FUJ00079816

Document title:	**CS Support Services Operations Manual**
Document type:	Operations Manual
Release:	N/A
Abstract:	This is the top-level procedures document describing the activities carried out by the Support Services Unit within ICL Pathway Customer Service
Document status:	APPROVED
Owner:	Peter Burden
Author & Dept:	Richard Burton, A&TC, Technical Authors Peter Burden
Contributors:	
Reviewed by:	
Comments by:	
Comments to:	Peter Burden
Distribution:	Customer Service Director CS Operations Services Manager CS Support Services Manager CS Infrastructure Services Manager Pathway document library SSC Manager OTT Manager

FUJ00079816

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL No.
1.0	24/08/98	First approved version	
1.1	23/07/99	First draft of revised version also incorporating parts of CS/MAN/002	
1.2	16/08/99	Updates from Mik Peach. Document Reference changed to CS/MAN/002	
1.3	17/08/99	Further updates from Mik Peach added	
2.0	22/09/99	Approved version	
2.2	24/1/00	Updated by Peter Burden	
3.0	7/2/00	Approved	

0.2 Approval Authorities

Name	Position	Signature	Date
Peter Burden			

0.3 Associated Documents

The version numbers and dates the following table shows are those that were current when this document was written. If you wish to look at one of these referenced documents, search for the document in the Pathway Document Library (PVCS) and refer to the latest version.

Reference	Version	Date	Title	Source
CS/MAN/001	2.0	11/02/00	ICL Pathway CS Operations Manual	Pathway CS
CS/MAN/003	3.0	11/02/00	ICL Pathway CS Operations Support Operations Manual	Pathway CS
CS/MAN/005	3.0	11/02/00	ICL Pathway CS Infrastructure Services Operations Manual	Pathway CS

FUJ00079816

Reference	Version	Date	Title	Source
CS/MAN/006	3.0	11/02/00	ICL Pathway CS General Information Operations Manual	Pathway CS
CS/FSP/006	0.3	08/12/97	End-to-End Support Process Operational Level Agreement	Pathway CS
CS/PRD/021	1.6	29/07/99	ICL Pathway Problem Management Process Definition	Pathway CS

0.4 Abbreviations/Definitions

Abbreviation	Definition
BRT	Business Recovery Team
CMT	Crisis Management Team
CS	Customer Service
CSRM	Customer Service Release Manager
KEL	Known Error Log
HSH	Horizon System Helpdesk
OCR	Operational Correction Request
OSD	Operational Services Division (of ICL)
OTI	Open Teleservice Interface
OTT	Operational Test Team
SSC	System Support Centre
SMC	System Management Centre

0.5 Changes in this Version

Version	Changes
2.0	Approved version
2.1	Updates following comments
3.0	Approval following updates

FUJ00079816

0.6 Changes Expected

Changes
None

FUJ00079816

0.7 Table of Contents

FUJ00079816

FUJ00079816

FUJ00079816

1 Introduction

This manual provides a high-level description of the activities of the Support Services Unit within Pathway Customer Service.

2 Scope

This manual primarily provides a description of the operations of the CS Support Services Unit. However, to put these operations in context, it also describes some of the activities of other units where they are relevant. This is particularly the case in the software release management area. There are other manuals that describe operations within the other areas of Pathway Customer Service.

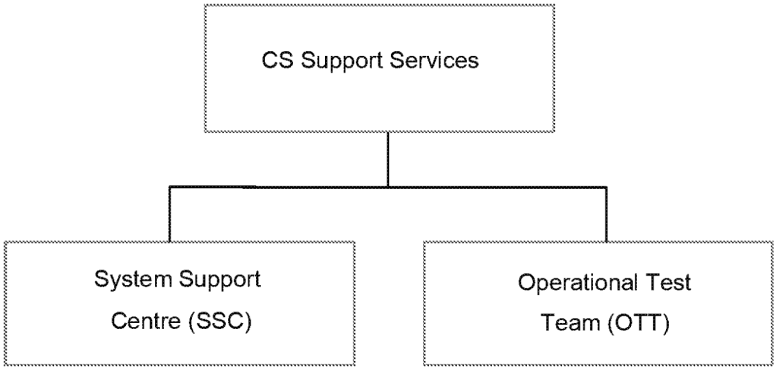
Where necessary, in addition to this manual, there are process documents, lower-level procedures and work instructions that describe some of the operations in more detail.

Appendix A, at the end of the manual, contains diagrams of some of the processes.

FUJ00079816

3 Overview

The purpose of the CS Support Services Unit is to support Pathway Customer Service in the day-to-day delivery of the Pathway solution. It consists of two groups of people as shown in the following diagram.



The functions of the individuals groups are:

- **System Support Centre (SSC)**
  Is responsible for all support activities, and, in particular, it provides third line support for all applications in the Pathway estate
- **Operational Test Team (OTT)**
  Tests all software fixes and, where applicable, changes to reference data to ensure there is no risk to the live service

FUJ00079816

4 System Support Centre

This section of the manual describes the operations and responsibilities of the System Support Centre (SSC).

4.1 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

4.1.1 SSC responsibilities to first and second line support

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 of 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

FUJ00079816

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
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:
    (a) Number of calls by priority currently outstanding with the SSC
    (b) Number of calls where resolution has been deferred to the next release
    (c) Number of calls by age currently outstanding with the SSC or fourth line support unit

4.1.2 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

FUJ00079816

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:
   (a) Software error
   (b) 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

4.2 Applications support

Appendix A in this manual contains process diagrams showing the roles of the support units.

4.2.1 Role of first line support

The HSH run by OSD, provides first line support to Horizon system users. The helpdesk has its own procedures, *Horizon System Helpdesk Incident Procedures (DSP/PRO/HH/010)*. The HSH uses Powerhelp, an application supplied by Astea Inc, as its helpdesk system.

When the HSH receives a service call, its first task is to determine whether or not the call relates to a hardware or software problem. For hardware problems, it contacts OSD to schedule engineers and, if necessary, spare parts to resolve the problem. Hardware and networking issues should be resolved through operational resilience or change control processes and should not be passed through to the SSC.

The HSH also does not pass requests for advice and guidance to the SSC that it can provide directly to the customer.

FUJ00079816

However, if it cannot resolve a call quickly, or if there is a possibility of a software problem, the Helpdesk transfers the call to the second line support team for further investigation.

4.2.2 Role of second line support

The System Management Centre (SMC) is also run by OSD and provides second line support to Horizon system users. On receipt of a call from the HSH, the SMC's first task is to determine whether or not the service call is a software code problem.

The SMC also uses Powerhelp as its helpdesk system. The system has an Open Teleservice Interface (OTI) link to the SSC's call management system.

