KMS Help Desk Client

KMS Help Desk client is installed on System Management Centre Tivoli workstations for support use in STE04 and BRA01 (DR standby site).

4.2.1.10 Network Banking Service Key Production Workstations

Three workstations were introduced to support the production of keys for the Network Banking Service. They are included for completeness and it should be emphasised that the live operation of the KMS service is not directly dependant upon them.

The Atalla 'Secure Configuration Terminal' is used to initially generate the keys for the Compaq Atalla HSM cards. These keys are then transferred to the Card Loading Workstation. Each Atalla card is installed in the Card Loading Workstation in turn and loaded with its keys. The Atalla card is then removed and installed on the NBX Authorisation Agent Servers (these have two cards), KMA Workstation or FTMS Gateway.

FUJ00080037

The Secure Pinpad Key Generation Workstation is used to generate keys for loading into Pinpads. These keys are loaded in to the Pinpads either by Hypercom or by a remote download facility.

Keys are used to sign [R]s and [A]s between the Counter and the Authorisation Agent Servers. Additional keys for the Network Banking Service are delivered to the NBX Authorisation Agents and Counters using existing Horizon processes.

4.2.1.11 Debit Card System Key Management

Many aspects of the requirements of the Debit Card System for key management are common to the Network Banking Service. However, over and above the NBX requirements, there is a need to deliver appropriate keys to the DCS Agent Servers and DCSM Servers.

Delivery of all keys for DCS utilises existing Horizon processes.

4.2.1.12 KMS Fail-over.

There are two KMA Servers, a primary KMA Server (in Bootle) and a secondary KMA Server (in Wigan). Each server advertises two connections to the network, a permanent connection and a switch-able resilient connection.

The switch-able connection relies on the Virtual LAN (VLAN) capability so that either KMA Server can take over the IP address reserved for the ‘current’ KMA Database. Three additional names KMSCURRENT, KMSSTANDBY and KMSINACTIVE are defined for the switch-able connections. These logical names are recorded in HOSTS files. The KMSCURRENT IP address is switched between the KMA Servers at times of fail-over to the secondary KMA Server and fallback to the primary KMA Server, whilst the KMS entries in the HOSTS files remain constant for all platforms connecting to the KMA Database.

In the event of the ‘prime’ KMA server failing or the failure of a campus, then FSCS operations will close down the ‘prime’ and transfer the KMSCURRENT IP address to the ‘standby’ and restart the ‘standby’. All 'clients' of the KMA server can then connect to the 'standby' via the KMSCURRENT IP address.

With this fail-over methodology, the ‘clients’ of the failed ‘prime’ KMA server do not require any modification to the destination IP address or to the route to that KMA server as the ‘standby’ is now the ‘prime’, with the same IP address and route.

The KMA application fail-over scripts, produced by KMA development, confirms the IP address changes before starting any KMA applications on the ‘standby’.

KMA Operations Guide REF10 provides full details, including to FSCS Operations, of the fail-over process

4.2.2 Auto-Configuration Service

4.2.2.1 Introduction

Counter PCs are built with a defined software baseline. Due to the time delay between PC build and installation, it is possible that the software level on the newly installed PC has become out of date.

FUJ00080037

Auto-Configuration is the process, at either rollout or change, by which gateway or slave PCs receive their personalised networking and printer details for operation within an outlet. In addition, as part of the Auto-Configuration process, it supports software catch-up as described in this section.

The Auto-Configuration Service is dependant upon the availability of the Host and Maestro, the Outlet Change Management Service, the Tivoli infrastructure, the Key Management Service, the VPN layer, Correspondence Servers and network communication through to the counters. However, the focus is placed upon the Auto-Configuration Service primary devices i.e. Auto-Configuration server and database, Auto-Configuration Signing server and the Boot Server/Loader.

4.2.2.2 Service Structure

Figure Four provides an overview of the Auto-Configuration Service and its primary interfaces.

4.2.2.3 Auto-Configuration Server

This is the server upon which the Auto-Configuration Database (ACDB) resides. There is one server located at each data-centre. The Auto-Configuration database holds the data necessary for the Auto-Configuration application to function.

Note that the Auto-Configuration server is not required to be online during the Auto Config process of counter installation et al. (The counter-specific files and data are held and distributed via Tivoli at a suitable point in time.)

4.2.2.4 Auto-Configuration Signing Server

The Auto-Configuration Signing Server provides a digital signature for Auto-Configuration generated files for verification by Tivoli on receipt and on delivery to the outlets. An Auto-Configuration Signing Sever is located at each data-centre.

4.2.2.5 Tivoli Infrastructure

Tivoli is the systems management tool used by the Horizon system to distribute software to the counter. The Tivoli infrastructure takes a feed from the Network Service Type (NSAT) process on the short-term performance database platform for the introduction of the bronze and silver service outlets for Network Banking (for their CHAP authentication process).

There is a feed, containing schedule data and other relevant information, from the OCMS server to Tivoli.

4.2.2.6 Radius Servers

Radius Servers are accessed via the Aggregate routers and provide Challenge Handshake Authentication Protocol (CHAP) authentication for the in-bound calls from ADSL, GSM and ISDN connected outlets.

4.2.2.7 Boot Service

The Boot service consists of a Boot Server platform (specifically for satellite outlets) and a Boot Loader platform (specifically for ISDN & ASDL outlets). These platforms provide the Boot Server Files, which contain the initial network information and host name, to outlet gateway PCs when they are initially installed or upon their replacement. A Boot Sever and Loader is located at each data-centre.

FUJ00080037

The Boot Server Files are transferred over a PSTN connection for ASDL and ISDN connected outlets and via the Satellite networks for BT VSAT outlets.

4.2.2.8 Riposte Layer

The applications at this level are updated with details of new counters via the Auto-Configuration database to establish data paths between the counters and the campus platforms.

FUJ00080037

The Auto-Configuration Service and Interfaces.

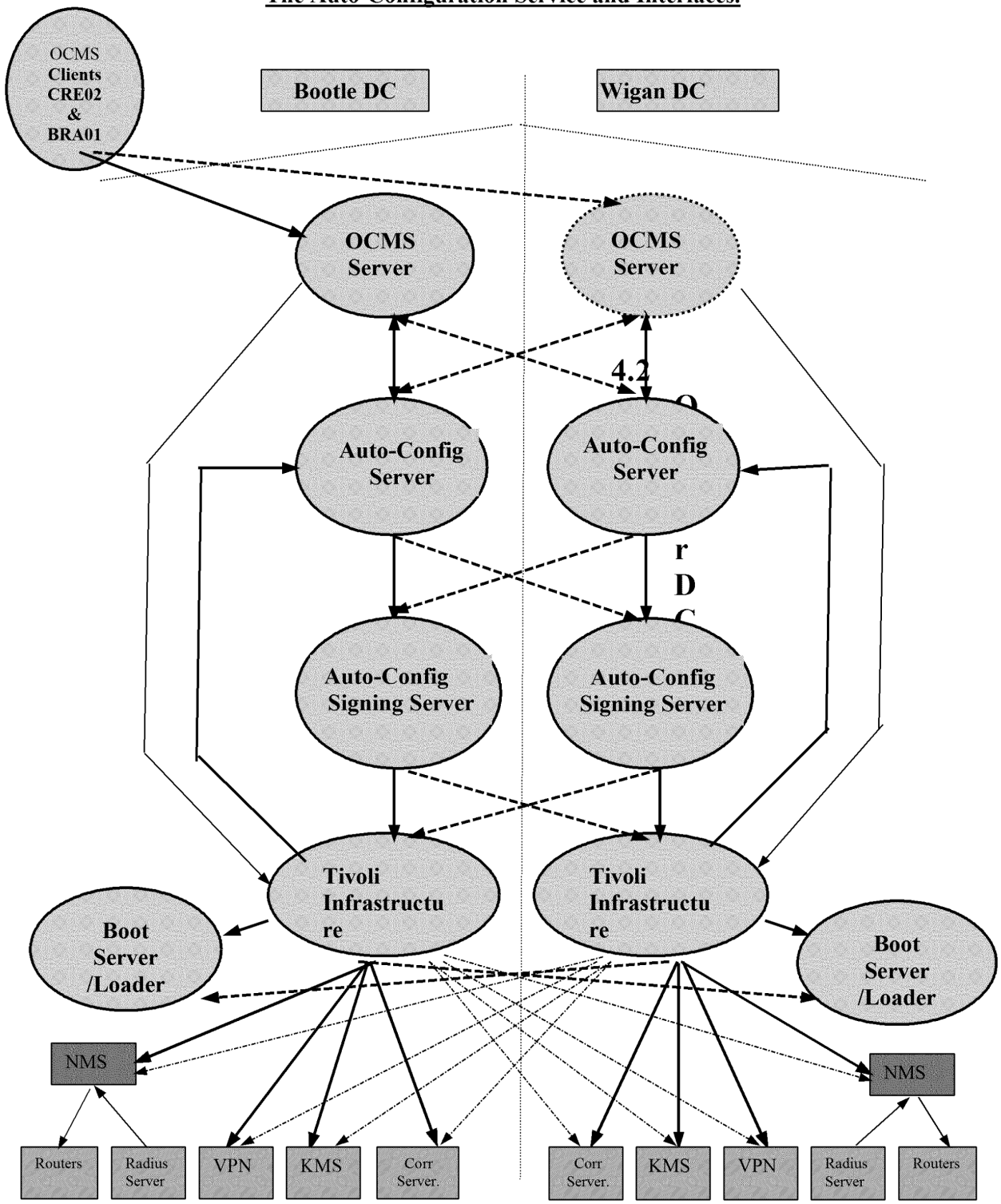


Figure Four

FUJ00080037

4.2.3 Outlet Change Management Service Structure

4.2.3.1 Introduction

The OCMS Server runs a Microsoft SQL Server database application which allows CS staff to manage a set of defined 'outlet change services'. OCMS provides facilities to allow Customer Services to record, schedule and manage planned changes which require physical change at the Outlet. Customer Services have agreed to provide specific services to Post Office Limited for each required change. The agreed changes that may be requested by Post Office Limited as planned Outlet Change are documented in the OBC Change Catalogue. Information is exchanged with OCMS suppliers, i.e. Tivoli, Auto-configuration.

Figure Five shows diagramatically the OCMS infrastructure.

OCMS Service Infrastructure

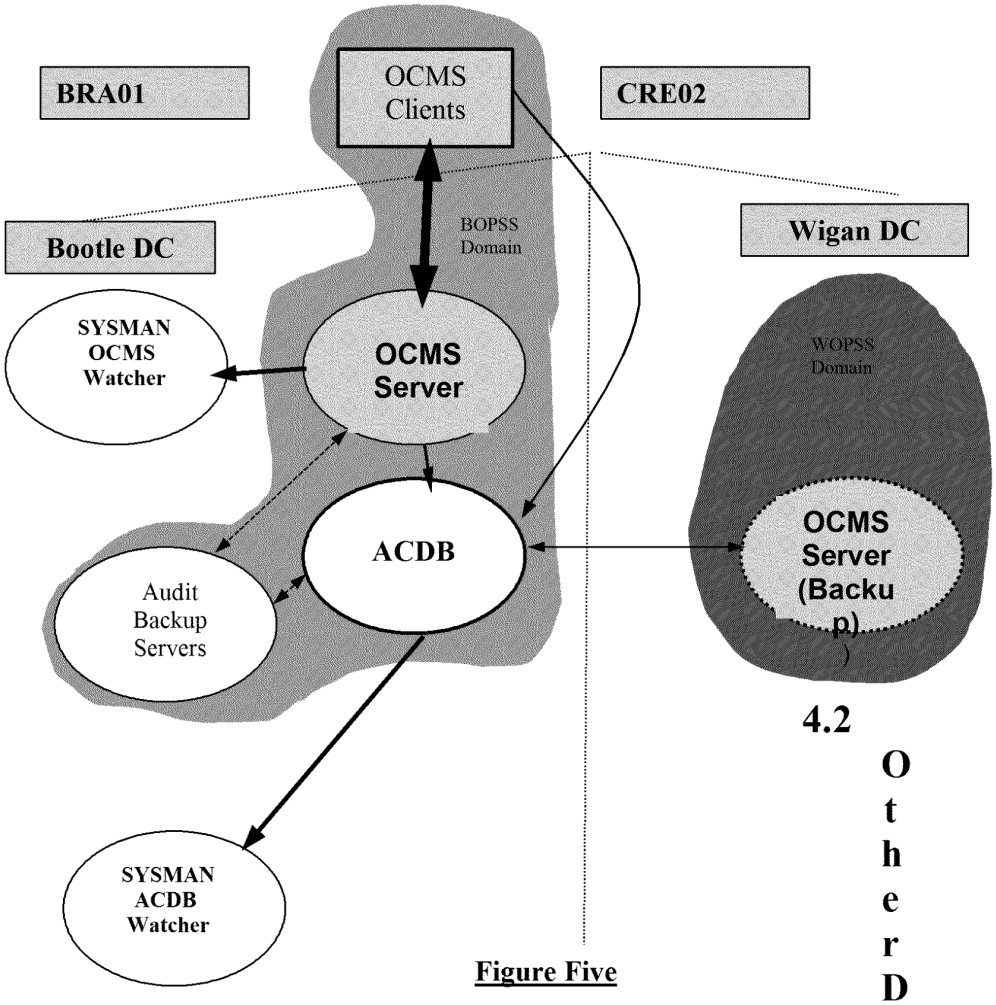


Figure Five

4.2 Other DC

FUJ00080037

4.2.3.2 Structure

4.2.3.2.1 OCMS Servers

There are two Proliant 1850R OCMS Servers, one in each Data-centre, both of which are capable of running the OCMS service. In normal operations one server would be active and the other acting as a warm standby.

The OCMS data is held in an SQL Server database and a variety of 'flat files' on local hard disk storage using RAID5. SQL mirroring software regularly copies data to the secondary server.

The OCMS servers are connected to the Data-centre host LANs.

4.2.3.2.2 OCMS Workstation

The OCMS Servers are accessed from, SecurID protected, OCMS Client workstations connected over an encrypted link to Wigan or Bootle from a private LAN in BRA01. CRE02 LAN connection is via a ISDN link.

For resilience three OCMS Workstations are available in CRE02 and two at BRA01. An additional OCMS Client workstation is available for System Management purposes at Wigan.

4.2.3.2.3 OCMS Data Transfer.

OCMS data is transferred externally to Auto configuration, Tivoli and FSCS. The OCMS Server has associated remote FTMS gateway servers for transferring data to and from FSCS.

A separate FTMS Local Gateway machine, which resides on the Data-centre secure LAN, for OCMS is included for transferring data to FSCS.

The Audit Server is used to copy off the OCMS files sent to Tivoli.

4.2.3.2.4 NT Domains.

The live OCMS Server and its Client Terminals will reside in the BOPSS NT domain. The backup OCMS Server will reside in the WOPSS NT domain.

4.2.3.2.5 OCMS Fail-over.

The OCMS Servers at both data centres use the same IP address on a VLAN. This allows the OCMS Client workstation to remain unchanged after fail-over from the primary to secondary OCMS server.

FUJ00080037

4.2.4 Management Information Services

4.2.4.1 Management Information Services Overview

The Management Information Service consists of three primary databases, i.e. the Data Reconciliation Service, the Transaction Enquiry Service and the Data Warehouse, all of which reside on the Database Server.

The NBX Network Banking RAC Model and the Debit Card RAC Model in REF3 illustrate the relationship of these three services/databases.

For operational details and contingency measures for the Database Server, the Data Reconciliation Service and the Transaction Enquiry Service please refer to REF3.

The RMGA Management Information Service does not have access to the APOP Voucher database which resides on the Database server. (An APOP Administration Service is available within Post Office Limited at their Northern Data Centre.)

FUJ00080037

4.2.4.2 Data Warehouse Service Introduction

Figure Six depicts the Data Warehouse External Architecture. The inputs or sources of data for the warehouse are shown on the left of the diagram, while the outputs or users of the data are shown on the right. The interfaces themselves will be detailed in the relevant Interface Specifications (EPIDs).

Data Warehouse External Architecture

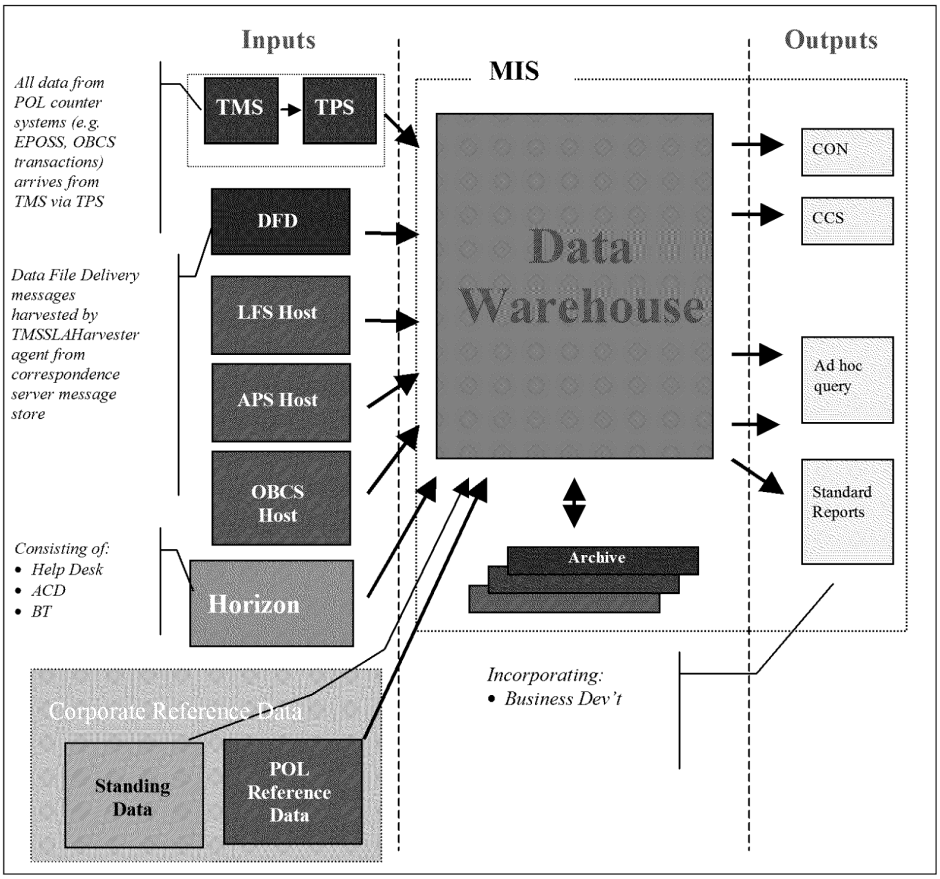


Figure Six

4.2.4.3 Structure

4.2.4.3.1 Data Warehouse Service Structure

The overall structure and functionality for contingency purposes may be represented as follows.

