Document Title:	Audit of Customer Service	
Document Type:	Report	
Abstract:	This report documents the outcome of an internal audit of Customer Service. The audit was one of a planned programme of audits within ICL Pathway for 1998. Its prime objective was to assess the state of the Customer Service operation for the advent of New Release 2 and National Rollout.	
Status:	APPROVED	
Distribution:	S. Muchow	J. Bennett
	M. Bennett	D. Groom
	J. Holmes	
	Library	
Author:	J. Holmes, B. Procter, S. Loam & G. Hooper	
Comments to:	S. Loam	
Comments by:		

FUJ00079786

0 Document control

0.1 Document history

Version	Date	Reason
0.1	18/01/99	First internal draft for comments
1.0	03/01/99	Issue incorporating comments received on draft
1.1	18/02/99	Revised draft following further comments
2.0	09/03/99	Issue incorporating all comments received

0.2 Approval authorities

Name	Position	Signature	Date
M. Bennett	Director Quality & Risk		

0.3 Associated documents

Reference	Vers	Date	Title	Source
IA/PLA/001	1.0		Internal Audit Plan 1998	
RS/REP/004a	0.1	04/01/99	Audit Report – SSC	

0.4 Abbreviations

ACP		Access Control Policy
APS		Automated Payment Service/System
AV		Anti Virus
BA		Benefits Agency
BES		Benefit Encashment Service/System
BPS		Benefit Payment Service/System
BSU		Business Support Unit
CAP		Corrective Action Plan
CAS		CAPS Access Service
CFM		(ICL) Computer Facilities Management
CMS		Card Management Service/System

CS		Customer Service
CP		Change Proposal
DLR		De La Rue
DPA		Data Protection Act
DRP		Disaster Recovery Plan
DSS		Department of Social Services
DW		Data Warehouse
EPOSS		Electronic Point Of Sale System
FRM		Fraud & Risk Management
HSH		Horizon System Helpdesk
KEL		Known Error Log
MIS		Management Information Systems
NR2		New Release 2
NRO		National Rollout
OCR		Operational Change Request
OLA		Operational Level Agreement
OTT		Operational Test Team
ORR		Operational Readiness Review
PAS		Payment Authorisation Service/System
PCHL		Payment Card Help Line
POCL		Post Office Counters Limited
PIR		Post Investigation Review
PUN		Pick Up Notice
RDMC		Reference Data Management Centre
RED		Reconciliation Exception Database
SLA		Service Level Agreement
SLAM		Service Level Agreement Monitor
SLCA		Crevice Level Contract Administration
SMC		Service Management Centre
SSC		Service Support Centre
TPS		Transaction Processing Service/System

0.5 Table of content

1 Introduction

Customer Service is an operational unit within ICL Pathway responsible for the delivery of "live" service to the post office outlets. Recently reorganised into three units - Infrastructure, Operations and Support - much of Customer Service's day-to-day service is delivered via suppliers both internal to ICL through Outsourcing and UKSS, and externally through De La Rue Card Technologies, De La Rue Secure Print and Alliance and Leicester.

It is the primary contact point with the customer for all support aspects of the Horizon solution.

2 Scope & Conduct

The audit forms part of the 1998 programme of planned Internal Audits into aspects of ICL Pathway's organisation and activities. While Internal Audit would normally be expected to assess and report on the controls present in an organisation the emphasis in this audit was to consider the activities and controls being established in Customer Service for the imminent implementation of New Release 2 and the onset of National Rollout, both of which will have a significant effect on Customer Service activities.

The audit was undertaken in accordance with the Terms of Reference (attached as Annex 1) on various dates between 26/11/98 and 14/01/99. It was originally planned to complete by Christmas 1998 with a draft report by 14/01/99. Sickness and alternative work pressures resulted in unforeseen delays and the late production of the report. This is regretted.

The time and co-operation of Steve Muchow, his managers and other members of his team during the audit is appreciated.