The HSH will have prioritised the call according to the criticality of the fault as follows:

Priority	Meaning	Notes
A	Business stopped	A post office that is wholly inoperative and unable to process any business
B	Business restricted	A post office that is restricted in its ability to transact business, for example, one counter inoperative
C	Non-critical	A post office that is working normally, but with a known incapacity, for example, an interim solution has been provided
D	Internal	An internal HSH/SMC problem, for example, a helpdesk PC or a telephone not working

SMC carry out any appropriate pre-authorised activities for resilience and recovery purposes as defined in their procedures. Both HSH and SMC have access to KELs (Known Error Logs) which contain authorised workarounds and repetitive manual action that they can implement.

If the service request call indicates a software problem which has been seen before, and for which a workaround is already available, the SMC follows its own internal procedures to ensure that the workaround is passed to the customer.

If the service request call indicates a software problem which has been seen before, and for which a workaround is not available, the SMC links the current call to the first call and does not pass the call to the SSC. This ensures that the SSC does not receive duplicate calls for the same problem.

If the service call indicates a software problem that has not been seen before, the SMC follows its own internal procedures to pass the call to the SSC, providing information about the problem and Pathway's exposure, that is, the

FUJ00079816

number of calls received and the potential number of counters that are affected. They also provide details about the software version installed on the platform.

4.2.3 Role of third line support

The System Support Centre (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
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

FUJ00079816

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

4.2.4 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.

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

FUJ00079816

4.2.4.1 Pathway Development and A&TC

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.

4.2.4.2 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.

4.2.4.3 OSD

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

4.2.4.4 Eicon

Eicon do not use the PinICL system, but require calls to be logged by calling IRRELEVANT. 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 30/12/1999 this was Dan Dixon,

The Eicon contract is held in FEL01 by the Finance Director

FUJ00079816

4.3 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:

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. It can also be completed by an SSC staff member who detects that the data in the system has become corrupted in the course of diagnosing a fault

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.

   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

The SSC staff member who is to perform the change:

3. Checks the electronic signature of the authoriser
4. Stores the OCR form and the signature file in the `received OCRs` folder on the SSC server
5. 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
6. Completes the relevant sections on the OCR form to confirm whether they have produced and tested a script or not
7. 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.

FUJ00079816

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

8. 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 OSD staff member

9. 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

10. The second person also electronically signs the form and emails it to either the SSC Manager or the SSC web site controller

11. 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:

12. Checks the electronic signatures

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

4.4 SSC reference kit

4.4.1 Overview

The SSC reference kit consists of two rigs at BRA01. One is the reference rig for the live system and the other is the reference rig for the next release of software.

OSD maintains both rigs. The live reference rig is operated and managed by OSD. The second rig is operated and managed by SSC staff.

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.

4.4.2 Updating the hardware asset register

The SSC maintains a hardware asset register for all of Pathway CS. The following section describes the procedure to add to and remove hardware from the asset register. Note that this procedure includes all CS IT kit not just reference kit.

FUJ00079816

4.4.2.1 Adding new hardware

Whenever hardware is added within Pathway CS at Bracknell the asset register is updated. The CS staff member sends an email to the SSC Manager in the following format:

Asset Serial	ICL serial number
Asset Manufact Serial	Manufacturer's serial number (non-ICL)
Asset Product	For example, Compaq Deskpro
Asset Owner	For example, Rig *xxx*
Asset Owner Building	BRA01
Asset Owner Location	For example, Rig Room
Asset Owner Charge Code	For example, UPA66
Asset Comments	For example, Correspondence Server C
Asset hw or sw	HW or SW
Owning Asset	For example, Rig name
Value at Purchase	If known
Date of purchase	Formatted as *dd/mm/yy*
Depreciation Years	Always 3
Current Value	Leave blank

4.4.2.2 Removing hardware

Whenever hardware is removed from Pathway CS at BRA01, the asset register is updated. The CS staff member sends an email to the SSC Manager in the following format:

Asset Serial	ICL serial number
Asset Manufact Serial	Manufacturer's serial number (non-ICL)
Asset Comments	Where to

4.5 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.

FUJ00079816

4.5.1 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.

4.5.2 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.

4.6 Diagnostic tools

4.6.1 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.

4.6.2 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
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:

FUJ00079816

(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

4.7 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.

4.7.1 Known Error Logs (KELs)

The intranet site holds known error details in Microsoft Word 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.

4.7.2 Change proposals

The intranet site holds copies of each Change Proposal (CP) in a searchable form as Microsoft Word 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.

4.7.3 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.

FUJ00079816

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.

4.7.4 Operational Change/Corrections

The intranet site holds copies of both SSC Operational Correction Requests and OSD 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.

OSD have control over the OSD 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.

4.7.5 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

4.7.6 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

FUJ00079816

4.8 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 following rigs in BRA01:

- Reference rig
- Live test rig
- Next release rig.

The build script for these PCs was written by OSD, but is held in the SSC. The PC build was performed in accordance with the Access Control Policy.

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.

4.9 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

FUJ00079816

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

FUJ00079816

5 Operational Test Team (OTT)

The Operational Test Team (OTT) within Pathway CS is responsible for testing fixes prior to their application to the live environment to ensure that they work and do not adversely affect the environment.

5.1 Overview

To test a software fix, the Operational Test Team carries out the following activities:

- Scheduling the testing
- Controlling the testing
- Recording rig problems
- Controlling OTT documents
- Recording the fix level of a rig

The following sections describe the process.

5.2 Scheduling testing

The main test scheduling task is carried out using the Release Management Microsoft Access Database in conjunction with the Release Management Forum that is chaired by the CSRM. The document, *Release note and testing scheduling system, Issue 2 (08/06/99)* describes how to use the database.

Note. At present, this document is not available from the Pathway document library; a copy can be obtained from its author, Pat Lywood.

Requests for testing also come into OTT from other Pathway units. For example, SSC, Pathway development, as well as from the Release Management Forum.

When the forum has decided to produce a fix for a particular problem, the CSRM provides the address on the Operational Test Rig to which the software is to be applied, completes the schedule of testing, and sends the release note to OTT.

The OTT Manager does the following:

1. Obtains an estimate of the time required to test the fix
2. Inputs the details to the Release Management Database to enable scheduling and subsequent tracking of the testing
3. Ensures that sufficient documentation is available for the testers. This includes the following items:

FUJ00079816

- Copy of the release note
- Details of the technical fault (this may require sending a PinICL back to the development team)
- Copy of any relevant PinICLs
- Copy of the handover note

4. Schedules the resource to test the fix
5. Updates the release note PinICL at the appropriate times.

   Normally, this is when testing is complete but also may record that the required test phases were completed successfully. The test phases may be:

   - Test before fix applied
   - Test after fix applied
   - Test after fix regressed

6. Liaises with OSD to get the fix applied to the test rig
7. Files the documentation when testing is complete.

   If the fix is rejected during testing due to a fault, OTT send it back to the relevant unit for correction. The same software fix release note is used, but the sign-off needs to be completed again from that point in the cycle onwards.