The "data warehouse process" is the set of operations/processes required to source, load, manage and publish data in the data warehouse. Typically, such processes involve data loading, "cleaning", transformation and aggregation. As noted in [1], data "cleaning" will not be conducted for the RMGA data warehouse. Figure Seven gives a conceptual overview of the processing required to operate the RMGA data warehouse.

Data Warehouse Conceptual Process Architecture

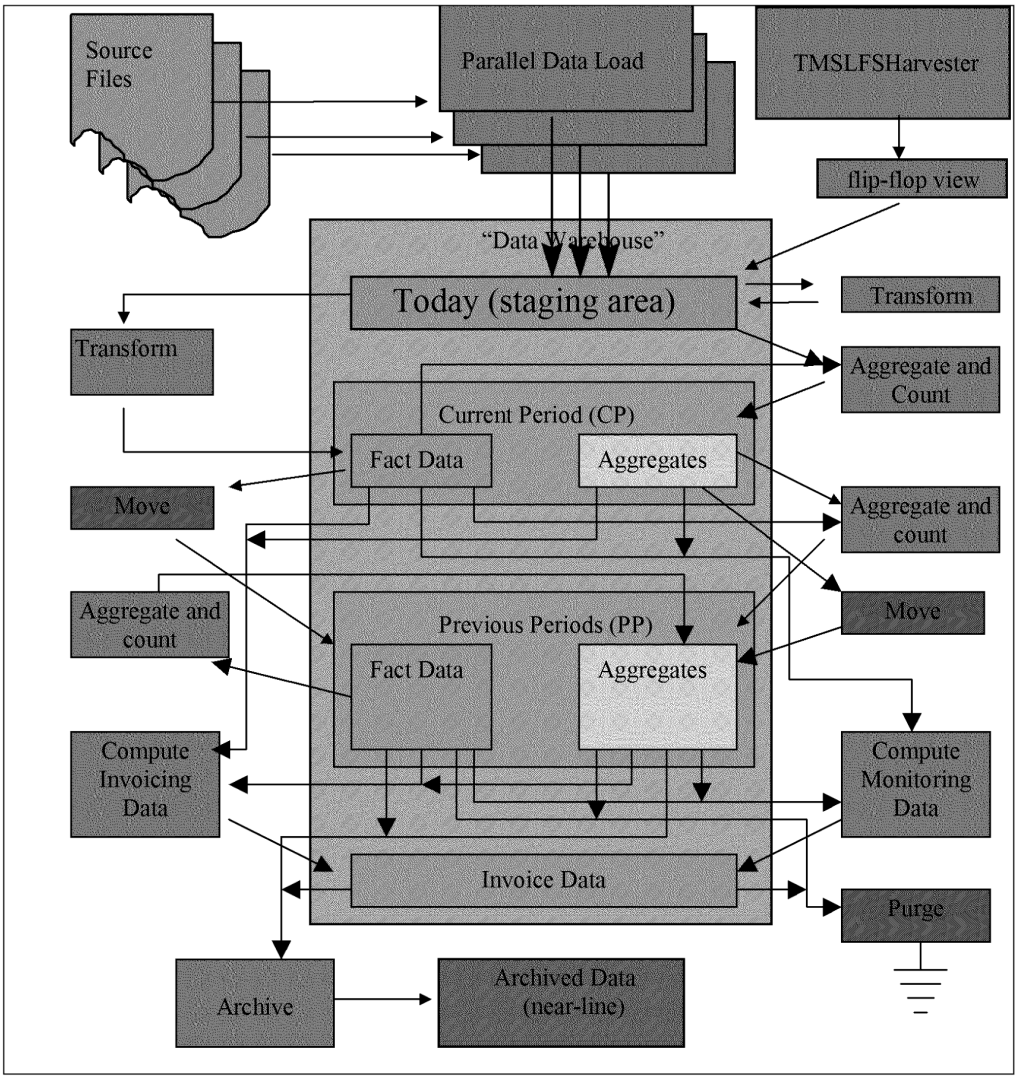


Figure Seven

In summary, data is provided by the source systems in the form of flat files uploaded to a dedicated area on the data warehouse. Note that the flat files are used to insulate the data warehouse from dependencies on the source systems' data models, software version etc. The source files are then loaded (in parallel, where appropriate) into a staging area within the data warehouse. This staging area holds a complete day's worth of data. Any transformations which may be required (e.g. derivation of values etc) will be performed on loaded data, and not as part of the load processes. The staging area will normally be the data source for processes which pre-compute daily aggregated totals. These pre-computed totals are required by invoicing (invoice data) and to satisfy end-user queries. The data in "today" is transformed into a dimensional structure and moved into CP. CP stores the data pertinent to the current period while it is being built up over the course of the week. Once the CP has been completed, the data is moved over to PP (this move requires no transformation). After the data has been moved, it is archived. Archived data is used by the "near-line" mechanism to allow data which is no longer on-line to be queried. CP and PP are the data sources for processes which pre-compute aggregates of grains greater than a single day (i.e. weekly and monthly)

FUJ00080037

The DFD feed is provided from an interactive harvested agent. This is contrary to the design goals of the DW to be able to operate asynchronously, and makes recovery a tricky operation. In principle the Agent Run Table TMS_ART_DWH will enable the harvesting to be restarted from the correct checkpoint in the message-store, but there is a risk that the data may have been archived (deleted) from the message-store due to old age, and Application Support assistance may be needed in re-harvesting. It is not a problem if duplicate data is harvested, as the DW will cope with this.

If the data was harvested late the first time, and after fail-over is harvested 'on time', then reports produced before and after fail-over may vary. This will not happen with feeds from data files.

No changes were necessary to the TPS Interface for the introduction of the NBX service.

4.2.4.4 The Data Reconciliation Service

The DRS is the component that provides reconciliation processing. It interacts with the Outlets, and the Horizon central systems.

Reconciliation takes places at several levels.

Between the FIs reported positions against [R], [A] and [C2] messages and the Horizon reported positions. Confirmed (i.e. reconciled) transactions are reported to the DRS as [C4] messages from the TES. Transaction exceptions are reported to the DRS as [D] messages:

[D] indicates an exception or error condition

Transaction details are forwarded to TIP based upon the reported end of day from each Outlet. The transaction details are derived from the [C1] messages. If a communications failure occurs, or other failure leading to delayed EoD reporting this flow may be delayed by (up to) several days. Existing EPOSS reconciliation measures are used to detect and report on discrepancies across this interface.

The DRS provides reconciliation between the FI's view and the TIP view by maintaining tables of each reported transaction outcome across each interface:

[C12] – as derived from the NBX Confirmation Harvester Agent

[C1] – as reported to TIP

[C2] – as reported to the TES by the DRS

[C4] – as reported from the DRS by the TES (derived from the LREC and REC files)

This position is maintained for each combination of IIN (range) and service. Since there is no single PO Ltd EoD cut off, settlement and reconciliation will both be based upon the MA settlement day boundary as a synchronisation point. This is notified to Horizon within the [A1] message and via trailer records within the [C4] file, such that each [C4] file can be recorded as associated with a FI posting day.

Where a zero-value [C0] is created following timeout of the [A], this value will be blank and the Settlement Date will be provided in the [C4] message. Normally such transactions will have no net settlement significance, although the original [A] may

FUJ00080037

generate a FI settled transaction posted on the day of authorisation, which is reversed on a later posting day, following receipt of the [C2]. The DRS will apply separate reporting category rules for dealing with exceptions reported by the NBE e.g. [D] which will require investigation and manual corrective adjustment.

The immediate status of any specific transaction will be reflected in one of the internal transaction states within the DRS.

4.2.4.4.1 Reconciliation Reporting – Horizon Outlets to DRS

There are two types of message flow between Horizon Outlets and the DRS.

1, Individual [C12] transactions. These are transferred throughout the day by the NBX Confirmation Harvester Agent. Harvesting is done on a continuous basis, with the [C12]s loaded into the DRS in recoverable commitment units, following normal replication of the [C1] messages within the EPOSS transactions

2, EoD transaction processing of [C11] transactions. As part of the normal EoD Campus processing, TPS transaction harvesting will occur following receipt of the EoD marker from Outlets. This provides a delineated set of completed transactions up to the Outlet declared EoD, which forms the basis for transaction reporting to TIP. (Subsequently such transactions also provide the basis for calculating the Cash Account report for TIP.)

NBX transactions included within the TPS harvesting will be forwarded to the DRS to provide an aggregated Outlet position to support reconciliation. Such transactions will be consistent with the Outlet reported transactions sent to TIP (other reconciliation measures detect inconsistencies within the TIP reporting stream), and will include the intended Cash Account Period (CAP) in which they will accounted by PO Ltd (as part of the TIP processing).

4.2.4.4.2 Reconciliation Reporting – RMGA DRS to PO Ltd

A number of reports are generated, some daily and some weekly, as defined in CS/SPE/011 – Network Banking End to End Reconciliation Reporting.

4.2.4.4.3 MIS Clients

FS RMGA Customer Service on a monthly, weekly and ad hoc basis, produce management reports. There are three MIS clients available at FS Bracknell, and for contingency purposes two MIS clients are available at STE04, for the production of these reports.

The TES Query Application is used by RMGA Service Delivery to access a read-only view of Network Banking Transaction details. A ‘3 tiered’ approach has been adopted using an Oracle Forms Server to query the TES Host Application and host the Query application logic. User access to the application is via a local Web Browser running the Oracle JInitiator Java Runtime Environment and Forms applet on the MIS clients.

FUJ00080037

4.2.5 POLFS Development and Test/QA Services

The Post Office Limited Financial Services SAP service consists of three elements a Production service, a Development service and a QATest service. The POLFS Production service is documented within the Horizon Services Business Continuity Plan REF3.

The POLFS Development and QATest service have been classified as supporting services and are therefore included in this plan.

The POLFS Development Service is hosted on a platform in the Fujitsu Bootle Data-centre, and the QATest Service is hosted on a platform in the Fujitsu Wigan Data-centre.

In the even of a disaster at Bootle or a major incident occurring with the Production server, the QATest server at Wigan may be invoked for disaster recovery purposes. Refer to REF3.

The POLFS Development and QATest services are normally available Monday to Friday from 08:00 to 18:00. However either could be available at other times by agreement.

There are no business continuity or disaster recovery requirements for either the POLFS Development and Test/QA services.

Post Office Limited users can run and print POL-FS financial reports from the POLFS Production system located in Bootle, by access through the POL Northern Data Centre. Additionally, Post Office Limited users are able to develop and test changes, along with Prism Development, on the POLFS systems in Wigan, again accessing these systems via the POL Northern Data Centre.

In the event that the POL Northern Data Centre is unavailable, Post Office Limited may decide to invoke POL NDC disaster recovery for the TIP remote Gateway at SunGard Hounslow and for EDG gateway at Prism's DR data-centre at Maidstone. POL and Prism users can then access the services in Bootle and Wigan via Hounslow.

Duty Manager Notes:

1) In the event of a RMGA OOH Duty Manager being informed of 'A' priority incident on either the POLFS Development and Test/QA services they are to inform the RMGA Client Interface Service Delivery Manager (Kirsty Gallacher).

2) Post Office Limited have accepted a POL-FS 'disaster recovery' fail-over time of 48 hours and the unavailability of the POLFS QA-Test service.

3) It is Post Office Limited decision whether or not to invoke the fail-over to their SunGard DR site at Hounslow and the time for full invocation is 48 hours.

4) In the event Post Office Limited invoke SunGard the SAP-Basis support team need to reconfigure IP addresses for POL print server at Hounslow.

FUJ00080037

4.2.6 System Management Infrastructure

4.2.6.1 Introduction

For the purposes of this document, System Management Infrastructure confines itself to those components of the Horizon solution involved in the provision of the Tivoli Enterprise management capability.

The capabilities and role of Tivoli are documented, in detail, in technical design documents.

The primary uses of Tivoli within Horizon are as follows.

4.2.6.2 Monitoring

Monitoring of events on central Horizon infrastructure and equipment including (in some instances via interfaces to other similar products) Sequent Host and Warehouse platforms, Sun Servers, Windows NT servers and workstations and network devices.

4.2.6.3 Software Distribution

Software distribution and software upgrade is supported by Tivoli. This has the facilities to manage and distribute software across multi-platforms e.g. to workstations, servers and counter PCs.

4.2.6.4 Structure

Figure Eight below shows the inter-relationship of the systems management products, within the horizon infrastructure, and the nodes being managed.

Within the Horizon infrastructure the Tivoli Management Environment consists of a single Tivoli Management Region (TMR) built on two layers. These layers are:

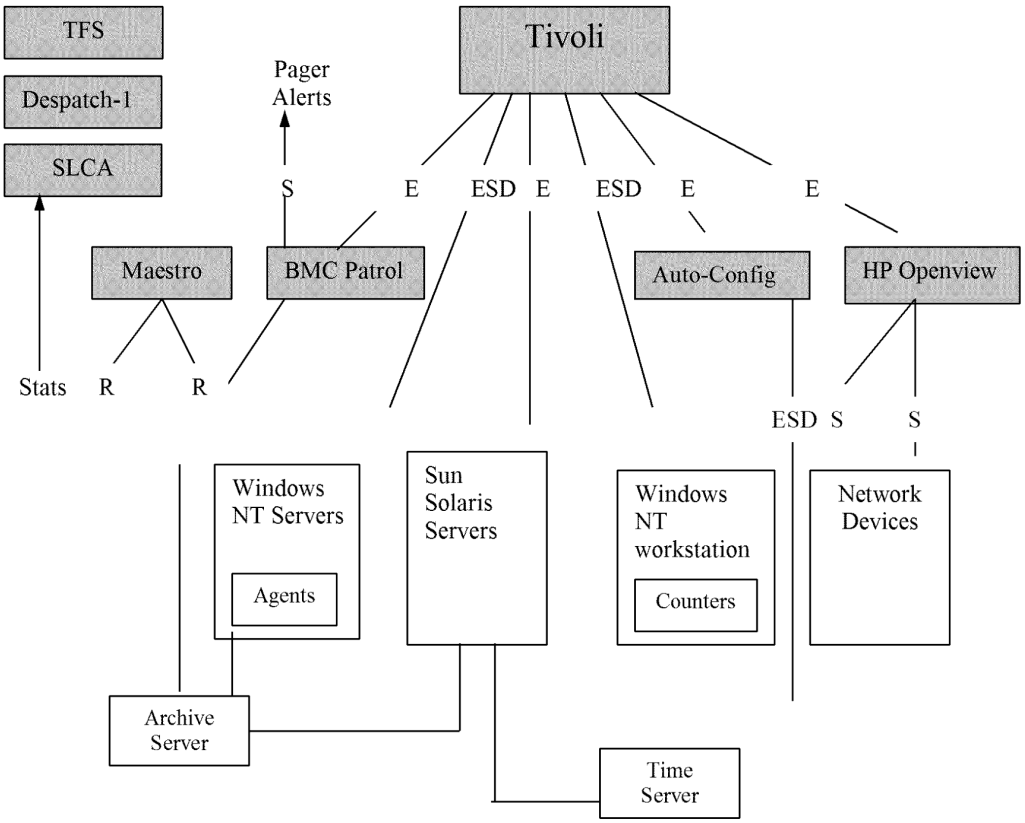
1. The Master TMR which manages the UNIX gateway servers and a small number of Windows NT servers at the campuses.
2. Gateway servers which act as proxy for the management of the remaining campus servers and the post office counters.

4.2.6.5 Equipment locations

The Tivoli systems detailed above are effectively duplicated across the two data-centres, Wigan and Bootle, and procedures for implementing contingency measures are operated by the MSS. Wigan is utilised as the primary data-centre for the System Management Service.

FUJ00080037

Horizon Systems Management Products



Legend

E Events

S Status Information

D Software Distribution

R Schedules running of

Management product

Managed Node

Figure Eight

FUJ00080037

4.2.7 Network Services

4.2.7.1 Branch Service Structure

Approximately 14,000 Post Offices are linked to two Fujitsu Services (Royal Mail Group Account) Data-centres by one of the network service types defined in Table One below. Table One also defines the contingency routing and/or fail-over network services types which are available for each service type.

For a more detailed description of these network service types please refer to REF 3.

