FUJ00079888

Document Title:	Operations Manual for the Customer Service Directorate
Document Type:	Manual
Release:	N/A
Abstract:	This document outlines the organisation and services provided by the Customer Service Directorate within Fujitsu Services Pathway
Document Status:	Approved
Originator & Dept:	A. Nicholson, Business Architecture Team
Contributors:	Richard Brunskill, Dave Law, Mike Stewart, Pat Lywood, Reg Barton, Graham Hooper, Dave Wilcox, Dean Felix
Reviewed By:	Peter Burden, Richard Brunskill, Dave Law, Mike Stewart, Pat Lywood, Reg Barton, Graham Hooper, Dave Wilcox, Dean Felix
Comments By:	
Comments To:	
Distribution:	Customer Service Management Team Fujitsu Services Pathway Document Management Fujitsu Services Pathway BMS Site

FUJ00079888

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue
0.1	26/9/01	First Draft
0.2	22/11/01	Issued for internal review
1.0	26/11/01	Updated following incorporation of review comments and issued as approved
1.1	28/2/02	Updated to include sections relating to SSC business recovery
2.0	1/5/02	Issued as approved

0.2 Approval Authorities

Name	Position	Signature	Date
Martin Riddell	Director, Customer Service		

0.3 Associated Documents

Reference	Version	Date	Title	Source
CS/QMS/001			Customer Service Policy Manual	Fujitsu Services Pathway
CS/QMS/002			Customer Service Process Manual	Fujitsu Services Pathway
CS/PRO/105			Local Procedure when raising a Purchase Order	Fujitsu Services Pathway
CS/PRD/021			Fujitsu Services Pathway CS Problem Management Process	Fujitsu Services Pathway
CS/PRD/023			Fujitsu Services Pathway Office Desktop Ordering Process	Fujitsu Services Pathway
CS/PRD/029			Process for Operational Business Change - Outlet	Fujitsu Services Pathway

FUJ00079888

CS/PRD/030			Process for Operational Business Change - Product	Fujitsu Services Pathway
CS/PRD/031			Fujitsu Services Pathway Business Continuity Management	Fujitsu Services Pathway
CS/PRD/050			Process for Operational Business Change Reference Data	Fujitsu Services Pathway
CS/PRD/058			Interface agreement for Reference Data	Fujitsu Services Pathway
CS/PRD/074			Fujitsu Services Pathway CS Incident Management Process	Fujitsu Services Pathway
CS/PRD/076			Service Visit Reply Card Process	Fujitsu Services Pathway
CS/PRD/081			Fujitsu Services Pathway CS End to End Customer Complaints Process	Fujitsu Services Pathway
CS/PRD/086			Release management Processes	Fujitsu Services Pathway
CS/PRD/090			Operational Business Change-Outlet Change-Invoicing Process	Fujitsu Services Pathway
CS/PRD/093			Fujitsu Services Pathway Divisional Alert Process	Fujitsu Services Pathway
CS/PRD/102			Fujitsu Services Pathway Field Service Management Process	Fujitsu Services Pathway

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

0.4 Abbreviations/Definitions

Abbreviation	Definition
AIS	Application Interface Specification

FUJ00079888

Abbreviation	Definition
AP	Automated Payment
APS	Automated Payment Service
BMS	Business Management System
BRE	Business Research Establishment
BSA	Business Support Analyst
CA	Contracting Authorities
CCP	Change Control Proposal
CD	Counter Development
CEM	Call Enquiry Matrix
CM	Configuration Management
CP	Change Proposal
CS	Customer Service
CSPM	Customer Service Problem Manager
CTO	Client take on
DM	Duty Manager
DN	Draft note
DPA	Data Protection Act
EPOSS	Electronic Point of Sale Service
FRMS	Fraud Risk Management Service
HSH	Horizon System Helpdesk
HSRF	Horizon Service Review Forum, a joint review of the service held between POL and Fujitsu Services Pathway
HSSM	Horizon System Service Management
IRF	Invoice Request Form
MCVP	Management Care Visit Programme
MIS	Management Information Systems
MSU	Management Support Unit
MTBF	Mean Time Between Failures
NBSC	Network Business Support Centre, part of POL's organisation
OBC	Operational Business Change
OLA	Operational Level Agreement

FUJ00079888

Abbreviation	Definition
ORR	Operational Readiness Review
OSG	Main Fujitsu Services Pathway contact in POL for product change
OSR	Operational Service Review
PinICL	A problem incident notice raised by Fujitsu Services Pathway
PM	Problem Manager
PMD	Problem Management Database
PMS	Pathway Security Manager
POL	Post Office Limited
PORF	Purchase Order Request Form
PPD	Processes and Procedures Description
PVCS	A Proprietary Configuration Management System developed by 'Merant International Ltd'
QMS	Quality Management System
RDCC	Reference Data Change Catalogue
RDMC	Reference Data Management Centre (a Fujitsu Services Pathway database)
RDS	Reference Data System (a POL database)
RDT	Reference Data Team
RED	Reconciliation Exception Database
RTR	Real Time Recording
SLA	Service Level Agreement
SLAM	Service Level Agreement Monitor
SLCA	Service Level Contract Administrator
SMB	Service Manager - Benchmarking
SMC	System Management Centre
SSC	System Support Centre
TIP	Transaction Information Processing

FUJ00079888

0.5 Changes in this Version

Version	Changes
2.0	None, Issued as approved

0.6 Changes Expected

Changes
Updated as a result of future planned review schedule

FUJ00079888

0.7 Table of Contents

FUJ00079888

1 Introduction

The mission statement of the Customer Service Directorate is:

"We provide cost effective services to the Post Office which meets our SLAs

The Post Office regard us as a valued partner

Fujitsu Services see us as the 'best of breed' service organisation"

This Operations Manual defines the key services that are provided by Customer Service to underpin the Mission Statement.

The following information is detailed:

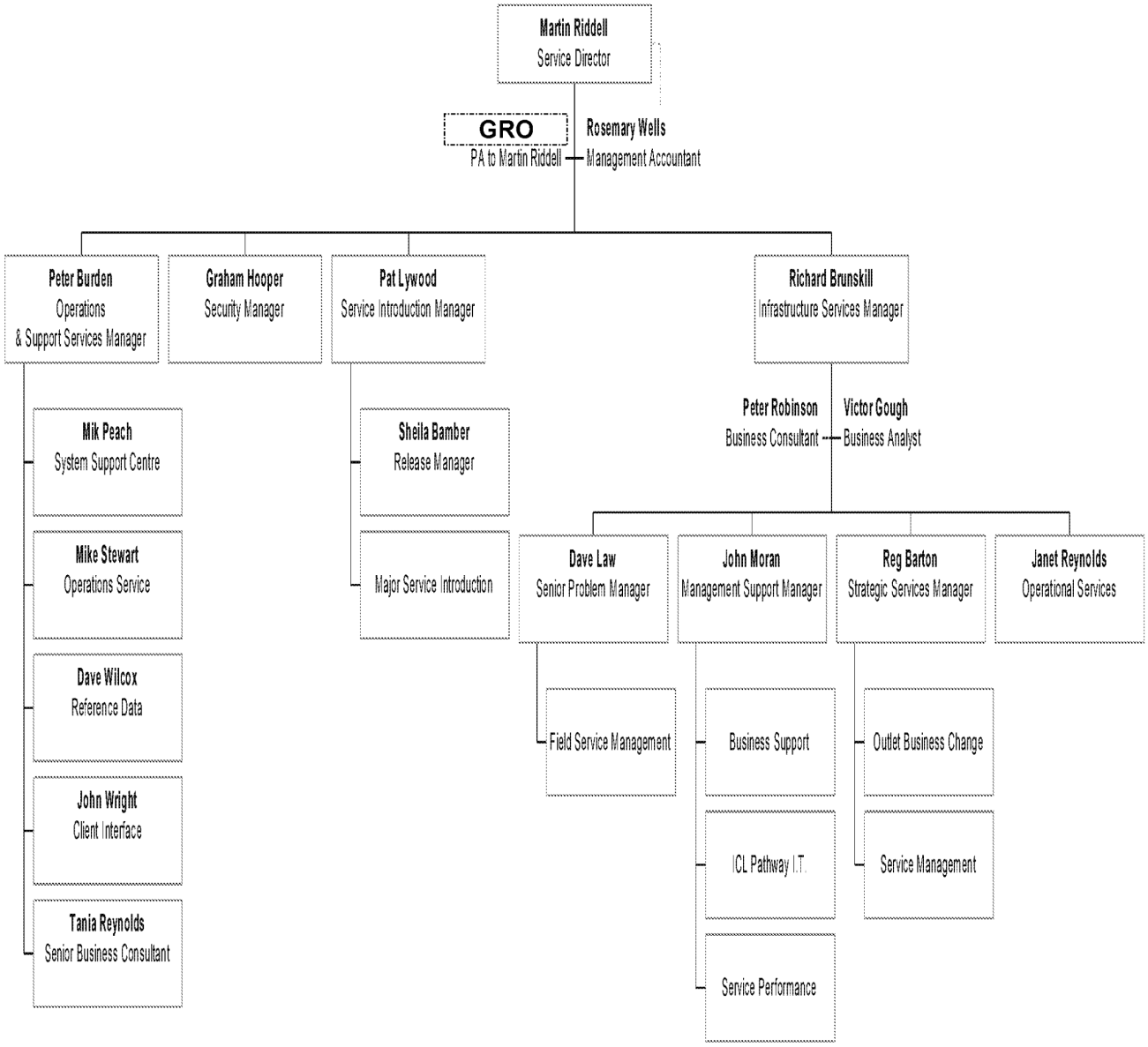
- Roles/Responsibilities
- Key processes owned/used
- Customer/Supplier Interfaces *(e.g. Formal reviews held)*

FUJ00079888

2 Organisation

At the time of approval of this plan the top-level organisation chart is as follows:

For the latest version please refer to the "organisation charts" section of the Fujitsu Services Pathway BMS intranet site.



FUJ00079888

3 Services Provided

3.1 System Support Centre

3.1.1 Overview

The principles by which the SSC operates are documented in *End-to-End Support Process Operational Level Agreement (CS/FSP/006)* which defines the responsibilities of the four levels of support towards each other. This document is effectively a service level agreement between the support units, outlining specific tasks and measures of success.

The aim of the SSC is to provide a support capability to Pathway that resolves technical problems in the minimum time and with the minimum amount of disruption to the service. The SSC aims to provide a centre of technical expertise for Customer Service, providing technical advice, guidance, and expertise relating to all parts of the Pathway system.

More specifically the SSC has responsibilities to:

First and second line support

Fourth line support

- Roles/Responsibilities

The responsibilities of the SSC to first and second line support, that is the Horizon System Helpdesk (HSH) and the System Management Centre (SMC) respectively, are to:

1. Receive incidents passed from the HSH and SMC

2. Ensure that any incidents received are maintained on the call management system. When updates are made to the calls that are relevant to the HSH or SMC, the SSC ensures that these updates reach the Powerhelp system

3. Ensure that the reported incident is resolved correctly and the solution is recorded on the PinICL system

4. Ensure that the incident and solution are passed back to the HSH and SMC call management system. The solution includes a full explanation for the problem and the action taken to resolve it

5. Ensure that the incident is resolved within the total time allowed by the contract between the customer and Pathway

6. Ensure that the HSH and SMC are made aware of the evidence requirements for any form of incident and that this documentation is fully maintained

7. Create and maintain a register of known deficiencies within the Pathway system and the solution to these problems, where known

8. Allow the HSH and SMC access to this register so that they can fulfil their function of filtering out known errors

FUJ00079888

9. Ensure that any solutions or workarounds they pass to the SMC have been tested and have been correctly authorised via the software release management process

10.Ensure that the HSH and SMC are supplied with documentation relating to new releases of software in sufficient time to enable their staff to become familiar with the product prior to its release

11.Ensure that, for any incident which has been solved and passed back to the Powerhelp system, the customer has been contacted and made aware of the call closure

12.Hold workshops and skills transfer sessions relating to technical aspects of the Pathway system and diagnostic techniques

13.Ensure that the following figures are available to the HSH and SMC on demand:

- Number of calls by priority currently outstanding with the SSC
- Number of calls where resolution has been deferred to the next release
- Number of calls by age currently outstanding with the SSC or fourth line support unit
- SSC responsibilities to fourth line support

The responsibilities of the SSC to fourth line support are to:

1. Log all calls on a call management system

2. Filter out all calls for which the problem is already known to the support community and for which a solution is already known or has been generated. This includes problems for which the SSC knows a resolution but has not yet incorporated the resolution into the known error log

3. Retain duplicate incidents in the PinICL systems and ensure that when the resolved incident is received by the SSC the duplicated calls are closed.

Duplicate incidents are repetitions of an incident that has already been passed to fourth line support.

4. Ensure that the correct evidence for any problem is collected prior to the incident being passed to fourth line support for investigation.

5. Ensure that any incident that requires investigation by fourth line support is assigned to the correct PinICL team depending upon the specific product in which the incident has occurred

6. Ensure that any updates made to incidents passed to the SSC are sent to the fourth line support units

7. Ensure that any calls passed to fourth line support units are passed in a timely manner. The timing varies depending on the priority of a call

8. Ensure that the priority of any incident is assessed and recorded correctly

9. Filter out all calls for which the problem is not one of the following:

- Software error

FUJ00079888

- Documentation error

10. Ensure that for any incident passed to fourth line support the exact area of the problem has been identified and, wherever possible, a workaround has already been produced

11. Ensure that, for any code error, a probable solution is indicated prior to passing the incident to fourth line support and, wherever possible, the proposed solution has undergone limited testing

12. Accept full responsibility for the product, including fourth line support, and for the production of any code required to resolve incidents, for areas of the Pathway system where the product has matured, that is, no further releases of the product are expected

13. Create and maintain a register of known deficiencies of the Pathway system and the solution to these problems, where known, and allow access to this register to fourth line units so that they can enter details of solutions created within their area

3.1.2 Role of the SSC relating to Application Support

The SSC within Pathway Customer Service provides third line support for most applications.

The SSC uses PinICL as its call management system and diagnostic database. Calls from second line support are transferred from Powerhelp to PinICL via an OTI link, and updates to the PinICL calls are transferred back to second line support using the same mechanism.

When the SSC receives a call from second line support, second line support has already assessed the call as a software problem and flagged it with the appropriate priority. The SSC handles the call as follows:

1. The SSC checks details of known problems on the intranet site to determine whether or not the problem is similar or identical to a problem already known.

2. If the problem is known, the SSC carries out any pre-authorised actions that are available to it, for example, workarounds in the KEL

3. If the problem is not known, the SSC checks the diagnostic evidence and, if necessary, obtains further evidence from the live system to determine the nature of the fault.

The SSC also uses its reference kit to recreate the symptoms reported by the customer and may then be able to obtain diagnostic data in a controlled fashion

4. If the problem is identified as a code fault, the SSC determines the area of code that has failed and, if possible, identifies a solution to the problem for fourth line support to implement. If possible, it tests the proposed solution before passing the call to fourth line support

FUJ00079888

5. If the problem is urgent, that is, a workaround has not been found, the SSC escalates the problem to fourth line support via PinICL. Note that any urgent corrective action is a one-off implementation of the solution to the problem.

If the problem is not urgent, for example, a workaround has been implemented, the customer is satisfied and the support call has been cleared, the SSC still passes the problem to fourth line support via PinICL to generate a permanent fix. However, the SSC Manager may lower the priority of the PinICL to reflect the lack of urgency of the problem

6. If the problem is not identified as a code fault, the SSC identifies the exact nature of the fault and isolates the system that caused the symptoms. This may happen, for example, when the code is operating within specification but the customer reports symptoms which were not expected

7. Once the SSC has passed the call to fourth line support, it remains responsible for ensuring that the call is dealt with in a timely manner and for informing the SMC and HSH of any updates to the call

8. The SSC identifies the software that needs to be released permanently to the live environment as the long-term solution to the problem and notifies the CSRM accordingly

Note. Closing calls on PinICL and Powerhelp

- The SSC closes a call on PinICL when a resolution has been identified for the call and the details passed to the SMC, for example, a definition of the release that will contain the fix, as detailed in the release management process
- The SMC and HSH use PowerHelp and close a call when the fix has been distributed to the relevant equipment. This may be fairly simple if it is on the central servers, but it may involve considerable work if it requires a code release to all post office counters.

3.1.3 Role of fourth line support

The fourth line support unit receives the request and does one of the following:

- Returns with a recommendation for action that the SSC can carry out
- Returns with a workaround that the SSC can progress as if it had generated it
- Rejects the request, for example, on the grounds that the problem will be resolved in a system software release that is due imminently
- Identifies a fix but does not produce it until authorised by the Release Management Forum

Where necessary, internal Pathway fourth line support also provides the interface with PinICL for external fourth line support units and updates the PinICL with progress reports.

FUJ00079888

A number of units provide fourth line support to the Pathway system as described in the following sections.

- Pathway Development

These development teams use the PinICL system to manage calls. Their process is essentially the same as the SSC with the exception that any development required to resolve a problem goes through the release management process.

The SSC and the development team discuss the problem and assign the PinICL call to either a specific development team, if the product has been identified, or to the general development team, if not.

If the development team requires additional information, it redirects the call back to the SSC, which returns the call to the development team once they have obtained the required additional information.

If a patch is produced to resolve the call, this is handled through the release management process.

- Escher

Escher also uses the PinICL system. The process for routing a call to Escher is via the Pathway development team and therefore the process is as described above.

- ISD

Generally where ISD acts as fourth line support, it also has responsibility for first, second and third line support - therefore, the procedures involved are entirely ISD internal procedures. In those instances where SSC, not ISD, provides third line support the procedures as defined in 4.2.4.1 will be followed.

- Eicon

Eicon do not use the PinICL system, but require calls to be logged by calling GRO GRO Note that this telephone diverts outside normal office hours to Eicon's Canadian call centre. 12 SSC staff are registered with Eicon as having the authority to raise calls, and 2 SSC staff members have undergone training with Eicon in diagnostic requirements.

Escalation to Eicon management for any issues is via the SSC manager and the Eicon Service manager. As of 03/09/2001 this was Dan Dixon,

The Finance Director holds the Eicon contract in FEL01

3.1.4 The Role of the SSC relating to Operational change

The SSC has access to the live system which can be used to correct data on the system when this has been corrupted in some way. The procedure for doing this is as follows:

The originator of the change:

FUJ00079888

1. Completes an Operational Correction Request (OCR) form for every change to data on the live system.

The originator may be anyone within ICL Pathway, but is normally the Duty Manager, or a Problem Manager or Business Support Manager when an incident or problem has been caused by an error in the data. An SSC staff member who detects that the data in the system has become corrupted in the course of diagnosing a fault can also complete it. In the case of an SSC staff member, the form is completed on the SSC web site direct, other people currently complete a Microsoft Word version of the form and use email.

2. Emails the OCR form to an authoriser, electronically signing it where possible, and where this is not possible, telephoning the authoriser to confirm that they are sending an OCR. For SSC staff members, the OCR form on the web must always be digitally signed.

The authoriser must be one of the following:

- Duty Manager
- Business Support Manager
- CS Operations Manager
- SSC Manager
- Release Manager

The authoriser:

1. Authorises the change, or reports back to the originator why they are not authorising the change

2. Forwards the OCR form to the SSC electronically with an encrypted electronic signature file, or in the case of the SSC manager digitally sign the web-held OCR.

The SSC staff member who is to perform the change:

1. Checks the electronic signature of the authoriser

2. Stores the OCR form and the signature file in the `received OCRs` folder on the SSC server

3. Wherever possible, produces a script to make the data change and tests the script on the SSC reference rig prior to running it on the live system

4. Completes the relevant sections on the OCR form to confirm whether they have produced and tested a script or not

5. Prior to making the change on the live system, documents the state of the affected part of the system and completes the regression path details on the OCR form.

Note. If no regression path is possible, this must be stated on the OCR form

FUJ00079888

6. Makes the change on the live system.

At least two people must be present when making changes to the live system. Normally these are SSC staff, but can be one SSC staff member and one person from the fourth line support unit responsible for the area in which the data change will take place, or one SSC staff member and one ISD staff member

7. On completing the data change, documents the state of the affected part of the system and mails an electronically signed copy of the OCR form to the second person who was present while making the change.

8. The second person also electronically signs the form and emails it to either the SSC Manager or the SSC web site controller. In the case of an SSC raised and authorised OCR, both staff members digitally sign the web-held OCR form.

9. Updates the PinICL and reports back to the originator to confirm that the change has been completed

The SSC Manager or SSC web site controller:

10.Checks the electronic signatures

11.Files the OCR in the completed OCR folder on the SSC server

3.1.5 SSC reference kit

- Overview

The SSC reference kit consists of a rig at BRA01.

ISD maintains the rig. The rig is formally "owned" by the Pathway Testing teams, but with an agreement for the SSC to take priority on it at no notice in order to reproduce an urgent fault.