   If multiple software fixes are included on one release note, one may fail while the others are successful. In this case, if the fixes are dependent on each other the whole release is rejected, or, if the fixes are independent the failed fix is omitted from the release, the rest continue and the failed element is re-scheduled to join the next release of fixes

8. Updates the release database to show the fix has been tested
9. Sends the software fix release note to OSD/SMC again. They remove the software from the rig, test the regression and then send the software fix release note back to OTT
10. OTT runs its test scripts to ensure the regression was successful and has not impacted any other part of the system
11. OTT sends the software fix release note back to Configuration Management as a sign off for their testing

5.3 Controlling testing

This section describes how the OTT control testing.

When fixes are fast tracked, some of the preparation, for example, documentation, may have been delayed until after the release has been distributed. Therefore, some of these activities are revisited to complete the full

FUJ00079816

schedule of preparation and testing as identified on the software fix release note.

1. The OTT Manager supplies copies of the following information, where relevant, to the testers:
   - Release note
   - Relevant PinICLs
   - Handover note
2. When a test has been scheduled, the testers carry out the following actions:
   (a) Produce the test script
   (b) Prepare any files required for the test
   (c) Carry out the test to confirm that the problem occurs as expected
   (d) Apply the fix to the test rig
   (e) Carry out the test to ensure the fix cures the documented problem.

   If the fix fails the test, return it to fourth line support for redevelopment and, if the fix is to a counter, regress the fix.

   If the fix passes the test, pass the relevant documents and the signed test script to the OTT Manager

5.4 Recording rig problems

Rig problems are recorded in log books. There is one log for each of the rigs used by OTT. The log book is kept by the counters belonging to the rig.

1. Whenever a problem is found on a rig, OTT makes an entry in the appropriate log book. The kind of incidents that are logged are:
   - Hardware faults on any of the kit
   - Errors reported by any of the kit
   - Communications faults
   - A fix applied to all hardware except counters
   - A fix removed from all hardware except counters
   - Anything for which a call is logged with HSH or SMC
2. The entry in the log book includes the following information:
   - Date of the incident.
   - Details of the incident
   - Call number - if the incident is reported to HSH or SMC

FUJ00079816

- Status of the incident with HSH or SMC. That is, Open, Closed, with HSH or SMC

3. When the incident is resolved, OTT updates the log with:
   - Closure information
   - Date of closure

5.5 Controlling OTT documents

This section describes how OTT maintain documents and notes.

OTT maintains all documents on the machine `Sscdiag2` in folder `OTTShare`. A single paper copy of each document and an associated index document is held in an appropriate manual.

Within `OTTShare` there are several sub-folders as follows :

Folder name	Use
`procedures`	All OTT procedures. Indexed in `procindex.doc`. Numbered sequentially in the format: `OTT/PRO/`*nnnn* where *nnnn* is a four digit number
`rig info`	Information about the rig used by OTT. For example, hardware specification, passwords and communications setup. Indexed in `riginfondex.doc`. Numbered sequentially in the format: `OTT/RIG/`*nnnn* where *nnnn* is a four digit number
`test info`	OTT test scripts. Where test details contain test files as well as a script they are in a unique folder on the host SE30. The folder has a name of the Release Note PinICL number. Indexed in the file `testindex.doc`. Numbered sequentially in the format: `OTT/TST/`*nnnn* where *nnnn* is a four-digit number.

5.5.1 Creating a new OTT document

To create a new OTT document, the OTT staff member carries out the following steps:

1. Allocates a new number for the document from the appropriate index file
2. Updates the index file to show the newly allocated number and prints a copy of it

FUJ00079816

3. Creates the new document using the appropriate template
4. Prints a copy of the new document
5. Files the paper copies of both the index and document
6. Informs other team members that they have created a new document

5.5.2 Updating an existing OTT document

To update an existing document, the OTT staff member carries out the following steps:

1. Locates the document by referring to the appropriate index file
2. Updates the document
3. Prints a copy of the new document
4. Files the paper copies of the index and document
5. Informs other team members that they have changed the document

5.6 Recording the fix level of the test rig

A white board documents the fix level of all the counters attached to the OTT rig.

OTT updates the white board whenever:

- A fix is applied or removed from a counter
- A counter is rebuilt or replaced

FUJ00079816

6 Business continuity

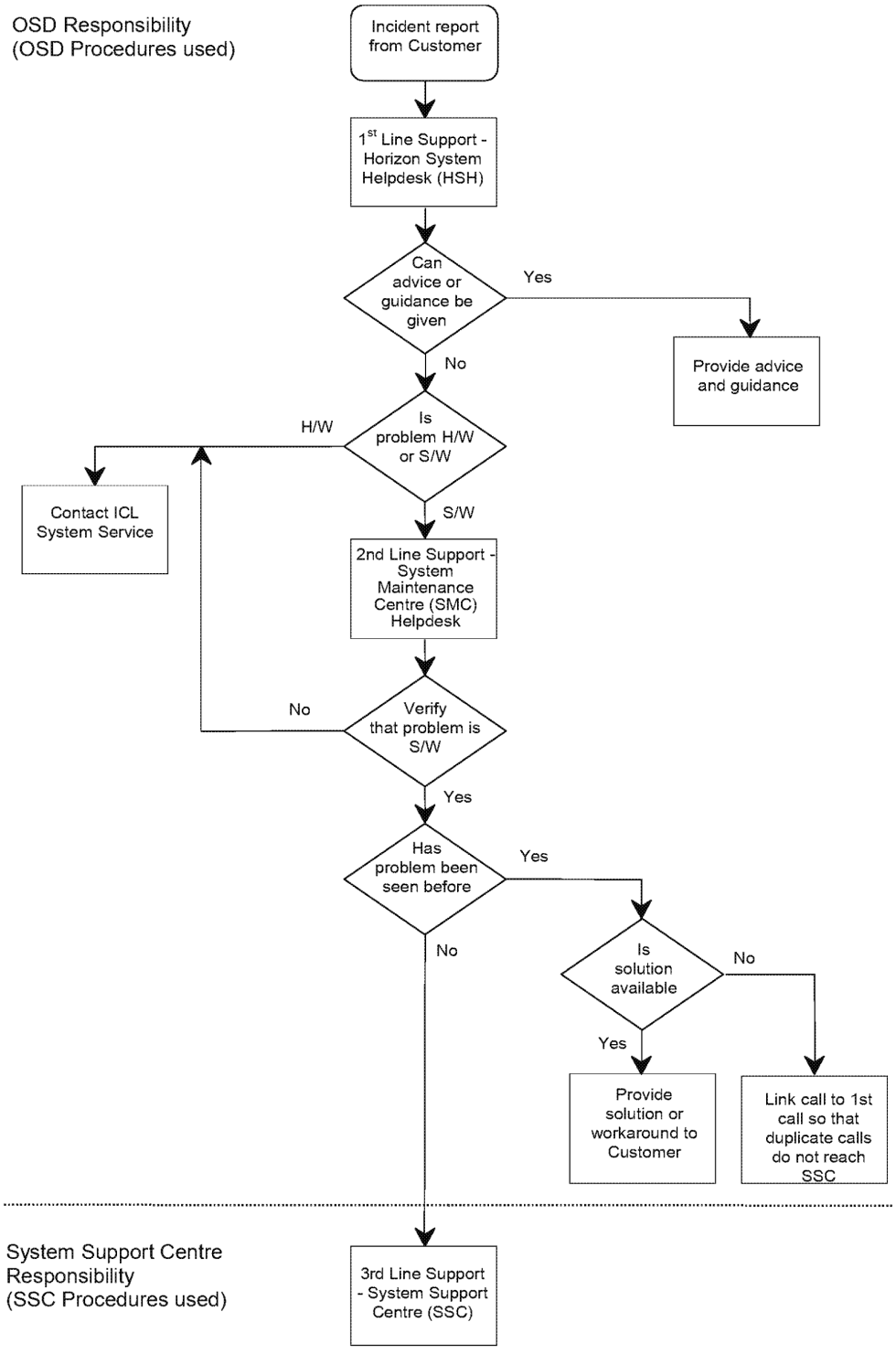
The Pathway CS Support Services Manager is responsible for ensuring that a business recovery plan is in place for the SSC. See Appendix C for details.