Service Type	Description	Valid Comms Type	Business Continuity Contingency
2	Satellite	VSAT	No contingency for loss of the base station in Turin Italy.
			Internet – Resilient network outside FJS control.
			BC contingency for loss of one of the following two POPs: TCY01, TCY02
4	Metered Bronze	ISDN	C&W diverse routing
9	Metered Silver Daytime	ISDN	C&W diverse routing
13	ADSL or PHU	ADSL IPStream	BC contingency available for the loss of one of the following four FJS POPs: SDC01 comms room 1, SDC01 comms room 2, TCY01 or TCY02
		PHU	Rural ISDN with C&W diverse routing
14	Branch Resilient Network Approx 1,800 outlets (ADSL with ISDN Backup)	ADSL + ISDN	See comments relating to ISDN and ADSL

Table One – Branch Network Service Types

The 'fail-over' network service types can also be represented as follows

Note: At S92/T10 a new IP Stream network service was introduced to enable more rural outlets, connected via either satellite or ISDN, to be migrated to ADSL. This created two service-types 13 and 14, i.e., an ADSL Data Stream and an ADSL IP Stream.

At T50/T60 FRIACO Silver Daytime C1 NST 7 Service was withdrawn.

It should be noted that outlets connected over ADSL IP Stream can be identified as they contain IPS_HOME or IPS_OFFICE within their BAS routers names.

FUJ00080037

RMGA Business Continuity Plan REF3 defines the primary RMGA Horizon services provided using the C&W network. This document also defines the risks and actions to be taken in the event of failure of network sub-components. RMGA Duty Managers refer to this document in the event of network failures.

This document provides an assessment of the risks and associated recovery plans provided by C&W as a supplier to Fujitsu Services RMGA. The Risk Assessment detailed in the RMGA Business Continuity plans focuses on the processes involved with the steady state (i.e. not new provisioning) maintenance of telecommunication services for the Horizon project.

4.2.7.2 Client Links

The Client links are defined as those circuits conveying data between the Fujitsu Services RMGA Data-centres and:

1, the Post Office Limited data-centre in POL NDC, e.g. for LFS, APS, POLFS and Reference Data;

2, all AP Client data centres, including EDS for the Card Account Receipt Service.

4.2.7.3 The Branch Resilience Network (BRN)

The Branch Resilience Network provides the following coverage:

- An automatic ISDN backup network for the largest ADSL branches. This is currently predicted to be 1800 branches.
- A backup on demand GSM service that covers all the ADSL and ISDN sites (Note: limited counter numbers would be available due to bandwidth limitations) This would involve an Engineer turning up within 48 hours after a network outage had started and installing the backup network. Once the fault had been fixed, the backup network GSM Modem would be removed.
- The ability to use the backup network, via GSM, for branch relocations if the main network had not yet been installed in the new location – this would use the facilities above.
- The backup network would use the same IP address as the main network. This means that all Post Master functions will work, albeit with less bandwidth than normal.

The Branch Resilient Network will not provide

- Software Distribution capability.
- The ability to use the backup network for new branches if the main network has not been installed.
- the functionality to replace the Gateway PC's (for branches where the main network link has failed and it is running on the GSM network
- Network resilience for satellite branches

For full details of the BNR functionality please refer to REF 14.

FUJ00080037

4.3 Operational Support Services

The Horizon operational support services can be categorised into a Support Services sub-group and an Operational Services sub-group.

The Support Services sub-group consists of the following teams:

The Horizon Service Desk who provide first line support;

For contractual reasons the business continuity aspects of the HSD are documented in a separate business continuity plan CS/PLA/015, REF4

The System Management Centre, who monitor and manage the Horizon RMGA IT infrastructure via the System Management tools detailed above in section 4.2.6. This team also provide second line technical support.

The System Support Centre (SSC), who primarily provides third line support services, and can provide assistance to the SMC in the monitoring and management of the infrastructure.

Fourth line support is provided either by the Royal Mail Group Account Development team or by external suppliers, e.g. Esher or Microsoft.

The Operational Services sub-group consists of the following teams:

The System Operate Service team who operate and administer the NT and Unix systems, Databases and manage the Horizon network infrastructure.

Customer Service operational teams are primarily based at BRA01. These include the Business Support Unit, Reference Data, SSC, Release Management and the Service Delivery Management teams.

RMGA Programme and Development operational support teams. These provide software and documentation change control (PVCS) and release control.

FUJ00080037

4.3.1 Support Services sub-group

4.3.1.1 HSD Service

Refer to CS/PLA/015.

4.3.1.2 The System Management Centre

The System Management Centre operational team is based in Fujitsu Services STE04 building. The team's primary function is to monitor and manage the RMGA Horizon infrastructure via Tivoli eventing, see section 4.2.6 above. The team provides 24 hours shifted service, every day of the year.

In the event of a major incident or disaster at STE04 the SMC have access to the RMGA disaster recovery room in the Fujitsu Services BRA01 building. The SMC have warm standby Tivoli equipment stored on site and network access to the Horizon estate.

4.3.1.3 The System Support Centre.

The SSC team primarily provide third line support. See Bracknell services in section 4.3.2 below.

4.3.1.4 RMGA Development and External Suppliers.

For completeness this subsection has been included to explain that RMGA Development and the development teams of external suppliers provide the final line of support, generally referred to as fourth line support.

4.3.2 Operational Services sub-group

4.3.2.1 The Systems Operate Service

In providing an ongoing managed service for the Systems Operate, FSCS will provide RMGA with a support service covering the following areas:

UNIX Support Service

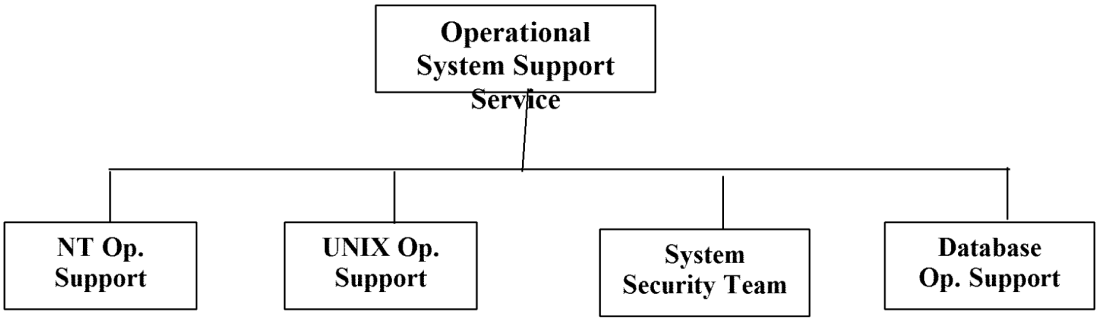
Database Support Service

NT Support Service

Systems Security Team

FUJ00080037

The overall structure and functionality for contingency purposes may be represented as follows for the Systems Operate Service (SOS):



4.3.2.1.1 Operational Support Service

In providing the Operational Support Service FSCS provide RMGA with a round-the-clock service, managing and supporting those parts of the RMGA Solution housed in the RMGA Data Centres at Wigan and Bootle. Below is a summary, which includes:

- Management of the hardware maintenance.
- Management of the environmental controls.
- Management of the infrastructure maintenance to agreed schedules.
- Operate the service in 'supervisor' mode for special maintenance activities.
- Management and archiving of system and user filestore.
- Production and maintenance of archive reports.
- Production and maintenance of filestore repair tapes.
- Monitoring of the key service elements, to ensure that service issues are identified at the earliest possible opportunity.
- Responsibility for investigating all faults and problems arising on the Supported Systems, resolving the First Line support faults and problems, and where appropriate forwarding unresolved support issues to the FSCS or RMGA support teams responsible.
- Monitoring of the workflow through the Supported Databases. The Supported Databases will be automated via the Maestro scheduler but will be monitored by FSCS staff in Trident House. Any event, which cannot be resolved by first line staff, will be progressed to FSCS technical support.
- Provision of a duty manager, based in Trident House. The duty manager will act as a point of contact for RMGA and Post Office Limited operations staff for day-to-day operational dialogue and any escalation issues. A duty manager rota will be provided on agreed periodic basis.
- Monitoring the capacity usage of the Supported Systems and Operating System Software and advise RMGA when limits are being approached. FSCS will also provide recommendations on remedial action to RMGA.

FUJ00080037

- Management of off-site storage of system archives and recovery information.
- Collection of necessary diagnostics to allow faults to be progressed to resolution.
- Management of diagnostic links to subcontractors.

4.3.2.1.2 UNIX System Support Service

The System Support Service will provide RMGA with comprehensive support for the Operating System Software from the FSCS Data Centre at Trident House Belfast. This will include:

- Software support and system administration activities
- Investigation and progression of all system alerts and dumps.
- General housekeeping of the system error logs and audit files.
- Maintaining UNIX teleservice interfaces.
- Introduction of new hardware components.
- Applying changes to user and group security as necessary.
- Maintenance of file and directory permissions.
- Changing to communication cataloguing information as required.
- Maintenance of the network configuration information.
- Integrity checks on file systems and recovering inconsistencies as necessary.
- Responsibility for managing to a successful resolution, all problems and faults associated with the Supported Systems.
- Resolving of faults and problems arising on the Operating System Software.
- Ownership of the operations manual covering all aspects of the services provided as part of the Systems Operate Service.
- Management of the Supported Systems and Operating System Software.
- Management of ongoing operating system support activities
- Performing back-ups and recovering as necessary.

4.3.2.1.3 Database Support Service

The Database Support Service will provide RMGA with comprehensive support of the Supported Databases including user facing support activities from the FSCS Data Centre at Trident House Belfast. Below is a summary, which includes:

- Database administration activities which include:
  - The set up of users after a new software installation or upgrade.

FUJ00080037

- Exporting of data.
- Creation/recreation of databases.
- Upgrade, migration or creation of databases.
- Changes to the Supported Databases using Change Management.
- The import of data from an export as required in support of the Supported Databases.
- Installation and testing of build software after any change, upgrade of the operating system, upgrade of database software, or after modifications to the Supported Databases.
- Monitoring the Supported Databases using BMC Patrol and software supplier supplied views; run regular checks to monitor table-spaces, availability and fragmentation, and when appropriate reorganise the database (where reorganise includes: export, recreate and import).

- Management of problems and faults associated with the Supported Databases by forwarding calls resulting from the above support activities to the appropriate support unit.
- Investigation of faults and problems arising on the Operating System
- Monitoring database utilisation and occupancy.
- Management of the Supported Databases under Change Management, recording software revision levels.
- Maintenance and administration of the Supported Database variables, under Change Management.

4.3.2.1.4 Windows NT Support Service

The Windows NT Support Service provides RMGA with comprehensive support for the Windows NT Software from the FSCS Data Centre at Trident House Belfast. Below is a summary, which includes:

- Operating Software support and system administration activities for the Supported NT Systems as follows:
  - Investigation and progression of all system alerts.
  - Undertaking general housekeeping of the system error logs and audit files.
  - Introducing new hardware components.
  - Applying changes to user and group security as necessary.
  - Maintaining file and directory permissions.
  - Maintaining network configuration information.
  - Performing integrity checks on file systems and recovering inconsistencies as necessary.
  - Performing back-ups and recovering as necessary.

FUJ00080037

- Responsibility for managing to a successful resolution, all problems and faults associated with the Supported NT Systems.
- Management of the Supported NT Systems and Windows NT Software, recording software revision levels and hardware modification status in accordance with the FS RMGA Change Control Process.
- Install new releases of the Windows NT Software such that the minimum release levels for the software, as recommended by the software supplier, are correctly maintained.
- Provision of ongoing operating system support activities.

4.3.2.1.5 Systems Security Team

The installation and configuration of RMGA firewall systems including: Wigan manager plus four gateways, Bootle manager plus four gateways, two LEW02 and two Bracknell firewalls. On each system, the Systems Security Team manage the UNIX hardware and operating system which includes users, file-systems, system backups and installed applications e.g. Checkpoint Firewall-1. The configuration of Checkpoint Firewall-1 rulebases is managed by the Network team.

4.3.2.2 Network Support Services

The Network Support Service provides RMGA with comprehensive support for all aspects of the Live RMGA Network and limited support of RMGA related test networks. The network service is provided by the Network Support team at the Wigan and Bootle data-centres. The service includes:

- On site support 24 by 7 for operations and network services.
- Investigation of all network related issues to 3rd line and progression and monitoring of those calls that go to 4th line support organisations.
- Progression and monitoring of WAN/ISDN and network hardware issues for non-Live RMGA related test environments that require 4th line support assistance.
- Monitoring of all network and some host elements of the live service using HP Openview.
- Automatic triggering of on call through paging on interception of critical Host events.
- Maintenance and support of all network hardware on the live estate.
- Management of Network hardware systems connected with the live service at remote sites.
- Management of IP address schemes and databases at all sites connected with the live service.
- Management of the cable infrastructure and databases at Wigan and Bootle Data-centres.

FUJ00080037

- Management of cable infrastructure at all Live remotes sites.
- Introducing new network hardware or configuration elements.

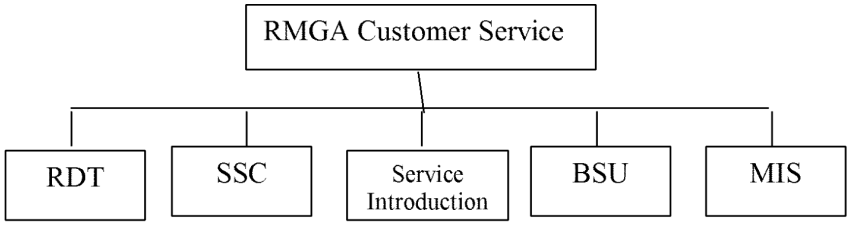
FUJ00080037

4.3.2.3 RMGA Customer Service

Fujitsu Services RMGA Customer Service support, operations and infrastructure services are provided primarily from the Fujitsu Services Bracknell (BRA01) building.

Fujitsu Services LEW02 has been designated the 'Disaster Recovery' site for the CS and essential Development support services which are provided from Bracknell.

The overall structure and functionality for contingency purposes may be represented as follows:



4.3.2.3.1 Reference Data Team

The Reference Data Team validates and processes live Reference Data in association with Post Office Limited at Chesterfield and the Post Office Limited Support Change Implementation Team who are also located in the Fujitsu Services BRA01 building.

The prerequisites to provide the service are:

Access to RDMS validation and verification counters; workstation access to live RDMS service; (Refer to REF3 for more detail of the RDMS service.)

Ability to receive Reference Data from, and send Reference Data to Post Office Limited at Chesterfield and BRA01 respectively;

Access to Fujitsu Services (RMGA) infrastructure services i.e. E-mail, MIS, Peak, TRIOLE For Service, PVCS.

Access to Post Office Limited E-mail system (OBC Network and OBC Product mailboxes)

4.3.2.3.2 Systems Support Centre

The Systems Support Centre (SSC) provides live support at 3rd line (and for some applications/services 4th line) level to various elements of the Horizon service and applications. The SSC also developed and support Peak, the third/fourth line incident management system.

The prerequisites to provide this service are:

Access to simulated test environments for recreation of application failures;

Access to live systems for problem diagnosis;

Access to Fujitsu Services (RMGA) infrastructure services i.e. E-mail, Peak, TRIOLE For Service, PVCS.

FUJ00080037

Please note that a Technical Bridge facility is available in BRA01. This is used by RMGA Service Delivery Management and the SSC for the management of major incidents and business continuity incidents. There is no direct DR capability for this facility which can be indirectly provided by the SSC, SMC and Data-centre operations.

4.3.2.3.3 Business Support Unit

The Business Support Unit (BSU) investigates and resolves all 'Business' or 'Reconciliation' incidents received from Post Office Limited.

The prerequisites to provide this service are access to the Business Incident Management (BIM) system, fax and telephone facilities.

4.3.2.3.4 Management Information Systems

The Management Information Systems (MIS) function processes Management Information collected and processed on the Data Reconciliation Service database and on the Data Warehouse.

The prerequisites to provide the service are:

Access from MIS Clients to the DRS and Data Warehouse databases, and to the MIS File server.

4.3.2.3.5 Service Introduction

Service introduction primarily consists of a Customer Service programme planning function and a Release Management function.

Release Management manage the release of software changes and Reference Data into the live environment across the Horizon service.

The prerequisites to provide the Release Management service are:

Access to live RDMS service;

Access to Fujitsu Services (RMGA) infrastructure services i.e. E-mail, Peak, TRIOLE For Service, PVCS.

Access to Post Office Limited, E-mail system (OBC Reference Data mailbox).

FUJ00080037

4.3.2.4 RMGA Programme and Development Operational Support

RMGA Programme team primarily provide the following two essential services which are required for the support of the Horizon infrastructure.

- Change Control;
- Authentication of software releases to the live estate.

4.3.2.4.1 Change Control

RMGA Programmes manage the PVCS, item version control system for the RMGA Horizon Programme. The primary PVCS server resides in BRA01 and a secondary server resides in LEW02. The databases on these severs are synchronised on an hourly basis over the Fujitsu Services Corporate network. In addition daily back-ups are also taken of the PVCS servers.

To access PVCS users require either 'PVCS Terminal' or PVCS Dimensions PC Client. PC client is installed on the Office PCs in both BRA01 and LEW02.

4.3.2.4.2 Configuration Management – Signing Server.

RMGA Programmes manage the day-to-day operations of the Configuration Management Signing server, which is used to authenticate software releases to the live estate. The primary CM Signing server resides in BRA01 and a secondary server resides in LEW02. The databases on these severs are synchronised on an hourly basis over the Fujitsu Services Corporate network. In addition daily back-ups are also taken of the Signing servers.

In the event of a disaster at BRA01 the Programme team can access the LEW02 CM Signing server using disaster recovery laptops at least one of which is held off site.

4.3.2.5 Development Operational Support

4.3.2.5.1 Live System Team

The Live System Test (LST) team, who reside within the RMGA Development organisation, test software changes about to be released into the live estate. This is achieved by proving the software changes on discrete test configurations that replicate the live software environment.

The prerequisites to provide this service are:

Availability of hardware test rigs upon which the live software set can be loaded and run;

Access to Fujitsu Services (RMGA) infrastructure services i.e. Peak, TRIOLE For Service, PVCS.