3 Management Summary

3.1 General

All the functions reviewed in this audit are managed effectively and have appropriate staff complements for the current requirements. Staff are competent and well motivated. Most issues that need to be addressed for the implementation of NR2 and National Rollout have been addressed or are currently being assessed. The principal general findings of this audit are:

- Whilst comprehensive process documentation has been prepared for all major functions, there is a general dearth of detailed procedure documentation such as would enable a new member of staff to operate with a minimal amount of training.
- In SSC, MIS and the Problem Management areas, staff operate with a large degree of autonomy. In the current scenario this has proved to be an effective way of working, largely due to the specialist and non-routine nature of the work undertaken. The audit raised concerns about the long-term succession of both the SSC Manager and the MIS Team Leader, in the event of their untimely departure from the company. In both cases there is appropriate short-term cover, but there are risks to Pathway in the longer term. The MIS Team Leader has sole responsibility for the volumetrics model, which is not documented. A successor to the SSC Manager has been identified, but is currently managing a separate department within Pathway; in addition, the personal relationship between these two people increases the risk that Pathway could lose both of them simultaneously. In the context of the specialised nature of their responsibilities and the scant detailed documentation mentioned above, this represents a risk to Pathway.

  <u>Management response</u>

  The SSC Manager has not agreed with the audit's conclusion on succession planning. His response is reproduced verbatim:

  - *I disagree that the relationship between my "successor" and myself poses any additional risk. We have not, in the past, changed jobs because of each other, or for reasons of location.*

The remaining paragraphs in the section provide an overview of the detailed findings but within the main body of the report there are also 1 recommendation in the area of NR2/NRO readiness (details in 4.2), 2 in DSS Services (4.8), 3 in POCL Services (4.9), 1 in Communications (4.10), and 4 in Annex 3, the summary of the SSC Security Review.

3.2 SSC (details in 4.3)

SSC are exercising adequate control over 4th line suppliers and their support processes are operating well. The detail section of the report contains 14 recommendations, with the following significant findings:

- Several systems currently in use have been developed in isolation and are not formally supported as part of the Pathway product set. The most significant such system is the SSC Intranet site; there are, however, three people in the SSC capable of maintaining it.
- Although staff are "security aware", there is not sufficient control over access to live systems.
- SSC are in a position to support NR2 in the live environment, but there are deficiencies in existing arrangements that will inhibit the SSC from supporting the target estate adequately.

3.3 BSU/RED (details in 4.4)

BSU/RED was audited in June 1998; the current status of that Corrective Action Plan is attached as Annex 2. They recently relocated to offices in BRA01 and have satisfactory arrangements for physical access security. The detail section of the report contains 2 recommendations, with the following significant findings:

- There is some concern about the impact of automation on workloads following NR2. Staffing decisions will only be made after NR2 trials.
- Processes for APS incident handling during NR2 are being prepared; non-BES elements cannot be gauged until NR2 testing. In addition, failures of APS/EPOSS transactions are perceived as more critical than BES transactions. It is anticipated that crucial problems will be resolved during live trials.
- The RED database is being supported internally by BSU/CS staff, only one of whom is fully conversant with the system. (Subsequent to the audit CP 1785 was raised to commission a feasibility study into the development of an Oracle solution.)

3.4 Problem Management (details in 4.5)

The Problem Management function is well managed and staffing is deemed appropriate – the staff complement is not expected to increase significantly to accommodate NR2 or National Rollout. The detail section of the report contains 3 recommendations, with the following significant findings:

- The Problem Management database is a subsection of the PinICL system, which does not have suitable functionality, in particular in its analytical capability and search facilities. Its replacement is currently being mooted.
- There is no procedure to ensure that the originator of a problem receives feedback. A proposal has been made that written approval should be obtained from BA/POCL before a problem is closed. This would be an ideal solution.

3.5 MIS (details in 4.7)

MIS deliver business information to enable service performance to be monitored at both the service and remedial levels. The detail section of the report contains 5 recommendations, with the following significant finding:

- When requests are made for ad-hoc reports the data in respect of encashments made or calls made to CMS/PAS are obtained from the Data Warehouse. The DW currently holds 26 weeks' data on-line; a formal request must be made for older data to be loaded. Currently the DW is unable to supply the required data in time for Pathway to meet the SLA. This situation may be aggravated, as there are moves afoot to further reduce the amount of data held on-line.

4 Detailed Findings

4.1 Customer Service Operation Now

The primary focus of this audit was to evaluate Customer Service's readiness for NR2 and National Rollout. In view of the fact that most of the processes are already in place under Release 1c, the approach taken was:

- Review the processes and procedures as they are being applied in R1c and establish whether changes are anticipated;
- Assess whether the internal controls are appropriate, considering both the current and future estates;
- Review the effectiveness and security of the current practices and assess their suitability and scalability for future needs.