The general requirement is for the SSC to have reference kit that mirrors as closely as possible the equipment in use at any post office. The function of this kit is to duplicate problems reported by customers in a controlled fashion. The SSC also uses the reference kit to provide a link to live system diagnosis and, where authorised, data change.

3.1.6 Diagnostic information

The SSC, as third line support for products in the Pathway system, has responsibility for ensuring that first and second line support units are provided with sufficient information to enable them to diagnose known problems correctly and to provide advice and guidance to the customers.

In this way, support requests from customers that are passed to the SSC should be restricted to either complex end-to-end process problems that require in-depth analysis of all of the systems involved or new software faults.

FUJ00079888

- Maintaining the Known Error Log on the SSC intranet site

The SSC generates and maintains a Known Error Log (KEL) system that uses searchable documents in HTML format. The mechanism for searching is a query entry in an intranet site. The KEL system is available to first, second, third and fourth line support units as well as SSC staff.

- Transferring knowledge between support units

The SSC intranet site has KEL search facilities and other useful diagnostic data, documents and tools.

SSC and SMC staff raise KELs based on customer-observed symptoms.

KELs are further maintained once the fault has been resolved.

Other diagnostic information, including support Guides for the various products are also held on the SSC intranet site, as are contact numbers for SSC and ISD staff. These documents are NOT controlled however, and in case of any doubt, reference needs to be made to the master copies of the documents which are held in PVCS.

3.1.7 Diagnostic tools

- Overview

The SSC develops and maintains tools that can assist in the diagnostic process. The SSC diagnosticians develop the tools themselves; the individual authors are responsible for maintaining these developments.

Development is performed on an ad hoc basis whenever there is a requirement to generate a tool to assist in the diagnosis of faults.

All diagnostic tools are registered on the SSC intranet site.

The tools themselves are made available to all members of the SSC and, where they are able to assist other support units within Pathway, they are made accessible together with any documentation about their use.

- Developing diagnostic tools

Before developing a diagnostic tool, establish whether or not the required tool has already been produced by reference to the diagnostic tools database on the SSC intranet site. This database contains details of known diagnostic tools developed in the SSC and by other support units.

1. If a suitable tool already exists, it should be used
2. If a suitable tool does not already exist, the SSC staff member:
   a) Defines the requirement for the tool to the SSC Manager
   b) Waits for authorisation before proceeding

FUJ00079888

3. If the diagnostician has sufficient development skills to develop the tool him or herself, the SSC Manager schedules the development work required

4. If the diagnostician does not have sufficient development skills to develop the tool, the SSC Manager:

a) If these skills are available within the SSC, identifies the resource required to develop the tool

b) If necessary, goes outside the SSC to obtain the development resource

5. Log the fact that the tool is being developed in the diagnostic tools database on the SSC intranet site and forward this information to all of the relevant units which may have use of this tool

6. Maintain a copy of the tool in the diagnostic database on the SSC intranet site

3.1.8 SSC intranet site

This site was created by and is maintained by SSC staff, although it provides a resource for other support staff within the Pathway estate.

The following sections describe the key features of the site. As the contents of the site are under constant review, the following details may change.

- Known Error Logs (KELs)

The intranet site holds known error details in HTML format, the contents of which may be searched for, in full text form. Documents are created to a defined template wherever possible. An application has been generated which limits the properties of the document to a subset of possible values, for clarity and ease of search. This application is made available to all support units.

The process for creating KEL entries outside of the SSC has not yet been formulated, but it is expected that no KEL will be allowed onto the system before it has been authorised by SSC staff.

- Change proposals

The intranet site holds copies of each Change Proposal (CP) in a searchable form as HTML documents. These documents are **not definitive**. As copies of the CPs are taken before they reach the Pathway Change Control Board the status of any CP is indeterminate - it may, or may not, have been approved.

Maintaining the CPs in this form allows diagnosticians to see that someone has looked at an activity in an area of the Pathway operations regardless of whether or not that activity was actually carried out.

- Release management

The Release Management database is held on the same server as the Intranet site. This database is used to control the flow of fixes through the Operational Testing processes and through release to the live environment.

FUJ00079888

The intranet site provides a controlled interface to this database, allowing searches to be made by:

- **Date**
  For example, show all fixes applied to the live environment since date *xxxx*
- **PinICL**
  For example, show the state of a PinICL in the release process (delivered, due to be tested, due to be released to live)

Similar searches can be made on a Release note as described for a PinICL.

- Operational Change/Corrections

The intranet site holds copies of both SSC Operational Correction Requests and ISD Operation Change Requests. The intention being to provide a mechanism in which both urgent and planned changes at the operational level can be viewed quickly.

ISD have control over the ISD change requests, and the SSC intranet site provides a repository and search mechanism only. For SSC Correction requests, inserting the data into the intranet server is mandated by the process – Appendix B of this document.

- Work Instructions

There is a requirement for Work Instructions which may augment, or temporarily replace documented procedures. These are logged and maintained on the SSC Intranet site. There is a password protection mechanism, so that only the SSC manager, or nominated deputy, can create new, or amend existing Work Instructions. All staff are allowed to search the work instructions

- Other facilities

The intranet site also contains smaller sections that provide:

1. Links to commonly used web sites
2. A bulletin board for SSC staff to add points of interest regarding the operation of the live system
3. Access to commonly used SQL queries and other items of code
4. Access to various documents relating to the live system

3.1.9 Access to the live system

All diagnostic staff in the SSC (product specialists and systems specialists) have access to the live system via PCs (see Appendix D for build details) that are connected to a private LAN in BRA01. Patch panels enable staff to use these PCs to access the test rigs in BRA01.

FUJ00079888

The build script for these PCs was written by and is held by the SSC. The PC build was performed in accordance with the Access Control Policy, and a copy is registered in PVCS.

Access from the PCs to the live system to the live system is controlled by SecureID, uses firewalls, and an encrypted link, and conforms to the Access Control Policy.

The SSC access to the system is for two purposes:

- Assist in diagnosis of problems on the live system
- Correct data which has become corrupted

In the second case, SSC staff may only correct data in response to an authorised Operational Correction Request and only then when there are two or more people present.

3.1.10 Additional technical support to Pathway CS

In addition to the normal support activities, the SSC provides other technical resources to Pathway CS. It is the only unit with sufficient access to the live systems to be able, for example, to analyse:

- Riposte message store
- Counter event logs
- Central system NT event logs

Consequently, the SSC runs daily checks for:

- Post offices that have not communicated with the central systems for 24 hours
- Any NT events that indicate that TIP processing has failed or that transactions have not been harvested

It is also able to respond to other specific requests such as:

- Number of reboots performed by each counter in the estate
- Analysing the message store to investigate a suspected breach of security at a counter or one of the central systems

CS units requiring such information contact the SSC Manager or the appropriate diagnostician who deals with the request as promptly as possible.

The SSC also acts as a development unit for tools which may be required by Fujitsu Services Pathway CS, and other (e.g. HSH/SMC) support units.

Such developments can be requested by any member of Fujitsu Services Pathway Customer Service, or by unit managers from other support units. The developments must be registered with the SSC manager, who will authorise the development, allocate the relevant staff, and maintain a record of the development being produced and the expected delivery times.

FUJ00079888

These developments are intended to improve the productivity of the staff requesting them, and do not form any part of the Fujitsu Services Pathway live estate, and are therefore do not conform to the documentation or testing standards required for the Fujitsu Services Pathway system.

3.2 Client Interface Management

3.2.1 Summary

This unit is responsible for the introduction and ongoing management of services relating to the client interfaces - HAPS, APS clients, LFS and TIP, ensuring the service is delivered within the agreed parameters and operational timetables.

Its responsibilities are:

- Service development including the preparation and review of processes, procedures and documentation, client liaison (including Client Take On), developing support arrangements and participation in test programmes.
- Service introduction including the development and delivery of a service introduction plan containing details of delivery milestones, SLA and OLA targets and support requirements.
- Ongoing Service Management support for implemented services covering operational reviews and service improvement planning, MIS analysis and problem management.

3.2.2 The Interface Services

There are a number of interfaces in place that facilitate the delivery of transaction files between the Fujitsu Services Pathway and POL infrastructure. These are different to the ISDN connections to POL Outlets. The service is responsible for ensuring that transactions, harvested from the POL Outlets, are delivered to POL, through the appropriate interface, in accordance with the Service Schedule Agreements. Each interface and its corresponding SLA is managed as an individual service, but in some areas may involve other interfaces.

The service provided is based on the contents of the Service Definition Agreements (Schedule *n*01), Service Levels and Remedies Agreements (Schedule *n*08) and the Service Management Agreement (Schedule *n*05). These are contract controlled documents and separate schedules are in place for each interface (*n* = character depicting specific interfaces).

There are four interface services:

HAPS, APS clients (of which there are several), TIP and LFS.

FUJ00079888

3.2.3 Service Introduction

As an aid to the Service Manager in delivering a full operational service around the interface in question, a service introduction plan (where appropriate) is prepared, which documents related information, requirements and actions. For example, this includes plans to date and milestone timescales, work still to be done, relating documentation, SLAs and OLAs, support requirements, contacts and links between interested parties.

The following activities take place for each interface in preparation for Live service. Some of the activities may over-spill into Live operation of the service.

- Liaison with the Development and Design teams to understand the Application Interface and Technical Interface Specifications created.
- Liaison with the Requirements team to review all agreements made and any service descriptions in place, if produced.
- Liaison with the client to commence the production of the OLA based on the SLA and specification details. Eventually to become a formal Operational Review meeting once the service is Live.
- Participation in Workshops to prepare or review procedures (if and when applicable).
- Liaison with internal support services to ensure that they are aware of the SLA and OLA commitments.
- Set up of Fujitsu Services Pathway/POL Service Review with agreed Agenda.
- Liaison with Business Continuity Manager to ensure Business Continuity and Disaster Recovery procedures are documented.
- Involvement in any operational test programmes, where requested.
- Produce or review any related documents within Fujitsu Services Pathway.
- Review of any related documents produced by third party suppliers.
- Review of any related documented produced by the customer, if requested.
- Participation in the production and review of Incident Matrix.
- Creation of risk registers.
- Creation of project plans, if required.
- Creation of new call categories within CEM, if required.
- Processing of Change Requests submitted through the Change Management process, if required.

FUJ00079888

- Set up and agreement of Client Take On (CTO) procedures, OLA and schedules (outside of normal service management activities and relating in APS only).
- General, ad-hoc communication with the customer, other internal teams and third party suppliers through phone calls and Email.
- Completion of actions arising from meetings held.
- Implementation of Disaster Recovery solutions, where appropriate (and in accordance with Change Management Procedures)

3.2.4 Service Management

The following activities either take place as standard processes or are managed on an ad-hoc basis in order to maintain or improve services.

- Chair or attend Service Reviews (if appropriate and at agreed intervals - usually monthly).
- Escalation point for service related Incidents and Problems. To be managed as per the standard procedures in place.
- Escalation point for service related customer complaints. To be managed as per the standard procedures in place (Incident or Problem Management procedures). Generally a reactive service.
- Review of OLA as part of Operational Review, as and when appropriate.
- Processing of Change Requests submitted through the Change Management process, if required.
- Review of daily transaction delivery reports produced by third party suppliers.
- Review of monthly SLA Management statistical reports produced internally (by MSU).
- Manage or review any relating plans, where appropriate.
- Ongoing review of procedures in place (any changes to go through Change Management process). Usually highlighted through Workshops or Operational Review meetings.
- Implementation of Disaster Recovery solutions, where appropriate and in accordance with Change Management procedures.
- Participate in scheduled Contingency Tests, where appropriate.

FUJ00079888

3.3 Operations Services

The Operations Services Unit is responsible for all aspects of live service operation. The unit is divided into a number of units as shown in the following diagram.

3.3.1 Availability management

The following sections describe the different areas of availability management.

- Duty management

This section describes operations relevant to the Duty Manager (DM).

The Duty Manager (DM) role is undertaken by Service Managers in CS Operations Services on a rota. A Duty Manager handbook contains phone numbers of Service Managers and other contacts, and copies of relevant procedures.

The DM receives escalated calls from:

- The Horizon System Helpdesk (HSH)
- The System Management Centre (SMC)
- The Management Support Unit (MSU) or the System Support Centre (SSC)
- POL Service Management

The DM decides whether or not the incident needs to be managed through Fujitsu Services Pathway Problem Management procedures.

The document *DSP/PRO/HH/010 Horizon System Helpdesk Incident Procedures* explains the types of calls that are escalated to the DM.

- Types of call

The prioritisation of calls is described in *Horizon System Helpdesk Incident Prioritisation CS/FSP/005*.

The DM receives calls from the HSH for the following circumstances:

- Specific A priority incidents (the different priority categories are described in *CS/FSP/005*)
- After the action times in the SLAs for both A and B priorities have elapsed

  When necessary, the DM also receives calls out of HSH working hours from the SMC/SSC or the ISD Duty Manager.

- Duration of cover

The daily DM rota, (Weekdays only, Operational Hrs 0800-1800), is operated by the Availability team.

FUJ00079888

At other times the OOH DM is resourced from a pool of Fujitsu Services Pathway Service Managers. Operational times are 1800-0800 weekly and 24 hour cover at the weekends Sat/Sun.

There is a Daily update at 0800 from the OOH DM to the Daily DM to hand over any outstanding calls or issues.

There is a daily update at 1800 from the Daily DM to the OOH DM to hand over any outstanding calls or issues.

The handovers at the end of each shift on any outstanding problems or issues, are by phone or in person to the relieving DM, although a DM may see a particular problem through to completion, even after their duty period has ended.

- Duty management procedure

  The overall duty management procedure is as follows:

1. The DM receives a high priority call that may indicate a possible problem
2. The DM finds out the details of the incident, problem or multiple incidents, and may make initial phone calls to the support units to help decide whether a problem exists (see 4.1.5 below).

   If the incident is not a problem, the DM informs the caller to deal with it through the normal A priority channels, ending the procedure.

   If the incident is a problem, the DM initiates the Problem Management Process as in the following steps
3. If the Problem Management Process is initiated, the DM (or maybe the PM Problem Manager, currently under review in PM forum) enters the details of the problem as a progress commentary in a new PinICL call in the PinICL Problem Management Database. The PinICL call is assigned to the Problem Management stack. However, if the problem needs to be dealt with immediately, the DM enters the details on to the database following completion of the immediate action. (If the incident occurred out of hours, then the problem is recorded at the earliest opportunity)
4. The DM appoints the Problem Manager (PM) most capable of handling the problem. In some cases, due to the levels of personnel available, the DM may be the PM, particularly if the incident has occurred outside normal working hours.

   If the appropriate PM is unavailable or unable to manage the problem, the DM escalates the problem to the appropriate Customer Service Manager who will help to decide who the PM should be
5. Following nomination, the DM enters the PM on to the Problem Database as the new owner (assignee) of the problem (this may already be done, see note in 3, currently under review). The PinICL record is updated, closed and possibly reviewed but remains on the Problem Management stack.

FUJ00079888

- Deciding whether a problem exists

To help decide whether an incident is a problem, the DM considers the following areas:

Areas of consideration	Problem criteria
Business impact	• Adverse publicity on Fujitsu Services Pathway. • Possible affects upon Release dates.
Time scales	• The predicted time to resolve an incident is unacceptable.
Customer dissatisfaction	• Widespread customer dissatisfaction.
Breadth of problem	• The incident affects more than 10 outlets. • Does the problem classify as an MBCI
Cost	• The financial cost to Fujitsu Services Pathway to resolve the incident is excessive and possibly impacts the Fujitsu Services Pathway budget.
Complexity	• A variety of resources that need managing are needed to resolve the incident. • Resources external to Fujitsu Services Pathway are required, such as input from POL.
Security	• The incident has possible security implications.
Impact on other organisations	• The incident impacts other organisations such as POL, and they need to be informed.

If the DM is in doubt as to whether an incident is a problem, the incident is resolved as a problem.

3.3.2 OCP changes

An operational change process (OCP) is also in operation. This process covers changes required to the live operation and provides an audit trail for all changes made to the operational estate (Not counter changes). This process is owned and administered by ISD Service Management on a daily basis. The Daily Duty Manager is responsible for the daily sign off as the CS representative but may well seek the advise and sign off from the responsible Service Manager. All other parties in CS Operations and ISD Operations are also signatories to the process.

3.3.3 Business continuity

A key requirement in the Fujitsu Services Pathway solution is that of business continuity, which is effected by producing operational processes and procedures to ensure that any component failure has minimal effect on the service provided. Refer to *CS/PRD/031 (Fujitsu Services Pathway CS Business Continuity Management)* which defines how Business Continuity is managed.

FUJ00079888

POL and Fujitsu Services Pathway recognise the term Business Continuity as having three closely related components:

- **Resilience**
  Steps taken to avert a loss of service or disaster or reduce the likelihood of a disaster or loss of service
- **Contingency**
  Interim processes and procedures adopted during the loss of service
- **Recovery**
  Business and technical arrangements to restore a lost system or service and manage the process of reversion to normal processing and full resumption of service

The principal requirement with respect to the provision of contingency plans is that they should conform to an overall service continuity framework. The document *Business Continuity Framework (CS/SIP/002)* and associated contingency plan documents for each component service of the Fujitsu Services Pathway solution have been produced and are regularly reviewed to ensure they meet the changing requirements of the service continuity framework.

The Business Continuity Framework document does the following:

- Provides a definition of the Business Continuity Framework and contingency plans as specified in Requirement 830
- Provides a detailed definition of Fujitsu Services Pathway deliverables associated with business continuity and the methods of review and assurance
- Defines the contents and format of the contingency plans
- Defines the overall test strategy adopted for testing of the contingency plans
- Defines the management processes for the management of Major Business Continuity Incidents

There are contingency plans for all the service elements of the Fujitsu Services Pathway solution. Most plans cover service elements but a few cover individual Fujitsu Services Pathway sites, which provide more than one service to the Horizon service.

Each contingency plan provides a summarised description of the service or services within its scope. It also describes the measures already taken to minimise the risk of not being able to provide those services.

The contingency plan then sets out what actions the relevant service managers need to take to instigate any recovery or contingency procedures specific to the provision of the service or services.

Each business contingency plan defines the initial and on-going test strategies. For each test, a test script has been produced which clearly explains the objectives of the test exercise and all details necessary to ensure that those objectives are achieved.

FUJ00079888

The document *Business Continuity Test Plan (CS/PLA/011)* brings together the testing requirements of all the contingency plans that have been generated and documents the schedule and methodology to be adopted for business continuity testing, both before National Rollout and on an ongoing basis.

3.3.4 Supplier management

- Overview

The Service Managers within the availability team perform supplier management. The suppliers involved are ISD (Network management, Operations and support), Sequent/IBM (mainframe systems) and Energis (Network provision). Suppliers and service performance is monitored and reviewed on a daily, weekly and monthly basis.

- Daily

Regular telephone contact between the Service Managers and suppliers is undertaken. This contact is used to manage issues and incidents that arise on a sometimes, daily basis. The service managers utilise management information from incidents and trends to support this regular contact.

- Weekly

The service (and supplier) performance is reviewed at a weekly meeting (names "prayers"). This weekly review looks at the issues and problems arising from the operation of services throughout the week identifying issues and placing actions on suppliers to address those issues.

- Monthly

Supplier performance is reviewed formally on a monthly basis, each supplier provides a monthly management report containing the supplier view of service availability, service exceptions, trends analysis and performance statistics. Additionally, Fujitsu Services Pathway produce monthly MIS statistics giving a view from an incident and problem perspective.

A monthly meeting, chaired by the Operations Services Manager, is held with all suppliers present to review overall and individual supplier performance.

3.4 Operational Support Services

Operational Services provide key administrative support to Pathway in order to service the requirements of its client more effectively.

Key areas of functionality are in: -

FUJ00079888

3.4.1 Problem Management

It is the responsibility of the Operational Services team to maintain the Problem Management Database. Problem Managers within CS raise calls on PinICL. These calls are transferred onto the Problem Management database. The database is updated daily and is accessible by POL via the RAS intranet and to Pathway via the CS intranet. A copy of the report can be found on V:/01public/A CS problem management report.

Operational Services liase with POL to maintain continuity of cross-domain problems. (POL sends Pathway a cross-domain report, each week, which is cross-checked with Pathway's own problem management database).

3.4.2 Change Proposal

Change Proposals (CP) are a means of cascading and obtaining approval of changes to the Pathway Programme. A meeting is held every week with representatives of all sections of Pathway to discuss CP's (PCCB). Change Management (CM) owns this process. CS has their own process to ensuring one voice of agreement from CS is passed onto the programme.

Operational Services are responsible for collating all CS impacts on a database and informing CM and therefore Pathway of their outcome. Change proposals are held within a library on PVCS, the tool for recording an audit trail of documents and change proposals for the Pathway programme.