FUJ00080037

5.0 Testing Strategy

5.1 Initial Testing

The initial testing of all business continuity contingency plans has been documented in the Business Continuity Test Plan (REF2). Some tests are focused at sub-service level, e.g. KMS, OCMS, however other tests are based upon a facility, e.g. the Loss of Major Site (BRA01). See the Business Continuity Test Plan (REF2) for fuller details.

5.2 Ongoing Test Strategy

This refers to how the contingency measures, in place for the Horizon Support Services, shall be periodically tested to ensure they are current and reflect the service model for those services as they mature.

This is provided by an ongoing series of business continuity tests at a predetermined frequency for the duration of the Fujitsu Services RMGA contract. The nature of these tests are documented in the Business Continuity Test Plan (REF2), which also contains a yearly test schedule.

FUJ00080037

6.0 Preventative Measures

It is a fundamental philosophy of the RMGA solution that wherever technically possible, all components of the service are designed in such a way as to ensure maximum resilience to failure by way of eliminating all possible single points of failure, i.e. by providing multiple platforms performing similar functionality both for performance and resilience.

As such the overall design process has at a single step reduced the risk levels to low across the overall Horizon solution.

6.1 Infrastructure Support Services

This concept is extended to the RMGA Data-centre's themselves, thus allowing the RMGA service to be delivered in part, or indeed in total, from either data centre should the need arise.

To complement this design philosophy, the overall Horizon solution adopts and demonstrates industry best practice in areas such as systems enterprise and operational management.

This provides the capability to monitor and report on virtually every hardware component and software application comprising the Horizon solution in general.

It also allows a significant amount of automation to be introduced into the overall Horizon capability, which in most situations allows more timely resolution of any failures that are experienced.

Detailed design documents are available which document at the very lowest level the exact architectural design of the Horizon solution, and is not the purpose or the intent of this document to replicate those details here.

The following gives a high level summary of the measures in place, within the Horizon solution, necessary to provide the Infrastructure Support Services.

6.1.1 The Key Management Service

6.1.1.1 KMS Servers and Database

The KMA and its database are mirrored between the main and standby sites using EMC hardware replication of the filestore. The architecture is very similar to that used for the host servers.

During normal operation, the standby KMA server is up and running its operating system, but the DBMS and KMA-related NT services are not running.

Fail-over is via operator intervention following similar procedures to those used for fail-over of the host servers. When the main KMA server has failed and the standby is in use, particular care should be taken over the integrity of any data

FUJ00080037

generated, since reliable mirroring of the data is not provided by the EMC system in this circumstance.

6.1.1.2 Data-centre Networks

Within each Data-centre the KM Server is connected to primary and secondary isolated KMS LANs. These LANs are connected via firewalls and Logical Campus Routers to the main Campus virtual LANs in each Data-centre. The two Data-centre main Campus LANs are connected via Cisco Catalyst switches to two 1Gbit links. One is provided by C&W and the other, contracted via C&W, provided by BT. Both KMA servers have unique IP addresses during normal running. In the event of detection of a failure on the primary KMA server, the secondary server has its IP addresses reset to that of the failed server and is restarted. Access to the KMS service continues as before from either campus, see section 4.2.1 for further detail.

6.1.1.3 Network to Data-centre(s)

Clients using the interactive distribution channel will be configured with the VLAN IP address of the current KMA server. The KMS entries in the HOSTS files remain constant for all platforms connecting to the KMA Database.

PO gateway PCs will additionally be configured with the IP of two VPN exception servers, one at each campus.

6.1.1.4 Tivoli Infrastructure

With the exception of the Certification Authority Workstation (which is not connected to the network), all processes in the Key Management Centre will be monitored by Tivoli, which will raise appropriate alarms if a process stops running.

(Software updates for the Key Management Centre (except CAW) are installed remotely by Tivoli software distribution.)

6.1.1.5 KMS Workstations

The Key Manager's primary workstation is at BRA01 and will normally available continuously. There are secondary workstations in physically secure areas at LEW02. In the event of loss of the primary workstation, the secondary can be brought into use at no more than 4 hours notice at any time and will then be available continuously until a new primary is installed. No KMS data is held on the KMA workstation

The Certification Authority workstation at BRA01 will normally be available continuously. A secondary Certification Authority workstation will be available at the same site as the Key Manager's secondary workstation whenever the secondary workstation is in use.

FUJ00080037

The Certification Authority Workstation is backed up to the KMA server each time it is used, hence it is effectively a standby machine.

In the event of failure of either Key Management workstation or either Certification Authority workstation the system will be recoverable or replaceable in less than 1 day.

6.1.1.6 Riposte Messaging System

Resilience of the Riposte messaging system is known to be high; therefore no additional measures have been included in the Key Management System to cover communication faults.

6.1.2 Auto-Configuration Service

To complement this design philosophy, the overall Horizon solution adopts and demonstrates industry best practice in areas such as systems enterprise and operational management.

This provides the capability to monitor and report on virtually every hardware component and software application comprising the Horizon solution in general and the Auto-Configuration Service in particular.

It also allows a significant amount of automation to be introduced into the overall Horizon capability, which in most situations allows more timely resolution of any failures that are experienced.

Detailed design documents are available which document at the very lowest level the exact architectural design of the Horizon solution, and is not the purpose or the intent of this document to replicate those details here.

Below is a high level summary of the measures in place at each layer of the Horizon solution necessary to provide the Auto-Configuration Service solution. Wherever appropriate, references to more detailed design documents have also been included.

6.1.2.1 Data Centre LANs

There are multiple connections to the Auto-Configuration Server, Signing Server and Boot Server/Loader and a VLAN to the OCMS server, see 4.2.2 and Figure Four. In the event of a failure of any Auto-Configuration Service component an alert is raised via HPOpenview and operational staff are paged. Automated processes have been implemented to re-route connections to the alternative LAN in the event of a LAN failure.

6.1.2.2 Firewall(s)

Firewalls exist in pairs to provide resilience. On failure of the primary the alternative firewall, of the pair, will take over responsibilities automatically.

FUJ00080037

6.1.2.3 Auto-Configuration Server(s)

A standby processor option is configured on the primary Auto-Configuration server. On failure of one of the processor units, a second processor is available to take control and continue operation. The data and system partitions are held on RAID filestore and are therefore protected from single disk failure.

The server has dual network cards for LAN connection thus protecting against single card failure.

The Auto-Configuration Database is replicated on to the secondary Auto-Configuration server at the alternate data-centre. Should the Auto-Configuration Server become unavailable, the database can be activated at the alternate site.

The database is checked for consistency and a security copy taken to cartridge on a daily basis. There is a cold backup of the entire system taken on a weekly basis. All backups are taken via the Audit Server.

All processes involved in the securing and mirroring of data, are monitored by Tivoli.

6.1.2.4 Auto-Configuration Signing Server(s)

If the primary Auto-Configuration Signing Server fails the Auto-Configuration Database Server will automatically attempt write to the alternative Auto-Configuration Signing Server at the secondary data-centre.

6.1.2.5 Tivoli Layer(s)

Tivoli is used to monitor the Auto-Configuration primary and standby servers and the Auto-configuration Signing Servers. For further details see 4.2.2 and Figure Four.

In the event of a failure of the primary Tivoli infrastructure a standby Tivoli layer is available at the alternative data-centre. If the Auto-Configuration Signing Server fails to write to the primary Tivoli infrastructure it will automatically attempt to write to the alternative Tivoli infrastructure at the secondary data-centre.

Tivoli provides storage facilities for the configuration data until it is required at the correct point in time on other platforms.

6.1.2.6 Radius Servers

The LNS routers use the Radius Servers to provide CHAP authentication for the inbound calls from ISDN, GSM and ADSL connected outlets. There are two Radius Server per campus for these services, as they contain the authentication details of all ADSL, GSM and ISDN connected outlets, there is contingency across the Horizon data-centres. The availability of Radius Server does not directly affect the Auto-Configuration Service.

FUJ00080037

6.1.2.7 Boot Server/Loader(s)

If the primary Boot Server or Loader fails a standby Boot Server or Loader is available at the alternative data-centre. If the Tivoli infrastructure fails to write to the primary Boot Server/Loader it will automatically attempt to write to the alternative Boot Server/Loader at the secondary data-centre.

The ISDN Primary Rate Interface connections to the Boot Servers are automatically switched by C&W on the loss of either Boot Server's 'Live Signal'.

6.1.2.8 Auto-Configuration Dependant Services/infrastructure.

The Auto-Configuration Service on the day of counter installation is dependant upon the availability of the Outlet Change Management Service, the Tivoli infrastructure, the Key Management Service, the VPN layer, Correspondence Servers and network communication through to the counters.

Note the OCMS service provides schedule and temporary change information to Tivoli. To the Auto-Configuration Service, OCMS provides address and outlet details changes. These actions will have been completed before installation takes place.

6.1.3 Outlet Change Management Service

This provides the capability to monitor and report on virtually every hardware component and software application comprising the Horizon solution in general and the OCMS solution in particular.

It also allows a significant amount of automation to be introduced into the overall Horizon capability, which in most situations allows more timely resolution of any failures that are experienced.

Detailed design documents are available which document at the very lowest level the exact architectural design of the Horizon solution, and is not the purpose or the intent of this document to replicate those details here.

Below is a high level summary of the measures in place at each layer of the Horizon solution necessary to provide the OCMS solution. Wherever appropriate, references to more detailed design documents have also been included.

6.1.3.1 OCMS Server

An OCMS server is available in both Wigan and Bootle data-centres.

6.1.3.2 OCMS Database

The OCMS data is held in an SQL Server database and a variety of 'flat files' on local hard disk storage. Data resilience is achieved by the use of RAID5. All processes performed, to secure the data, are monitored by the Tivoli OCMS watcher.

FUJ00080037

6.1.3.3 Firewall(s)

Each of the firewalls is paired to provide resilience. In the event of a firewall failure its relevant pair will take over its responsibilities automatically.

6.1.3.4 Network to Data-centre(s)

Cable & Wireless IP Select network connections exist between the Horizon secure LAN at Fujitsu Services BRA01, and at LEW02, and to each Data-centre. Thus data can be routed via alternative Data-centre and inter campus LAN should either of the primary connections be unavailable.

A 128KBit ISDN connection is available from CRE02 to each data-centre.

6.1.3.5 Tivoli Infrastructure

Tivoli OCMS Watcher is used to process files from the OCMS primary and standby servers.

6.1.3.6 OCMS Client Workstations

Three OCMS Client Workstations are available in BRA01 and seven OCMS Client Workstations are available in CRE02. An additional OCMS Client Workstation is available at Wigan.

In the event of a disaster at either BRA01 or CRE02 OCMS service will be provided from the alternative Fujitsu Services site. In event of a disaster at Wigan OCMS System Management service can be provided from either CRE02 or BRA01.

6.1.4 Data Warehouse

To complement this design philosophy, the overall Horizon solution adopts and demonstrates industry best practice in areas such as systems enterprise and operational management.

This provides the capability to monitor and report on virtually every hardware component and software application comprising the Horizon solution in general and the Data Warehouse/MIS solution in particular.

It also allows a significant amount of automation to be introduced into the overall Horizon capability, which in most situations allows more timely resolution of any failures that are experienced.

Detailed design documents are available which document at the very lowest level the exact architectural design of the Horizon solution, and is not the purpose or the intent of this document to replicate those details here.

Below is a high level summary of the measures in place at each layer of the Horizon solution necessary to provide the Data Warehouse/MIS solution. Wherever appropriate, references to more detailed design documents have also been included.

FUJ00080037

6.1.4.1 Database Server/ Data Warehouse

The Data Warehouse runs, on the Horizon Database server, a Fujitsu-Siemens Primepower 650 platform under Solaris 9 with ESF 2.3.

The server is provided with dual power supplies and has RAID-5 disk arrays.

The Database server has been provided with dual fibre-channel EMC Symmetrix Disk Arrays using SRDF over the dual inter-campus 1GB intercampus links.

The Database server has Timefinder for Business Continuity Volumes, with Veritas Volume Manager.

The Database server runs CA BrightStore EnterpriseBackup controlling a StorageTek L180 tape library.

6.1.4.2 Database Server Resilience

There is a secondary Database server at the alternative Campus which can be used in the event of a total unrecoverable failure on the primary Database server or at the primary campus. As a guide it takes approximately two hours to fail-over to and restore the secondary Database server. The time is dependant upon the size of the databases.

6.1.5 System Management Infrastructure

6.1.5.1 Loss of Network Communications to Wigan

In the event of MSS at Wigan becoming isolated, due to the loss of network devices, MSS staff can be relocated to either the Bootle data-centre or to STE04. During the relocation process MSS staff can advise SMC staff at STE04, via telephone links, on how to provide the MSS service. There is also a small team of MSS staff based in STE04 who could provide a partial service.

6.1.5.2 Loss of Network Communications to STE04

In the event of STE04 becoming isolated, due to the loss of network devices, SMC staff could relocate to BRA01 in approximately three hours from the time a decision is taken. During the relocation process SMC staff could request assistance from the MSS in Wigan and the SSC in BRA01.

6.1.5.3 Buildings –Wigan - MSS

With the loss of Wigan it is planned that the MSS staff would relocate to the Bootle Data-centre, in approximately one hour, where previous arrangements have been made. Alternatively, MSS staff could, on an emergency basis, be relocated to either Data-centre (Wigan or Bootle). There is also a small team of MSS staff based in STE04 who could provide a partial service.

FUJ00080037

6.1.5.4 Buildings – STE04 - SMC

With the loss of STE04 it is planned that the SMC staff could relocate to BRA01 in approximately three hours from the time a decision is taken. It is also possible for some staff to operate a TRIOLE For Service from STE04. If necessary it is also possible to run SMC functions from MSS Wigan, either using MSS as a temporary cover, or via SMC staff relocating to Wigan.

6.1.5.5 People - MSS

The MSS is operated on a 'two shift' basis. In the event of the loss of employees from one shift, staff from the unaffected shift would be available. There is also a small team of MSS staff based in STE04 who could provide a partial service.

6.1.5.6 People -SMC

The SMC is operated on a "24 by 7" basis. In the event of the loss of employees from one shift, staff from the unaffected shift teams would be available to transfer to an alternative site, or operate from STE04.

6.1.6 Network Services

6.1.6.1 C&W Preventative Measures

The core C&W network has been designed to provide resilience through the deployment of SDH technology. The network is made up of a series of interlocking rings, should one half of the ring fail (e.g. fibre break) the traffic will be routed to its destination via the other half of the ring.

Both C&W (NMC) and BT (NMC) have network management centres that monitor and control their respective networks 24 hours per day, 365 days per year. In the event of a fault being detected the appropriate maintenance team is despatched to rectify the problem in the shortest possible contracted timeframe.

6.1.6.2 Fujitsu Services RMGA Data Centres - Bootle and Wigan.

The Bootle and Wigan campuses are networked over DWDM links, one provided by BT and one provided by C&W although both are contracted via C&W. Over each of the two DWDN links 2 presentations are provided to RMGA, one 1 Gbit Ethernet and one 1 Gbit Fibre channel-link. The 1 Gbit Ethernet providing the Intercampus IP network and the 1 Gbit Fibre Channel supporting the EMC SRDF link. The two DWDM link are diversely routed.

Within each site or data-centre each fibre route terminates on physically separate transmission equipment, which is powered via the sites UPS.

6.1.6.3 Fujitsu Services SDC01 & TCY01/02 Data Centres.

The Fujitsu Services ADSL IPStream infrastructure utilises four Points Of Presences in the FJS Southern Data Centre 01 comms rooms 1 and comms room

FUJ00080037

2, and at TeleCity01 and TeleCity02 Data-centres. The DLS LNS routers are configured to provide contingency across the four Points Of Presence.

6.1.6.4 Post Office Limited Northern Data Centres

Access to the POL NDC site is via C&W separately routed Cable & Wireless IP Select network connections. The resilience of these circuits is also high due to the fact that there is no common point of failure between each site and the data-centres. Each data-centre has two separately routed Cable & Wireless IP Select network connections back to two separate C&W Synchronous Network Access Points (SNAPs). Connectivity between SNAPs and the RMGA data-centres is provided by C&W fibre, via the C&W backbone.

6.1.6.5 WAN Circuits.

Asymmetric Digital Subscriber Line (ADSL) technology has also been implemented within the C&W MPLS data network. Each ADSL Outlet has a connection through a specific C&W Broadband Access Servers and therefore for ADSL outlets this is a single point of failure within the C&W MPLS network.

For all outlets there are single points of failure within the BT network, namely at some local serving exchanges where an ISDN2 line to a PO outlet terminates. This would result in the loss of communication with a number of PO outlets, but 'local exchange failures, would be limited to a small geographical area.

6.1.6.6 Cable & Wireless Network Management Centre

The C&W Network Management Centre is a 24-hour manned facility based at Bracknell. In the event of the unavailability of the Bracknell site the C&W NMC shall relocated to the Watford disaster recovery site.

6.1.6.7 Cable &Wireless core/switched network Capacity

The C&W network (including interconnects) is continuously being expanded to meet forecast traffic levels, in addition to which the C&W core switched network and interconnect links with BT are monitored on a continuous basis to ensure that the routes are sufficiently sized to cope with the actual traffic levels. Where it is forecast that congestion is likely to occur then additional capacity will be provisioned, if this is not already included in the general network expansion.

The C&W network has already been configured such that all RMGA calls have two routes (primary and secondary) between C&W switches, hence if one route is temporarily congested the call will automatically route via the second choice.

FUJ00080037

6.1.6.8 Capacity into Data Centres

The capacity of the access network to the data-centres at Bootle and Wigan has been designed to ensure that each data-centre is capable of fully supporting the predicted maximum network traffic.