4.2 Customer Service Readiness for NR2 & NRO

4.2.1 SSC

The SSC is in a position to provide support for NR2 in a live environment. There are however some deficiencies in existing arrangements which would not allow the SSC to support adequately the target estate. These have been identified and action plans developed for their resolution. Progress against deficiencies is monitored actively and status included as part of the regular monthly report produced by the SSC Manager.

All deficiencies impacting on readiness for NRO have been identified and are similarly monitored and reported.

Whilst this audit found the current structure to be operating effectively and standing procedures correctly practised it is recommended that CS management undertake a review into the possible effect on staff resource management of a ramp up to National Rollout.

4.2.2 BSU

BSU have budgeted for an anticipated additional two staff in April 1999 and a further four staff during the initial stages of the live trials for NR2 (expected to last until the end of 1999). This requirement is by no means certain, as likely non-BES workloads are extremely difficult to gauge. NR2 trials will be used to inform decisions on future staff requirements together with ongoing monthly reviews/analysis of incident volumes. Human Resources have made arrangements with an agency to assist with the future recruitment of appropriate candidates. Staff training will be given "on the job" by existing BSU analysts. The specific nature of BSU/RED work makes this the only viable option.

Processes for APS incident handling during NR2 are being prepared (CS/PRO/058). BSU have estimated the likely impact of new payment types at NR2 on the volumes of BES related incidents and are anticipating an increase of 35-40 a month. Extrapolation to an NRO environment has indicated the need for approximately 30 staff but this requirement will be reviewed regularly during NR2. The Section does not anticipate a significant variation in the type of BES related referrals at NR2, although volumes are expected to increase. The majority of problems during R1c related to transactions that for one reason or another were not committed at the PO counter. These have already been identified and appropriate fixes created. Increases are also likely to arise from EPOSS/APS transactions that, for the most part, are an unknown quantity.

BSU have made arrangements to ensure that every R1c incident will be replicated on the NR2 test rig prepared by Design & Development. Experience suggests a need for this given the peculiar nature of some of the reconciliation issues that have occurred in the past.

On-line access to Oracle/Discover tools will prove invaluable in obtaining information quickly. This will release staff to concentrate on the investigation of reconciliation cases.

BSU are represented at a newly created series of joint ICL Pathway/Horizon Reconciliation Workshops (the first of which took place during w/c 7.12.98). These will help identify and resolve problems and continue throughout NR2. Processes and procedures for this are currently being prepared.

BSU intend to develop a parallel RED system solely for non-BES reconciliation cases. The driver for this initiative comes not from the inability of the current REDv3.3 system to handle both types of transactions but rather as a way of providing a more customer-focused RED report for the Contracting Authorities. It also ensures that information pertinent only to one Contracting Authority is not made available to the other. The proposed system would utilise the same hardware/software and would be governed by the same access protocols and procedures. BSU are aiming to develop this during the early part of 1999. (Subsequent to the audit CP 1785 was raised to commission a feasibility study into the development of a solution in line with the overall Pathway architecture.)

4.2.3 Incident/Problem Management

Incident/Problem Management staff will be able to support NR2 in the live environment, including NRO. Due to the nature of issues handled here it is anticipated that their workload may increase with the release of NR2, necessitating more problem managers for about six weeks. Incidents accepted as problems relate to the specification, design and implementation of service components hence are not dependent on the volume of transactions. Currently about two incidents per month are accepted as problems, with about a dozen being open at any time. Extrapolating their experience from the release of 1(c), they are appropriately staffed (service managers take on the role of managing problems within their areas of expertise).

4.2.4 MIS

MIS (Contract Administrator and SLAM) are being developed specifically for NR2. National Rollout is not expected to present exceptional problems - the increased estate will result in an increase in the volume of transactions, but is not expected to impact the types of MIS information produced. Any changes to Contract Administrator after

NR2 will require a CP, which will be costed according to the work needed (including additional staff if appropriate).

4.3 Service Support Centre

The SSC is a major and complex element of Customer Service. This part of the report is based on visits made during the summer of 1998 and the actual audit visits made during November 1998.