Specific functions include: -

- Use the CP Access Database to record all CS impacts.
- Chasing actions that arise from meeting of the Pathway Change Control Board.
- Update CP status changes.
- Manage Customer change Notes, Customer Change Requests
- Relay costing of impacts to the Finance department.
- Manage the life cycle of the CP process on behalf of Pathway Customer and suppliers/contractors like ISD.

3.4.3 Non Polling

Operational Services play an important part in managing all Non Polling incidents of outlets in the Pathway programme. Non Polling impacts services in the outlets and can attract a penalty if left unattended.

A report is produced from the TIVOLI web of all outlets that have not polled overnight. Operational Services updates this report with additional outlet information and cascades this to POL, SMC, Pathway and Energis. This triggers off the investigative process (amongst the above-mentioned teams) for non-polling until every incident is resolved. Operational Services analyses and

FUJ00079888

investigates non-polling incidents on a daily basis and prepares updated reports, which are distributed, to POL, SMC and Energis. Relevant reports produced are - 1. Initial Non Polling report 2. Non Polling analysis and 3.Non polling updates.

3.4.4 Duty Management

As part of Pathway's contractual commitment to the customer, CS has an obligation to service customer requirements 24 hours/365 days. Operational Services organise and distribute rotas of Service Managers on duty. Time sheets of duty managers are checked and validated and passed to Payroll.

3.4.5 Operational Change Requests

For any operational system changes authorised electronic signatures have to be received from Security, SSC, Duty Managers, Development etc. Operational Services manage the approval aspect of this process by cascading the authorised electronic signatures between all the relevant parties and returning the completed electronic authorisation to ISD for action.

3.4.6 Security

All Pathway staff visiting a Post Office outlet are required to have a valid security pass issued by POL. Operational Services process the documentation for security clearance and manage the process of requesting and issuing of temporary and 3 year passes between Fujitsu Services security and POL security.

3.4.7 General Activities

Activity	Driver	Frequency
Adhoc printing from PVCS and PinICL for CS Staff	MI	As required
General PinICL and PVCS training	MI	As required
Maintaining Pathway Telephone Directory	MI	As required

3.5 Reference Data Management

The overall objective of this team is to manage, in conjunction with other units in Fujitsu Services Pathway, all aspects of POL supplied Reference Data and associated Fujitsu Services Pathway Reference Data delivery to the live environment.

The Reference Data Team (RDT) is responsible for the management of Reference Data to support Operational Business Change (OBC) .

The RDT is responsible for the control of product reference data, as follows:

- POL product changes, such as the price of stamps

FUJ00079888

- Fujitsu Services Pathway generated changed to support POL changes
- Other Fujitsu Services Pathway generated changes, such as the menu hierarchy
- AP Client and services changes

The end-to-end process is described *in Process for Operational Business Change - Product (CS/PRD/030)*

The RDT is also responsible for control of outlet reference data changes in support of the service delivered by the OBC team. The RDT team is also responsible for providing a source of information to other parts of the Fujitsu Services Pathway and Post Office organisation with respect to Reference Data. This sometimes necessitates members of RDT providing varying levels of support, dependant on the nature of the problem being investigated.

3.5.1 Change types

The reference data changes that are covered by this process fall into two types: basic and advanced.

Change type	Description
Basic	Basic changes are those that Fujitsu Services Pathway can implement without prior notice. They consist of changes to reference data that can be implemented with no more than the basic control and release activity by Fujitsu Services Pathway. The data that forms the content of these changes is referred to as 'Class 1' data.
Advanced	Advanced changes are those which need additional activity by Fujitsu Services Pathway before the change can be implemented for example, updating the Menu Hierarchy with a new button. Different advanced changes require different activities by Fujitsu Services Pathway. The activities may be: • Load Type B data (see below for definition of Type B data) • Create Type C data (see below for definition of Type C data) • Manage additional information (see below for definition of additional information) • Validate the change • Maintain documentation • Formal authorisation

FUJ00079888

3.5.2 Types of data

Data type	Description
Type A data	Data that is sent electronically from the POL RDS system to the Fujitsu Services Pathway RDMC system, over an agreed interface, as defined in the AIS document (application interface specification) see *Application Interface Specification Reference Data to Fujitsu Services Pathway (BP/IFS/007)*
Type B data	Data that is sent from POL to Fujitsu Services Pathway, but not over the interface from the RDS to the RDMC. For various reasons, this data has not been included in the Type A AIS, although it may become Type A data in the future for example, scales tariffs. Type B data is received either via the gateway between POL and Fujitsu Services Pathway or as an electronic file by email or on floppy disc, will be passed as an electronic file for example, over email or via a floppy disc
Type C data	Data that Fujitsu Services Pathway must create to support requested changes to the Horizon system for example, changing Menu Hierarchy, cash account and other report layouts. POL must explain what result is expected for Fujitsu Services Pathway to implement the change, for example, for a new core product, where the new button should go in the menu hierarchy
Additional information	Several changes require additional information or 'objects'. Additional information may be needed as follows: • To allow Fujitsu Services Pathway to create Type C data, for example the position of a new button • Because objects such as tokens are needed for Fujitsu Services Pathway to complete the testing phase

3.5.3 Activities

The following activities are involved in implementing Reference Data changes:

1. Receiving Type A data - Basic change data
2. Receiving Business Change Request
3. Receiving Type A – Advanced change
4. Receiving Type B data
5. Receiving additional data
6. Monitoring progress
7. Requesting and loading Type B and C data

FUJ00079888

8. Validating and Verifying Reference Data changes

9. Receiving authorisation

10.Releasing change

The activities performed depend on the type of change and are defined in the *RDCC (CS/IFS/001)*.

3.5.4 Product change activities

RDT carry out the following activities to implement product changes:

- Receiving Type A (and B) data-Basic change Basic changes require only simple reference data changes and can typically be implemented quickly and easily. The document Receiving Type A Reference Data (CS/PRO/074) describes the procedure for the RDT to receive and process Type A Reference data.

  Again *Assessing the impact of a change request (CS/PRO/077)* describes the procedure for the RDT to assess the impact of a Business Change Request and to create a plan for implementing the change

  1. Receiving Type A data-Advanced change. Advanced changes require Fujitsu Services Pathway Customer Service to undertake additional activities, such as creating Type C data, and take longer to implement. For Advanced changes, POL submit a Business Change Request to Customer Service.

  2. Receiving Type B data. As described in Receiving Type A data.

  3. Receiving Additional Information
  Some changes require additional information or objects from POL, such as position of new buttons.

- Monitoring
  The RDT monitor progress on BCRs using a number of tools including the RDMC workstation

- Requesting and loading Type B and C data. The document *Requesting, managing and loading Type B and C Reference Data (CS/PRO/078)* describes the procedure for the RDT to create a request for Counter Development to create Type B and C Reference Data, and to load the data when received from Counter Development on to the RDMC database

- Validating and Verifying Reference Data changes

  For product changes the data is validated internally. POL BSM receive verification Reports and in most cases they are able to view the change on dummy counters in Farnborough. POL BSM verify the data and authorise it for release to Live.

  For outlet changes verification reports are produced and sent to the Network Change Authoriser (NCA) of the territory the change is concerned with. The NCA authorises the release of the data by returning an OBC24 form.

FUJ00079888

- The service description for the APS Token Verification Service is described in *APS Token Verification Service Description for Release 2 (CS/FSP/016).*

  The RDT validate APS Client data changes provided by POL by carrying out the activities described in the document *AP Token Verification procedure (CS/PRO/079)*

  In the event that validation of verification fails, additional data is supplied by POL or Fujitsu Services Pathway, as necessary, and the process is repeated
  Authorisation
  POL BSM Authorise changes to reference data associated with BCRs.

- Releasing

Once Reference Data has been authorised by POL BSM, it is released to live by the RDT. This procedure is described in *Releasing Reference Data to the Live Environment (CS/PRO/081)*

3.6 Message Broadcast Service

A document (CS/OLA/022, Communications Interface Agreement, v.1.0) has been written to describe the processes involving the Post Office and Fujitsu Services Pathway in the authoring, validation and broadcasting of items for broadcast using the Message Broadcast Service. The document covers processes and responsibilities for the authorship and validation of messages, and summarises the end to end procedures for originating the information and for getting it to the required destination. It also ensures that all personnel involved in the process (including HSH) get sufficient visibility of all messages.

Detailed processes related to the use of the Message Broadcast Service itself are contained in a POL authored document: Message Broadcast Service Management Framework (PON/BSM/PRO/001).

3.6.1 Validating POL originated Articles

The same document (CS/OLA/022) also describes the processes involving POL and Fujitsu Services Pathway in the authoring and validation of articles written for publication (usually in Counter News, but not exclusively), and authorised temporary procedures (ATPs). It covers processes and responsibilities for the authorship and validation of articles. Its aim is to ensure that both organisations are aware of their individual responsibilities, in the authorship and validation of Horizon related information being distributed to post office outlets. It also ensures that all personnel involved in the process get sufficient visibility of all relevant articles. The validation cycle within Fujitsu Services Pathway includes HSH and the technical authors.

The end to end procedures for originating the information and for getting the article to the required destination are covered in a POL authored document Working Level

FUJ00079888

Procedures for the Implementation of Authorised Temporary Procedures (CHE/APR/008).

3.7 SSC Business Recovery Plan

3.7.1 Fujitsu Services Pathway Generic

3.7.2 Introduction

This appendix provides instructions for staff working for Fujitsu Services Pathway SSC on how to respond to a major incident affecting the building at BRA01, personnel, assets or the business.

The SSC is responsible for the safekeeping and communication of the business continuity plan within the team.

This plan has been developed to ensure that Pathway can recover from a major disruption in a timely and efficient manner. However, the existence of this plan alone does not guarantee a successful recovery. This plan must be kept current as personnel, equipment, facilities, and business processes change. The participants in the recovery process must know and understand their roles in the execution of the plan. Physical and information environments on which the plan depends must be monitored to ensure that they are being maintained and are available for recovery if needed. Furthermore, the plan must be tested regularly for validity.

3.7.3 Objectives

The primary objectives of the SSC business continuity plan are:

- to provide a tested vehicle which, when executed, will permit an efficient, timely resumption of all critical business functions in order to continue operations
- to contain, within acceptable levels, the financial and operational impacts that Pathway could suffer following a disruption
- to minimise impacts upon customers
- to minimise the impact to the public and to the industry image of Pathway

3.7.4 Scope

This plan provides for recovery of the SSC operations within one working day of a disruption.

The plan covers:

- staff relocation
- communication with customer and suppliers
- recovery of critical records

FUJ00079888

- rebuild of critical equipment

3.7.5 Assumptions

The Plan has been developed with the following assumptions:

- correct data files are backed up and stored remotely
- office IT at FEL01 will be available within 2 hours of invocation
- all necessary critical records have been stored offsite and can be recovered within two hours after an incident has been notified to the SSC Manager or his deputy

3.7.6 Change Management

This plan will be reviewed regularly

- Change Checklist

Changes that may affect the plan are:

- SSC personnel and related details
- critical business functions
- third Parties providing support to the SSC
- software
- hardware
- critical records.

3.7.7 Audit

Audit of the plan will be conducted according to the Fujitsu Services Pathway Audits policy and annual plan.

3.7.8 Testing

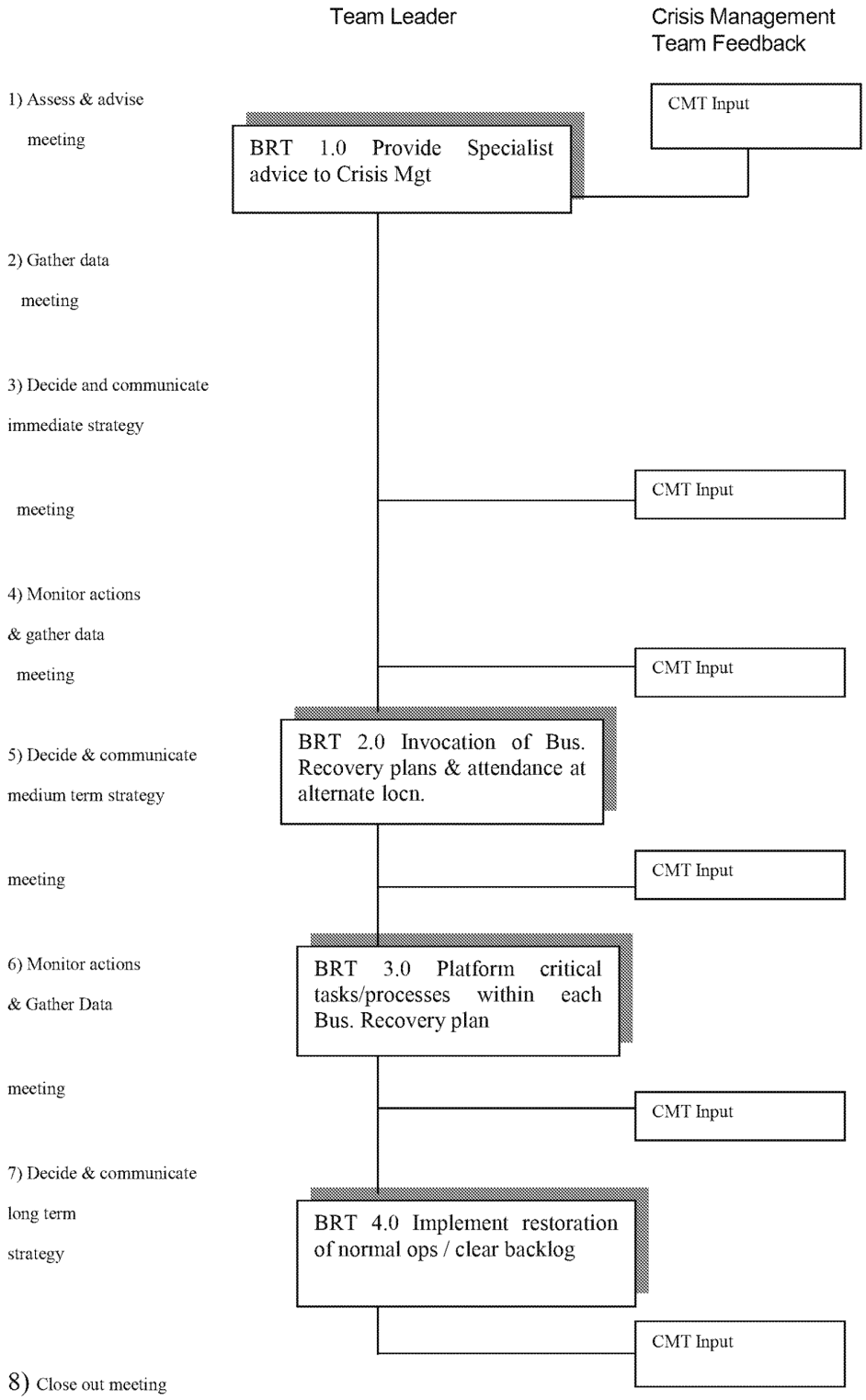
The plan will be reviewed once per annum or when significant organisation changes take place. Any resulting plan changes will be collated and incorporated into this document and the plan re-issued.

3.7.9 Business continuity process at Pathway

This plan is derived from the document "Business Recovery Plan 704 Systems Support Centre", which defines the Pathway business continuity process (BCP).

The following flowchart shows the flow of high level activities that make up the BCP.

FUJ00079888



FUJ00079888

3.7.10 SSC specific

3.7.11 Strategy explanation

In the event of a disaster affecting BRA01 which is so severe that the existing arrangements for UPS, backup generators etc are ineffective, that there is a total building loss, then some SSC staff will move to FEL01.

SSC access PCs, which are used to access the live system, have been built and will be maintained in a secure area in FEL01.

A room in FEL01 which has been set up with the required firewall and connections to the live service will be used, and SSC staff will connect their own PCs into the available sockets.

OSD staff will be required during this process as a final check on the connections to the live system through routers and firewalls.

SSC maintains all essential data on the SSC web site, off site copies of which are held by both the senior technician and the SSC manager. These copies will be used if necessary to recover the web site, which contains diagnostic information, including Known Error Logs.

3.7.12 Pre-disaster Actions

3.7.13 SSC Contact numbers

Surname	Forenames	Home phone No.	Status
Anscomb	Jim	GRO	
Ballantyne	John		
Carroll	Patrick		Senior Technician
Chambers	Anne		
Coleman	Richard		
Critchley	Graham		
Foster	Bob		
Greenwood	Kath		
Harvey	Martin		
Hawkes	Chris		
Longley	Barbara		SSC Coordinator
Maxwell	Gary		
O'Connor	Aidan		

FUJ00079888

Surname	Forenames	Home phone No.	Status
Parker	Steve	GRO	Senior Technician
Patel	Rakesh		
Peach	Mik		SSC Manager
Rowe	Diane		
Seddon	Dave		
Simpkins	John		
Simpson	Garrett		
Squires	Steve		
Steed	Paul		
Streeter	Neil		
Wright	Mark		

3.7.14 Action Checklist

TL-BRT1.0.1	**Team Leader or Deputy notified of an Incident by a member of CMT. Record name of caller.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT1.0.2	**Ensure that the Crisis Controller or Deputy has been informed**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT1.0.3	**Ensure that all staff stay by a telephone on stand by until otherwise informed**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT1.0.4	**On receiving a call from the CMT, please ensure that the following is ascertained before undertaking any unrequested actions:**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT1.0.5	**1.Exactly what has happened ?**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL BRT1.0.6	**2.Who has been informed?**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT1.0.7	**3.What is the impact ?**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT1.0.8	**4.What is the estimated time of inoperability ?**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRTI.O.9	**5.Do 1 need to go to the alternate location ?**	Start Date/Time:	End Date/Time:	Complete: Y / N

FUJ00079888

TL-BRT1.0.10	**6.Do 1 need to contact other staff ?**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT1.0.11	**7.How do 1 contact the CMT ?**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL BRT2.0.33	**Ensure that all staff are accounted for.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.34	**Obtain details regarding any personnel seriously affected by the Incident**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.35	**Contact Deputy (as available) and ensure that all other team members are contacted as soon as is reasonable**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.36	**When will you attempt to contact these staff again ?**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL BRT2.0.1	**Check with next of kin if these staff are away or on holiday etc.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.2	**Leave message that they are to contact the Team Leader before returning to work.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.3	**If unsure of the situation and cannot confirm it via the CMT, everyone should stay near the telephone that the CMT has the number for and await instruction**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.4	**Keep in regular contact with Team Members to reassure them that the situation is under control and provide advice.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.5	**When notified by the CMT, ensure that you and your staff pack and proceed to your Alternative Team Location as requested.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.6	**Identify any critical activities, documents, or actions possibly affected by the Incident**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.7	**Identify all critical aspects of work in progress**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.8	**Identify the key events that have recently occurred to the company.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.9	**Identify any deadlines that may occur soon.**	Start Date/Time:	End Date/Time:	Complete: Y / N

FUJ00079888

TL-BRT2.0.10	**Identify the extent of any lost data.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.11	**Identify any catch-up processes that may be required to perform.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.12	**Identify any work around procedures that may be required.**	Start Date/Time:	End Date/Time:	Complete: Y N
TL-BRT2.0.13	**Identify any special staffing requirements for the organisation.**	Start Date/Time:	End Date/Time:	Complete: Y N
TL-BRT2.0.14	**Identify any special projects that may alter the recovery priorities.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.15	**Inform the CMT members of the business requirements identified**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL BRT2.0.16	**Start the Incident Log**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.17	**Create a staff location list for all members of staff.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.18	**Assist with all personal problems arising from the Incident.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.19	**Maintain status information on any company personnel receiving medical treatment or other disaster related services.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.20	**Report the level of employee assistance being provided to the CMT.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.21	**If appropriate, arrange for petty cash to be made available.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL-BRT2.0.22	**If appropriate, arrange for hotel accommodation to be made available for members of staff.**	Start Date/Time:	End Date/Time:	Complete: Y / N
TL BRT2.0.23	**If appropriate, arrange travel for relevant members of staff.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.24	**Identify and arrange for essential equipment to be provided.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL BRT2.0.25	**Stand down other non-essential personnel & services.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.26	**If required to work at alternative location or away from home, consider the checklist items below:** **- Business Continuity Plan**	Start Date/Time:	End Date/Time:	Complete: Y/ N

FUJ00079888

	- Mobile phone **- Charger & spare batteries** **- Travel plugs** **- Laptop - Charger & spare batteries** **- Money & Credit cards** **- Food & Beverages** **- Change of clothes** **- Overnight Bag** **- Own contact list** **- Passwords** **- Security Pass** **- Medicine - for personal use** **- Organiser / diary** **- Keys** **- Passport** **- Driving License**			
TL-BRT2.0.27	**Inform close family of departure to Alternate Site or Crisis Management Site.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.28	**Provide the Incident Management Team with a contact list with the alternate site locations at which each team member is located**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.29	**Support Resumption Management in filling requests for additional personnel.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.30	**Assist in the creation and maintenance of internal phone directories to ensure communication among relocated business areas as necessary.**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.31	**Use company credit card where possible to pay for critical expenses and keep receipts safe so they can be sent to Finance staff**	Start Date/Time:	End Date/Time:	Complete: Y/ N
TL-BRT2.0.32	**Do not exceed a reasonable level of expenditure without authority from the CMT.**	Start Date/Time:	End Date/Time:	Complete: Y/ N

FUJ00079888

3.7.15 External Contacts

Listed below are the contacts who may need to be informed following an incident.