6.1.6.9 Transaction Network Services UK LTD Service Structure.

The network links provided by Transaction Network Services are currently limited to one X25 link from Bootle and Wigan Data-centres to Streamline for the DCS online debit card transactions. Contact details for TNS are detailed in section 13.

6.2 Operational Support Services

6.2.1 The System Management Centre

In the event of a major incident or disaster at STE04 the SMC have access to the SMC disaster recovery room in the Fujitsu Services BRA01 building. The SMC have warm standby Tivoli equipment stored on site and network access to the Horizon estate.

6.2.2 The Systems Operate Service

6.2.2.1 Environment Monitoring Facilities

Trident House Operations staff continually monitor the environmental facilities against the threat from fire or flood.
Examples would be:

• Loss of mains power	UPS and Generator take on load
• Loss of UPS	Generator takes on load
• Loss of generator	UPS takes load although only short life approx 20- 30 minutes
• Loss of Air Con	Standby unit kicks in
• Flood warnings	Water Detection systems will give early warning

Early detection is the key to the preparedness, the building disaster detection facilities are regular tested and appropriately maintenance in accordance with contractual agreements. In the event a problem is detected, which may affect the live service kit, the appropriate support group responsible for implementation of fault resolution or instigation of disaster recovery will be immediately contacted. FSCS has a comprehensive maintenance and call out contract, covering all environmental kit. All contractors are on a 4 hours response to site basis agreement, as detailed in an earlier section, and as resilience is built into the main systems, only minor disruption should occur.

FUJ00080037

6.2.2.2 Activation

Once an event has occurred that will impact the provision of the UNIX and NT Service and/or the Operational Service, then in all instances the 'Activation' procedure will be invoked and a TRIOLE For Service call will be raised with the SMC or HSD.

This section defines what action will be taken in the event of a service break to minimised the impact during the service outage.

6.2.2.3 Loss of Documentation server

The document server is part of the office infrastructure and is located at the Trident House operation-centre. A secondary document server is based in Bridgeview. The contents of the secondary server are automatically updated at 19.00 each evening from the primary server. The secondary documentation server is accessed as part of the Systems Operate Services test 11.

6.2.2.4 Loss of Power

In the event of a power failure the UPS will activate and keep all FS systems up and running whilst the standby generator activates. The backup generator will take effect approximately 30 seconds after the failure. The lighting and air conditioning will have no power [due to being non-UPS supported] for the 30 seconds it will take for the generator to come in, emergency lighting will immediately be activated as the mains is lost.

6.2.2.5 Loss of Telephone exchange

In the event of the loss of 'land-line' telephone networks at either Trident House or Bridgeview operation-centres mobile phones would be used as a backup contingency measure. All Belfast based SOS staff are provided with company mobile phones. The Services Manager would liaise with the Horizon Help Desk to ensure a full awareness of the situation.

6.2.2.6 Loss of Trident House

In the event of a disaster that left Trident House inaccessible, Support Service fail-over would be instigated in accordance with the FSCS Support Contingency site fail-over procedure. Actions to restore all the required support functions will be managed through incident management procedures as detailed in this document.

6.2.3 RMGA Customer Services

6.2.3.1 RMGA CS Preventative Measures Overview

Fujitsu Services RMGA has developed plans to provide CS operational and support services from LEW02 in the event of a disaster or unexpected incident at

FUJ00080037

Fujitsu Services (RMGA) Bracknell. REF11 details the disaster recovery equipment for CS operational use at LEW02. This equipment consists of a mixture of hot and warm 'standby' equipment. The hot standby servers and workstations are connected to the live infrastructure and maintained, by the FSCS SOS at a fully operational state. The warm standby workstations are stored in a 'ready-for-use-state'.

The provision of operational documentation for all aspects of service delivery is mandated and allows RMGA to ensure that the service is delivered in a consistent way that satisfies not only service level requirements but also the quality model.

Internal business walkthroughs are conducted on an annual basis to assess the preparedness of any new service element for implementation.

6.2.3.2 RMGA CS Incident Management

In the event of an incident occurring at Bracknell the Fujitsu Services (RMGA) Incident Controller for Bracknell will be informed, See REF12. The Incident Controller referring to the Incident Management Plan will inform all CS Business Recovery Team Leaders of the event, instigate the raising of a TRIOLE For Service call to escalate the incident and, if necessary, contact the Fujitsu Services (RMGA) Crisis Management Team.

The Incident Controller will decide which CS teams and individuals are to be relocated to Fujitsu Services LEW02, other Fujitsu Services sites, or are to work form home. The Incident Management Team members will instruct the Business Recovery Team managers of the invocation of relocation and the Business Recovery Team managers shall decide which team members will be relocated.

The call will meet the HSD escalation criteria, so it will be escalated to the Fujitsu Services (RMGA) Duty Manager. The Duty Manager will use the processes described in REF4.

If the criteria for a major Business Continuity Event are satisfied (REF5) the Duty Manager will escalate the incident to the Fujitsu Services (RMGA) Business Continuity Manager as a Business Continuity event.

6.2.3.2.1 Peak - Support Incident Management

The Peak Support Incident Management service is provided by the SSC.

The primary Peak server is installed in BRA01 and the secondary Peak server resides in LEW02. The database on this sever is synchronised on an hourly basis over the Fujitsu Services corporate network. In addition daily back-ups are also taken of the Peak servers.

The Peak Client is installed on the Office PCs in both BRA01 and LEW02.

FUJ00080037

6.2.4 RMGA Programme and Development Operational Support

6.2.4.1 RMGA Programme Support Services

RMGA Programme team primarily provide the following three essential services which are required for the support of the Horizon infrastructure.

- Change Control;
- Third and fourth line support incident management;
- Authentication of software releases to the live estate.

6.2.4.1.1 Change Control

A RMGA Programmes secondary PVCS server resides in LEW02.

The databases on this severs is synchronised on an hourly basis with the BRA01 PVCS server via the Fujitsu Services corporate network. In addition daily back-ups are also taken of the PVCS servers.

To access PVCS users require either 'PVCS Terminal' or PVCS Dimensions PC Client which is installed on the Office PCs in both BRA01 and LEW02.

6.2.4.2 Configuration Management – Signing Server.

The RMGA Programmes secondary Configuration Management Signing server resides in LEW02. The database on this sever is synchronised on an hourly basis with the BRA01 Signing server via the Fujitsu Services corporate network In addition daily back-ups are also taken of the Signing servers.

In the event of a disaster at BRA01 the Programme team can access the CM Signing server at LEW02 using disaster recovery laptops at least one of which is held off site.

6.2.4.3 Development Operational Support

6.2.4.3.1 Live System Team

The Live System Test (LST) team, who reside within the RMGA Development organisation, test software changes about to be released into the live estate. This is achieved by proving the software changes on discrete test configurations that replicate the live software environment.

The prerequisites to provide this service are:

Availability of hardware test rigs upon which the live software set can be loaded and run;

FUJ00080037

Access to Fujitsu Services (RMGA) infrastructure services i.e. Peak, TRIOLE For Service, PVCS. Disaster Recovery facilities are available at BRA01 for the LST service.

FUJ00080037

7.0 Preparedness Measures

Preparedness in the Horizon context is defined as, those measures taken to ensure the technical solution and business processes supporting that solution deliver the service that they are designed to deliver, in such a way as to meet and exceed the service level.

7.1 Testing

From a technical standing, functionality is proven by testing the solution at a unit, system and business integration level.
This functional testing has been complemented by performance and security testing to ensure that the solution is both scaleable and secure.

Internal business walkthroughs are conducted on a regular basis to assess the preparedness of any new service element for implementation.

In preparation for any Horizon Release, in conjunction with Post Office Limited, a full end to end processing rehearsal and test is performed where the whole solution and supporting processes are run as if live for a period of several days.

It is usual for this to include a rebuild of all operational platforms used in the delivery of the service which further validates the accuracy of operational procedures and configuration management processes.

7.2 Service Management & Delivery

From a business perspective, this process starts by establishing very exacting and specific service level agreements with all suppliers to the Horizon Service which are constantly monitored and reviewed.

The provision of Operational documentation for all aspects of service delivery is mandated and allows RMGA to ensure that the service is being delivered in a consistent way that satisfies service level requirements.

7.3 Risk Analysis

Section 11 contains an extensive risk analysis of the end to end supporting services incorporated in this plan.

This identifies potential risks to those supporting services, the assessed probability of that risk occurring, the impact of that risk becoming a reality and the contingency activity or plans necessary to contain such an occurrence with minimum impact to those supporting services.

FUJ00080037

8.0 Contingency Measures

Contingency measures are 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.

8.1 Recognition

The Horizon solution includes a Systems management capability to monitor and report on events that occur upon all the platforms involved in the service delivery and counters.

The process of monitoring and managing the Network components and Routers is performed by a combination of the products ***HP OpenView and CISCO works***.

BMC patrol is used to manage the Unix systems and the applications, which run upon them.

Maestro provides scheduling facilities for the Host and Agent processes.

Tivoli is used to manage and monitor the Sun Solaris Servers and Windows NT platforms directly, and takes event information from BMC Patrol and HP Open View, to provide a comprehensive management view of the entire solution at any time.

Events that may lead to a break in the APS service will be recognised either by operational observation at a console running one or more of the systems management products, by a pager call from BMC Patrol.

Through the escalation processes the RMGA Duty Manager and Business Continuity Managers will be informed of a disaster or major event at Fujitsu Services operational sites.

8.2 Activation

Once an event has occurred that will impact the provision of the NBS Service, then in all instances a call will be raised with the HSD.

There are a number of scenarios where the capability of the Systems Management environment will trigger an operational script to run upon the platform/application that have suffered the problem, to correct the failure. Operations personnel may override this.

FUJ00080037

8.3 Incident Management

Personnel at the HSD will carry this out. If the incident cannot be resolved by the HSD at the time of the call it will be routed to the appropriate support unit for resolution. At the same time if the incident meets the HSD escalation criteria, it will be escalated to the Fujitsu Services RMGA Duty Manager.

If the criteria for Cross-Domain Business Continuity Management are satisfied the Duty Manager will escalate the problem to the RMGA Business Continuity Manager who will own the problem as a Business Continuity event.

Note: Post Office Limited may also escalate Business Continuity events directly to the RMGA Duty Manager.

8.4 Initiation of Recovery Procedures

Where this is a RMGA only incident, this would usually be instigated by the support team charged with supporting the equipment upon which the failure has occurred, as soon as possible, and certainly with intent to resolve the incident within the relevant Service Level Agreement.

Depending on the severity of the incident, there may be some dialogue between the Duty Manager and the support function to agree on the most appropriate course of action.

Wherever there is a Cross Domain incident, the resolution would be instigated at the time when all parties affected had agreed the course of action:

In the case of a Business Continuity incident, this would be after the Business Continuity Team had agreed a plan of action, see Section 11, Plan Activation.

FUJ00080037

9.0 Recovery Of Normal Service

All aspects of the Services infrastructure within RMGA are managed operationally by the Core Services division of Fujitsu Services (FSCS).

As such, the process of recovering from an event causing an impact to the service will by definition involve FSCS in performing an operational activity to resume the full service.

FSCS have developed an Operations Procedures Manual Index (REF7) from which operational and recovery processes and procedures are identified, for all possible failures in the end to end Horizon Services.

Thus in its simplest form, normal service could be resumed by the Duty or Problem manager liaising with the support team, agreeing when the recovery action should be run, and then carrying that activity out.

Where the recovery action is dependent upon a third party, e.g. Prism or Post Office Limited, the support dialogue would take place between the support teams, and the problem management dialogue would take place between the appropriate management.

FUJ00080037

10.0 Impact & Risk Assessment

10.1 Risks Identified Against the Horizon Services

The matrix below detail the identified risks to the data processing elements of the Horizon Services.

The nature of the service changes between the day and night schedules. However to improve the usability of this plan the worst case Critical Impact Timing for each service element incident has been used.

Day time processes are primarily concerned with Counter transactions and Help Desk processes, Night time processes are primarily concerned with preparing for the next counter day, and processing the transactions that have been processed during the Post Office Core day. This is reflected in the actions against the identified risks.

As a matter of normal operational practice, a call would be placed against HSD if any of the identified risks materialised.

The intention is that the list identified can act as a guide to personnel assessing and managing any incident affecting the Horizon service.

The matrix contain a column identified as probability with a range of 0 to 4. These estimate the probable risk of failure. It must be emphasised that these are not percentages and should be considered simple weighting factors.

As a guideline the following occurrence ratings have been allocated:

Rating	
0	Less than one incident is predicted per year
1	One incident is predicted per year
2	Two incidents are predicted per year
3	Approximately three incidents are predicted per year
4	Ensure that appropriate contingency measures are taken e.g. duplicate routing or the holding of spares on site.

The probability of failure of major elements of the service is low because:

1, There has been a high level of resilience and duplication built into the infrastructure.

2, Extensive validation has been performed upon the infrastructure.

3, The Fujitsu Services RMGA project team has developed a vast knowledge of component failure and service availability over the past three years.

Where a Potential MBCI or MBCI has been designated as being triggered and there is no reference to section 11.3 then there are no further contingency actions to be performed over and above normal operational incident processes and the actions already identified within the risk table.

If a failure occurs during or after any hardware or software change, then consider regressing the change.

FUJ00080037

Please Note: This business continuity plan is one of three. If the RMGA Duty Manager (or other authorised person) is unable to find the failed infrastructure components in the plan they are mandated to refer to CS/PLA/079 The Horizon Services Business Continuity Plan and CS/PLA/015 The Horizon Service Desk Business Continuity Plan.

The risk assessment identifies the Critical Time Factors for activation of contingency measures as defined in the Business Continuity Framework REF1. For on-line service, e.g. NBX 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 'Impact' column contains the statement General Horizon Services. This impact from a Support Service Perspective refers to a potential impact to primary services, e.g. APS, TPS, as well as software drops, Reference Data releases, counter management etc.

FUJ00080037

.

10.2 Risks Identified Against

Notes: 1) The following trigger table details the non-availability of the Primary component, and the Primary and Standby components. The non-availability of support services Standby servers, e.g. OCMS, ACS, etc, or network components should be treated as a loss of resilience and resolved via normal incident management processes.

2) **Branch Network Resilience** - No entries have been included in this table for the loss of ADSL and the ISDN/GSM service for outlets where BNR has been implemented. If there is a loss of online services for Branches that have lost their primary connection through ASDL and secondary through ISDN/GSM please treat the failure as an MBCI Trigger and the RMGA BCM is to inform the POL BCT.

3) No entries have been included in this table for the POLFS Development or QATest infrastructure as there are no contingency or DR requirements for these services. Refer to CS/OLA/049 for details of the OLA for these services.

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
A) Key Management Service, WAN and Workstations						
1	KMA Office Workstations	Failure of the primary Certification Authority Workstation (BRA01)	1	8 hrs	**No Impact**	Resolve via Incident Management Use the secondary Certification Authority Workstation at LEW02.
2	KMA Office Workstations	Failure of both Certification Authority Workstations (BRA01 & LEW02)	0	2 hrs	Public Key Certificates cannot be produced. This will become critical after 2 days.	Resolve via Incident Management

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
3	KMA Office Workstations	Failure of the primary KMA Workstation (BRA01)	1	8 hrs	**No Impact**	Resolve via Incident Management Use the secondary KMA Workstation at LEW02.
4	KMA Office Workstations	Failure of all KMA Workstations (BRA01 & LEW02)	0	2 hrs	The Key Management Application, running on the KMA server, cannot be administered. **This will become critical after 1 day.**	Resolve via Incident Management **Potential MBCI** **Inform POL BCT**
5	KMA Office Workstations	Failure of the primary KMS Admin Workstation (BRA01)	1	8 hrs	**No Impact**	Resolve via Incident Management Use the secondary KMS Admin Workstation at LEW02.
6	KMA Office Workstations	Failure of both KMS Admin Workstations (BRA01 & LEW02)	0	2 hrs	The Key Management Application, running on the KMA server, cannot be administered. This will become critical after 7 days.	Resolve via Incident Management In an emergency consider the SSC workstations at BRA01.
7	KMA Office Workstation	Failure of an IP Select Wide Area Network (CE or PE).Routers	1	4 hrs	**No Impact**	Resolve via Incident Management

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
8	KMA Office Workstations	Failure of both IP Select (either CE or PE) Wide Area Network Routers at BRA01.	0	2 hrs	**No Impact**	Resolve via Incident Management Consider invoking KMS Security Management functions via the 2Mbit BRA-01 to LEW02 to the Data-centres links.
9	KMA Office Workstation	Failure of BRA01 and LEW02 IP Select (either CE and/or PE) Wide Area Network Routers.	0	1 hr	The Key Management Application, running on the KMA server, cannot be administered. **This will become critical after 1 day.**	Resolve via Incident Management Consider using the SOS KMA workstation in Belfast

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
10	Managed Key Service	Failure of Offline Key Generation Workstation (BRA01)	1	1 day	The Key Generation Workstation is only required every 2 years. The Key Manager will ensure there is adequate time to rebuild the workstation before it is required.	Resolve via Incident Management
11	SSC Support KMS Workstations	Failure of KMS Admin Workstation (BRA01) (For BRA01 IP Select WAN refer above.)	1	4 hrs	**No Impact**	Resolve via Incident Management Provide SSC support function from the Security Managers Workstation at BRA01 or alternatively LEW02 if required.
12	Primary & Secondary Campus – Network Infrastructure	Failure of primary IP Select (CE or PE) Wide Area Network Router at Bootle	1	4 hrs	**No Impact**	Resolve via Incident Management
13	Primary & Secondary Campus – Network Infrastructure	Failure of both IP Select (either CE or PE) Wide Area Network Routers at Bootle	0	2 hrs	**No Impact**	Resolve via Incident Management Route KMS LAN traffic to the data-centre via the secondary campus. **Potential MBCI** **Inform POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
14	Primary & Secondary Campus – KMS LAN	Primary Firewall Failure	1	4 hrs	**No Impact**	Resolve via Incident Management Use the secondary KMA Firewall
15	Primary & Secondary Campus – KMS LAN	Primary and secondary Firewall Failures	0	2 hrs	**No Impact**	Resolve via Incident Management Route KMS LAN traffic to the data-centre via the secondary campus. **Potential MBCI** **Inform POL BCT**
16	Primary & Secondary Campus	Failure of primary KMA LAN	1	4 hrs	**No Impact**	Resolve via Incident Management Use the secondary KMA LAN