FUJ00079816

7 Appendix A Process diagrams

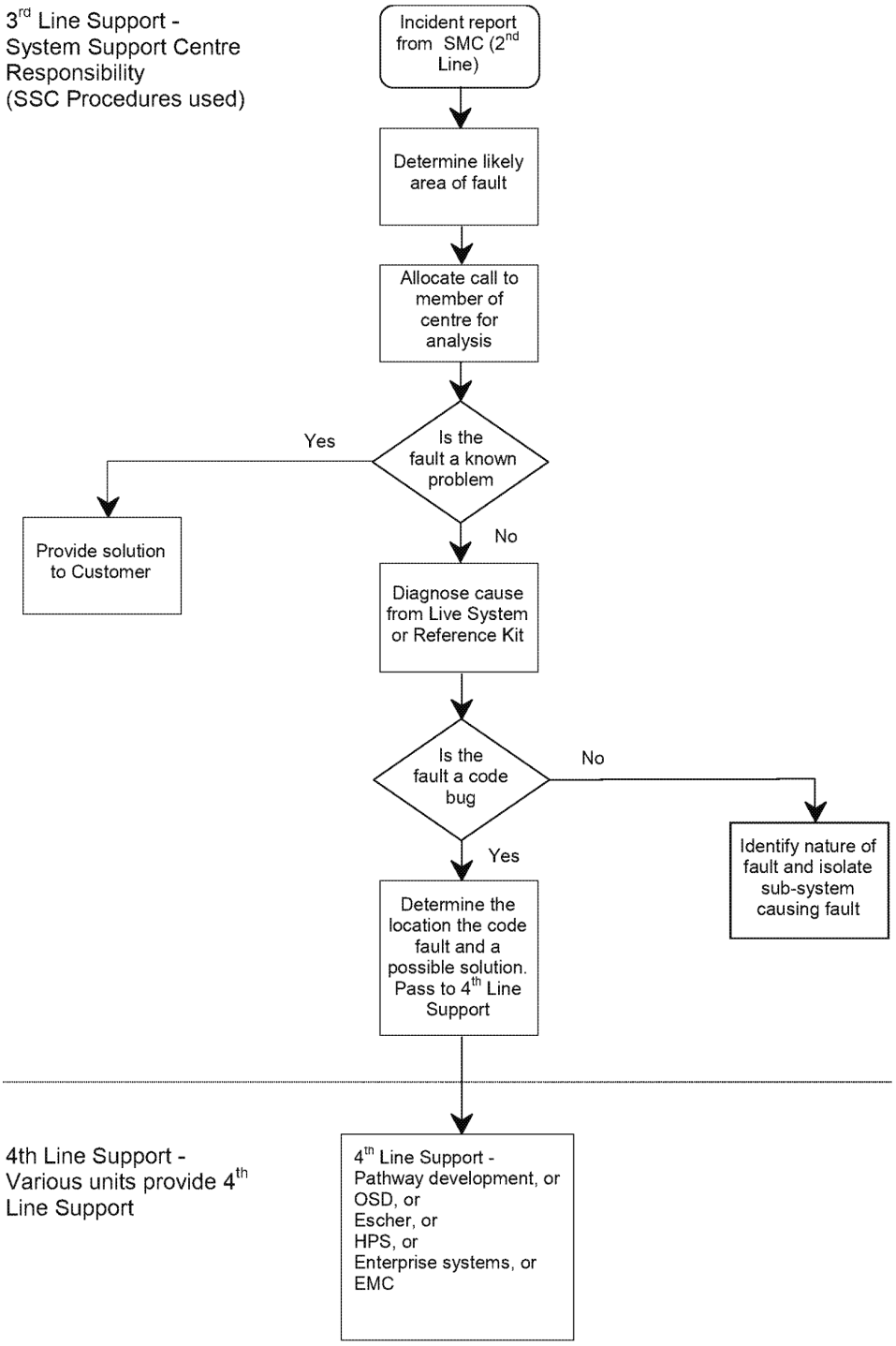
A.1 First and second line support

FUJ00079816



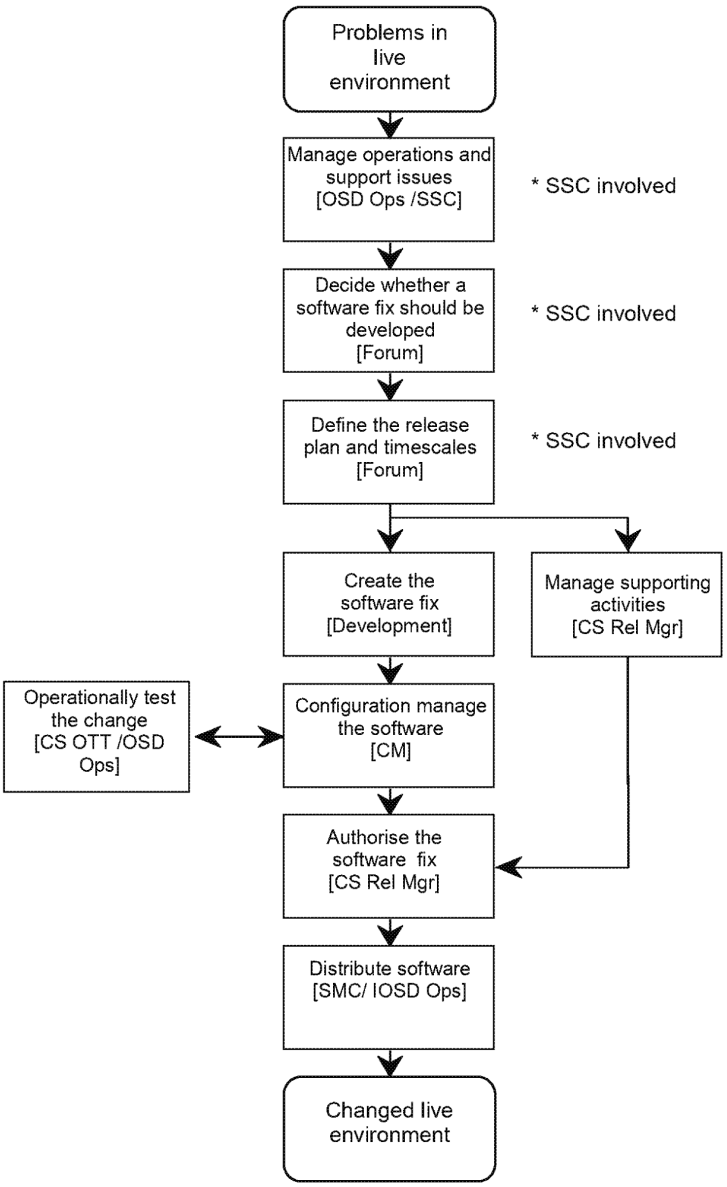
A.2 Third and fourth line support

FUJ00079816



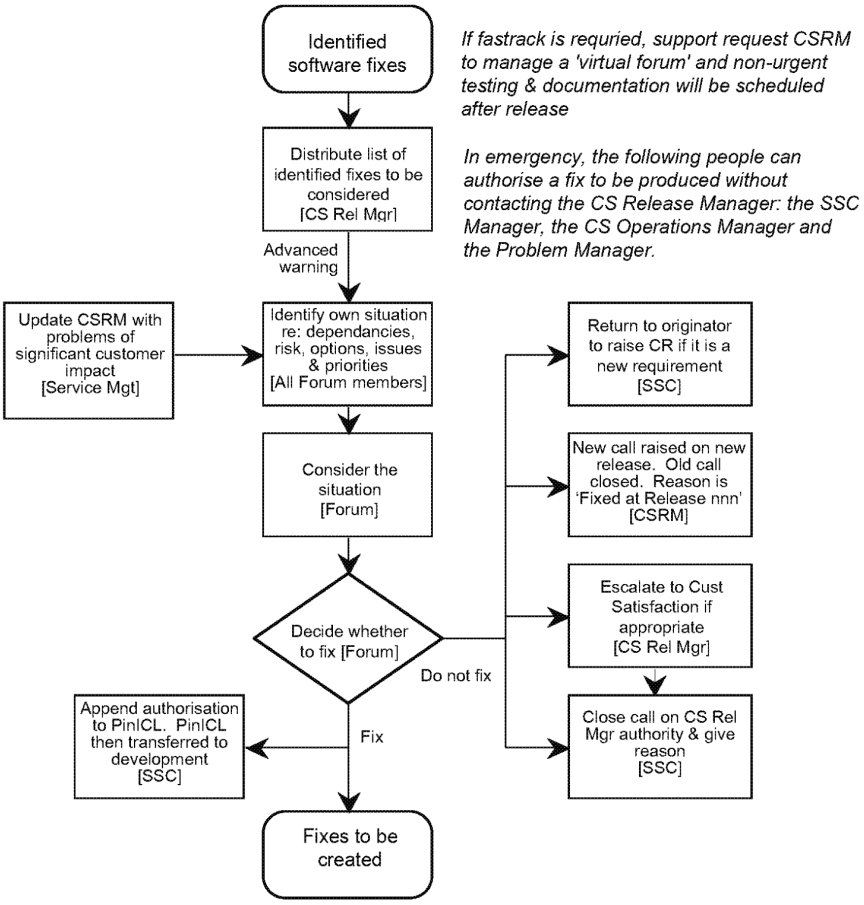
FUJ00079816

A.3 Support and release management process



FUJ00079816

A.4 Deciding whether a software fix should be developed



FUJ00079816

8 Appendix B Operational Correction Request form

The following page contains an example of an OCR form.

FUJ00079816

ICL Pathway SSC Operational Correction Request (OCR)

OCR Title	

Raised by (Name)		Location	
Date/time raised		Type of change (e.g. SQL script)	
System to be changed (e.g. PAS/CMS)		Required to be done by (date/time)	

Associated PinICL number	

Authorization signature		Authorizer (Print name)	
Authorization date		Authorizer position	

DATABASE Changes		FILE Changes	
Table name		File name	
Parameter description		File location	
Helpdesk screen		Location of backup	

Purpose and details of the change

FUJ00079816

Regression path	
Work done by (SSC signature)	
Work done by (Print Name)	
Witnessed by (SSC or 4th line signature)	
Witnessed by (SSC or 4th line Print name)	
Completed at (Date and time)	
Was change tested on reference rigs prior to application to live	YES / NO
System state before change	
System state after change	
Comments	

See notes on the reverse of this document for the procedure for use.

FUJ00079816

ICL Pathway SSC Operational Correction Request Process

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 correction originator must –

i) Complete an OCR form for every correction to data on the live system.

This can be done by anyone within ICL Pathway, but is normally completed by the Duty Manager, other Problem Manager or Business Support Manager when an incident or problem has been caused by an error in the data. It can also be completed by SSC staff members who, in the course of diagnosing a fault detect that the data in the system has become corrupted.