Name:	**OSD Belfast**	**Work:**	
Address:	Belfast	Home:	
		Fax:	
		Mobile:	
		EMail Address:	
	Contact Name:	Unix Team – Andy Gibson	GRO
		NT Team – Darren Dillon	GRO
Name:	**HSH / SMC**	**Work:** GRO	GRO
Address:	STE09	Home:	
		Fax:	
		Mobile:	
		EMail Address:	
	Contact Name:	Ian Cooley	
Name:	**BRA01 Access Security consultants -**	**Work:** GRO	
Address:	Via Workplace Technology	Home:	
	Fax:		
	Mobile:		
	EMail Address:	Mike.Wood GRO	
	Contact Name:	Mike Wood /Paul Sinclair	
Name:	**Pathway Development**	**Work:** GRO	GRO

FUJ00079888

Address:	FUJITSU SERVICES FEL01	Home:	
	Fax:		
	Mobile:		
	EMail Address:	GRO GRO	
	Contact Name:	Peter Jeram	
Name:	**CS Support Services Manager**	**Work:** GRO	GRO
Address:	Fujitsu Services BRA01	Home:	
	Fax:		
	Mobile:		
	EMail Address:	GRO GRO	
	Contact Name:	Peter Burden	

3.7.16 Vital Records

This list contains all the vital records for the department. These records should be re-created as part of the departmental recovery process.

Record Name: Operation Manual

Media Type: Word document

Recovery Source: PVCS

Source Contact Details: Alex Hanson CM

Required By: All SSC staff

Record Name: Back Up Procedures

Media Type: HTML Pages

Recovery Source: SSC Web site backup copies

Source Contact Details: SSC manager, SSC Senior technician

FUJ00079888

Required By: All SSC staff

Record Name: **Department Contact List**

Media Type: HTML Pages
Recovery Source: SSC Web site backup copies
Source Contact Details: SSC manager, SSC Senior technician
Required By: All SSC staff

Record Name: **Known Error Log / OCP database**

Media Type: HTML Pages
Recovery Source: SSC Web site backup copies
Source Contact Details: SSC manager, SSC Senior technician
Required By: All SSC staff

Record Name: **SSC support CD**
Media type: Compact Disc
Recovery Source: SSCDIAG4 backup copies
Source contact details: SSC Manager, SSC Technicians
Required by: All SSC Staff

3.7.17 Critical Equipment

Listed below is information regarding the equipment that may be required following an incident.

Equipment Name:
Description: SSC Build PCs
Location: FEL01
Required By: All SSC staff who have moved to FEL01
Owner: SSC Manager

FUJ00079888

Quantity: 5

Requirements Over Time :Required 4 hrs after disaster declared

Equipment Name:

Description: SSC Web server / Powerhelp access PC

Location: FEL01

Required By: All SSC staff who have moved to FEL01

Owner: SSC Manager

Quantity: 1

Requirements Over Time :Required 4 hrs after disaster declared

Equipment Name:

Description: Access to Powerhelp

Location: FEL01

Required By: SSC Co-ordinator

Owner: SSC Manager

Quantity: 1 link

Requirements Over Time :Required 4 hrs after disaster declared

Equipment Name:

Description: Access to live system

Location: FEL01

Required By: SSC Diagnosticians

Owner: OSD

Quantity: 5 links to live system, with connectors available, firewall access

Requirements Over Time :Required 4 hrs after disaster declared.

3.7.18 SSC Back up Facilities at FEL01

The kit will be located in meeting room 6 - "D" block (M6).

Reception will be able to give directions and a swipe card that works for D block (normal cards will not work).

FUJ00079888

The Pathway private network is patched to lap point 21 in the meeting room.

OSD Service Management (e.g. Steve Gardiner or Ken Wood) will set-up/remove this patch. This network point will be used via a 16 port hub to drive all the red network PC's

The Pathway public network is patched to point H10 in the meeting room. This should be directly connected to the PinICL admin system (SSCPublic)

SSCFEL01 - SSC workstation (connected to Red network Hub)

SSCFEL02 - SSC workstation (connected to Red network Hub)

SSCFEL03 - SSC workstation (connected to Red network Hub)

SSCFEL04 - SSC workstation (connected to Red network Hub)

SSCFEL05 - SSC workstation (connected to Red network Hub)

SSCFEL06 - SSC workstation (connected to Red network Hub)

SSCPublic - PinICL system. (connected to public network point H10)

SSC staff logon to the workstations using their normal PWYDCS username and password.

TCP/IP details

Red network via hub:-

SSCFEL01
SSCFEL02
SSCFEL03
SSCFEL04
SSCFEL05
SSCFEL06 GRO

Netmask:
Gateway:
WINS:
WINS: GRO

Public network via lap point H10:-

SSCPUBLIC GRO

FUJ00079888

Netmask

Gateway

GRO

Password details for these PC's can be found in the file \SSC\passwords.txt.asc on the SSC Support CD. This is a PGP encrypted file which can be opened by the following keys:-

Mik Peach, Steve Parker, Richard Coleman, John Simpkins

3.7.19 SSC PC Build Details

Full details of the SSC workstation build are found in the file \SSC\SSCWorkstationBuild.doc on the SSC support CD.

3.8 Outlet Business Change

3.8.1 Overview

Outlet Business Change (OBC) refers to the service managed by the CS Strategic services Unit OBC team, to deliver agreed physical and configuration changes to the Horizon counter system at post offices where requested by a change order from Post Office Limited.

Agreed changes are those changes defined as Post Office Limited requirements within the Operational Business Change catalogue (document ref CS/REQ/006) and such changes are planned with a lead-time in advance of delivery.

3.8.2 Types of Outlet Business Change

By managing planned OBC change, the CS Strategic Services Unit supports the delivery of the following Post Office Limited required change types:-.

- PLANNED office refurbishment (same counter configuration)
- PLANNED office opening (new counter configuration)
- PLANNED office closure (either temporary or permanent)
- PLANNED office relocation (either same or new counter configuration)
- PLANNED office counter increase or decrease
- PLANNED office counter change (trolley or mobile)
- PLANNED office counter peripheral change (display type or weigh scales)
- PLANNED office change communications type (VSAT to ISDN or vice versa)
- EMERGENCY office closure (unplanned temporary closure)

FUJ00079888

- PLANNED office re-opening (following an emergency closure)
- BASIC and ADVANCED reference data changes to office details

3.8.3 Process for Outlet Business Change

The OBC process stages determine the implementation of each type of change.

- CS OBC team receives and processes the change orders from Post Office Limited
- CS OBC team check orders for conformance to the service predefined time-scales
- CS OBC team liase with Post Office Limited, Network Transformation
- CS OBC team schedules service components with CS service suppliers
- CS service suppliers deliver service components to the post office.
- CS OBC team manage the end to end service process, which links all of the component services together, and ensures the success of the change
- A completion record for all changes is sent to the customer

3.8.4 Key OBC Service Suppliers

The OBC process stage is resourced and delivered by approved service suppliers.

- Energis provide post office communications infrastructure either through BT for an ISDN service solution or through HOT for a VSAT service solution.
- ISD provide site survey and preparation services through RoMec, and Horizon equipment services through UKSS engineering.
- ISD also provides Horizon system configuration services through MSS and SMC.
- Pathway CS SSC provides software support for OBC.

3.8.5 OBC Service Management

The CS OBC Service Manager has a team of Service Controllers each owning the changes for a geographical territory. The Horizon estate is split into three territories, North, West and East, and maps onto the organisational structure of the Post Office Limited Network Transformation Team territory. The Service Controllers each have responsibility for up to 60 post offices changes per month, and control these changes by liasing with the customer and suppliers on a daily basis. The following document set governs the delivery of the OBC service: -

- CS/REQ/006 – OBC Change Catalogue
- CS/PDN/015 – Outlet Change Service Descriptions
- CS/PDN/017 – Outlet Change Schedule of Service Prices

FUJ00079888

- CS/IFS/003 – Fujitsu Services Pathway / Post Office Limited, Interface Agreement for OBC - Outlet
- CS/PDN/029 – The Management Process for OBC - Outlet

3.8.6 OBC Service Monitoring

There is a continuous stream of change activity, which is active work in progress. The delivery of change is subject to daily monitoring and ongoing telephone and electronic mail discussion with suppliers and customers.

An OBC database is used to monitor and control operational changes and a new tool, OCMS will enhance OBC scheduling and monitoring from January 2002.

3.8.7 OBC Service Completion

When Post Office Limited wish to alter the details a change that has been previously ordered on an OBC20 form, they request an amendment by issuing an OBC21 request to the OBC team. Records are kept in the OBC database of all OBC services that have been delivered, and these are used to calculate the payment for services on a monthly basis. An invoice is then generated and sent to Post Office Limited for payment.

Fujitsu Services Pathway has declared a limit for the maximum number of OBC changes that can be delivered over a period. This is expressed as a percentage of the live estate averaged over one year, and is documented in The Management Process for OBC. Post Office limited can request that this limit is increased by raising a Change request to Fujitsu Services Pathway.

3.8.8 OBC Service Review

Regular monthly reviews are held between the customer (Post Office Limited Network Transformation Meeting), and the CS OBC Service Manager, to discuss any OBC service issues and to look for ways to improve or enhance the service delivery process. The CS OBC Service Manager also holds regular reviews with the Service Managers from the suppler organisations, with this same objective.

3.8.9 Horizon Rollout Tail

The OBC service has been used to manage the National Rollout tail activity, installing the 93 remaining post offices taking over the task from the Fujitsu Services Pathway Implementation Directorate.

3.9 Field Service Management

3.9.1 Overview

The role of the Fujitsu Services Pathway Field Service Manager is to manage system problems that affect individual Post Office outlets. As a result, the impact of the problem on Post Office business will be minimised, and service

FUJ00079888

levels/customer satisfaction is maintained. Root causes to problems will be identified, and actions applied to ensure that the circumstances do not recur.

The FSM team is field-based, and geographically spread across the UK. Each FSM is responsible for an area of the country.

The role operates within the overall framework of the Fujitsu Services Pathway Customer Service Problem Management Process, the End-to End Customer Complaint Process, and the Fujitsu Services Pathway/POL Problem Management Interface Agreement, and the high level process is documented separately in the Field Service Management Process Document CS/PRD/102.

By reference to extracts from the Horizon System Helpdesk logs, or in response to referrals from other members of Fujitsu Services Pathway Customer Service, the Field Service Managers identify individual Post Offices where there appears to be an underlying problem giving rise to a higher than expected level of incidents. A visit to the outlet is then requested through Post Office Ltd BSM, and subsequently visited by the Field Service Management. All relevant information is collected during the visit to assist the FSM with a problem investigation. If immediate actions do not resolve the issues at the outlet, then an entry is made on the Problem Management Database, and reviewed regularly at a joint meeting with the Post Office Ltd Problem Manager.

The Field Service Managers act as Problem Managers within Fujitsu Services Pathway Customer Service team, with focus on individual office issues. As such, they may be appointed as Problem Managers within the terms of the Fujitsu Services Pathway Customer Service Problem Management Process (Ref: CS/PRD/021) by the Duty Manager, in response to cross-domain problems raised by POL BSM. Additionally, within the terms of the Problem Management Process (Ref:CS/PRD/021), responsibility for specific office problems may be passed to the appropriate FSM by any other Problem Manager (Ref Para. 5). The Field Service Managers also participate in the Management Care Visit programme.

3.10 Service Management

3.10.1 Overview

The Strategic Services Unit exists to ensure that the services required by Post Office Limited and agreed and offered by Fujitsu Services Pathway at the post office counter, and in conjunction with the National Business Support Centre, are available when needed and meet the service level commitments associated with those services. The Strategic Services Unit ensures that the Horizon system is properly implemented and operated across the post office estate, and remains usable for the post office to conduct daily business for the duration of the Fujitsu Services Pathway contract.

FUJ00079888

The Strategic Services Unit has responsibility for conformance to the following processes that have been implemented through the service management frameworks and agreed with Post Office Limited:

- The Incident Management Process
- The Problem Management Process
- The Complaint Management Process

Service Management is provided by the Strategic Services Unit to manage the quality and SLA conformance of suppliers to deliver the following services to post offices as contracted for between Post Office Limited and Fujitsu Services Pathway.

- Operation of the Horizon Systems Helpdesk
- Operation of post office break fix engineering service
- Operation of the OBC service (Section 3.6)

The Service Management focus is on providing a consistent and reliable service to resolve incidents and problems encountered in the Horizon estate, while managing customer and supplier relationships with the objective of continuous service improvement. In addition the Strategic Service Unit has a service management function that seeks opportunities to improve customer satisfaction with the Horizon system in the post office outlet environment through direct feedback from the end users. To achieve this the Strategic Services Unit:-

- Provides Service Management resource for managing problems
- Takes Service Management action on issues raised on engineer reply cards
- Allocates Service Managers to the Management Care Visit Programme
- Takes ownership of the Customer Complaint Process.
- Monitors supplier performance on a daily and weekly basis
- Reviews suppliers on a monthly basis at the Operational Service Review

The Strategic Services Unit is also responsible for the development and evolution of these services to support the product life cycle and the introduction of new products over of the duration of the Horizon Programme.

3.10.2 Key Processes – Incident Management

The Strategic Services Unit has the overall responsibility of ensuring that the Horizon System Helpdesk function is being performed effectively by the Fujitsu Services Pathway service supplier, and the SLAs are monitored daily by the Service Manager pick up any deviation in performance. The Service Managers have objectives to ensure that:-

- The Incident Management process supports the flow of incidents through the support chain, and that matters relating to the quality and performance of

FUJ00079888

suppliers operating the incident management process are properly addressed and resolved.

- The Incident Management process supports the prompt resolution of incidents and achievement of agreed service levels.
- Trends, multiple incidents, or incidents with serious business impact are properly captured and recorded as problems in the Problem Database and the Service Manager takes ownership and manages the problem through to resolution.
- Customer complaints are recorded and dealt with appropriately and in an acceptable timescale, and are escalated where necessary.
- A nominated Service Manager from the Strategic Services Unit performs the Duty Manager role during core day hours on two days of every week.

3.10.3 Key Processes – Problem Management

All Service Managers in the Strategic Services Unit take on the role of Problem Manager for specific problems within their area of responsibility or expertise. They manage problems in accordance with the Problem Management process, providing weekly updates to the Problem Management Database.

3.10.4 Key Processes – Complaint Management

The Strategic Services Unit manages the Customer Complaints Process on behalf of Pathway Customer Service. This involves following steps for each complaint received:-

- Receive complaints proper to Fujitsu Services Pathway CS from Post Office Limited or

  directly to Fujitsu Services Pathway.
- Log and acknowledge the complaint with the complainant
- Investigate the complaint
- Provide a response to the complainant in the appropriate manner
- Close the complaint record once it is agreed that all concerns have been answered
- Identify any improvement opportunities and ensure a plan is put in place to action them
- Monitor all complaint calls received at HSH Helpdesk for conformance to resolution times, accuracy and consistency of responses.
- Measures the success of improvement initiatives by monthly reviews of complaint statistics at the Operational Service Review with key service suppliers and the NBSC Helpdesk Forum.

FUJ00079888

- Hold a quarterly meeting with the NBSC Customer Relations team to look at trends and process improvement opportunities.

Note it is not Fujitsu Services Pathway policy to pay compensation to a complainant but reimbursement of costs will be considered if investigations show this to be justified in particular circumstances.

3.10.5 Key Processes – Customer Satisfaction

The SVR process allows feedback on service delivery to be monitored by the Strategic Services Unit. A card (Reply Card) left at the post office following an engineer's visit allows a Postmaster to comment on the quality of the service provided by an engineer during their visit, and it also invites comment on the service provided by the Helpdesk. The SVR process has several stages:-

- Ordering of new cards and arranging for any changes with printer supplier
- Distribution of new cards to the Engineer Support Managers
- Engineer gives a card to the Postmaster following a visit to a post office
- Cards have prepaid postage and are returned by Postmasters direct to the Strategic Services Unit address
- The Service Manager carries out an initial sift to identify urgent complaints or concerns before passing them to be input into the SVR database
- Issues are referred to the appropriate section/s for comment and action and comment
- Any serious concerns by a Postmaster is responded to by letter
- A meeting with the relevant support staff is held bi-monthly to review statistics and levels of customer satisfaction/ concerns

To monitor the post office end user's perception of post-implementation services, the Strategic Services Unit participates in the Management Care Visit Program (MCVP) - a monitoring program implemented to ensure Fujitsu Services Pathway fully understands the Postmaster's view of the service that Fujitsu Services Pathway delivers.

The MCVP involves senior Fujitsu Services Pathway managers visiting randomly selected post offices and collecting feedback using an aide memoir for the interview.

The resulting information gathered on these visits is collated and entered into a database to identify common issues and facilitate statistical reporting. Each Service Manager is targeted with completing 12 post office visits per year.

FUJ00079888

3.10.6 Key Processes – Problem site monitoring

Problem sites are identified weekly, based on statistics of top ten callers to the Horizon System Helpdesk. The top ten post offices will initially include all categories of calls, however for the purposes of this analysis, Software/ Hardware/ Network calls will be ignored (these areas are dealt with separately by Field Service Managers). The top ten are then analysed to identify specific problems with the objective of identifying any gaps in training of the user for the site as a whole or in a specific area. Those post offices identified as being significantly above the average for calls to the Helpdesk, will be raised as Problem Sites on Fujitsu Services Pathway Problem Database through normal Problem logging channels to Post Office Limited BSM.

3.10.7 Key Service Suppliers

The key suppliers monitored through the OSD Service Review process by Strategic Services are:

- Horizon System Helpdesk – who provide the point of contact for post offices reporting Horizon system and service problems.
- UK System Service – who provides engineer services at the post office for both incident resolution and OBC services.

The Fujitsu Services Pathway Management Support Unit is an internal supplier to the unit. The MSU provides service performance information used by the Strategic Services Unit to monitor and improve the service delivered to the customer. The performance data is held on the CS Intranet – a local web site.

Additionally the following document set provides essential information for, the successful, delivery of business as usual activity to the Post Office Outlet.

[CS/FS/005 HSH Incident Prioritisation]

[CS/FSP/002 HSH Call Enquiry Matrix]

[CS/PLA/015 HSH Continuity Plan]

[CS/PRD/021 Fujitsu Services Pathway Problem Management Process]

[CS/PRD/074 Fujitsu Services Pathway Incident Management Process]

3.10.8 Service Monitoring

A good customer/supplier relationship is essential to the successful delivery of service to Post Office Limited. Therefore a set of monthly service reviews are vital to the success of this relationship. All service reviews follow an agreed format, having an agenda, a chairperson, an action list, and minutes.

The specific set of reviews the Strategic Services Unit play an active part in are:

- The Horizon Service Review Forum where Fujitsu Services Pathway performance in the delivery of the end to end service is reviewed with Post Office Limited Business Service Management, against contracted SLAs.

FUJ00079888

- The HSH/NBSC Review Forum – where operational matters effecting the delivery of helpdesk service to the post office are reported and reviewed by participation of representatives from both customer and supplier helpdesks.
- The Network Transformation Forum where OBC service performance and issues are reviewed.
- The Operational Service Review, where the "key" suppliers performance is reported and reviewed.

3.10.9 Service Development

Service Managers have the responsibility for introducing services to support new Horizon products and early participation at the design and specification stage of a development programme is necessary to ensure a successful implementation.

3.11 Problem Management

3.11.1 Purpose

Problem Management exists within the Infrastructure Services function. The aim of problem management is to identify and manage the removal of the root causes of issues that cause incidents to be raised from within the Fujitsu Services Pathway estate.

A problem is an underlying cause that may or may have already resulted in incidents and potentially exists when a defect in the specification, design, production, implementation, or use of any of the service components results in any aspect of the service not meeting expectations.

A problem will be raised when the impact of the defect is substantial enough to warrant action to eradicate it. The problem will be closed when it has been agreed that the underlying cause has been fixed or removed.

3.11.2 Source of Problems

Problems arise from various sources within the Horizon operational estate and can be identified by customer representatives, Field Service Managers or Fujitsu Services Pathway staff managing and supporting the day-to-day operations of the Horizon estate.

POL identifies issues based upon feedback from within a number of their operational units. POL raise the potential problem via the Fujitsu Services Pathway daytime Duty Manager.