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
17	Primary & Secondary Campus	Failure of both KMA LANs	0	2 hrs	There will be an impact on FMS Engineers replacing gateways at outlets. **Minimal Impact**	Resolve via Incident Management Use the secondary KMA server at the alternative data-centre **Potential MBCI Inform POL BCT**
18	Bootle Campus	Failure of KMS Admin Workstation	1	8 hrs	**No Impact**	Resolve via Incident Management Use an alternative Admin Workstation in Belfast, BRA01 or LEW02
19	Primary & Secondary Campus	Failure of the Primary KMA server	1	8 hrs	Manual fail-over is required to the backup KMA server Only affects outlets requiring new or replacement counters. **Minimal Impact**	Resolve via Incident Management Use the alternative KMA server at the alternative data-centre **Potential MBCI Inform POL BCT**
20	Primary & Secondary Campus	Failure of both KMA servers	0	2 hrs	Public Key Certificates cannot be produced for delivery to outlets. This will become critical after 2 days. There will be an impact on FMS Engineers replacing gateways at outlets. **Minimal Impact**	Resolve via Incident Management **MBCI Trigger Go To 10 4.1 Inform POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
B) Auto Configuration Service, WAN and Workstations						
21	Auto-configuration Database Server	Disk Fail	1	24hrs	**No Impact**	Resolve via Incident Management The system will automatically recover using the RAID-5 disk array. An alert will be raised to inform operations of failed disk.
22	Auto-configuration Database Server	Processor Failure	1	24 hrs	**No Impact**	Resolve via Incident Management System will automatically reboot using the Compaq recovery option. An alert will be raised to inform operations of failed processor.
23	Auto-configuration Database Server	LAN Card	1	24hrs	**Minimal Impact**	Resolve via Incident Management Alert raised via HPOpenview For single LAN network card failures an automatic switch will be activated to the secondary network card.
24	Auto-configuration Database Server	Total Service Failure at the primary Campus.	0	24hrs	**Minimal Impact**	Resolve via Incident Management Switch to the alternative Auto-Configuration Server at the secondary campus.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
25	Auto-configuration Database Server	Total Service Failure at both the primary and secondary Campus	0	4hrs	There will be delays to the implementation of outlet changes and the replacement of base units. **Impact: POL, RMGA, FSCS**	Resolve via Incident Management **Potential MBCI Inform: POL BCT**
26	Auto-configuration Database	Database	1	24hrs	**Minimal Impact**	Resolve via Incident Management Daily back ups of all changes are taken, logs can be replayed to find at what point a failure occurred. If required switch to alternative Auto-Configuration Server at the secondary campus.
27	Auto-configuration Signing Server	Disk Fail	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Signing Sever fails the Auto-Configuration Server automatically tries the transfer to the alternative Signing Server

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
28	Auto-configuration Signing Server	Processor failure	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Signing Sever fails the Auto-Configuration Server automatically tries the transfer to the alternative Signing Server
29	Auto-configuration Signing Server	LAN Card	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Signing Sever fails the Auto-Configuration Server automatically tries the transfer to the alternative Signing Server
30	Auto-configuration Signing Server	Memory	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Signing Sever fails the Auto-Configuration Server automatically tries the transfer to the alternative Signing Servers
31	Auto-configuration Signing Server	Signing Server service not running	1	24hrs	**Minimal Impact**	Resolve via Incident Management Attempt to restart the failed service, if this fails introduce the secondary Signing server
No.	**Service Element**	**Risk**	**Proba-**	**Critical**	**Impact**	**Action**

			bility	Time Factor		
32	Auto-configuration Signing Servers	Loss of both Signing Servers	0	4 hrs	There will be delays to the implementation of outlet changes and the replacement of base units. **Impact: POL, RMGA, FSCS**	Resolve via Incident Management **Potential MBCI Inform: POL BCT**
33	Boot Server/Loader	Disk Fail	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Boot Server/Loader fails Tivoli automatically tries the transfer to the alternative Boot Server/Loader Tivoli completes transfer when space on the Boot Server/Loader is available.
34	Boot Server/Loader	Processor failure	1	24 hrs	**No impact**	Resolve via Incident Management If the transfer to one Boot Server/Loader fails Tivoli automatically tries the transfer to the alternative Boot Server/Loader.
35	Boot Server/Loader	LAN Card	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Boot Server/Loader fails Tivoli automatically tries the transfer to

FUJ00080037

						the alternative Boot Server/Loader
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
36	Boot Server/Loader	Memory	1	24hrs	**No impact**	Resolve via Incident Management If the transfer to one Boot Server/Loader fails Tivoli automatically tries the transfer to the alternative Boot Server/Loader
37	Boot Server/Loaders	Loss of both Boot Server/Loaders	0	24 hrs	There will be delays to the implementation of outlet changes and the replacement of base units. **Impact: POL, RMGA, FSCS**	Resolve via Incident Management **Potential MBCI** **Inform: POL BCT**
38	Boot Server/Loader	Network Connection –via the IP Select Network (PSTN number).	3	24 hrs	There will be potential delays to the implementation of outlet changes and the replacement of base units. **Minimal Impact**	Resolve via Incident Management Ensure C&W switch the network connection to the alternative Boot Server/Loader
C) Outlet Change Management Service, WAN and Workstations						

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
39	OCMS Client	Primary OCMS Workstation (CRE02)	2	10 days	**No Impact**	Resolve via Incident Management Use secondary workstation
40	OCMS Client	Primary and Secondary OCMS Workstations (CRE02)	0	10 days	**No Impact**	Resolve via Incident Management Use OCMS workstations at the alternative Fujitsu Services site, i.e. Wigan or BRA01.
41	Fujitsu Services (CRE02) to Data-centre Network	The ISDN Link failure	0	10 days	**No Impact**	Resolve via Incident Management Use OCMS workstation at the alternative Fujitsu Services site.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
42	OCMS Primary Service	Loss of the primary OCMS server, database or service.	1	24hrs	Potential delays in receiving data from OCMS Potential loss of relocated outlets **Minimal Impact**	Resolve via Incident Management Use the alternative OCMS Service at the Secondary Campus
43	OCMS Primary Service	Loss of the primary and secondary OCMS servers databases or services.	0	24hrs	Delays in receiving data from OCMS Potential loss of relocated outlets **Impact: FSCS, RMGA**	Resolve via Incident Management **Potential MBCI** **Inform: POL BCT**
D) Database Servers for MIS						
44	Database Servers	Primary Database Server	1	4 hrs	Potential delay in producing	Resolve via Incident

FUJ00080037

					reports and trend analysis. **Impact: FSCS, RMGA**	Management. Invoke manual fail-over to the secondary Database server at the alternative campus.
45	Database Servers	Primary and secondary Database Servers	0	Immediate	Non-availability of the Data warehouse or Data Reconciliation Service Databases Delays in producing reports and analysing trends. **Impact: FSCS, RMGA**	Resolve via Incident Management **Potential MBCI** **Inform: POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
46	Database Server & POLFS storage	StorageTek L180 Double Drive failure	3	4hrs	Reduced ability to generate security copies of data. **Impact: FSCS, RMGA**	Resolve via Incident Management Manual intervention of schedule to allow backup to complete using remaining units
47	Database Servers & POLFS storage	StorageTek L180 Library failure either data-centre	1		Unable to perform cold back ups until the unit is repaired. The schedule would be stopped awaiting repair. **Impact: FSCS, RMGA**	Resolve via Incident Management Manual intervention of schedule to allow backup to complete using remaining units
48	Database Servers & POLFS storage	Single MDS9120 switch failure, either data-centre	0	4hrs	Cross campus data synchronisation will be maintained via the alternate MDS9120 switch in that Data-centre	Resolve via Incident Management
49	Database Servers & POLFS storage	Failure of both MDS9120 switches within one Data-centre	0	immediate	Unable to synchronise the EMC disc arrays across campuses **Impact: FSCS, RMGA**	Resolve via Incident Management **MBCI Trigger Inform: POL BCT**
50	Database Servers & POLFS storage	C&W or BT–single 1 Gbit Fibre Channel supporting the EMC SRDF link failure	1	4hrs	Cross campus data synchronisation will be maintained via the alternate 1 Gbit Fibre Channel	Resolve via Incident Management
51	Database Servers & POLFS storage Campus - Network	C&W and BT– Both 1 Gbit Fibre Channel supporting the EMC SRDF link failure	0	Immediate	Unable to synchronise the EMC disc arrays across campuses **Impact: FSCS, RMGA**	Resolve via Incident Management **MBCI Trigger Inform: POL BCT**

FUJ00080037

52	Database servers & POLFS storage	EMC Symmetrix Disc Array failure (excluding total array)	3	4hrs	No defined single points of failure within an array. Once any failed unit is repaired then there will be a recovery procedure depending on the job that was being processed at the time of fail. **No Impact**	Resolve via Incident Management
53	Database servers & POLFS storage	Primary EMC Symmetrix Disc Array failure (Total array failure)	1	4hrs	Loss of all Databases etc on the Bootle array. Consider performing a controlled fail-over of Bootle Data-centre services to Wigan.	Resolve via Incident Management **MBCI Trigger Inform: POL BCT**
54	Database servers & POLFS storage	EMC Control Centre failure	0	4hrs	Use the ECC in the alternative Data-centre **No Impact**	Resolve via Incident Management
55	Database Servers & POLFS storage	Application Data corruption	1	5 days	No MIS applications. Requirement to restore / rerun previous transaction data to catch up. Processing will stop. **Impact: FSCS, RMGA POL**	Resolve via Incident Management Consult with FSCS. Investigate corruption and possibly restore database to last database copy and reapply updates.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time**	**Impact**	**Action**

FUJ00080037

				Factor		
56	MIS Client	All MIS Clients at BRA01 for any reason	1	5 days	Potential delays in producing management reports. **Impact: RMGA**	Resolve via Incident Management Use the MIS clients that are available at the other sites (STE04 or LEW02).
57	Data feeds	Loss of one or more data feeds from other services for any reason	3	1 to 5 days	The Data Warehouse will wait for the feed to become available and then continue processing. (See actions) **Impact: FSCS, RMGA**	Resolve via Incident Management Either resolve problem at source system or switch to Secondary system – time of day and day of week will contribute to decision. May be possible to use a dummy feed and run the real feed later.
E) Data-centre Infrastructure						
58	Data-centre LAN infrastructure	Single LAN Failure	1	24hrs	**No Impact**	Resolve via Incident Management Alternative LAN Activated
59	Data-centre LAN infrastructure	Dual LAN Failure	0	24hrs	Unable to provide any supporting services from primary Campus **Impact: FSCS, RMGA**	Resolve via Incident Management Switch services to the secondary campus. **Horizon Services MBCI Inform: POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
60	Primary Database Server	Database Server hardware, software or Maestro failures	1	4 hrs	General Horizon Services **Minimal Impact**	Resolve via incident Management. Fail-over to the Host at the Secondary Campus **Horizon Services Potential MBCI** **Inform: POL BCT**
61	Primary & Secondary Database Servers	Database Server hardware, software or Maestro failures	0	Immediate	General Horizon Services **Minimal Impact**	Resolve via incident Management. **Horizon Services MBCI Trigger** **Inform: POL BCT**
62	Primary Campus - Network	GSN Platform Failure	1	2 hrs	General Horizon Services **Minimal Impact**	Resolve via Incident Management.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
63	Primary & Secondary Campus - Network	C&W or BT– 1Gb single link failure	1	2 hrs	General Horizon Services	Resolve via Incident Management. Use the secondary 1Gb link **Horizon Services Potential MBCI** **Inform: POL BCT**
64	Primary & Secondary Campus - Network	C&W and BT– Both 1Gb link failure	0	Immediate	General Horizon Services	Resolve via Incident Management. **Horizon Services MBCI Trigger** **Inform: POL BCT**
F) Data-centre – Generic Agents and Correspondence Servers						
65	Primary & Secondary Campus – Agent layer	Single Agent Failure at either campus (H/W, O/S or application)	2	N/A	**No Impact**	Resolve via Incident Management.
66	Primary & Secondary Campus – Agent layer	Total Agent Failure at one campus (H/W, O/S or application)	1	2hrs	General Horizon Services	Resolve via Incident Management.
67	Primary & Secondary Campus – Agent layer	Total Agent Failure at one campus and the loss of one Agent at the secondary campus (H/W, O/S or application)	0	1hr	General Horizon Services **Minimal Impact**	Resolve via Incident Management. **Horizon Services Potential MBCI** **Inform: POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
68	Primary & Secondary Campus – Agent layer	Total Agent Failure at one campus and the loss of more than one Agent at the secondary campus (H/W, O/S or application)	0	Immediate	General Horizon Services **Impact: POL, RMGA, FSCS**	Resolve via Incident Management. **Horizon Services MBCI Trigger** **Inform: POL BCT**
69	Primary & Secondary Campus – TMS layer	Single Correspondence Serve Failure (H/W, O/S or application)	1	N/A	**No Impact**	Resolve via Incident Management. Switch to secondary correspondence server.
70.	Primary & Secondary Campus – TMS layer	Dual correspondence server failure, any cluster at either campus (H/W, O/S or application)	1	2hrs	General Horizon Services **Minimal Impact**	Resolve via Incident Management.
71	Primary & Secondary Campus – TMS layer	Three correspondence server failures in any cluster (H/W, O/S or application)	0	1hr	General Horizon Services **Impact: POL, RMGA, FSCS**	Resolve via Incident Management. **Horizon Services Potential MBCI** **Inform: POL BCT**
72	Primary & Secondary Campus – TMS layer	Four correspondence server failures in any cluster (H/W, O/S or application)	0	1hr	General Horizon Services **Impact: POL, RMGA, FSCS**	Resolve via Incident Management. **Horizon Services MBCI Trigger** **Inform: POL BCT**

FUJ00080037

G) System Management Infrastructure (Tivoli, OMDB)						
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
73	Wigan Data-centre Tivoli primary systems (normally based in Wigan)	Data-centre failure / down	0	Immediate	Loss of all tasks and possible loss of software distribution services. No events being processed. **Impact: SMC, MSS, RMGA**	Resolve via Incident Management. MSS begin Tivoli Site Fail-over. **MBCI Trigger Inform: POL BCT**
74	Bootle Data-centre Tivoli secondary systems (normally based in Bootle)	Data-centre failure / down	0	Immediate	Loss of all tasks and software distribution services to 50% of Outlets. **Impact: SMC, MSS, RMGA**	Resolve via Incident Management. MSS begin Tivoli Gateway Fail-over. **MBCI Trigger Inform: POL BCT**
75	Master TMR server (Wigan)	Hardware / OS / Software Failure or other outage.	1	1 Hr	Loss of Tivoli management capability pending recovery or fail-over. **Impact: SMC, MSS, RMGA**	Resolve via Incident Management. MSS begin Tivoli Server Fail-over. Upon fix restore from backup if necessary.
76	Standby TMR server (Bootle)	Hardware / OS / Software failure or other outage.	1	4 Hrs	Loss of resilience. **Impact: MSS**	Resolve via Incident Management. MSS begin fix / rebuild as required Upon fix restore from backup if necessary.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
77	Primary OMDB Server (Wigan)	Hardware / OS / Software failure or other outage.	2	Immediate	Loss of Tivoli management capability and 'eventing' pending recovery or fail-over. **Impact: SMC, MSS, RMGA**	Resolve via Incident Management. MSS to fail-over to the secondary OMDB Server.
78	Secondary OMDB Server (Bootle)	Hardware / OS / Software Failure or other outage.	2	4 Hrs	Loss of resilience for OMDB server. **Impact: MSS**	Resolve via Incident Management. Upon fix restore from backup if necessary.
79	Gateway Servers (Wigan & Bootle)	Loss of use of any single gateway server	2	Immediate	Some loss of management control for a portion the outlets. **Impact: SMC, MSS, RMGA**	Resolve via Incident Management. Service can be restored by migration of services to an alternate gateway server.
80	Gateway Servers (Wigan & Bootle)	Loss of use of multiple gateway servers	0	Immediate	Significant loss of management control for a portion the outlets. Potential for reduced performance following migration to alternate servers **Impact: SMC, MSS, RMGA, POL**	Resolve via Incident Management. Service can be restored by migration of services to an alternate gateway server.
81	SMDB server (STE04)	Loss of use of the primary for any reason	1	> 4 Hrs	Loss of access to non-polling information **Impact: SMC, RMGA**	Resolve via Incident Management. Switch to backup sever in BRA01
No.	**Service Element**	**Risk**	**Proba-**	**Critical**	**Impact**	**Action**