ii) Email the OCR form to an authorizer, electronically signing it where possible, and where this is not possible, telephoning the authorizer to confirm that the OCR is being sent.

The correction authorizer must be one of the following -

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

The correction authorizer will

i) Authorize the correction, or report back to the originator to specify why the correction is not being authorized

ii) Forward the OCR form to the SSC electronically with an encrypted electronic signature file.

The SSC staff member who is to perform the correction will

i) check the electronic signature of the authorizer before proceeding

ii) Store the OCR form and the signature file in the "received OCRs" section on the SSC server

iii) Wherever possible, produce a script to make the data correction, and test this on the SSC reference rig prior to it running on the live system. Sections in the OCR form confirm whether or not this has been done.

iv) Prior to the correction being made, document the state of the affected part of the system on the OCR form.

v) Prior to the correction being done, complete on the OCR form the regression path details. If no regression path is possible, then this must be stated.

vi) When corrections are to be made to the live system, at least two people must be in attendance. This will normally be SSC staff, but can be one SSC staff member and one person from the 4th line support unit responsible for the relevant area in which the data correction will take place, or one SSC staff member and one OSD staff member.

FUJ00079816

vii) On completion of the data correction, document the state of the affected part of the system and mail an electronically signed copy of the OCR form to the "witness". The witness will then also electronically sign the form and email it to either the SSC manager or the SSC web site controller.

viii) Update the PinICL and report back to the originator to confirm that the correction has been completed.

The SSC manager or SSC web site controller will

ix) Check the electronic signatures

x) File the OCR in the "completed OCR" section on the SSC server.