The units managing the day-to-day operations and support of the horizon estate escalate potential problems to the duty manager. The duty manager will decide if the issue in hand is to be treated as an incident, a problem or a major business continuity incident. This is usually decided based on the operational impact, severity and visibility of the issue.

FUJ00079888

The Field Service Managers (FSM) interface on a daily basis with the outlets and identify "problem" outlets from various sources such as trend analysis of incidents raised, feedback from outlets and POL. The FSM will arrange visits to outlets to interview the outlet staff and ascertain the scope of the issues within the outlet. Many of these issues are resolved within the FSM processes but those not resolved may require elevation to problem level. On such occasions these problems may be entered directly to the problem management database.

3.11.3 Resources

Problem management within Fujitsu Services Pathway is resourced from the various operating and service management units within Customer Service. Problems are allocated to individual problem managers depending on areas of knowledge and expertise, areas of responsibility and availability. The service managers who operate as duty managers in Infrastructure Services carry out this allocation

In addition there is a senior problem manager with normal problem management responsibilities plus specific tasks such as problem management skills development, mentor to service managers, monitoring problem updates etc.

There is a problem management database, which provides the basis for the recording and management of problems controlled by a database administrator

A database administrator has responsibility for general maintenance of the database, ensuring that problem managers submit updates, production of reports and ensuring that information on the database is available to POL.

3.11.4 Role of the Problem Manager

The role of the Problem Manager is to co-ordinate the resolution of a problem and act as a single point of contact for everyone involved with the problem. Essentially this is a management function.

The actions carried out to achieve the required outcome are: -

- Investigate and establish the facts

  Understand and evaluate all the information available.

- Define the problem

  Articulate and record the problem and success criteria

- Assess the impact and urgency

  Establish the impact of the problem on the customer and Fujitsu Services

- Establish responsibilities

  Identify the solution owner; agree actions, resources and contingencies.

- Monitor and report on progress

  Continually review/update reports on plans, actions and timescales.

FUJ00079888

- Escalate where necessary

  Escalate to Divisional or Corporate Alert when necessary.

- Evaluate success and close the problem

  Agree the successful conclusion and close the problem.

3.11.5 Key External Interfaces

As well as the ongoing day-to-day interfaces with other departments internal to Fujitsu Services Pathway, there are a number of external organisations that are crucial to the problem management function.

- POL

  Both Fujitsu Services Pathway as the supplier and POL as the customer have responsibilities for the delivery of a problem management service. It is crucial to the success of this service that Fujitsu Services Pathway and POL work together in all aspects of problem management.

  It is inevitable that there are occasions during problem investigation where it is not clear in whose area of responsibility a problem lies. It is essential that a clear understanding exist as to how information and knowledge will be shared on these occasions.

There is an agreement that sets out this working relationship between Fujitsu Services Pathway and POL for the problem management interface between POL (BSM) and Fujitsu Services Pathway Customer Service. (Ref. CS/IFS/008). This defines the interaction required between POL and Fujitsu Services Pathway when cross boundary problems are raised and reviewed.

The document defines: -

i. the individual and joint responsibilities of each party
ii. problem notification between POL and Fujitsu Services Pathway and between Fujitsu Services Pathway and POL
iii. problem acceptance
iv. problem control and status
v. review processes
vi. escalation
vii. potential MBCI's
viii. agreed priority levels

FUJ00079888

- ISD

  As a key service supplier for Fujitsu Services Pathway to the Horizon outlets ISD has a crucial role to play in the resolution of problems.

  There is an agreement that sets out this working relationship between Fujitsu Services Pathway and ISD for the problem management interface between ISD Service Management and Fujitsu Services Pathway Customer Service. (Ref. CS/IFS/009). This defines the interaction required to identify, raise and manage problems across the two divisions.

  The document defines: -

  - the individual and joint responsibilities of each party
  - problem types
  - problem control and status
  - review process

- Other

  There is, on occasions, a requirement for Fujitsu Services Pathway to interface with other third party suppliers either directly or via POL or ISD in relation to Problem Management. These third parties are contracted to Fujitsu Services Pathway, POL or ISD and the interface is by the appropriate route and subject to the terms of the contract.

  Examples are Energis, BT, Escher, Tivoli, Cap Gemini etc.

3.11.6 Review Processes

- Cross-Domain Problem Management Forum

  The cross domain problem management forum is held monthly prior to the Horizon Service Review Forum (HSRF) and is intended to highlight and discuss any problems that are cause for concern and may be discussed at the HSRF.

  Either party can identify specific problems to be included in the agenda and also deals with process issues and progressing outstanding actions.

- Post Implementation Review Meeting (PIR)

  A PIR is carried out if the Problem Manager on either side is unhappy with the way a problem is resolved or managed. The PIR reviews the way the problem was handled and looks to highlight the areas that did not operate well and require improvement, either within the operation of the process or the process itself.

  The output of the PIR is to initiate improvement actions to ensure that the process is operated as it should be or ultimately improved.

FUJ00079888

Any action points arising from a PIR will become agenda items at the Gross Domain Problem Management Review Forum.

3.11.7 Documentation

The following documents are specific to the function of Problem Management: -

CS/PRD/021	Fujitsu Services Pathway Problem Management Process.
CS/PRO/063	Fujitsu Services Pathway Customer Service Problem Management Procedure.
CS/PRO/110	Fujitsu Services Pathway Customer Service: Problem Management Database Procedures.
CS/IFS/008	Fujitsu Services Pathway/POL Interface Agreement for the Problem Management Interface.
CS/IFS/009	Fujitsu Services Pathway/ISD Interface Agreement for the Problem Management Interface.
CS/PRD/101	Incident Management for Virus Alerts

The following documents are associated with the function of Problem Management: -

CS/QMS/001	CS Policy Manual.
CS/QMS/002	CS Process Manual.

3.12 New Service Introductions

The purpose of the CS Service Introduction Team is to support Fujitsu Services Pathway Customer Service in the introduction of new facilities and changes to the existing Fujitsu Services Pathway solution. The prime functional units are:

- **Change management**
  Responsible for the management of Change Proposals within Customer Service. Responsible for the scheduling of changes to the Fujitsu Services Pathway Live estate.
- **Service Introduction**
  Responsible for ensuring that Customer Service is prepared for new services being introduced to the Fujitsu Services Pathway solution.
- **Major release Implementation**
  Responsible for the organisation and successful completion of major upgrades to the live estate.
- **Release Management (RM)**
  Responsible for the release of software changes to the live estate.

FUJ00079888

- **Release budget Management**

  Responsible for providing an estimation of costs for running a live service including the new service.

  Responsible for providing an estimation of costs for the implementation of software changes and the subsequent actuals.

3.12.1 Change Management

This section of the document describes the role that the Service Introduction Team plays in Change management.

The aim of the unit is to ensure that all changes to the estate are managed in a controlled way through Customer Service.

More specifically the unit has responsibilities to:

- Manage CPs through Customer Service
- Schedule changes to the live estate via the RATS forum
- Liaise with the rest of Fujitsu Services Pathway on any potential changes forecast
- Interface with the ISD Operational change process

3.12.2 Manage CPs through Customer Service

The unit is responsible to the programme for all changes from a Customer Service viewpoint by gaining an impact view from all units within CS and reviewing those impacts on a weekly basis. Ensuring that CPs submitted by CS staff meet the required criteria and are targeted at the correct release date.

3.12.3 Change timetable

Weekly CS change review meetings are held and are attended by management representatives from Infrastructure Services, Operations and Service Introduction. The objective of these meetings is to review the latest position regarding CPs on the PCCB agenda and ensure that all impacts and actions are completed. No minutes are produced for these meetings.

The output from these meetings is reported at the weekly Project Change Control Board.

3.12.4 Change management administration

The operations support team is responsible for the following processes with change management:

- Registration of change proposals (CP) from within Fujitsu Services Pathway that require impacting by Customer Service staff or/and their suppliers.

FUJ00079888

- The collation and filtration of all impact statements and the response to Change Management with the impacts in a timely manner.
- Reception of supplier change proposals (SCP) for impact within Fujitsu Services Pathway
- Tracking of approved CP action through to implementation or completion
- Management of actions arising from CP impacting and approval processes
- Production of change management MIS reports specific to Customer Service and its suppliers

All CPs or SCPs raised within Customer Service are managed by the operations support team. The team is the prime interface between Customer Service and its suppliers into the Fujitsu Services Pathway change management system. All CPs or SCPs are recorded onto the CP database and managed through its lifecycle from a Customer Service viewpoint.

CPs are issued daily at various priorities and the team identifies who within CS or its suppliers needs to provide an impact statement. The impact statements are chased and then collated into a CS response, these are provided to CM for review by the PCCB.

3.12.5 Schedule changes via RATS

The RATS forum is a regular meeting held between the Service Introduction Team; Operations and Support and various other parts of Fujitsu Services Pathway, including representatives from Development Directorate.

The aim of the forum is to ensure that all changes to the live estate, outside of a major release, are scheduled and hence implemented in a controlled manner. Where possible changes are grouped together to minimise the number of changes on the live estate and to obtain efficiencies in testing.

The following items are considered during scheduling:

- Business impact and hence urgency of the change
- Dependencies on the change
- Grouping with other changes
- Implications for testing

CPs that are targeted at an interim Fujitsu Services Pathway release are also discussed at the forum. The aim of the forum is to identify a potential time when the CP can be implemented to live and agree or otherwise that the CP can go ahead at the targeted release. For the scheduling of CPs, and agreement that a CP can be implemented during a specific interim release the following items are considered:

- All impacts supplied on the CP

FUJ00079888

- Potential delivery dates of software changes from Development
- Additional hardware procurement
- Business impact and hence urgency of the change
- Dependencies on the change
- Grouping with other changes
- Implications for testing

Once the scheduling of a CP has been considered an impact from RATS is entered on PVCS.

The Release Management Team performs the administration of the RATS forum. This activity includes:

- the selection of CPs for discussion
- bringing forward all other items for scheduling
- updating the CPs with the result of the forum
- updating the other relevant control system with relevant details

3.12.6 Potential changes

The unit has a responsibility to liaise with the other Fujitsu Services Pathway units regarding potential changes that are under discussion for implementation.

This is to ensure that any planning is realistic in terms of implementation on the live estate.

3.12.7 Operational change

An operational change process (OCP) is also in operation. This process covers changes required to the live operation and provides an audit trail for all changes made to the operational estate that are made outside of the Release Management process. The OCP service is managed and run by ISD on a daily basis. The Service Introduction Team is responsible for the management processes within CS for this service and any service developments.

The SSC has access to the live system, which can be used to correct data on the system when this has been corrupted in some way. The procedure for doing this is controlled via an OCR.

The SSC ensures that the relevant control systems are kept current and administration activities required by managers within Customer Service are met.

3.12.8 Service Introduction

This section of the document describes the role that the Service Introduction Team plays when a new service is required of the operational system.

FUJ00079888

When a new service is required to become part of the live operational service there are a number of activities that need to be undertaken with Customer Service to ensure the implementation is smooth and complete. These activities are co-ordinated by the Service Introduction Team.

3.12.9 Major activities

The major activities involved in the area:

- Ensure all of Customer Service and its suppliers are aware of the new service requirement
- Liaise with the main Fujitsu Services Pathway project manager for implementation of the new service to ensure Customer Service concerns and requirements are met
- Ensure the various units with Customer Service and its suppliers are aware of any requirements on them from the new service
- Ensure the various units with Customer Service and its suppliers are ready to meet any additional requirements on them from the new service
- Produce and agree a service introduction plan
- Collate revised costings for running the new operational services

3.12.10 Major Release Implementation

This section of the document describes the role that the Service Introduction Team plays in the implementation of a major new release.

When the Fujitsu Services Pathway programme plans a major new release it is the responsibility of the Service Introduction Team to manage the implementation of that release to the live estate. This involves a number of activities that are not necessarily all done by the same individual:

- Agreeing the implementation dates
- Liaising with POL
- Production of implementation plan
- Production of Release notes and strategy documents
- Accepting handovers from PTU and TDA
- Organising the actual upgrade slots and their manning
- Post upgrade activities

3.12.11 Implementation dates

The actual implementation dates for a major release are documented at the high level on the Programme Plan.

FUJ00079888

The Customer Service implementation plan and Level 3 plan should ensure the dates on the Programme plan are correct.

The dates and timings of the upgrade are agreed with POL; ISD; SMC; MSS and Development Directorate.

Any conflict in dates with other activities is resolved between the various parties. Conflicts should be easily identifiable on the CS Management plan.

3.12.12 Liaison with POL

There are numerous levels of communication with POL relating to any specific major release implementation. These are detailed below:

3.12.13 Release migration strategy

This document is produced by SIT and is based on the migration strategy produced by the TDA. It should be approved by the manager of CS and be agreed with the customer prior to the upgrade. There is normally one version for the counter and one for the data centre if this is appropriate.

3.12.14 Release Note

This document is produced by SIT and is based on the Release note provided by PTU. It should be approved by the manager of CS.

3.12.15 Post upgrade report

This document is produced by SIT and is based on the experience of the upgrade and the first two weeks running following the upgrade. The manager of CS should approve it. There is normally one version for the counter and one for the data centre if this is appropriate.

3.12.16 Support Notice

This document is produced by SIT and is based on the arrangements for the upgrade. It should be approved by the manager of SIT.

3.12.17 Release authorisation

Release authorisation can take one of two formats depending on the size of the release.

- Small releases

  For small releases no formal criteria is defined. POL sign off the release to live via an email based on the contents of the Release Note; migration strategy and discussions regarding the status of the release.

FUJ00079888

- Large releases

For large release formal release authorisation criteria are agreed and reviewed on a regular basis prior to the upgrade. These criteria work on a traffic light system and criteria can be set against Fujitsu Services Pathway and other POL suppliers e.g. OpTIP.

3.12.18 Status reviews

Regular meetings are held with POL to review the status of all the planned upgrades.

3.12.19 Implementation plan

An implementation plan is produced by SIT to cover all activities required to complete the upgrade.

The plan itself covers all activities, both pre and post upgrade, to ensure that all requirements are met and all dependencies are recognised.

The plan is based on the migration strategy that is produced by Development Directorate. The plan is reviewed on a regular basis with all parties taking part, or interested in the upgrade.

3.12.20 Documentation

Most of the documentation produced has been covered in the adjoining sections. A few additional documents are covered here. These are for internal Fujitsu Services Pathway use only.

3.12.21 Support Notice

This document is produced by SIT and is based on the arrangements for the upgrade. It should be approved by the manager of SIT and covers all internal contacts.

3.12.22 Authorisation criteria

Release authorisation can take one of two formats depending on the size of the release. This criteria controls the handover from Development Directorate to Customer Service.

- Small releases

For small releases no formal criteria is defined.

- Large releases

For large release formal release authorisation criteria are agreed and reviewed on a regular basis prior to the upgrade.

FUJ00079888

3.12.23 Handovers from PTU and TDA

A number of formal handovers are required from other parts of Fujitsu Services Pathway into Customer Service before the release will be authorised for live usage.

3.12.24 Release Note

A Release note is provided by PTU to documents the contents and outstanding issues with the release.

3.12.25 Sign off

A sign off form is received from PTU to confirm that the release is tested and ready for release to the live estate.

A separate sign off may be provided for the counter and data-centre part of any upgrade.

3.12.26 Migration strategy

Development Directorate provides a migration strategy. It provides details on the method to be used for migrating the live estate.

3.12.27 Actual upgrade

The major activities involved in the upgrade are split between the data centre and counter. The activities are very dependent on the content of the actual release. The order for release is documented in the Release Note provided by Development Directorate.

3.12.28 Post upgrade activities

A number of activities are often left until the main part of the data centre upgrade is complete. The activities are very dependent on the content of the actual release. The order for release is documented in the Release Note provided by Development Directorate.

3.12.29 Release Management

This section describes the operations performed by Customer Service Release Management team. The CS Release Manager (CSRM) is responsible for authorising changes to the live Horizon environment.

The following procedures are described:

- Deciding whether a software fix should be developed
- Defining the release plan and time scales
- Managing the delivery of supporting services

FUJ00079888

- Creating the software fix
- Re-raising a release note
- Authorising the software fix
- Completing the release process

3.12.30 Deciding whether a software fix should be developed

This section describes how Fujitsu Services Pathway CS decides if a fix should be implemented for a problem.

1. Fujitsu Services Pathway CS holds a Release Management Forum weekly to decide what fixes should be created and to assess the impact of any associated risk. Representatives of each unit involved in the software release process should attend the RMF meeting as follows:
   - System Support Centre
   - Fujitsu Services Pathway Development
   - Operational Test Team
   - Configuration Management
   - Customer Service
   - Fujitsu Services Outsourcing
   - Other units as required

   The SSC represents the customer in the RMF in terms of the calls made to the helpdesks. The Service Managers know of other problems that are significant to the customer, through parallel escalation processes. The Service Managers feed their knowledge into the RMF through the CSRM
2. The CSRM sends a list of all outstanding open calls to each member in advance of the RMF meeting, allowing the attendees to identify their requirements.

   The calls are cleared calls, that is, have a corrective action in place and are awaiting closure, either because the decision has not been made whether to create a fix, or the decision has been made to create a fix and it has not been completed
3. Each attendee brings with them information about the dependencies, priorities, risks, issues, alternative options and time scales for the open PinICLs. It may not be possible to estimate how long certain activities will take until the priorities have been agreed, therefore, some information may not be available until after the RMF meeting

FUJ00079888

4. The open calls are discussed, with the information provided by the members. For example, details of any workaround and business impact, until the situation is understood. Then the RMF decides whether a release is required

5. If SSC consider a problem too urgent to wait for the weekly RMF meeting, it requests the CSRM to fast track the fix.

   The CSRM assesses the situation and, based on the priorities of each unit, the risk of releasing the fix, the alternative options, any dependencies between fixes and any other issues, decides either the problem can wait until the weekly RMF meeting or agrees to a fast track solution.

   If the fix is fast tracked, the CSRM holds a virtual forum by taking the release request to each RMF member (in person or by phone, fax or PinICL) for input and sign off. The activities in the high level plan are reduced to a minimum before the release and the rest of the activities, for example, documentation, are carried out after the release has been made.

   In an emergency, the following people can authorise a fix to be produced without contacting the CS Release Manager:

   - SSC Manager
   - CS Operations Manager
   - Problem Manager

   If this happens, the person authorising the fix ensures that the CS Release Manager is informed so that the release process can incorporate the fix.

   Where an emergency fix has been applied to get systems up and running, release management processes may be applied retrospectively

6. If the RMF decides not to develop and release a fix, one of the following actions takes place:

   (a) The RMF decides that a live problem can wait until the next major software release. In this case, the CSRM clones the call on the new release and returns the call on PinICL to EDSC.

   (b) If the original is not a live fault it is up-versioned and returned to Gen Dev.

   (c) The RMF identifies the call as not being a problem at all, that is, the perceived shortfall is the way the system was designed to work. RMF returns the call to the originator so they can raise a change request for an enhancement to the system

   (d) If rejection is considered to have significant impact to the customer, the CSRM escalates the problem to Strategic Services before authorising closure of the call

Note: Fourth line support PinICLs include problems that are not in the current live environment. These are not relevant to the release management process and are managed by development. However, if a fourth line support PinICL identifies a

FUJ00079888

problem in the current release, the RMF decides whether or not to postpone the fix.

3.12.31 Defining the release plan and time scales

Once the decision has been made to create a fix; the following issues may need to be taken into account.

1. Any dependencies between calls
2. Any situations where a new release will run in parallel to an old release before the old release is upgraded.
3. The priority of each fix according the different needs of each CS unit.
4. CSRM updates the report for POL, for which they are currently responsible, with the expected completion date to resolve the call
5. For most releases, the delivery date is not significant. The release is simply distributed at the earliest convenient time. For releases that have a significant date line, the following steps are taken:

   - Each unit involved in the release provides details of the time scales in which they can complete the required work
   - All parties involved agree to a high-level plan for each release

   The CSRM is responsible for determining the availability of the Operational Test Rig. and co-ordinating the allocation of users to it.
6. The CSRM:

   (a) Creates a software fix release note

   (b) Captures all the information and raises a release PinICL for each release.

   The Release PinICL references all the PinICL calls (or HSH / SMC calls) that it covers and each original PinICL call is updated with the new Release PinICL number. Progress queries on the original PinICL calls are found by reference to the software fix release note attached to the new Release PinICL

   (c) Attaches the release note to the PinICL and sends it to PIT
7. The manager for each unit updates the release PinICL with details of their progress
8. The CSRM monitors the progress of the software fix release note by accessing the release PinICL and manages any deviations from the high-level plan to ensure that all units are aware of the delay and the impact can be minimised. The CSRM does this by negotiation with the different units in the release process both in and outside of the RMF.