FUJ00080037

			bility	Time Factor		
82	SMDB server (BRA01)	Loss of use of the secondary for any reason	1	> 24 Hrs	Loss of resilience **Impact: SMC, RMGA**	Resolve via Incident Management.
83	SMDB servers in STE04 and BRA01	Loss of both primary & secondary for any reason	0	>4 Hrs	Loss of access to non-polling information **Impact: SMC, RMGA**	Resolve via Incident Management. Revert to using the OMDB server to collect the required information
84	SMC Web server	Loss of primary server in STE04	1	> 4 Hrs	Various information including SMC KELs would not be available **Impact: SMC, RMGA**	Resolve via Incident Management. Switch to secondary server
85	SMC Web server	Loss of secondary server	1	> 48 Hrs	Loss of resilience **Impact: None**	Resolve via Incident Management.
86	Single TEC Server	Hardware, Operating System and Application Failures	1	12 Hrs	16% reduction in capacity pending recovery. **Impact: MSS**	Resolve via Incident Management. Automatic Fallback engaged in event of failure of client TECs.
87	Single Delivery Server	Hardware, Operating System and Application Failures	2	4 Hrs	Some loss in capacity. **Impact: MSS**	Resolve via Incident Management. Resilience across data-centres in event of failure. Diagnose fault. Rebuild failed server.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
88	Data-centre to SMC RMGA Network	Any loss of single connection	1	24 Hrs	Possible slowing of access from SMC. **Impact: SMC**	Resolve via Incident Management. Networks to diagnose and resolve. Dual connection to systems through Wigan or Bootle.
89	Data-centre to SMC RMGA Network	Any loss of both connections	0	Immediate	No system management capability, no view of the live services **Impact: SMC, RMGA, POL**	Resolve via Incident Management If total loss and not resolved within 2 hours may need to initiate contingency plan / site relocation. **Potential MBCI Inform: POL BCT**
90	Data-centre to Wigan (MSS) RMGA Network	Any loss of connection	1	8 Hrs	Minimal impact dual connection to systems through Wigan or Bootle. **Impact: MSS, RMGA, POL**	Resolve via Incident Management. Networks to diagnose and resolve If total loss and not resolved within 8 hours may need to initiate contingency plan **Potential MBCI Inform: POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
91	Single Tivoli Desktop SMC	Hardware, software, operating system, application.	2	N/A	Nominal as alternative desktops available as staff work shifts. **Impact: None**	Resolve via Incident Management. Affected personnel use spare Tivoli desks. Hardware call raised as appropriate. Rebuild completed as necessary.
92	Single Tivoli Desktop Wigan (MSS)	Hardware, software, operating system, application.	1	24Hrs	Nominal as alternative desktops available as staff work shifts. **Impact: None**	Resolve via Incident Management. Affected personnel use spare Tivoli desks. Hardware call raised as appropriate. Rebuild completed as necessary.
H) Data-centre LAN Infrastructure (to Outlets)						
93	Primary & Secondary Campus – Network Infrastructure	Single Core Router Failure	1	N/A	**No Impact**	Resolve via Incident Management.
94	Primary & Secondary Campus – Network Infrastructure	Multiple Core Router Failure	0	2 hrs	General Horizon Services	Resolve via Incident Management.
95	Primary & Secondary Campus – Network Infrastructure	Total Core Router Failure	0	Immediate	General Horizon Services **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI Inform: POL BCT**
96	Primary & Secondary Campus – Network Infrastructure	VPN Policy Management Server Failure	1	10 Days	**No Impact**	Resolve via Incident Management.
No.	**Service Element**	**Risk**	**Proba-**	**Critical**	**Impact**	**Action**

FUJ00080037

			bility	Time Factor		
97	Primary & Secondary Campus – Network Infrastructure	Single inbound VPN Server failure	1	4 hrs	**No Impact**	Resolve via Incident Management.
98	Primary & Secondary Campus – Network Infrastructure	Dual inbound VPN Server failure	0	Immediate	Counter management via Tivoli TMR processes affected. General Horizon Services **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services Potential MBCI** **Inform: POL BCT**
99	Primary & Secondary Campus – Network Infrastructure	VPN Loopback Workstation	1	N/A	**No Impact**	Resolve via Incident Management.
100	Primary & Secondary Campus – Network Infrastructure	VPN Exception Server	1	4 hrs	**No Impact**	Resolve via Incident Management.
101	Primary & Secondary Campus – Network Infrastructure	VPN Exception Servers (i.e. in both Data-centres)	0	Immediate	General Horizon Services **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI** **Inform: POL BCT**
102	Primary & Secondary Campus – Network Infrastructure	Single Agg Router Failure	2	N/A	**No Impact**	Resolve via Incident Management.
103	Primary & Secondary Campus – Network Infrastructure	Multiple Agg Router Failure	1	2 hrs	General Horizon Services **Minimal Impact**	Resolve via Incident Management.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
104	Primary & Secondary Campus – Network Infrastructure	Total Agg Router Failure	0	1 hr	General Horizon Services **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI Inform: POL BCT**
105	Primary & Secondary Campus – Network Infrastructure	Single Core Router Failure	2	N/A	General Horizon Services (Impact on one Correspondence server/cluster) **Minimal Impact**	Resolve via Incident Management. Ensure SSC are consulted on replication backlog before reintroducing the router.
106	Primary & Secondary Campus – Network Infrastructure	Dual Core Router Failure	1	2 hrs	General Horizon Services (Impact on two Correspondence servers/cluster) **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Ensure SSC are consulted on replication backlog before reintroducing the routers. **Horizon Services MBCI Trigger Inform: POL BCT**
107	Primary & Secondary Campus – Network Infrastructure	The Summary Router Failure	0	1 hr	**No Impact.**	Resolve via Incident Management. Connection will continue via the Summary router in the alternative Data-centre.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
108.	Primary & Secondary Campus – Network Infrastructure	Single LNS Router Failure	1	N/A	**No Impact.**	Resolve via Incident Management. Connection will continue via the secondary LNS router in that Data-centre.
109.	Primary & Secondary Campus – Network Infrastructure	Multiple LNS Router Failure	0	2hrs	General Horizon Services **Minimal Impact**	Resolve via Incident Management. Connection will continue via an alternative LNS router in the secondary Data-centre.
110.	Primary & Secondary Campus – Network Infrastructure	Total LNS Router Failure	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI Trigger** **Inform: POL BCT**
111.	Primary & Secondary Campus – Network Infrastructure	Primary Post Office Access LAN failure	0	2hrs	**No Impact.**	Resolve via Incident Management. Connection will continue via the secondary Access LAN

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
112	Primary & Secondary Campus – Network Infrastructure	Primary and secondary Post Office Access LAN failure	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Reconfigure connections via secondary data-centre. **Horizon Services MBCI Trigger Inform: POL BCT**
113	Primary & Secondary Campus – Network Infrastructure	Primary Metered ISDN/GSM LAN failure	0	2hrs	**No Impact.**	Resolve via Incident Management. Connection will continue via the secondary Metered ISDN/GSM LAN
114	Primary & Secondary Campus – Network Infrastructure	Primary and secondary Metered ISDN/GSM LAN failure (Between LNS and Agg routers)	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Reconfigure connections via secondary data-centre. **Horizon Services MBCI Trigger Inform: POL BCT**
115	Primary & Secondary Campus –Management LAN	Primary Metered ISDN/GSM Management LAN failure	0	2hrs	**No Impact.**	Resolve via Incident Management. Connection will continue via the secondary Metered ISDN/GSM management LAN

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
116	Primary & Secondary Campus –Management LAN	Primary and secondary Metered ISDN/GSM Management LAN failure	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Reconfigure connections via secondary data-centre. **Horizon Services MBCI Trigger Inform: POL BCT**
117	Primary & Secondary Campus- Network Management LAN	Primary Cisco Secure Server	0	2hrs	**No Impact.**	Resolve via Incident Management. Switch to the secondary Cisco Secure Server.
118	Primary & Secondary Campus- Network Management LAN	Primary and secondary Cisco Secure Server	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Reconfigure connections via secondary data-centre. **Horizon Services MBCI Trigger Inform: POL BCT**
119	Primary & Secondary Campus- Network Management LAN	Primary Radius Server	0	2hrs	**No Impact.**	Resolve via Incident Management. Switch to the secondary Radius Server.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
120	Primary & Secondary Campus- Network Management LAN	Primary and Secondary Radius Server	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Reconfigure connections via secondary data-centre. **Horizon Services MBCI Trigger** **Inform: POL BCT**
121	Primary & Secondary Campus- Network Management LAN	Primary Cisco Syslog Server	0	2hrs	**No Impact.**	Resolve via Incident Management. Reconfigure connections to the Syslog server in the secondary data-centre.
I) Network Links to Outlets						
122	Primary & Secondary Campus – Network Infrastructure	IP Select (CE or PE) single Wide Area Network router at Bootle or Wigan	1	N/A	Traffic to outlets will continue via the secondary CE or PE router for that data-centre **No Impact.**	Resolve via Incident Management.
123	Primary & Secondary Campus – Network Infrastructure	IP Select (CE or PE) Dual Wide Area Network routers failure at Bootle or Wigan	0	2hrs	Traffic to outlets will continue via the alternative data-centre General Horizon Services **Minimal Impact**	Resolve via Incident Management.
124	Primary & Secondary Campus – Network Infrastructure	C&W Data Network Service Failure of primary exchange (ADSL IP Data)	1	4 hrs	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Ensure C&W has switched to secondary exchange.

FUJ00080037

						Horizon Services Potential MBCI Inform: POL BCT
125	Primary & Secondary Campus – Network Infrastructure	C&W Data Network Service Failure of primary and secondary exchanges. (ADSL IP Data)	0	Immediate	General Horizon Services via the C&W Data Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI Trigger Inform: POL BCT**
126	Primary & Secondary Campus – Network Infrastructure	Fujitsu Services single POP failure. (ADSL IP Stream)	1	4 hrs	General Horizon Services via the IP Stream Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Ensure Fujitsu Core Services switch to the secondary POP. **Horizon Services Potential MBCI Inform: POL BCT**
127	Primary & Secondary Campus – Network Infrastructure	Fujitsu Services Dual POP failure. (ADSL IP Stream)	0	Immediate	General Horizon Services via the IP Stream Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI Trigger Inform: POL BCT**
128	Primary & Secondary Campus – Network Infrastructure	Single BT Central Network Service failure (ADSL IP Stream)	1	4 hrs	General Horizon Services via the BT IP Stream Network **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. Ensure Outlets have switched to the secondary BT Central Network. **Horizon Services Potential MBCI Inform: POL BCT**
129	Primary & Secondary Campus – Network	Dual BT Central Network Service failure.	0	Immediate	General Horizon Services via the BT IP Stream Network	Resolve via Incident Management.

FUJ00080037

	Infrastructure	(ADSL IP Data)			**Impact: FSCS, RMGA, POL**	**Horizon Services MBCI Trigger Inform: POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
130	Primary & Secondary Campus – Network Infrastructure	Single ISDN Router Failure, i.e., at either Wigan or Bootle.	1	N/A	**No Impact**	Network traffic should be routed via the ISDN router at the alternative Data-centre Resolve via Incident Management.
131	Primary & Secondary Campus – Network Infrastructure	Failure of the ISDN Routers at both Wigan and Bootle	0	Immediate	General Horizon Services (Loss of service to ISDN connected outlets) **Impact: FSCS, RMGA, POL**	Resolve via Incident Management **Horizon Services MBCI Trigger** **Inform: POL BCT**
132	Primary & Secondary Campus – Network Infrastructure	C&W ISDN Service Failure of primary exchange	1	4 hrs	General Horizon Services **Minimal Impact**	Resolve via Incident Management Ensure C&W has switched to secondary exchange. **Horizon Services Potential MBCI** **Inform: POL BCT**
133	Primary & Secondary Campus – Network Infrastructure	C&W ISDN Service Failure of primary and secondary exchanges.	0	Immediate	General Horizon Services **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. **Horizon Services MBCI Trigger Inform: POL BCT**
134	Primary and Secondary Campus – Network Infrastructure	Single FJS Core ISP Satellite LNR router failure	1	4hrs	**No Impact.**	Resolve via Incident Management.
135	Primary and Secondary Campus – Network	Dual FJS Core ISP Satellite LNR router failure	0	Immedia te	All BT VSAT Branches (approximately 60) will lose	This equipment is supplied and managed by FJS Core ISP

FUJ00080037

	Infrastructure				communications with the RMGA Data-centres. **Business Impact: POL**	Resolve via Incident Management **Horizon Services MBCI Trigger** **Inform: POL BCT**
136	Network (To Outlets)	Satellite Service Failure. Loss of BT equipment at Turin.	1	Immediate	Loss of online services for 1 or more BT VSAT Branches **Impact: FSCS, RMGA, POL**	Resolve via Incident Management **Horizon Services MBCI Trigger** **Inform: POL BCT**
137	Network (To Outlets)	ISDN BT Tail Loss of network connection to individual outlets	2	Immediate	General Horizon Services **Minimal Impact**	Resolve via Incident Management **(Refer to Appendix One for Outlet MBCI Triggers)**
J) Post Office Outlets						
138	Post Office Counter	Single Counter Failure (H/W, O/S or application)	3	N/A	General Horizon Services **Minimal Impact**	Resolve via Incident Management.
139	Post Office Counter	Multiple Counter Failure (H/W, O/S or application)	1	4hrs	General Horizon Services **Minimal Impact**	Resolve via Incident Management.
140	Post Office Counter	Total Counter Failure (H/W, O/S or application)	0	Immediate	General Horizon Services	Resolve via Incident Management. **(Refer to Appendix One for Outlet MBCI Triggers)**

FUJ00080037

K) Royal Mail Group Account Customer Service Bracknell						
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
141	Fujitsu Services (RMGA) Bracknell site	Unavailable through fire/flood/bomb/ industrial action/ unspecified disaster	0	Immediate	Unable to provide any Bracknell based services. **Impact: RMGA, POL**	After obtaining confirmation from the BRA01 incident controller that it is a genuine fire or disaster invoke Business Continuity and relocate provision of services to LEW02 **MBCI Trigger Inform POL BCT**
142	Fujitsu Services (RMGA) Bracknell site - building	Mains power unavailable / interrupted	1	36 hrs	**No Impact**	Power supply maintained by UPS and backup generator
143	Fujitsu Services (RMGA) Bracknell - building	UPS non functioning	1	36 hrs	Unscheduled closedown of all systems and equipment. **Minimal Impact.**	Backup Generator powered up. All systems restarted to provide capability
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**

FUJ00080037

144	Fujitsu Services (RMGA) Bracknell - building.	Total power loss including backup generator Unavailable and/or non functioning	0	Immediate	Unable to provide any Bracknell based services. **Business Impact: RMGA POL**	Invoke Business Continuity and relocate provision of Ref. Data service to LEW02 **Potential MBCI Trigger Inform POL BCT**
145	Fujitsu Services (RMGA) Bracknell - building	Air conditioning failure	1	4 hours	Equipment overheating leading to unscheduled closedown. No ability to change Reference Data, software fixes. No ability to progress diagnosis of software problems. **Minimal Impact**	Resolve problem via maintenance contract. Switch off non-essential equipment and instigate the immediate hire of cooling units.
146	Fujitsu Services (RMGA) Bracknell - building	Telephone system unavailable	1	1 hour	No ability to receive incoming calls or faxes. No ability to use dial-up facilities for access to POL email for Reference Data. **Minimal Impact**	Use mobile phones.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**

FUJ00080037

147	Fujitsu Services (RMGA) Bracknell site - network	IP Select (CE or PE) single Wide Area Network router failure	1	8 hours	**No Impact.**	Failure resolved using normal support routes. Alternative network access achieved via LEW02 and/or Bootle route. Possible degradation in response times
148	Fujitsu Services (RMGA) Bracknell site - network	IP Select (CE or PE) Dual Wide Area Network routers failure	2	8 hours	**No Impact.**	Failure resolved using normal support routes. Alternative network access achieved via LEW02.Possible degradation in response times
149	Fujitsu Services (RMGA) Bracknell site - network	Bracknell to LEW02 network router failure	2	8 hours	**No Impact.**	Failure resolved using normal support routes. Alternative network access achieved automatically via Wigan and/or Bootle route. Possible degradation in response times.
150	Fujitsu Services (RMGA) Bracknell site - network	Bracknell to LEW02 network circuit failure C&W IP Select network	2	8 hours	**No Impact.**	Failure resolved using normal support routes. Alternative network access achieved automatically via the remaining C&W IP Select link. Possible degradation in response times.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**

FUJ00080037

151	Fujitsu Services (RMGA) Bracknell site	LST rig components failure	2	24hrs	Unscheduled interruption to testing. **No Impact**	Replacement sourced from spare equipment holding. Rebuild from scratch using build scripts
152	Fujitsu Services (RMGA) Bracknell site	Personal Workstation failures	2	72hrs	Unscheduled interruption to user. **No Impact**	Shared use of alternative.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
153	Fujitsu Services (RMGA) Bracknell site	BIM System corruption	1	24 hrs	Manual recording of incidents. (POL have copies of previous BIM reports which are published on a daily basis) **Minimal Impact**	Restore from backup. Provide paper BIM notes as applicable.
154	Fujitsu Services (RMGA) Bracknell site	Total loss of MIS IT infrastructure	0	24 hrs	Delays in MIS team accessing Data Reconciliation Reports. **Minimal Impact**	Alternative MIS clients and MIS File Server are available at LEW02

FUJ00080037

155	Fujitsu Services (RMGA) Bracknell site	Total loss of LST IT infrastructure	0	24 hrs	**Minimal Impact**	A hot Standby LST rig is available in LEW02
156	Fujitsu Services (RMGA) Bracknell site	Total loss of SSC IT infrastructure	0	Immediate	**Minimal Impact**	SSC may invoke DR using remote working lap tops. Warm standby workstations are also available at LEW02.
157	Fujitsu Services (RMGA) Bracknell site	Total loss of Technical Bridge infrastructure	0	Immediate	**Minimal Impact**	Utilise the facilities of the SMC and SSC to provide Technical Bridge coverage. Also consider DR kit at LEW02.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
158	Fujitsu Services (RMGA) Bracknell site	Failure of the Primary PEAK Incident Management Server	1	8 hrs	**Minimal Impact**	Resolve via Incident Management. Invoke Secondary Peak Server at LEW02

FUJ00080037

159	Fujitsu Services (RMGA) Bracknell site	Total loss of RDT IT infrastructure	0	24 hrs	There is no immediate impact due to the loss of Ref. Data IT Infrastructure. **Impact: RMGA, POL**	Invoke Business Continuity and relocate provision of Ref. Data service from LEW02 Note RDMC Admin Workstation is available in STE04 **Potential MBCI Trigger Inform POL BCT**
160	Fujitsu Services (RMGA) Bracknell site	Failure of one POL E-mail laptop	2	N/A	**Minimal Impact.**	Use one of the other mailboxes.
161	Fujitsu Services (RMGA) Bracknell site	Failure of all laptops or POL e-mail service	1	24 hrs	Inability to receive/transmit requests/authorisations etc to/from POL. **Minimal Impact.**	Revert to fallback facilities, e.g. telephones, floppy disc, fax, etc.
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
162	Fujitsu Services (RMGA) Bracknell site	Failure of RDMS one workstation	1	N/A	**No Impact.**	Use one of the other workstations. A Hot standby RDMS workstation and RDMS catalogue server is available in LEW02.
L) Core Services Operations Supporting Infrastructure						

FUJ00080037

163	FSCS SOS Operations	Failure of primary KMS Admin Workstation (Trident House - Belfast)	1	8 hrs	**No Impact**	Resolve via Incident Management Use the secondary Admin Workstation at Bridgeview (Belfast)
164	FSCS SOS Operations	Failure of primary Wide Area Network Router. (Trident House)	1	4 hrs	**No Impact**	Resolve via Incident Management Use the secondary Wide Area Network Router.
165	FSCS SOS Operations	Failure of both Wide Area Network Routers. (Trident House)	0	2 hrs	**No Impact**	Resolve via Incident Management Use the secondary Admin Workstation at Bridgeview (Belfast).