FUJ00079816

9 Appendix C SSC Business Recovery Plan

9.1 Section 1 ICL Pathway Generic

9.1.1 Introduction

This appendix provides instructions for staff working for ICL 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.

9.1.2 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

FUJ00079816

9.1.3 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
- rebuild of critical equipment

9.1.4 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

9.1.5 Change Management

This plan will be reviewed regularly

9.1.5.1 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.

9.1.6 Audit

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

FUJ00079816

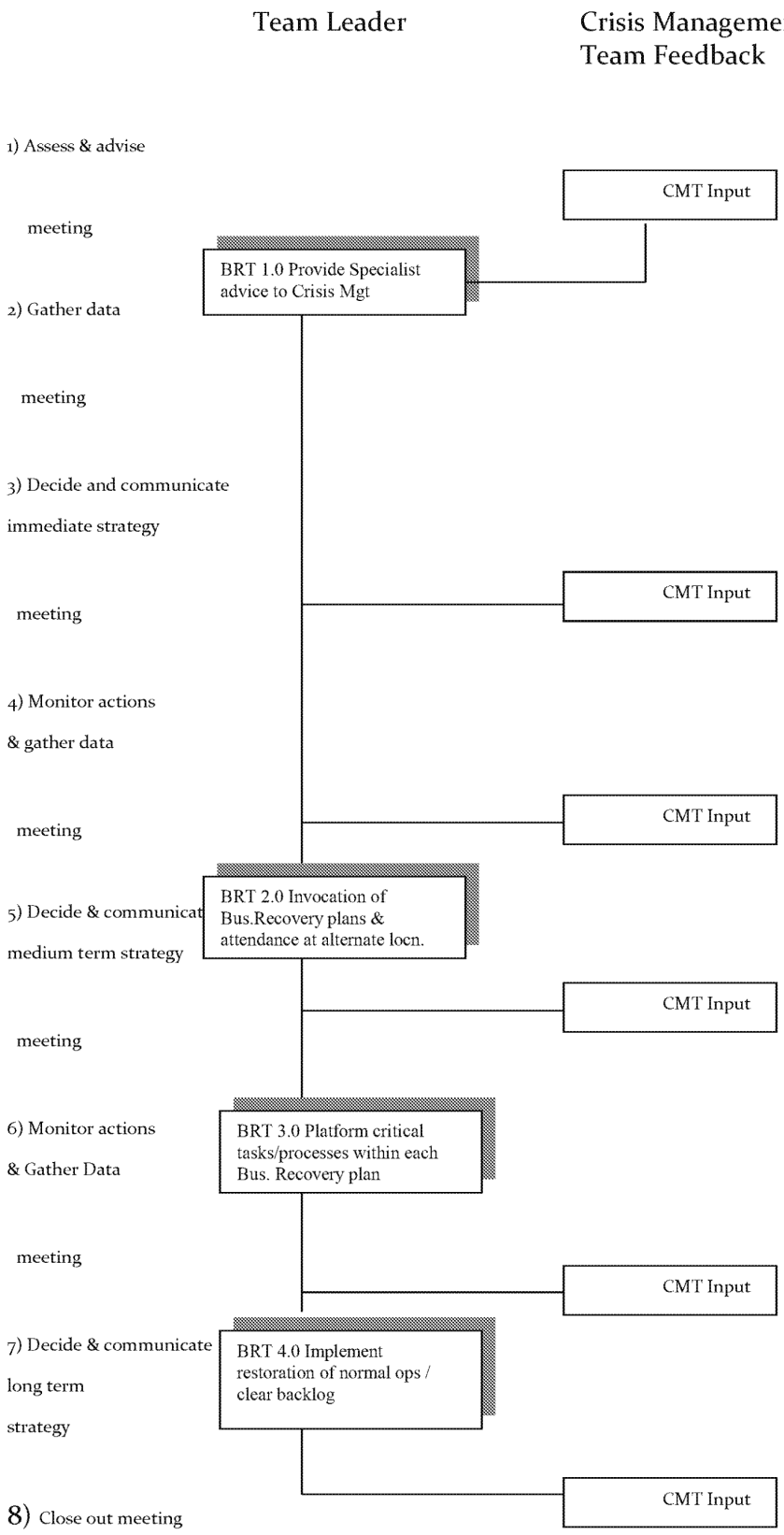
9.1.7 Testing

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.

9.1.8 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.

FUJ00079816



FUJ00079816

9.2 Section 2 SSC specific

9.2.1 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.

9.2.2 Pre-disaster Actions

1. Ensure that the essential documentation on the SSC web site is correctly backed-up, and that off-site copies are maintained.
2. Ensure that essential equipment is lodged at the backup site (FEL01) in a secure area
3. Ensure that the essential SSC staff who will travel to FEL01 in the event of an emergency have access to the site, and to the secure area where the kit is maintained.
4. Ensure that OSD have installed, and are maintaining the required communications connections from the backup site to the live estate.

9.2.3 SSC Contact numbers

Surname	Forenames	Home phone No.	Status
Anscomb	Jim	GRO	
Carroll	Patrick		Senior Technician
Coleman	Richard		
Croshaw	Mike		

FUJ00079816

Surname	Forenames	Home phone No.	Status
Kiang	Lina	GRO	
Kumar	Sampath		
Longley	Barbara		Coordinator
Obeng	Catherine		
Parker	Steve		Senior Technician
Patel	Rakesh		
Peach	Mik		Manager
Rowe	Diane		
Simpkins	John		Senior Technician
Simpson	Garrett		
Steed	Paul		

9.2.4 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-BRTLO.9	**5.Do 1 need to go to the alternate location ?**	Start Date/Time:	End Date/Time:	Complete: Y / N
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

FUJ00079816

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
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

FUJ00079816

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** **- 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**	Start Date/Time:	End Date/Time:	Complete: Y/ N

FUJ00079816

	- 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

FUJ00079816

9.2.5 External Contacts

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

Name:	**A&TC**	**Work:** GRO	GRO
Address:	Belfast	Home:	
		Fax:	
		Mobile:	
		EMail Address: GRO	
	Contact Name:	Kevin Madden	
Name:	**HSH / SMC**	**Work:** GRO	GRO
Address:	STE09	Home:	
		Fax:	
		Mobile:	
		EMail Address: GRO	
	Contact Name:	Brendan Nugent	
Name:	**Orbis -**	**Work** GRO	
Address:	Via Workplace Technology	Home:	
	Fax:		
	Mobile:		
	EMail Address:	GRO	
	Contact Name:	Mike Wood / Bill Jardine/Paul Sinclair	
Name:	**OSD**	**Work:** GRO	GRO
Address:	Belfast	Home:	
		Fax:	
		Mobile:	
	EMail Address:	GRO	
	Contact Name:	Gerry Boyce	
Name:	**OSD**	**Work:** GRO	GRO
Address:	Belfast	Home:	
		Fax:	
		Mobile: GRO	

FUJ00079816

	EMail Address:	GRO	
	Contact Name:	Paul Canavan	
Name:	**Pathway Development**	**Work:** GRO	GRO
Address:	ICL FEL01	Home:	
	Fax:		
	Mobile:		
	EMail Address:	GRO	
	Contact Name:	Peter Jeram	

FUJ00079816

9.2.6 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

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

FUJ00079816

9.2.7 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

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 Coordinator

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

FUJ00079816

Owner: OSD

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

Requirements Over Time :Required 4 hrs after disaster declared.