   If necessary, the CSRM escalates problems to Service Management

FUJ00079888

Notes:

1. The CSRM owns the plan
2. A release PinICL is a different kind of PinICL to those used by SSC so that it is not counted in problem statistics

3.12.32 Managing the delivery of supporting services

Other units may be involved in the release process who are not part of the normal RMF, for example, training, helpdesks, documentation, bench-marking, hardware installation. In most cases fixes will not affect these units, but, if any of these units are involved, the CSRM co-ordinates their activities, identifying any testing requirements and receiving notification from the units when their preparation are complete, as follows:

- For HSH and SMC: notification of operational readiness
- For documentation: notification of completion of update, and the documentation itself, so that CSRM can distribute it
- For hardware: notification of operational readiness.
- For user training: notification that the training material is ready, trials of the material are scheduled on the Operational Test Rig, training is delivered where necessary

Provided that all the supporting preparation is complete, CSRM sign off the release note.

Note that the time taken for the distribution of the documentation has to be taken into account in the delivery schedule of the release.

Most fixes do not normally affect any of these other units.

3.12.33 Creating the software fix

Fourth line support creates the fix and the Tivoli installation scripts, and unit tests and documents the fix. Any fixes that fail testing must be recreated.

Fujitsu Services Pathway development complete the release note with details, such as the affected estate, and send it via PinICL to Configuration Management. If external fourth line support is involved, Fujitsu Services Pathway development manage them and complete the release note on their behalf.

3.12.34 Re-raising a release note

A software fix could fail in LST or it could be applied in the wrong way. When a failed fix is investigated and the content of the release is found to be at fault, then one or more new work-packages are developed. CSRM withdraw the original software fix release note and raise a new one to cover the new work-package(s).

FUJ00079888

3.12.35 Authorising the software fix

The CSRM authorises the software fix release, having:

1. Ensured that all testing and preparation is complete
2. All sign offs have been attained.

3.12.36 Completing the release process

1. Either ISD/SMC or ISD Service Management distributes software. After the software has been distributed, CSRM receive notification of the success or otherwise of the release:
   - If ISD/SMC or ISD Service Management confirm the successful release of the software, CSRM receive the release PinICL from CM. If the delivery was only to the pilot estate, which may be the case for high risk fixes, CSRM authorise the full delivery to go ahead
   - If the distributing unit report problems with the distributed software, CSRM may authorise the regression of the release. (Regression means withdrawing the software fix that had been installed)
2. Provided that the release is successful, CSRM sign off the release note as complete. CSRM then close the release PinICL.

3.12.37 Work Instructions

A set of work instructions complement the processes above. They are held on the Customer Service V drive with an index at v:ReleaseMgt\CSRM Working Documents\DocPlan_Index_1

3.12.38 Software Distribution Service Review

A review is held on a monthly basis with the unit providing the software distribution service.

3.12.39 Release budget management

This section of the document describes the costs that are maintained by the Service Introduction Team.

Costs associated with service introduction are collected in several places:

1. When the Fujitsu Services Pathway programme is discussing new business opportunity it is the responsibility of the Service Introduction Team to manage the estimation of the costs associated with:
   - implementation
   - subsequent live running of the new service.
   - other CS involvement e.g. SLA measurement changes

FUJ00079888

a. When the Fujitsu Services Pathway programme plans a major new release it is the responsibility of the Service Introduction Team to manage the costs associated with the implementation of that release to the live estate. Estimates are made prior to the implementation and actuals are produced after the event.

b. When the Fujitsu Services Pathway programme plans a new service it is the responsibility of the Service Introduction Team to manage the estimation of the costs associated with the live running of the new service.

c. When an interim counter fix is applied to the live estate in isolation (i.e. with no other fixes going at the same time) the actual ISDN line charges are found out and recorded.

3.13 Management Support

3.13.1 Business Support

- EPOSS and APS reconciliation

  Reconciliation incidents may arise for a number of different reasons. In most cases there is a mismatch between the information held in different parts of the Fujitsu Services Pathway system. The task of the Business Support (BS) section is to investigate and financially resolve reconciliation incidents. If a similar reconciliation incident occurs a number of times, the BS team identifies it as a problem incident to be managed through the problem management process.
  Possible incidents that may occur are:

  - Unmatched transaction reversals
  - Transaction rejection by TIP
  - Incidents raised by clients
  - Incidents raised by customers
  - EPOSS counter reconciliation report errors
  - APS reconciliation reports

  The Business Support Analyst investigates Business Incidents.

- Daily APS and EPOSS reconciliation report retrieval and checking

  Following the implementation of release CSR+, the full set of APS and EPOSS reconciliation reports are delivered automatically to the appropriate folder held on the MIS Client PC situated within MSU. These reports are available daily before 08.00hrs. In the event that a system problem prevents this automatic process from being completed, both APS and EPOSS reports will be extracted from central systems by CS / SSC and delivered to CS /MSU daily via e mail to be available before 08.00hrs.

FUJ00079888

The Business Support Analyst will retrieve and analyse the reports daily. If any errors are present on the reports, these will be investigated and any incidents and queries will be identified and reported to POL.

- Investigating reconciliation incidents

  This section describes the general procedure that the BS follow to investigate all types of reconciliation incidents. The BS:

  1. If an error has been identified, the Business Support Analyst will raise and log a call. This call will provide a unique reference number. This log will also provide a PinICL, which will detail the error on the report.
  2. Business Support Analyst will raise a Business Incident Management Service Report (BIMS) including details of the rejected transaction. Where applicable a Manual Error Report (MER) is issued.
  3. SSC are notified of the error via the PinICL and they will investigate the reason for the transaction rejection/error by checking the transaction details for invalid or corrupted fields.
  4. SSC provide the BS team with the correct details using the PinICL and entering the findings onto BIMS.
  5. This BIMS report is issued to POL on a daily basis at the end of the business day.

- Dealing with recurring reconciliation incidents

  This section describes the procedure to deal with recurring reconciliation incidents.

  This procedure is jointly carried out by the BS Team and the Customer Service Problem Manager (CSPM). The CS Problem Manager investigates the incident after the Management Support Unit has dealt with the financial reconciliation.

The procedure is as follows:

1. If the same or similar reconciliation incident occurs more than once, the BS team reports it as a problem incident to the Customer Service Problem Manager (CSPM) by sending an email requesting investigation of the incident.

   The email contains details of the type of incident and the PinICL reference number. In addition, the BS team passes hard copies of all similar incidents to the CSPM.

2. The CSPM progresses the incident investigation after the BS team has carried out financial reconciliation. The BS team requests a response time from the CSPM of less than two weeks.

FUJ00079888

3. The CSPM sends a progress report detailing the findings of the investigation to the MSU on an agreed date.
4. On receiving the progress report, the MSU updates the existing System Incident Log (SIL).
5. If POL or the Horizon System Service Manager (HSSM) request further investigation of the problem incident, the MSU issues an updated System Incident Log (SIL) report to POL and HSSM for information.

Invoicing: If a MER is issued to supply details of missing or erroneous transactions, Pathway are liable for an agreed charge. MSU manager and POL agree on a monthly basis the level of this charge based upon the number of MER's issued. If agreement cannot be reached between the two parties, a Case Law referral form is completed by the MSU manager and passed to Pathway Commercial for discussion and agreement with the POL counterpart. The subsequent decision is then used as a precedent for similar incidents, which may occur.

- Dealing with reconciliation enquiries

  Enquiries resulting from POL being unable to complete a reconciliation of the Fujitsu Services Pathway reports to their internal totals are referred to the Horizon System Helpdesk.

  The Helpdesk logs the call and provides a call reference number. If the query is resolved during this initial call, the Helpdesk closes the call.

  If the Helpdesk is unable to resolve the query, it passes the call to the Fujitsu Services Pathway BSU reconciliation team who take over ownership of the call and communicate directly with POL to resolve it.

  The reconciliation team logs all the calls that they receive requiring investigation as reconciliation queries and maintains a full audit trail.

- Archiving the reports

  Customer Service hold electronic copies of all reconciliation reports for seven years and are able to provide copies of any reconciliation report or file on request within this period.

- Monitoring and Managing Customer Satisfaction

  The MCVP process is being reviewed while Fujitsu Services Pathway work with the POL to decide how they wish to progress this activity.

- MCVP

  To monitor the users' perception of Fujitsu Services Pathway's post-implementation services, the Management Support Unit manages the Management Care Visit Program (MCVP) - a monitoring program implemented to ensure Fujitsu Services Pathway fully understands the Post

FUJ00079888

Masters view of our service. The MCVP involves senior Fujitsu Services Pathway representatives visiting selected post offices and collecting feedback using a predefined interview pack. It is expected around 500 outlets per annum will be visited.

- Training

  Before the interviewers have any contact with the post offices, the Management Support Unit-Business Support Manager will:

  1. Explain the purpose and the goals of the MCVP.
  2. Go through the interview procedure and questionnaire in detail.
  3. Present all other relevant documentation.
  4. Answer any questions and addresses any concerns raised by the interviewers.

  All interviewers will be briefed to inform them that each interview must follow a standard procedure so that the results can be fairly compared and a true analysis obtained.

- Preparations and documentation

  The interviewers will be sent electronic copies of relevant documentation, plus hard copy interview packs containing all relevant reference documentation. The interviewers maintain the interview packs as necessary and take them to interviews. The interview pack contains:

  - Procedure document (including the Interviewer's Summary Guide)
  - Phone script
  - Sample forms
  - Other documents that the questionnaire refers to
  - Questionnaire
  - List of post offices to contact

  The interviewer will then arrange interviews at the Post Office Outlets allocated to them, attend and conduct the interview and complete the MCVP report.

- Service Visit Records

  In addition to the MCVP the Management Support Unit also runs the Service Visit Reply card process, which is used to monitor the service performance achieved by Fujitsu Services engineers who visit outlets to conduct remedial or change activity.

FUJ00079888

Through this process Post Masters are able to comment on the quality of the service provided by an engineer during his visit, including any related contact to the Horizon System Helpdesk (HSH).

- Routine monthly analysis

  The Business Support Unit carries out an initial analysis of the returned cards and pick out any issues needing immediate action. Having done this, the cards are then passed to the Management Support Unit for monthly analysis and formal reporting purposes. Generally reports cover:

  - The percentage of feedback cards returned compared with total visits made. Fujitsu Services System Service provide the number of total visits made.
  - The percentage of positive and negative responses by question.
  - Comments on key areas of satisfaction or dissatisfaction.

3.13.2 Service Performance

The efficient provision of information to the customer, Fujitsu Services Pathway and ICL / Fujitsu staff about the performance of the Fujitsu Services Pathway system is a key part of the Service Performance component of the Fujitsu Services Pathway solution. This activity is managed by MSU in Fujitsu Services Pathway Customer Service, with emphasis placed on the following specific areas:

- The monitoring of service performance (in accordance with Service Level Agreements, where applicable), raising and in some cases resolving any issues arising there from
- The support of the activities of the CS organisation and the broader Pathway Fujitsu Services organisation through the provision of management information(MI) on both a regular and ad-hoc basis
- To support Post Office counters Ltd (POL) through the provision of information on an ad hoc basis

  In practical terms, this is achieved by means of a number of clearly identifiable data extraction, processing and reporting activities that can be categorised according to the nature of the requirement, i.e. what they are driven by:

- Legislative obligations
- Contractual obligations
- Good business practice
- Issue management and investigation

  For the most part, these activities are periodic (daily, weekly monthly or quarterly) but some are event driven. The following table identifies the

FUJ00079888

specific deliverables according to frequency and associated activities that help monitor service performance:

Activity	Driver	Frequency
Service Performance Report	MI	Weekly
Service Review Book	Contract	Monthly / Quarterly
Vital Statistics Report	MI	Monthly
Business Incident Management Report	Contract	Monthly
SLA Remedial Calculations	Contract	Quarterly
Ad Hoc Query	Customer	As Req
Outlet Data Maintenance	MI	Daily
Powerhelp Data Extraction	MI	Daily
HSH Performance Reporting	MI	Daily
Non polled Outlet Reporting	MI	Daily
YG Pilot Rollout Programme Monthly Report	Customer	Monthly
YG Daily Call Statistics	MI	Daily
YG Weekly Call Extraction	MI	Weekly
YG Weekly Transaction Extraction	MI	Weekly
Benchmarking	Contract	Monthly
OBCS Volumes & Values	MI	Monthly
Daily Call Volumes	MI	Daily
Slow Running Report (AHQ 317)	MI	Weekly
PDA Transaction Volume (Report 202)	MI	Monthly
AP Monthly Transaction Volume (Report 344)	MI	Monthly
Data Extraction and Maintenance • Non Polling Outlets • Restarts • All Calls	MI/Customer	Daily/Weekly or as required
Field Service Manager's Weekly Report	MI	Weekly
Field Service Manager's Monthly Report	MI	Monthly

FUJ00079888

- Producing and scheduling MIS reports

  The Service Performance team produces MIS reports that measure and monitor system and business performance. This is done on a regular or adhoc basis, as can be evidenced in the table above.

- Ad hoc report queries

  This section describes how MSU deals with ad hoc report queries in a controlled manner to provide a response within five working days. Requests for ad hoc reports come from a single point of contact within POL Service Management, or internally from departments within Fujitsu Services Pathway

  The procedure is completed by one of the MSU Information Analysts as follows:

  1. When MSU receives an ad hoc report query, (via the Ad Hoc Query Mailbox) on an *Ad Hoc Query Request Form*, the analyst updates the *Ad Hoc Query Database* with details of the request and issues an immediate confirmation of receipt by return of e-mail. The Analyst will also estimate the length of time the report will take to produce or advise if the information cannot be supplied.
  2. The Ad Hoc Query Database enables MSU to control the requests that it receives. If an ad hoc report is requested on a regular basis the Analyst asks the requestor to confirm the frequency with which the report is required and if the expectation is that the report is to continue, MSU will request the originator to raise the appropriate Change Request documentation.
  3. If the Analyst estimates that the ad hoc report will take longer than 5 days to complete, agreement with the requestor is sought for an extension to the timescale. This is confirmed by e-mail via the Ad Hoc Query Mailbox.
  4. When the report has been run and the results sent to the requestor, or if the requestor cancelled the request, the Analyst will close the request and file details of the report within the Ad Hoc Query Database

- Service Review Book

  The Service Review Book (SRB) is a monthly document that reports on service performance for the previous calendar month. It is issued to Post Office Networks (POL) and Fujitsu Services Pathway Management.

  The SRB has two issues, a data only version - to be issued on the fifth working day of each month, via e-mail, and a data & comments version - to be issued on the tenth working day of each month, via e-mail.

FUJ00079888

Each end of POL quarter (Feb, May, Aug, Nov), as well as producing the data for that month, quarterly data is also produced.

This report identifies key areas within the Horizon solution and analyses volumetrics and service performance information, in line with the Contract.

The MSU Information Analysts complete the report.

1. Obtain Transaction volumetrics from the Data Warehouse using the Business Objects reporting tool for the applicable transaction streams requiring analysis. Obtain Help Desk call details and volumetrics from the Powerhelp system or local databases using either the Business Objects reporting tool or Access queries. Obtain System Service calls from local database. Obtain Training information from Strategic Services Team. Obtain Business Incidents from Business Support Team.
2. Analyse the information retrieved according to the requirements of the report.
3. Present the data in the agreed manner – either in tabular or graphical format.
4. Alert respective departments within Fujitsu Services Pathway of any adverse performance noted.
5. Pass the completed report sections to the Intranet Administrator to place into the Customer Service Intranet site.
6. Issue email copies of the report to the Management Team and POL Management.

- Weekly Service Performance Report Production

  MSU publishes a Weekly Service Performance Report for the Fujitsu Services Pathway Management Team and others (on a need to know basis.) This report contains data one week in arrears to enable the data to be collected from the outlets. Wherever possible though, an up to date position is reflected within this report. A reporting week is from Sunday to Saturday.
  This report identifies key areas within the Horizon solution and analyses volumetrics and service performance information.

  The MSU Information Analysts complete the report.

  1. Obtain Transaction volumetrics from the Data Warehouse using the Business Objects reporting tool for the applicable transaction streams requiring analysis. Obtain Help Desk call details and volumetrics from the Powerhelp system or local databases using either the Business Objects reporting tool or Access queries.
  2. Analyse the information retrieved according to the requirements of the report – these
     are ongoing and can change week on week.

FUJ00079888

3. Present the data in the agreed manner – either in tabular or graphical format. Include a
written analysis of any trends and observations.
4. Alert respective departments within Fujitsu Services Pathway of any adverse performance noted. This should be completed via the PinICL system.
5. Pass the completed report sections to the Intranet Administrator to place into the Customer Service Intranet site.
6. Issue hard copies of the report to the Management Team or others as requested.

- Service Level Agreements

  The following sections describe how MSU monitors and maintains Service Level Agreements for all Fujitsu Services Pathway contracts that are under formal change control.

- Maintaining Service Level Agreements

  Fujitsu Services Pathway stores and maintains service performance measures and related data within a software application called the Service Level Contract Administrator (SLCA). MSU maintains all parameters that relate to the service levels on the SLCA via File Controller access.

  MSU uses the SLCA to:

  - Raise a CP for a change of service performance measure agreed between customer, Fujitsu Services Pathway and associated supplier
  - Change parameter values via the *Maintain performance measure* facility in the SLCA
  - Change the effective 'from date' for all changes made
  - Log changes using the audit module within the SLCA application giving cross-references to the changes
  - Check that the electronic changes are reflected within the commercial contracts of the Customer, Fujitsu Services Pathway and associated supplier

  MSU uses the SLCA for manual update to:

  - Enter details from source data in the format and structure defined in the contract standing data application
  - Validate data before input and after input before commit
  - Log changes using the audit module within the SLCA
  - Retain all source data used as input for audit purposes
  - Input manual performance measures source data in the required time-frame for the period under review

FUJ00079888

- Monitoring Service Level Agreements

Fujitsu Services Pathway has responsibilities to demonstrate to its customer that it:

- Monitors service delivery in all areas where performance measure criteria exist
- Applies service management at all levels with alerts raised where service falls below expectation

SLA conformance information is obtained from the Data Warehouse, MSU developed databases and information supplied from the Pathway suppliers. Following is a list of data gathered or generated by System Performance:

- HSH Telephony: Conformance information calculated by ISD and delivered to MSU daily
- HSH Call to Resolution: Call details obtained by ISD and delivered to MSU daily where conformance is calculated
- System Service: Call details obtained by ISD, amendments to call duration are calculated by ISD and supplied to MSU on a daily basis where conformance is calculated
- Data File Delivery: For all Data File Delivery SLAs, MSU run queries against the Data Warehouse. These are:
  - APS / OBCS / TPS / APS Client
  - APS Ref Data / OBCS Stops / Ref Data
  - LFS

- Business volumetrics

The Fujitsu Services Pathway programme is significantly affected by the level and variance of business volumetrics. The baseline for volumetrics is the reference source of the Workload Brief, subsequently updated and maintained as the Workload Compendium. This is a customer-owned document from which the Service Performance Unit generates enhanced supporting business volumetrics on behalf of Fujitsu Services Pathway.

The outputs from this impact analysis are the prime source of data for planning and sizing activities carried out by the Fujitsu Services Pathway development teams and by Fujitsu Services Pathway's suppliers.

When a new version of the Workload Compendium is issued, the Service Performance Unit carries out an impact analysis on any changed areas. If the level of change in any area is greater than 5%, the Service Performance Unit notifies the Fujitsu Services Pathway Director, Finance and Commercial to enable contractual variance analysis to be carried out and provides associated impact analysis data.

FUJ00079888

Supplementary impact can arise from changes to supplier-related volumetrics as described in the following sections. They are dealt with and processed in the same manner as changes to the Workload Compendium.

After carrying out the impact analysis of any changes, the Service Performance Unit updates the Fujitsu Services Pathway Business Volumetrics portfolio. This portfolio is the means by which business volumetric changes are communicated to Fujitsu Services Pathway.

Implementing business volumetrics processing is described in associated work procedures and instructions held by the Service Performance Unit.

- Horizon System Helpdesk volumetrics

  The Service Performance Unit maintains Horizon System Helpdesk (HSH) call volumetrics. The HSH volumetrics model provides data about HSH call volumetrics during the whole life of the Fujitsu Services Pathway system. In particular, it produces daily and monthly analyses.

  The outputs from the model are a main source of data for planning and commercial use by the HSH supplier as well as for sizing activities by the Fujitsu Services Pathway development teams.

  The key input parameters that contribute to re-appraisal of the HSH call volumetrics model and result in a new issue of the model are changes to:

  - Workload Compendium
  - Horizon plan
  - Fujitsu Services Pathway commercial model
  - System MTBF parameters

  Less significant changes that result in reappraisal of the HSH call volumetrics model and result in an update to the current model are:

  - Minor adjustment in roll-out programme profile
  - Correction to key commercial ratios
  - Minor update to Fujitsu Services Pathway commercial model
  - Minor changes in Workload Compendium
  - Minor changes in Horizon plan

  In addition to the above, MSU and the HSH Manager hold a quarterly review of the key ratios relating to inappropriate calls handled by the HSH. Where they agree, they adjust the key ratios accordingly and release a new version of the current HSH model.
  Before releasing a new version of the model, either within Fujitsu Services Pathway or externally, the Service Performance Unit ensures that the Director, Customer Service, validates the model and the Director, Finance and

FUJ00079888

Commercial, authorises it. Fujitsu Services Outsourcing receives a copy of each variant of the HSH call volumetrics model output.