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
166	FSCS SOS Operations	Failure of both KMS Admin Workstations and/or WAN routers at both Trident House and Bridge view.	0	1 hr	**No Impact**	Resolve via Incident Management If required relocate appropriate SOS Staff to Bootle, BRA01 or LEW02
167	Belfast Trident House to RMGA Network	Single Router Fail	1	4 hrs	**No impact**	Resolve via Incident Management. Use alternative router

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
168	Belfast Trident House to RMGA Network	Dual Router Fail	0	1 hr	Loss of network communications from Trident House, no direct system management possible **Impact: FSCS**	Resolve via Incident Management. Temporary support can be provided by staff based in Wigan or Bootle, or who are working outside Belfast Relocate support staff to Bridgeview **Potential MBCI** **Inform: POL BCT**
169	Access to Belfast Trident House	Total loss of access for any reason	1	1 hr	No direct system management possible **Impact: FSCS**	Resolve via Incident Management. Temporary support can be provided by staff based in Wigan or Bootle, or who are working outside Belfast Relocate support staff to Bridgeview **Potential MBCI** **Inform: POL BCT**
170	Belfast Trident House Phone System	No landline telephones, for any reason	1	Immediate	**No impact**	Resolve via Incident Management. Use mobile phones as required
171	Belfast Trident House Skilled staff	Loss of up to 50% specialised support based in Belfast	0	48 hrs	**Minimal Impact**	Both UNIX and NT staff are cross-trained to cover all support areas.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
172	Belfast Trident House – SOS People (including industrial action)	Loss of all specialised support based in Belfast	0	Immediate	Unable to provide SOS service from Belfast **Impact: POL, RMGA, FSCS**	A level of service can be provided by SOS staff based at the Wigan and Bootle data-centres in conjunction with SSC support **MBCI Trigger** **Inform: POL BCT**
173	Belfast Trident House - various scenarios fire, flood, storm.	Unable to run service/part or all	0	Immediate	No direct system management possible from Trident House - Full service affected. **Minimal Impact**	Temporary support can be provided by staff based in Wigan or Bootle, or who are working outside Belfast Relocate support staff to Bridgeview **Potential MBCI** **Inform: POL BCT**
174	Belfast Trident House - Building	Aircon failure 1 unit	1	4 hrs	Equipment running at higher than normal temperature **Minimal Impact**	Resolve via Incident Management/Fault procedure. Review switching off any non-essential equipment SOS Duty Manager to contact System Support Manager.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
175	Belfast Trident House - Building	Aircon failure 2 or more units	0	2 hrs	Kit overheating, higher potential for failures **Impact: FSCS**	Resolve via Incident Management/Fault procedure. Review switching off any non-essential equipment or relocating support staff to Bridgeview SOS Duty Manager to contact System Support/Operations Manager. **Potential MBCI Inform: POL BCT**
176	Belfast Trident House - Building	Mains Power failure	1	36 hrs	Ensure UPS and generators switch in. **Minimal Impact. FSCS**	Resolve via Incident Management/Fault procedure. SOS Duty Manager to contact System Support/Operations Manager.
177	Belfast Trident House - Building	Generator failure	0	4 hrs	No resilience in power loss scenario. **No impact** (Assuming mains power still available.)	Resolve via Incident Management/Fault procedure. SOS Duty Manager to contact System Support/Operations Manager.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
178	Belfast Trident House - Building	UPS failure not on load	0	4 hrs	No seamless changeover if power loss scenario/systems crash. **No impact** (Assuming mains power still available.)	Resolve via Incident Management/Fault procedure. SOS Duty Manager to contact System Support/Operations Manager.
179	Belfast Trident House RMGA Domain Controller	Loss of the RMGA Domain Controller	1	24 hrs	Potentially unable to provide direct system management. **Minimal Impact**	Resolve via Incident Management/Fault procedure. Revert to either the Bridgeview Backup Domain Controller or Bootle/Wigan Domain Controllers
180	Belfast Trident House - Network	Loss of Trident House LAN	0	1 hr	Loss of network functionality at Trident House. Unable to provide direct system management. **Minimal Impact**	Resolve via Incident Management. Temporary support can be provided by staff based in Wigan or Bootle, or who are working outside Belfast Invoke Systems Operate business continuity procedure and relocate support staff to Bridgeview **Potential MBCI Inform: POL BCT**
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**

181	Belfast Trident House - Network	Loss of Insight Manager Workstation	1	1 hr	**No Impact**	Resolve via Incident Management. Use the resilient Insight Manager Workstation within the Trident House environment.
182	Belfast Trident House - Network	Loss of the Trident House BTI box	1	24 hrs	**No Impact**	Resolve via Incident Management. All pager messages will be raised from the Bootle and Wigan BTI boxes.
183	Belfast Trident House - Network	Trident House to RMGA Single Router Fail	1	4 hrs	**No impact**	Resolve via Incident Management. Use alternative router
No.	**Service Element**	**Risk**	**Proba-bility**	**Critical Time Factor**	**Impact**	**Action**
184	Buildings	Loss of one or more major building.	0	Immediate	The service(s) provided from the building are severely disrupted or terminated **Impact: FSCS, RMGA, POL**	**MBCI Trigger** **Inform: POL BCT**
M) Core Services SMC and MSS						
185	Buildings Wigan (MSS /SMG)	Total loss for any reason	0	> 1 hr	The service(s) provided from the building are severely disrupted or terminated.	Invoke Wigan MSS site contingency plan. Some services can be provided

FUJ00080037

					Impact: SMC, MSS, RMGA	by MSS team members based in STE04. **MBCI Trigger** **Inform: POL BCT**
186	SMC - STE09 buildings	Any total loss of use by SMC	1	> 1hr	The service(s) provided from the building are severely disrupted or terminated **Impact: SMC / RMGA**	Invoke SMC site contingency plan. Some services can be provided by MSS in Wigan. **MBCI Trigger** **Inform: POL BCT**
187	SMC (MSS / SMG) people Wigan	Any total loss	0	> 1 hr	Extremely unlikely since staff work on shifts and from home - 3rd line support and development capability lost **Impact: MSS, SMG, RMGA**	Invoke Wigan MSS contingency plan. Some services can be provided by MSS team members based in STE04. **MBCI Trigger** **Inform: POL BCT**

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
188	People SMC (STE04)	Any total loss	0	> 1hr	Extremely unlikely since staff work on shifts – 2nd line support, system monitoring, software distribution capability lost **Impact: SMC, RMGA**	Invoke SMC contingency Plan. Some services can be provided by MSS in Wigan. **MBCI Trigger** **Inform: POL BCT**
189	People	Loss of staff at one or more locations.	0	Immediate	The service(s) provided by a team are severely disrupted or terminated **Impact: POL**	**MBCI Trigger** **Inform: POL BCT**
N) Cable & Wireless Operations and Network						
190	C&W Data-centres to C&W network	Switch/SNAP/fibre fail	2	5 hrs	Resilience designed into solution. **No impact.**	Resolve via Incident Management. Use alternative routes
191	C&W Post Offices into C&W network	ISDN2 fail/ BT LSE fail	3	2 days	Minimal, Post Offices able to continue working. **Impact: POL**	Resolve via Incident Management. FSCS/C&W CCC fault reporting process.
192	C&W Network congestion issues (ISDN network)	C&W and or BT Network	3	1 day	Slow data transfer. **Impact: FSCS, RMGA**	Resolve via Incident Management. C&W and BT traffic monitoring – traffic re-routes instigated.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
193	C&W Network congestion issues (C&W data network)	C&W IP Select Network	3	4 hrs	Slow data transfer. **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. C&W monitoring – traffic re-routes instigated.
194	C&W Bracknell NMC unavailable e.g. bomb/fire	C&W, Bracknell Network Management Centre	0	1 hr	A NMC disaster recovery site is available at Watford. **Impact: FSCS, RMGA, POL**	Resolve via Incident Management. C&W Disaster recovery processes. **Potential MBCI** **Inform: POL BCT**
195	C&W Evacuation of BT SMC	BT SMC	0	1 hr	**Impact: C&W**	Resolve via Incident Management. BT DR document
196	C&W FSCS change process	New Post Office Provision	2	45 days	C&W require 45 working days notice to provide ISDN service to a new Post Office. **Impact: POL**	Resolve via Incident Management. FSCS change control document.

FUJ00080037

No.	Service Element	Risk	Proba-bility	Critical Time Factor	Impact	Action
197	C&W ISDN2 not available for new Post Office	New Post Office Provision	1	45 days	Minimal, Post Office able to continue working. **Impact: POL**	Resolve via Incident Management. C&W to provide alternative solution, e.g. satellite.
198	C&W National Number Change	RMGA Data-centre routers	1	6 months	Parallel running of old and new numbers. **Impact: RMGA, POL, C&W**	Resolve via Incident Management. RMGA to reprogram data-centre routers for new numbers.

FUJ00080037

10.3 Summary of Contingency Actions

The following are additional contingency actions to be taken for the risks identified in table 10.2.

10.3.1 KMS Service/KMA Servers

If the KMS service is unavailable, e.g. both KMA servers fail there are no additional contingency actions available. This will become critical after 2 days because PMMC recoveries, base unit swap-outs and new installations are not possible at counters.

FUJ00080037

11.0 Post Office Limited failures impacting RMGA Services

11.1 Post Office Limited failures impacting RMGA RDMS Service

The RMGA RDMS is reliant upon Reference Data initially being supplied by POL Chesterfield. Further more, this service is dependent upon the POL Reference Data verification processes at Bracknell. Non availability of either of these POL facilities or services will inhibit the operation of this RMGA Service.

The availability of Post Office outlets to utilise the RDMS to the customer is a further prerequisite of the end to end service provision.

Non availability of one or more post Office outlets restricts the availability of the service and may trigger a Business Continuity event.

11.2 POL and AP Client failures impacting RMGA APS Service

11.2.1 Post Office Limited

The availability of Post Office outlets to provide the Automated Payment Service to the customer is a further prerequisite of the end to end service provision.

Non-availability of one or more post Office outlets restricts the availability of the service and may trigger a Business Continuity event, see Appendix One.

11.2.2 AP Clients

The availability of the Automated Payment Clients to receive the transaction files is a further prerequisite of the end to end service provision.

Non-availability of one or more of the AP Clients restricts the availability of the service and may trigger a Business Continuity event.

The Fujitsu Services RMGA plans and procedures for dealing with this situation can be found in the Client Specific Operational Level agreements (CS/OLA/003 – Generic AP Client OLA from which all specific Client OLA's are derived).

11.3 Post Office Ltd failures impacting RMGA TPS Service

Non-availability of TPS service at POL NDC, or the disaster recovery site at Isleworth, or one or more Post Office outlets restricts the availability of the service and may trigger a Business Continuity event, see Appendix One.

11.4 Post Office Ltd and Supplier failures impacting RMGA NBS Service

The non-availability of one or more of the Financial Institutions or one or more Post Office outlets can restrict the availability of the Network Banking Service and may trigger a Business Continuity event

FUJ00080037

11.5 Post Office Ltd and Supplier failures impacting RMGA DCS Service

The non-availability of the Streamline Debit Card System, or one or more of the Card Issue services, or one or more Post Office outlets can restrict the availability of the Debit Card Service and may trigger a Business Continuity event.

FUJ00080037

12.0 Plan Activation

Once the criteria for Business Continuity have been satisfied, i.e. a MBCI Trigger from the table of risks in section 11, then after a call had been placed and appropriate details logged at HSD, the problem ownership is passed to the Fujitsu Services RMGA member of the Business Continuity Management team.

After compiling all relevant information, and if necessary communicating this to the other members of the BCMT listed below in section 14, a full impact assessment will be conducted to determine if the joint Business Continuity Management Processes detailed in REFs 5 and 6 will be invoked. This will be done in conjunction with Senior Managers, relevant Business Units and Expert Domains as appropriate

If the Joint BCM processes are invoked, the next steps will be to agree who from the BCMT owns the MBCI.

The BCMT will then agree a plan of action and agree upon the recovery and contingency activities to be carried out. Again, this will be done in conjunction with Senior Managers, relevant Business Units and Expert Domains as appropriate.

The agreed plan will then be monitored and reviewed until such time as the MBCI impacting the APS service has been resolved, and the MBCI closed.

FUJ00080037

13.0 Contact List

13.1 Normal Processes

Organisation	Contacts	Telephone Number
Fujitsu Services RMGA	Duty Manager Or Office Hours applicable Service Delivery Manager	Pager:
	CS Head of Service Management	Office: Mobile:
(MBCI Contacts)	Business Continuity Manager	Office: Mobile:
	CS Head of Service Management	Office: Mobile:
FS Core Services	Network Manager	Office: Mobile:
SOS Networks	Network Management Centre Manager	Office: Mobile:
FS Core Services SOS NT and UNIX	SOS NT and UNIX Manager	Office: Mobile:
	Technical Support Manager	Office: Mobile:
FS Core Services SMC	SMC Manager	Office: Mobile:
	Business Stream Manager	Office: Mobile:
FS Core Services HSD	HSD STE04 Duty Manager	Mobile:
	HSD (STE04) Operations Manager	Office: Mobile:
	Business Stream Manager	Office: Mobile:
Post Office Limited	Business Continuity Manager	Office: Mobile:
	Systems Operations Manager	Office: Mobile:

GRO

FUJ00080037

13.2 Escalation Processes

Escalation Level	Level 1	Level 2	Level 3	Level 4
Fujitsu Services RMGA	OOH Duty Manager Pager: GRO Or Office Hours applicable Service Delivery Manager	Service Delivery Manager BCM Office: GRO GRO Mobile: GRO GRO	CS Head of Service Management Office: GRO Mobile: GRO	Customer Service Director Office: Mobile: GRO GRO
FS Core Services **Networks**			Network Manager Office: GRO Mobile: GRO	Networking Management Centre Manager Office: GRO GRO Mobile: GRO GRO
SOS NT and UNIX			NT&UNIX Manager Office: GRO Mobile: GRO	Technical Support Manager Office: GRO GRO Mobile: GRO GRO
SMC			SMC Manager Office: GRO Mobile: GRO	Bus Stream Mgr Office: GRO GRO Mobile: GRO GRO
HSD			HSD Ops Mgr Office: GRO Mobile: GRO	Bus Stream Mgr Office: GRO GRO Mobile: GRO GRO
Post Office Limited			Business Continuity Manager Office: GRO Mobile: GRO	Systems Operations Manager Office: GRO Mobile: GRO

FUJ00080037

14.0 APPENDICES

Appendix One: Post Office Outlet Trigger Table.

The following table provides guidance on identifying the severity and classification of incidents that have an adverse affect on Post Office outlets. All problems, which are an exception to the 'normal' incident profile and fit within any of the categories defined below should be escalated to the RMGA Business Continuity Manager for consideration.

Not Geographically Concentrated Outlets.	
Less than 200 outlets affected for less than 0.5 of a trading day	**A problem**
Less than 200 outlets affected for between 0.5 and 1 trading day	Potential MBCI
Less than 200 outlets affected for more than 1 trading day	Potential MBCI*
Between 200 and 800 outlets affected for less than 2 hours of a trading day	A Problem
Between 200 and 800 outlets affected for more than 2 hours but less than one trading day	Potential MBCI
Between 200 and 800 outlets affected for more than one trading day	Potential MBCI*
800 and more outlets affected	Potential MBCI*
Geographically Concentrated Outlets.	
Between 10 and 20 outlets affected for less than 0.5 of a trading day	A Problem
Between 10 and 20 outlets affected for between 0.5 and one trading day	Potential MBCI
Between 10 and 20 outlets affected for more than one trading day	Potential MBCI*
Between 20 and 100 outlets affected for up to 1 hour of a trading day	A Problem
Between 20 and 100 outlets affected for between 1 hour and 0.5 of a trading day	Potential MBCI
Between 20 and 100 outlets affected for more than 0.5 of a trading day	Potential MBCI*
More than 100 outlets affected	Potential MBCI*