9.2.8 SSC Back up Facilities at FELO1

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).

There will be 7 PC's set up there:-

SSCFEL01 - SSC workstation

SSCFEL02 - Webserver

SSCFEL03 - SSC workstation

SSCFEL04 - SSC workstation

SSCFEL05 - SSC workstation

SSCFEL06 - SSC workstation

SSCPublic - PinICL system.

Logon to the workstations using PWYDCS username and password. These are the same as BRA01 workstations except:-

1) The webserver is on the private network as well
IRRELEVANT.

When launching IE for the first time Micro$oft will insist on using their wizard to setup internet access. Ignore it (select the option as already setup by SSC staff) and whenever it is necessary to access the web server just find the file c:\PathIE\pathway.htm and double click on it (it is possible to setup this file as the default page for IE). This file has links to the SSC web server and the Tivoli web server.

Other details

==========

IP address range:-

FUJ00079816

SSCFEL01 IRRELEVANT

SSCFEL02 IRRELEVANT

SSCFEL03 IRRELEVANT

SSCFEL04 IRRELEVANT

SSCFEL05 IRRELEVANT

SSCFEL06 IRRELEVANT

Netmask: IRRELEVANT

Gateway: IRRELEVANT

WINS: IRRELEVANT

WINS: IRRELEVANT

Private network is patched to point 21 in the meeting room.

OSD Service Management (e.g. Steve Gardiner or Ken Wood) can setup/remove this patch

SSCFEL01 and SSCFEL03 have administrator username/password as per all the SSC workstations.

SSCFEL02 administrator: IRRELEVANT

SSCPUBLIC administrator: IRRELEVANT

SSCPUBLIC IRRELEVANT

Netmask IRRELEVANT

Gateway IRRELEVANT

Public network is patched to point H10 in the meeting room.

FUJ00079816

10 Appendix D SSC PC Build Details

10.1 SSC workstation build eL

Hardware used: Base Fujitsu eL, PIII 500

128mb memory and 8mb Rage Pro graphics card.

10.1.1 Build process

1) Basic NT build using PIT products (see Initial products)

2) Add SSC products (see Additional products / customisation over PIT build)

At this point the disc image is ghosted off to \\SSCDIAG1\e$\ghost51c\images\wkseL01.gho

3) When building a new PC, the ghost image is downloaded using a DOS network load disc which connects to \\SSCDIAG1\ghost51c to run ghost. This is used to overwrite the system hard disc with the image wkseL01.gho.

4) Run various actions to finish build (see "At desk" action for SSC workstation build).

10.1.2 Initial products

Initially built with (PIT builds) :-

NTWKS40A_2_0_B008 (\\sscdiag1\packages\NTWKS40a)

Removed customisations Remposix.img and Isdn.img

(note after build, local admin password is IRRELEVANT)

Network card U/S after initial build.

copy Intel drivers from Fujitsu CD-ROM (\drivers\network\intel) to floppy disc

Install pro+ network card from a:\

SSC_WKS_2_0_B001 (\\sscdiag1\packages\ssc_wks_2_0_B001)

FUJ00079816

Map Y: to \\SSCDIAG1\E$ before calling _INSTALL.bat

10.1.3 Additional products / customisation over PIT build

1) Rename "My Computer" to SSCBRA00

2) Install Mach 64 VT-B driver

Increase desktop to 1024x768

65536 Colours

70 Hertz

3) Remove "My Briefcase" from Desktop

4) Install pkzip 2.04g to c:\zip

5) CD-Rom drive letter changed to I:

Shortcut added to AllUsers\Desktop

6) Winzip 6.3 installed to c:\Program Files\winzip

Installed with "classic" interface.

Shortcut added to AllUsers\Desktop

7) Textpad 3.2.5 installed to c:\Program Files\textpad

Associated .txt documents with textpad

Shortcut added to AllUsers\Desktop

8) Installed wingrep 2.0 to c:\Program Files\wingrep

Updated to 2.1

Shortcut added to AllUsers\Desktop

9) Message store utility (1.0) installed

to c:\Program Files\Message Store Utility then upgraded

to 2.2 (see 16 below)

Shortcut added to AllUsers\Desktop

10) rclient.exe copied to c:\winnt

Command prompt changed to red text on black and 500 line buffer

11) Installed Exceed 6.1 with the following custom options

Allow all users of machine to see installation

install to c:\Program Files\exceed.nt

user directory c:\Program Files\exceed.nt\user

install

FUJ00079816

All Xserver related components

HWM

Host explorer

FTP for windows explorer

No registration

No Xserver password

Traceroute

Xsession, Xstart

Customise

Telnet profiles generated for BVNW01 and Livetest

X set to single window (800x700)

New xrdb.txt (increse size of xterm, add scroll bars)

Add c:\Program FIles\exceed.nt\hwm.exe to exceed toolbar

Generate wstart (xsession) file to start exceed and

hwm (sscwks.ses)

Shortcut to sscwks.ses placed on AllUsers\desktop

Shortcut to telnet placed on AllUsers\desktop

Shortcut to HWM placed on AllUsers\desktop

12) Install IE4.01

Standard install - no desktop change

Delete outlook express from desktop

Create C:\PathIE

Copy Pathway.gif and pathway.htm to C:\PathIE

Launch IE - Select "already have connection" in wizard(sic)

Change default home page to C:\PathIE\pathway.htm

Move Internet explorer program group to all users

Amend HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\

Main\Default_Page_URL to "C:\PathIE\pathway.htm"

FUJ00079816

13) Install Excel 97, Access 97, Word 97

Delete "setup for IE3.02" from desktop"

Install Office SR-1

Remove "office startup" from allusers\startmenu\programs\startup

Install value pack (text data access drivers)

Shortcut to Word, Access, Excel placed on AllUsers\desktop

14) Formatted file utility installed to c:\Program Files\ffutil

All current definition files copied to

c:\Program Files\ffutil\Definition Files

Shortcut moved to "all users"

15) NT Posix utilites copied to c:\posix

c:\posix added to system %PATH%

16) Added JSim archive viewer to system.

This was mainly in an attempt to get v2.2 of the

message store utility going, because this install

loads every ocx under the sun! And it worked.