MSU updates the Fujitsu Services Pathway Business Volumetrics portfolio with details about changes to the HSH model. This portfolio is the means by which business volumetrics changes are communicated throughout Fujitsu Services Pathway.

Implementing HSH call volumetrics processing is described in associated work procedures and instructions held by MSU.

Ad hoc analysis volumetrics:

MSU deals with ad hoc analysis volumetrics as they arise. It obtains source data either from the existing volumetrics models or by specific enquiry to the Fujitsu Services Pathway Service Performance Data Warehouse by access to a Business Objects Universe.

MSU only accepts requests for ad hoc data volumetrics from sources who are authorised to have access to the data. Requestors must make requests to MSU on an Ad Hoc Query Request Form. The Service Performance Unit supplies the form to the requestor either electronically or as a hard copy.

MSU reviews requests for ad hoc volumetrics and, if it finds them acceptable, gives the requestor an estimate of:

- Delivery time
- Format of results
- Constraints that limit the resolution of the query
- Limits to be applied

If it is unable to progress the query, MSU gives:

- Reasons for not progressing the query or for delay
- Costs that may need to be met
- Limitations of use of any data to be provided

MSU aims to provide a response to all queries within a time frame commensurate with business need and cost in an effective and professional manner.

Implementing ad hoc volumetrics query processing is described in associated work procedures and instructions held by MSU.

- Field Service Manager Statistics

  MSU provides weekly and monthly statistics to a team of Field Service Managers. This team is responsible for the proactive identification and management of system problems that affect individual Post Office outlets. The idea is to minimise the impact of problems on Post Office outlet business and to restore service levels and customer satisfaction.

FUJ00079888

The weekly FSM report **can** be divided into the following categories: -

1. Record of outlets with the highest incidents of Environmental (E), Hardware (H), Complaint (M), Network (N), Operational (O) and Software (S) related calls on a national and regional basis.

2. Details of all the above calls

3. Frequency of calls by FAD code that conform to the above criteria over a 13 week period.

4. Details of calls filtered by *key words*

The monthly FSM report include:-

1. Monthly record of outlets with the highest incidents of Environmental (E), Hardware (H), Complaint (M), Network (N), Operational (O) and Software (S) related calls on a national and regional basis.

2. Frequency of calls by FAD code that conform to the above criteria over a 13 week period.

3. Monthly report of top 30 outlets with the highest incidents of 'restarts'.

4. Two-month variance analysis of calls per outlet.

- CS intranet site

The CS Infrastructure Services unit provides and maintains an intranet site for use by Fujitsu Services Pathway Customer Service and senior Fujitsu Services Pathway management. The site address is currently:

GRO

The site is based on a Windows NT Personal Web Server; the documents are created using MS FrontPage.

Currently, the site provides the following facilities and information:

- Management information reports
-
- Pathway CS organisation and contact information
- Noticeboard
- CS procedures and operations manuals
- Site search

FUJ00079888

The CS intranet site administrator is responsible for maintaining and developing the site. This includes the following tasks:

- Updating and archiving reports
- Managing usernames and password access to report pages
- Updating organisational information. Note that staff are expected to update their own personal and contact details
- Ensuring that procedures and operations manuals on the site are updated to reflect the latest versions of documents in the Fujitsu Services Pathway library

3.13.3 IT Infrastructure

The CS Infrastructure Services Unit is responsible for ordering all Office Desktop equipment for Fujitsu Services Pathway. The process involves a number of people and departments within and outside Fujitsu Services Pathway:

- The originator of the request for IT equipment
- The CS Infrastructure Services IT administrator who manages the ordering process
- The Fujitsu Services Pathway Accounts Department which raises the purchase order and pays the invoice
- The supplier who supplies the goods or service

The following description of the process is divided into three sections:

1. Raising an order
2. Processing an order
3. Receiving the goods

- Raising an order

  To raise an order:

  1. The individual originating the order identifies the requirement and technical specifications of the equipment.

     For standard desktop equipment, for example, PCs and printers, CS Infrastructure Services are able to advise on what to purchase and the suppliers to use so a detailed technical specification need not accompany such requests. For non-standard orders, for example, specific software or servers, it is the responsibility of the originator to determine the specifications and technical requirements

  2. The originator checks with CS Infrastructure Services to see if the proposed supplier is already registered on the ordering system.

FUJ00079888

If there is a known supplier, the originator checks with the CS IT department to find out if they have the supplier's information. For a new supplier, the originator provides the supplier's bank details and a copy of the supplier's company letterhead showing the VAT number with the purchase request

3. Having established the specification and technical requirements the originator completes a *Purchase Order Request Form (PORF)*. Refer to *Local Procedure when raising a purchase order (CS/PRO/105)* when raising the order
4. The originator takes the completed PORF to his or her department manager for approval.
5. The originator sends the completed PORF to the IT administrator in the CS Infrastructure Services Unit together with any quotations they have obtained and any Change Proposals they have raised.

- Processing an order

  To process an order after the originator has completed the PORF:

  1. The IT administrator checks the PORF and decides whether the order is a standard, blanket, or call off order. See *Purchasing Goods and Services (PA/PRO/020)* for more details. He or she then assigns a reference number to the order.
  2. The IT administrator checks that the correct cost centre code has been used and obtains authorisation of the completed PORF from the manager of the CS Infrastructure Services Unit.

     If an order is rejected, the IT administrator informs the originator of the reason for the rejection
  3. The IT administrator enters the order details on to the Oracle Database and passes the PORF to the Accounts Department for the purchase order to be raised. The Accounts Department creates the purchase order, adding supplier account codes and giving the purchase order a unique number.
  4. The Accounts Department returns a hard copy of the purchase order to the CS IT department within 24 hours of receiving the PORF.
  5. The IT administrator attaches a copy of the purchase order to the rest of the order information and enters the details of the order onto a spreadsheet for reference purposes, such as monthly analysis.
  6. The IT administrator faxes the purchase order to the supplier together with an order Acknowledgement Form.
  7. The supplier faxes the Acknowledgement Form back to Fujitsu Services Pathway to acknowledge receipt of the order and advise Fujitsu Services Pathway of the expected delivery date.

FUJ00079888

8. The IT administrator emails the originator with the expected delivery date so that the originator can arrange to accept the delivery when it arrives

- Receiving the delivery

  To receive the delivery:

  1. When the goods are delivered to Fujitsu Services Pathway, the IT administrator is contacted and informs the originators asking them to collect and sign for the goods.

     Note: CS Infrastructure Services do not store deliveries. Once they have advised the originator of a delivery, the originator must make arrangements to collect the goods.

     If the goods are delivered off-site, the supplier sends a copy of the delivery note to the CS IT administrator. An appropriate person on-site checks and signs for the goods and informs the CS IT administrator of any problems.

  2. The IT administrator files a copy of the delivery note with the rest of the order documentation.

  3. The supplier sends the invoice directly to the Fujitsu Services Pathway Accounts Department. The Accounts Department checks the invoice against the original purchase order. When they are satisfied that the invoice matches the purchase order, they send the invoice to the originator.

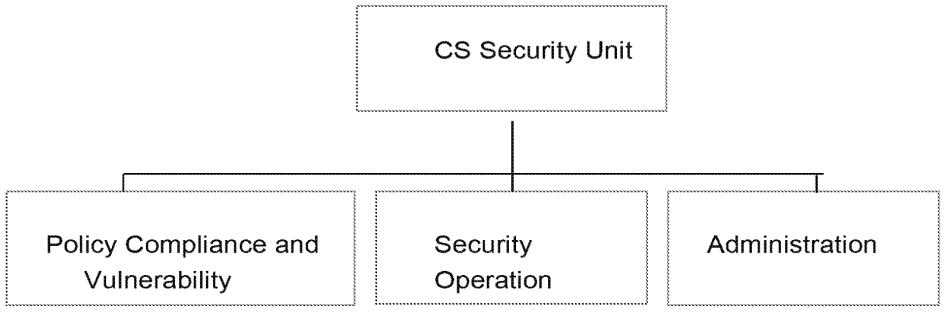
  4. The originator checks the invoice against the delivered goods to confirm that they also match and, if so, returns the invoice to the Accounts Department for payment.

3.14 Security Management

3.14.1 Overview

The purpose of the CS Security Unit is to protect Fujitsu Services Pathway's investment in IT assets, and to ensure the confidentiality, integrity and availability of all information conveyed, processed or stored, by the services it provides. It supports Fujitsu Services Pathway in all operational security matters to maintain Fujitsu Services Pathway's legal and contractual obligations.

The function of the Unit is organised in three work categories as shown in the following diagram. Diagram has been removed.



FUJ00079888

3.14.2 Policy Compliance and Vulnerability

This considers two main requirements, both of which are considered of equal importance from a security perspective.

a) It is the policy of Fujitsu Services Pathway Limited to protect its investment in IT assets, and to ensure the confidentiality, integrity and availability of all information conveyed, processed or stored, by its services. These are set out in relevant security related sections of the Codified Agreement.

b) Fujitsu Services Pathway must remain fully compliant with relevant UK legislation, UK and European regulations and Fujitsu Services Group IT Security policies and continue to meet the security obligation placed on it under contract. It is therefore essential to track and anticipate emerging UK and European regulations that could affect Fujitsu Services Pathway's operation and ensure that an ongoing programme of compliance and audit review is maintained in order to respond appropriately to any changes in risk.

Activities in this area are supported by compliance with and maintenance of, various security-related CCDs, policies and security audit reports.

3.14.3 Security Operations

This comprises those activities that support day to day operational security requirements. These are discrete activities that are carried out in order for Fujitsu Services Pathway to meet its specific security functional activities under contract.

Activities in these areas are supported by specific process / procedural documentation and manuals.

3.14.4 Administration and Organisation

This comprises those activities that support the way in which the Security Unit conducts its work and how it interfaces with other parts of Fujitsu Services Pathway, the Customer and other 3rd party contacts and suppliers.

The Unit's structure consists of the Pathway Security Manager (PSM) with direct reports consisting of Security Functional Managers and Security Analysts. The PSM reports directly to the Director of Customer Service.

3.14.5 Policy Compliance and Vulnerability

- Security Policy

3.14.5.1.1 Primary Security Policy

Primary security policy is embodied in the Fujitsu Services Pathway Security Policy (RS/POL/002). This document is consistent with the requirements of the ISO Code of Practice for Information Security Standards (ISO17799) and draws

FUJ00079888

its authority from Schedule AO2 of the Codified Agreement. RS/POL/002 is a CCD and is included in the CCD list (SUP/CON/001).

The Security Policy is applicable throughout Fujitsu Services Pathway and identifies specific roles and responsibilities for Security within the organisation. It is subdivided into high-level policy statements that are commensurate with the key controls of ISO17799 and in line with Fujitsu Services Group IT Security Policy.

Specific security enforcing policy is contained in the Security Functional Specification (RS/FSP/001). This document is also a CCD and is supported by various security-related Contract Referenced Documents – most notably the Pathway Access Control Policy (RS/POL/003).

Other relevant policies include Customer initiated and owned security documentation with which Fujitsu Services Pathway must comply but which POL is responsible for maintaining. The Unit's primary interface with the Customer is via the POL IT Security Conformance Manager.

- Maintain extant policy.

All policy has to be maintained in order to comply with legal, contractual and best-practice obligations. The activities necessary to support this requirement are reflected in the annual CS Security activity plan and the security policy documentation. It is also mandated by other Fujitsu Services Pathway Programme Office documentation.

3.14.6 Document Management.

CS Security maintains its documentation set and undertakes reviews in accordance with Programme Office / Document Management guidelines (PA/PRO/010) and via the use of the Programmes PVCS facility (CM/MAN/003).

The primary documentation set is N_A_CS_SECURITY_%. Some relevant documentation is also contained in the documentation set maintained by the Fujitsu Services Pathway Audit Manager.

The Fujitsu Services Pathway Security Manager is responsible for ensuring compliance with Programme Office procedures and may delegate responsibility for document maintenance to the Analyst responsible for the specific area of work in question.

Relevant procedural security documentation is also available on the Business Management System (BMS) website.

3.14.7 ISO17799 and Group IT Security Policy.

- Overview

ISO17799 is the British Standard for Information Security Management. It provides a proven, internationally recognised best-practice framework upon which to maintain information security within Fujitsu Services Pathway and has been

FUJ00079888

adopted by Fujitsu Services Group Security (GISI) as part of the Group IT Security Policy (CPM21) and overarching Group Security Policy (CPM20). Compliance with the Standard is also reflected within the Codified Agreement. .

ISO17799 facilitates development and maintenance of an Information Security Management System (ISMS) through:

- A Security Policy;
- An assessment of security threats, vulnerabilities and risks;
- An ongoing programme of compliance.

- Application within Fujitsu Services Pathway

ISO17799 guidelines are reflected for the Fujitsu Services Pathway environment in RS/PRO/028, which is available to all staff.

It has been identified that whilst this document provides an accurate reflection of the requirements of ISO17799, it does not provide the most appropriate way of communicating these throughout the organisation or for placing the operational responsibility for ensuring specific compliance with staff Line Managers.

A project has therefore been initiated to implement a revised plan for maintaining ISO17799 compliance within the organisation.

3.14.8 Legislation

Fujitsu Services Pathway is required under Law and within the requirements of contract to comply with all applicable legislation. Apart from compliance with Common Law, Fujitsu Services Pathway has specific obligations is respect of the Data Protection, Police and Criminal Evidence and Regulation of Investigatory Powers Acts.

CS Security maintain an interface with Fujitsu Services Group Legal Services and with Masons (The Fujitsu Services Pathway Solicitors) to ensure that its input to legal issues and activities on behalf of Fujitsu Services Pathway are commensurate with overarching Fujitsu Services and contractual obligations. It undertakes this directly or via the Director of Commercial and Finance or Fujitsu Services Pathway Commercial Manager.

CS Security also reviews emerging legislative issues by visiting various Government and Legal web-sites. Its primary interface to the Customer is via the POL Commercial Manager.

3.14.9 Data Protection Act (DPA)

The Data Protection Act 1998 came into force on the 24.10.01 and deals with the necessary requirements to ensure that the confidentiality of personal information is maintained. The Act is based on a number of Data Protection Principles and is far-reaching in scope.

FUJ00079888

CS Security ensures that Fujitsu Services Pathway and its operational systems are in line with extant DPA legislation. It provides DPA input to existing and new projects as required and assistance and information to the customer and other Fujitsu Services Pathway employees. The Unit considers the likely impacts of the updated legislation on Horizon and works with the Customer and other interested parties to identify and address areas of non-conformance within Fujitsu Services Pathway and the Horizon system.

An important element is ensuring the appropriate level of awareness is introduced and maintained amongst Fujitsu Services Pathway staff. This is achieved via various workshops, seminars and leaflets.

3.14.10 Police and Criminal Evidence Act (PACE)

Compliance with the relevant sections of PACE is relevant in connection with the investigation support that Fujitsu Services Pathway provides to POL. This is primarily in respect of the prosecution of Post Office counter staff who abuse POL rules for the management of the Horizon system and of benefit claimants who seek to defraud the OBCS system that is operated via the Horizon Infrastructure. POL maintains interfaces with relevant investigation staff in the Department for Work and Pensions.

The Unit's interface with the Customer is via the Consignia Group Internal Crime Manager.

3.14.11 Regulation of Investigatory Powers Act (RIPA)

RIPA provides regulatory controls for the investigation of suspected criminal activity. It is relevant in connection with the detection and prosecution of individuals by POL and in the production of data related evidence from the Horizon system.

The Unit's interface with the Customer is via the Consignia Group Internal Crime Manager.

3.14.12 Penetration Testing

- Scope

Fujitsu Services Pathway is contractually obliged to provide and maintain a secure system that protects the confidentiality, availability and integrity of the data it processes and stores.

Periodically Fujitsu Services Pathway is required to demonstrate that the Horizon system has adequate protection mechanisms to obviate the possibility of a successful attack by hacking or denial of service activities. In these instances the Fujitsu Services PSM will enlist the help of a reputable external company to undertake penetration tests of the Horizon infrastructure and produce a report detailing recommendations for improving security controls.

FUJ00079888

- Testing

Testing is sensitive and is generally undertaken on a test environment that replicates the live service. The Security Manager works closely with consultants from the chosen Company and, where appropriate the Customer, to produce detailed testing scripts. Testing requires support from various Development and Testing units within Fujitsu Services Pathway.

3.14.13 Supplier/Product Testing &Assurance

CS Security undertakes periodic risk assessments and reports on 3rd Party suppliers of products and services to the Horizon system. This provides assurance that the security requirements placed upon Fujitsu Services Pathway under contract are adequately reflected in the supplied services.

Inputs include service and product specifications. Outputs include security assessment reports and recommendations for the Fujitsu Services Pathway Board and/or Contract Managers

3.14.14 Compliance Projects

Periodically a number of reviews are undertaken by CS Security on a project management basis to ensure compliance with high-level legal, policy or contractual obligations. These may be instigated as a result of changes in legislation, Fujitsu Services Group policy or the contract with the Customer. Resource is sourced from within the Unit but may require the use of outside consultants. The implementation of any recommendations is generally effected via CP.

Two such projects are related to ISO17799 compliance and DPA compliance.

3.14.15 ISO17799 Compliance

A current review is underway to ensure that ISO17799 guidelines are adequately reflected and enforced within the Fujitsu Services Pathway environment.

It has been identified that whilst this document provides an accurate reflection of the requirements of ISO17799, it does not provide the most appropriate way of communicating these throughout the organisation or for placing the operational responsibility for ensuring specific compliance with staff Line Managers.

A project has therefore been initiated to implement a revised plan for maintaining ISO17799 compliance within the organisation. Work has started on preparing the information security control grid that will facilitate self-assessment schedules for ISO17790 compliance. The objective of this exercise is to identify and produce a gap analysis to record all non-compliance throughout the various Pathway divisions. Implementation of a corrective action programme will then be progressed across the Pathway organisation through the ISO17799 Workshop Group as part of ISO9001 accreditation work.

FUJ00079888

CS Security and Pathway Internal Audit are working together on a tool to measure Fujitsu Services Pathways compliance to ISO17799.

3.14.16 DPA Compliance

The Data Protection Act 1998 came into force on the 24.10.01. The new Act has widespread impact across Fujitsu Services Pathway and the advent of Network Banking brings with it additional responsibilities for the protection of personal information.

CS Security are undertaking a review to ensure that the legal and contractual basis upon which Fujitsu Services Pathway records, processes and stores personal information on behalf of POL and its Agents is fully agreed and reflected in the Codified Agreement.

The Unit will consider the likely impact of the updated legislation on Horizon and progress compliance in conjunction with interested parties. Compliance with the DPA will be achieved through a combination of input to relevant processes and procedures and awareness programmes.

3.14.17 Security Audits

Cs Security undertakes a number of audits in accordance with Security Policy and the CS Security annual activity plan. The audits are designed to ensure ongoing compliance with security policy and operational processes and are often undertaken in conjunction with Pathway Internal Audit.

The Security manager is responsible for undertaking these audits and may designate or co-opt other Fujitsu Services Pathway resources as required.

Target areas for the audits are determined by various factors including associated recommendations from other Pathway Compliance Units, reported security events, requests from the respective Business Unit Managers or as a result of changes in the actual or perceived threats to Fujitsu Services Pathway assets. Security Audits general involve a site visit and review of relevant physical, IT, personnel and documentary processes and procedures. They require close liaison with designated staff in the target business unit and the undertaking of various interviews with relevant staff.

The scope of the audits varies according to circumstances but the requirements of ISO17799 and legal/contractual obligations are generally used to form an opinion of compliance.

The output is a report with recommendations where appropriate. Corrective actions are documented in a Corrective Action Plan (CAP) which are monitored until completed by the actionee.

3.14.18 Security Awareness

CS Security has an obligation under contract to provide a programme of ongoing security awareness for both Fujitsu Services Pathway and POL/POL staff. This is

FUJ00079888

designed to reinforce general security messages consistent with the requirements of ISO17799 and also to target areas where non-compliance has been reported.

Maintenance of the security awareness programme is the responsibility of a designated security analyst within CS Security. There is an equal responsibility placed on line managers within the various Business Units to ensure that security awareness is fostered in the day-to-day working environment.

- Awareness Programme for Pathway

It is essential that all staff working for Fujitsu Services Pathway receive appropriate security awareness at the earliest opportunity. New recruits to Fujitsu Services Pathway receive a security handout and briefing as part of their induction training.

Security awareness is an ongoing activity and has to be reinforced periodically with advice and guidance. This is normally based on a theme and supported by the requirements of ISO17799. The awareness programme documented in RS/MAN/001 is updated periodically to reflect changes in the prevailing threats.

The Business Management System is used as a mechanism to provide links to associated security documents in an easily searchable, intuitive manner.

- Awareness for Post Office

Post Office personnel are informed and advised of appropriate best security practices, based on ISOI7799 by newsletter articles. It is important that the format, style and content are relevant, pragmatic and understandable and the appropriate training vehicle is discussed with POL.

Examples are used wherever possible to highlight potential issues and solutions proposed in a pragmatic and appropriate way.

3.14.19 Change Control

- OCP Authorisation

All operational change potentially affecting the security of the live estate requires appropriate authorisation by the PSM or designated deputy. This includes changes to security enforcing components or code such as firewall rulebases.

CS Security input to the Operational Change Process used within both CS and ISD Operations to manage and authorise OCPs. The "CSPathwayCP" mailbox sends OCPs to the Security Manager and Deputy who consider whether the change is commensurate with extant security policy and procedures and then authorise or reject the proposal.

Contingency arrangements are in place with Security ASD in the event that the PSM or deputy is unavailable.

FUJ00079888

- CSCP Review

CS Security manages formal Change Proposals via the CSCP Review Process. The security impact of all CPs is considered by the PSM and resultant impacts are fed back to the "CSPathwayCP" mailbox for action. The Unit also complies with the Pathway "Change Order" process.

The Unit is also responsible for raising CPs relating to security changes and supports these throughout the change life cycle.

- CP Review

CS Security inputs as appropriate to PCCB/CCB deliberations on various CPs that have a security impact.

3.14.20 Problem Management

- PinICL Support

The Unit has access to the PinICL system and has four security-related "stacks" in respect of both security policy and operational security issues.

- CS Problem Process

CS Security provides input as appropriate to the CS Problem Management Database and provides regular updates on problem resolution.

3.14.21 Business Risk Assessment

CS Security provide ongoing daily support to security compliance by undertaking risk assessments of operational processes and procedures used within Fujitsu Services Pathway in support of the Horizon system.

All operations and applications have a security element and the Unit receives requests from Business Units throughout Pathway for security related advice. The Unit facilitates problem resolution by undertaking discrete assessments to establish the threats, vulnerabilities and risks associated with emerging issues and uses these to balance security requirements against the need for operational expedience.

This requires a full understanding of both legal and contractual liabilities. Relevant staff in all Pathway Business Units are consulted as required.

3.14.22 Security Operations

- Security Event Management (SEM)

3.14.22.1.1 SEM System

The Tivoli SEM system is used primarily by CS Security to track and report events of security significance. The Unit has access to a SEM workstation to which related events are forwarded for monitoring and analysis. A designated Analyst within CS Security is responsible for the daily monitoring of the system.

FUJ00079888

Effective Security Event Management relies partly on identifying new features and vulnerabilities introduced by new systems. Operating system and applications are reviewed accordingly to optimise security configurations and minimise security weaknesses. Tivoli Event Filters are configured and updated where appropriate to trap security related event messages according to their severity. Events may be recorded and forwarded purely for reassurance that processes are working properly or conversely to alert CS Security to inappropriate activity for investigation. Virus incidents are one such type of alert.

3.14.22.1.2 Security Incidents & Investigations

Incidents can be categorised as potential and actual. They vary according to severity and how many systems are affected. Initial analysis will determine the type of incident, scope and frequency. All incidents are logged and details recorded for trend analysis and to facilitate a controlled, co-ordinated and timely response. A disciplined approach is required to ensure that accurate facts are promptly obtained and reviewed.

Maintaining the integrity and confidentiality and availability of associated data and information is critical. Evidence may be required for prosecution and/or for company disciplinary procedures.

3.14.22.1.3 Event Analysis & Reporting

Trend analysis is used to help identify procedural or technical weaknesses and inform corrective actions.

Outputs from analyses are used specifically to ensure that excessive system access is minimised and all users operate systems according to the rule of least privilege. As the understanding of existing systems improves, enhancements to security can be carefully assessed. Reports are referred to the PSM for action.

3.14.23 Key Management

The Horizon system is required to provide a secure centrally managed facility that gives end-to-end protection to Post Office business streams. The Horizon system and its associated business systems use cryptography extensively to protect the integrity and confidentiality of business data.

Key management encompasses the creation, distribution, protection, installation, monitoring and periodic replacement of cryptographic material. Cryptographic material may be either manually or automatically managed within Pathway:

Manual cryptographic keys are the responsibility of the Security Manager who is the designated Crypto custodian for Pathway;

Automated cryptographic keys are managed by the Key Management System (KMS) under the control of the Key Manager.

FUJ00079888

- Manual Key Management.

Most cryptographic keys are managed automatically by KMS. Some however are generated in a secure offline environment, supplied on a floppy disk and then installed manually on the appropriate platform.

Primary key inputs are provided internally via the Managed Key Service (part of IPDU Cryptography) or regularly by CESG. The latter undertakes regular audit reviews of arrangements for the physical protection of key material.

The CS Security Manager is the designated Cryptographic Key Custodian for Fujitsu Services Pathway and utilises a small group of designated Key Custodians and Key Handlers in both ISD and POL to operate the manual key management service. Primary responsibilities are to:

- manage the manual cryptographic estate
- oversee the secure production of manual keys
- monitor manual key expiry and instigate renewal
- control keys for central servers and existing FTMS applications
- receive, register and log use of specified manual cryptographic keys
- manage enforced key changes that are outside KMS control and ensure a smooth transition as required
- investigate provision of the existing manual key processes within KMS

- Process and Procedures

  Procedures for cryptographic keys are carefully controlled and documented. Monthly audits of existing key holdings are undertaken and actual or potential breaches are reported immediately to the Director of CS and the subject of immediate investigation.

  All cryptographic key activities are undertaken in a secure operating environment to minimise potential for compromise whilst handling removable media.

- KMS Key Management

The KMS automates many key management processes and, from a central point of control, shields the Pathway business services from the complexities of key administration. KMS was developed by Fujitsu Services Pathway to meet contractual obligations to the Post Office. Its main features are:

- Centralised control and automated key management;
- Secure delivery of cryptographic material across the live Pathway estate;
- Support for Pathway's operational cryptographic needs.

FUJ00079888

The CS Security Key Manager administers the Key Management System. All activities conducted through the Key Management platforms are in accordance with the KMS User Guide, RS/MAN/006. The main functions of the role are to:

- create, certify and distribute the keys installed at the Post Office and campus platforms to meet planned migration/rollout/re-roll dates
- monitor the status of key material proactively and on request
- undertake forced key changes as necessary
- investigate outstanding deliveries, in particular delays to routine key changes
- conduct additional CA Public Key (CAPU) validity checks as necessary
- produce management status reports on request
- administer Key Management system data changes
- check the Key Management task list daily for new actions
- record and resolve problems in conjunction with first, second, third and fourth line support
- maintain the KMS User Guide and update as appropriate for planned new developments

3.14.23.1.1 Functional Changes

The Key Manager maintains contact with other Pathway Units and keeps informed about proposed KMS functionality and other changes that affect the provision of KMS. To this end the Key Manager responsibilities are to:

- keep up to date with Pathway developments such as Network Banking, Your Guide and EFTPOS
- review existing and emerging documents for the proposed introduction of new cryptographic features
- keep abreast of KMS developments and issues so as to provide timely advice to management of any KMS functionality impacts
- be aware of KMS System test results and any impact these might have on programme delivery timescales
- provide KMS assistance towards the smooth transition to OCMS.

3.14.23.1.2 KMS Event Logging

The KMS is concerned with two main types of event, Tivoli events and KMA events. Tivoli events are reports of incidents detected by applications running on the operational systems; KMA events are used to trigger cryptographic activities such as distributing keys to an outlet.

The Key Manager is responsible for periodic checking and investigation of any failures relating to the following automated KMA events and for re-scheduling them to run again if necessary:

FUJ00079888

- Preparing and creating client keys for installation prior to Post Office outlet rollout.
- Activating and distributing keys to a client.
- Permanent or temporary closure of a Post Office outlet.
- Re-opening of a Post Office outlet.

The KMS Auditor is involved in the investigation of Tivoli events. Tivoli systems management provides the primary means of managing the Pathway systems. When an application detects a security problem the local platform logs an event which Tivoli harvests. Security events are separated out and forwarded to the Pathway Security Analyst acting in the KMS Auditor role.

In addition, the Key Manager and KMS Auditor perform the following activities:

- Responding to events forwarded by the SMC
- Examining the Application and System event logs on request.

3.14.23.1.3 Security Controls

The KMS system is operated in a secure environment to:

- ensure the integrity of all keys on all relevant platforms
- interpret audit trail and task-generated output - noting, escalating and responding to security breaches as appropriate
- protect removable media
- oversee any hardware or software changes to the CAW or Key Manager Workstations as arranged
- avoid disclosure or loss of any assigned tokens, passwords and safe combinations

3.14.24 Audit Data Extractions

This section describes an overview of the activities and control used for the extraction of audit data from the audit servers. This information may be requested by POL Investigation/Audit personnel to support their regulatory activities or by Fujitsu Services Pathway for problem management purposes.

- Data Extractions for POL

Data extractions for POL are requested by the Consignia Group Internal Crime Manager via a Request for Information (RFI) form. The form details the outlet FAD code and date range for which the data is required and the relevant priority of the request. A designated analyst in CS Security uses the Fujitsu Services Pathway Legato GUI to provide an audit trail of all work carried out on the Audit Servers and to identify which files are needed to fulfil the relevant RFI. Tivoli is used to identify the appropriate cluster number, which is then used to check the results from the GUI. An OCP is raised to enable ISD Network staff based at the datacentres to identify and load the required tapes. Once all the files have been restored, they are seal checked and a message store is generated. The requested

FUJ00079888

set of information is then extracted with the use of Riposte Query and burnt to closed CD

- Service Delivery Review

CS Security carries out data extractions in respect of 50 RFIs per year with a maximum burst rate of 7 per calendar month. This non-formal agreement with POL is subject to contractual agreement. Future service levels are the subject of an impending CR. There is no specified time frame in which to complete RFI's and priorities are agreed on an ad-hoc basis.

- Pathway Data Extractions

Fujitsu Services Pathway SSC occasionally request audit data to help investigate Horizon System Issues. These requests have a lower priority than all POL RFI's and are actioned as soon as possible. SSC request data extractions by raising a PinICL on the CS Security "Data Extraction" stack.

- CD Preparation & Despatch

All RFIs are burnt to 'closed' CD, to ensure the data can not be modified. The CD is virus- checked with the latest anti-virus software. The data is provided in both Excel 95 and 98 formats. Also included is a "Read me" word document explaining what is contained on the CD, which virus scan engine and virus definition were used to check the CD and who to contact in the event of a query.

CDs may contain sensitive information and are sent special delivery to the POL requestor or delivered by hand to SSC.

3.14.25 Investigation Support

Fujitsu Services Pathway has no current contractual obligation to provide prosecution support to POL. CS Security currently provide this support on a "without prejudice" basis pending contractual agreement.

- Collation of Evidence

Evidence in support of POL internal investigations and in support of POL's obligations to the Department for Work and Pensions is collated from a number of different sources. Transaction data is gathered from the Audit Server. Data in support of system integrity is sourced from the HSH (Powerhelp calls), MSU (non-polling) and PinICLs. The latter provides evidence to support the attestation that the outlet under investigation was operational during the period in question. CS Security has direct access to the HSH Website.

- Preparation of Witness Statements

CS Security currently provides three types of witness statements:

- An overview of the Horizon system and its associated integrity controls;

FUJ00079888

- An overview of the Horizon system and its associated integrity controls together with a statement in support of an evidential CD containing data produced in response to an RFI.
- An overview of the Horizon system and its associated integrity controls together with a statement in support of an evidential CD containing data produced in response to an RFI and an explanation of the Order Book Control System.

- Legal Requirements

In order to provide admissible evidence CS Security ensures it keeps up to date with emerging or changing legislation. This information is sourced via appropriate web-sites or via the Consignia Group Internal Crime Manager as part of the regular Joint Audit and Security Liaison Meetings

- Court Attendance

CS Security provides witnesses to attend Court if required to support statements. Whilst Fujitsu Services Pathway has no contractual obligation to do this it does so to avoid formal subpoena.

CS Security personnel provide statements of fact. They are not expert witnesses. Where expert witness testimony is required other members of Fujitsu Services Pathway or ISD Operations may be required.

3.14.26 Virus Management.

- Anti-Virus Measures

Maintaining updated Anti-Virus protection on the Live Estate and reporting potentially infected files preserves the integrity and availability of the data throughout the Horizon System. Automatic notification and prompt virus incident response is included in CS/PRD/101 and RS/PRO/043, currently being incremented for final review and formal baseline.

CS Security manages the implementation of virus checking software on the live Horizon estate. This involves the initial distribution and ongoing updates of anti-virus software onto selected workstations and servers within the Pathway Live Estate.

- Software Delivery Processes

Initial delivery is via Tivoli MANLCF and regular monthly updates of the latest anti-virus definition files utilises a procedure created specifically for delivery of Common Objects. This procedure requires only one release note to enable the PIT team to produce a Fast Track baseline, thus eliminating the need for using Work Packages. Full details are contained in the project IVCS PID (DE/PRD/002) and details of the delivery procedure are contained in PA/PRO/045.

FUJ00079888

- Event Reporting & Analysis

Virus event reporting is via both manual and automatic notification. These are outlined in RS/PRO/043.

Manual alerts rely upon the raising of a call, via the HSH Helpdesk, by users of workstations that receive a virus warning. ISD Operations monitor event logs on servers and also raise a Helpdesk call.

Automated alerts capture relevant NT events and forward them in real time via Tivoli to both SMC and CS Security. CS Security analyse details to understand the threat and to inform corrective actions. Where appropriate the software Vendor is contacted for advice and guidance.

- Review of Virus Threats

CS Security undertakes daily checks of emerging viruses and other malware via automatic e-mail notification from various Vendors and via the Web. Notification is also received from Fujitsu Services Group. These are used to inform threats and determine the required defensive measures.

- Horizon Pass Management

(CS Security provide contingency for this activity)

All Pathway staff and Engineers needing access to Post office outlets require a Horizon Security Identity Pass. This pass provides authorised persons with suitable identification that can be verified by Post Office Managers via a call to the Post Office Regional Help line.

The associated procedure is co-ordinated by Pathway in conjunction with POL and Fujitsu Services Group Security. The requester completes the necessary forms and the application is vetted by POL. Once approved Fujitsu Services Group Security issue the pass to CS Security, which forwards to the appropriate individual.

Management also involves replacement, temporary, invalidated and cancelled passes and details are provided twice a week to POL.

- Horizon Passes Audit

An audit of all Horizon Security Passes is performed every 6 months to ensure that CS Security has captured, invalidated and destroyed all Horizon Security Passes belonging to ex-employees and contractors of Fujitsu Services Pathway.

3.14.27 Live System Access

- Live Access Authorisation

Security policy mandates that all users requiring access to the live system have to be approved by CS Security. This is a fundamental security access control requirement.

FUJ00079888

The procedure involves the completion of an application form, which is authorised by the individual's Business Unit Manager. This is forwarded to CS Security who validates the request and sends to ISD Operations via the ISD mailbox for activation on the system.

- Token Administration

Security policy mandates that all users who access the live system from locations remote from the datacentres do so via secondary token authentication. Fujitsu Services Pathway uses SecurID tokens for this purpose. Tokens provide additional assurance as to the identity of users.

Tokens are managed by a designated member of CS Security who maintains a record of receipt, allocation and destruction and undertakes a quarterly review to ensure the cancellation of tokens that are no longer required. The associated activation of Tokens on the system is undertaken by ISD Operations.

Tokens are supplied by RSA Security and administered by Aslan.

3.14.28 Fraud/Security Countermeasures and Investigations

- Countermeasures

CS Security keeps up to date with developments in Fraud and Security countermeasures and uses this to inform risk assessments. The Section subscribes to various publications and journals and maintains informal contact with like-minded groups via e-mail and the Web.

- Internal Investigations

The Unit undertakes internal investigations into alleged or suspected abuse of assets by Fujitsu Services Pathway personnel. Investigations are undertaken in conjunction with HR, the Director of CS and other senior managers.

3.14.29 Security Administration

- Security Board

The Fujitsu Services Pathway Security Board owns Fujitsu Services Pathway's Security Strategy and determines the adequacy of security policy. The Security Board includes representatives that are nominated by the Director, Customer Service and participants including Horizon Security Liaison staff, represent a broad range of interests to ensure that alternative perspectives are considered. Whenever necessary, the Security Board can commission independent specialists to undertake studies, investigations or audits.

The Security Board meets as required.

FUJ00079888

- S4 Forum

The S4 Forum is a group that includes representatives from security-related roles within Fujitsu Services Pathway. These include CS Security and ASD Security personnel. This informal group meets generally on a fortnightly basis to discuss matters of general security interest and potential future impact.

- Joint Audit / Investigation Meetings

The PSM attends the Joint Audit / Investigation meetings that are arranged on a quarterly basis by the Fujitsu Services Pathway Audit Manager. Participants include the Consignia Group Audit Manager and Internal Crime Manager.

The remit of the Group is to discuss and resolve any issues relating to audit and the provision of audit data in support of investigations.

- GISI Liaison

The Unit maintains contact with Fujitsu Services Group Security to ensure that Group IT Security Policy is adequately enforced throughout Fujitsu Services Pathway.

- Event Management Forum

CS Security is represented on the Event Management Forum, which is organised by the SMC. This meets monthly and discusses incidents of recurring high-volume system events with a view to ensuring that KELs are accurately maintained and event filtering is optimised.

- Customer Care Visits

The PSM undertakes Customer Care Visits in accordance with the agreed CS programme.

3.15 Management Accounting

The CS Management Accountant follows the Fujitsu Services Pathway processes to establish and maintain the operating forecast for Customer Service. These processes are defined in the Processes: Planning and Reporting (PM/PRO/001)

The Management Accountant follows the Month-end forecast procedure (CS/PRO/106) to update the previous month's forecast with the following elements:

- The Fujitsu Services Pathway Project Plan
- New Change Proposals (CPs), with CS costs
- Update from other parts of Fujitsu Services forecasts, that is, from Infrastructure Services Division (ISD)
- Actual figures of costs for the month from the Oracle Financials system

FUJ00079888

- Forecasts from CS Service unit managers, with advice from the management accountant.
- Forecasts from the CS Director
- Head Count (number of staff) from Human Resources

Once the forecast has been reviewed by the Fujitsu Services Pathway Directors, the final operating forecast for the month is given to the CS Director, the CS Direct Reports and Fujitsu Services Pathway Finance.

Actual costs in Oracle Financials are made up from invoices and financial adjusting journals made by the CS Management Accountant and Fujitsu Services Pathway accountants. The invoices are checked as described in *Local Procedure when Receiving Invoices for Authorising (CS/PRO/103)*.

When raising a purchase order, in preparation for an invoice, staff are referred to *Local Procedure when Raising a Purchase Order (CS/PRO/*105*)*.

3.16 Management Planning

CS Planning produces three different types of plans, namely:

Major Release Management Plan

- CS time recording plans for "Business as Usual" and chargeable activities
- Release specific Level 4 plans

3.16.1 Major Release Management Plan

The CS Major Release Management Plan is an informational document used to draw together various levels of plan from several sources to present all the information in a single document. It contains data from:

The Programme Level 1, 2 & 3 plans

CS Level 4 Release Introduction plans

ISD Scheduled activities document

CS Business Continuity plans.

The Major Release Management Plan is updated with information from these sources at least monthly and distributed to each CS Manager & Service Manager.

FUJ00079888

3.16.2 CS Time Recording Plans

Two time recording plans exist within Customer Service; one covers those activities deemed as 'Business as Usual' for which no time and materials charges are made, the second covers those activities resulting from additional business which is charged to the customer on a time & materials basis.

The Business as Usual plan is fairly static and requires little change except for occasional organisational moves. The RTR Administrator in Feltham processes the change requests to this plan.

The additional business plan, known as the CS CCN plan, is more dynamic, with new business activities being approved every week. Each new business activity, for which CS have to undertake work, is added to the plan once it is authorised for work to commence. Resources and timescales are added as listed in the approved change document. A weekly interchange between the CS CCN plan and the RTR Time-Recording system keeps the plan up to date with time booked to each chargeable activity.

3.16.3 CS Release Specific Level 4 Plans

Level 4 plans are produced for every major activity involving work on the Live Horizon System. These plans are at detailed timed activity level. A major upgrade may consist of over a thousand such detailed activities and to get to this level of detail involves many hours of preparatory meetings starting several weeks before the main event. The major dates are taken from the Programme Level plans but there is feedback from the level 4 plans up to the Programme Level plans to ensure that changes resulting from the detailed planning