17) Shortcuts added to desktop

eventvwr.exe

textpad.exe

notepad shortcut to lmhosts (\\PBOPWYDCS01\nameres\lmhosts)

shortcut to floppy drive

shortcut to C:\ drive

NOTE: Ensure all desktop shortcuts are in "AllUsers" desktop

18) Setup Crystal Audit drivers

19) Tivoli desktop software v3.1.4

FUJ00079816

Installed to c:\tivoli\desktop

Shortcut created to "c:\tivoli\desktop\tivoli.exe -port 8002" on desktop

Hosts file amended to include IRRELEVANT WMASTER001 WSYSMASTER001"

When the desktop is launched - logon to WMASTER001

Login name must be PWYDCS\xxxxx01 (uppercase PWYDCS)

20) Quick view plus 5.0 Installed along with Adobe Acrobat 3.01

Shortcut added to "AllUsers" desktop for both.

21) C:\AgentEvents added. install.cmd run. See readme.txt

22) Installed LT1_WP_3941 for RQueryUK

Failed to install because msvbvm50.dll not present.

Copied from old workstation and registered. Install runs OK.

copied ripostesetup.bat to rtools

copied _sleep.exe to c:\

copied riposte licence file to c:\rtools

Riposte now runs up OK on licence 13 (supplied with WP3941)

rqueryuk fails to run up.

Copied Cir server rtools to workstation

Re-installed Riposte on update17

Riposte service disabled at startup.

23) Added directory c:\Pwayzip with Pwayzip.exe

24) Added NR2 hosts and lmhosts files:-

c:\winnt\sytem32\drivers\etc\nr2hosts.txt - hosts

c:\winnt\sytem32\drivers\etc\nr2masterlmhosts.txt - master lmhosts

copied nr2clientlmhosts to lmhosts

FUJ00079816

copied nr2hosts to hosts

25) Installed Visual studio 6 enterprise
Setup forced install of IE4.01
Custom install - VB, VC++ and tools only
This immediately fixed all problems loading RQueryUK etc
(figures - it loads just about every dll/ocx under the sun!).
Installed MSDN July 99

26) Shortcut to RQueryUK.exe and Rclient.exe added to desktop

27) netuse.txt amended and copied to desktop

28) Amend SecureNT_Install_Groups_And_Users.cmd
at the end of section :LOCALPWYDCS add:-

NET LOCALGROUP "Administrators" "PWYDCS\SSC Apps MAN" /ADD

10.1.4 "At desk" action for SSC workstation build.

The SSC workstations are initially built by loading a ghost image of the basic system. This document details the actions required to complete the build when the PC has been connected to the "red" (live system) LAN.

Parts of this procedure requires administrator access to the PYWDCS domain.

The local administrator password on this workstation build is IRRELEVANT

When restoring the ghost image, change size of the C partition to 3960

Required actions

1) Create D drive

FUJ00079816

On first boot, run up disc administrator. Create partition in spare space and format as D: (volume label DATA).

2) Change SID and system name

Login as local administrator

Use NewSID to amend the workstation SID and system name:-

Newsid /a SSCBRAxx

Amend Desktop shortcut "SSCBRA00" to new workstation name.

2a) Install Windows NT SP5

Install office SP2

3) Add workstation to the PWYDCS domain

Under Control Panel / Network / Protocol change IP address and Gateway address for TCP/IP

Gateway = IRRELEVANT

WINS = IRRELEVANT

Under Control Panel / Network / Identification

Change domain SSCBRA01 to domain PWYDCS

System should be restarted after these changes

4) *Installing the NT Security*

- Log on as Domain Administrator. (Domain PWYDCS, PDC = PBOPWYDCS01 - IRRELEVANT)
- Locate and open the Secure NT folder in the root of C
- Run the _Install_Secure_NT_Workstation.cmd
- Follow the on screen prompts. When asked to select if the system is for Live or Test, select "L" for live.

FUJ00079816

- Installation will now complete.

Note…

The "_Install_Secure_NT_Workstation.cmd" file MUST be run again after the Trusts are set up in the PDC.

5) Add domain user to local administrators group

a) PC's used in BRA01 - The PWYDCS domain user name for the person using this PC should be added to the local administrators group, e.g.

NET LOCALGROUP "Administrators" "PWYDCS\spark01" /ADD

b) PC's used in FEL01 - Because these PC's are not specifically allocated to any one person it is necessary to add SSC Apps SUP to the administrator group e.g.

NET LOCALGROUP "Administrators" "PWYDCS\SSC Apps SUP" /ADD

6) Changing the Administrator Account Name and Password

- Start "User Manager " from the Start Menu
- From the "UserName" list, select the Administrator Account by double-clicking it.
- On the "User Properties" window enter the new Password IRRELEVANT and Confirm-Password
- On the "User Properties" window blank out the Description text box
- Click the "OK" button to save the changes
- With the "Administrator" Account still highlighted, select the menu option "User", "Rename"
- On the "Rename" window enter the new Account Name (**sscdeaduser**)
- Click the "OK" button to save the change
- Close "User Manager"

7) Implementing BIOS Level Security

Reboot system.

At the prompt, press F2 to enter setup

- Move the Floppy Drive or Drives below the hard drive in the boot Sequence in the boot menu
- Remove the CD ROM Drive (if fitted) from the Boot Sequence in the boot menu
- Set the Supervisor Password to IRRELEVANT in the Security menu
- Set the "User setup access" to "Limited access"
- Save the new BIOS Settings

FUJ00079816

- Exit the BIOS Settings Menu
- Reboot the machine if required

8) First user logon

Logon as the PWYDCS\username

a) Internet explorer will insist on putting up its splash screen for two logons. On the second logon, click the option to turn it off!

Launch IE. Tell the "wizard" (sic) that you already have an internet connection.

IE will then revert to using the microsoft site as the default (again despite registry changes in the build). Set default to c:\PathIE\pathway.htm.

b) Mouseware will insist in re-setting up the mouse (despite the fact it has already been done in the build!).

Click YES

Click next

Select appropriate side for mouse position (watch out for left handers!)

Click next

Click next

Click Finish

c) Setup printer access to SSCBRAP

d) Reset options for cmd prompt. Red text, 500 line buffer.

STOP HERE - SecureID on NT not required yet.

9) Instructions For Configuring ACE/Agents SecureID

1. Copying the ACE/Server configuration files to the target Machine

- Collect the following files from the ACE/Server Administrator

  SDCONF.REC and SERVER.CER for standard builds, along with SERVER.KEY for the Remote Admin Workstation.

- Place these files in C:\WINNT\SYSTEM32.

FUJ00079816

- Place the IP address of the ACE/Server in the following location on the target machine: C:\WINNT\SYSTEM32\DRIVERS\ETC\HOSTS BTLFENT01 - IRRELEVANT

2. Enabling SecureID strong authentication in the Control Panel

- Open Control Panel and select the ACE/Agent applet
- Enable the following :
- Local Access Security
- Challenge All Users
- Enable Screen Saver Security
- Enable Reserve Password, supplying a Password of IRRELEVANT in the process.