4.3.1 SSC Responsibilities

The Service Support Centre (SSC) is responsible for all support activities and specifically for providing 3rd line support for all applications in the Horizon estate. It handles the end-to-end management and disposition of service calls made to the HSH and all incidents referred from HSH with the exception of those relating to known faults or those associated with hardware failure. It diagnoses problems, understands the solution and manages any resultant fixes. Incidents may be referred to 4th line support groups for action as appropriate (fixes are not written by SSC).

Obligations of SSC to HSH/SMC and of SSC to 4th line Support Units are documented (CS/MAN/002). The principles by which the SSC operates are documented in the End-to-End Support Process Operational Level Agreement (CS/FSP/006) which outlines the responsibilities of the four levels of support towards each other.

Pathway's Security Technical Design Authority indicated that the SMC were requesting tool support that exceeded their remit and would grant them an inappropriate level of access. This was discussed with the SSC Manager, who indicated that:

- The SMC's remit has not changed; it remains as documented in contract SB001 and the Access Control Policy (ACP);
- The ACP, in documenting the SMC's responsibilities, defines three functions but only defines tool sets for two of them. A CP will be raised to remedy this omission.

It is recommended that the CP is raised to ensure that the SMC has appropriately controlled access to the live system and the appropriate tool sets, to enable them to meet their contractual obligations.

.

4.3.2 Application Support Process

All calls from 2nd line support are sent via PowerHelp on an OTI link and transferred to PinICL before presentation to SSC. A typical PinICL daily live load at R1c totals 10-20. The Co-ordinator monitors constantly the status of all incidents liaising with both the 2nd line originators, the 3rd line Diagnostician and the 4th line Support Unit to whom any associated fix has been referred. When a subsequent fix has been created and implemented the Co-ordinator also notes and closes the PinICL.

Serious concerns were expressed by the SSC Manager that the number of software calls currently being received from the 2nd line is greatly in excess of projected figures (70% of all calls instead of 23%). If scaled to the NRO environment this would result in a flood of calls being received by SSC, which could not cope without a commensurate increase in staff resources.

It is recommended that this matter is investigated by Customer Service and, if evidence of calls being wrongly transferred is found, a corrective action plan put in place at the SMC to address the problem.

4.3.3 Personal Data

Sensitive, personal information can sometimes be attached as evidence to PinICLs and passed around an unsecured network. This is further complicated by the fact that no clear guidance on what constitutes "personal data" has been provided (i.e.: name alone, name+address, name+date of birth etc). In addition, personal information can sometimes be sent on PinICLs via Pathway Development to Escher in Boston USA. Personal customer information is generally classified by HM Government (and therefore by DSS) as "Restricted". As such its electronic transfer overseas is prohibited unless it is suitably encrypted using HMG approved algorithms.

The main threats to personal information come from:

a. persons who gain unauthorised access to the information on the system

b. persons who have authorised access to the system but use the information contained for purposes other than those for which they are granted access.

There are two distinct issues here:

- The requirements of the DPA, the new EU Directives on Data Protection and the definition of what constitutes "Personal Information";
- The requirements of HMG on the protection of information protectively marked "Restricted" and subsequently transmitted overseas.

With regard to DPA issues, initiatives have been undertaken in both SSC and BSU to sanitise information attached to PinICLs by removing unnecessary client sensitive data. In practice, however, the information attached to PinICLs is largely determined by what the 4th line Support Units require in order to create and test the necessary fix and it is not always practical or appropriate to remove information.

This is an extremely sensitive issue and there are serious implications for the protection of personal information. Consideration has been given to the encryption of the entire PinICL system as a means of reducing the risk of compromise. This is not however considered an appropriate or viable solution.

It is recommended that ICL's Commercial & Legal Group is approached to:

- *provide a formal definition of what constitutes "personal data", to be used in contracts, and*
- *review contracts with 4th line suppliers and other recipients of PinICLs to ensure that Pathway has adequate legal protection via contractual obligations placed on recipients of the data.*

It is further recommended that line management undertake random checks on incidents of access to, or transmission of, personal data to assure themselves that such access or transmission was justified.

As for the requirements of HMG, the transmission overseas of personal information attached as evidence to PinICLs is unacceptable and an urgent solution or compromise must be reached. (This function is not controlled by Customer Service.)

It is recommended that urgent steps are taken by Pathway Development to ensure that information attached as evidence to PinICLs and sent overseas is either sanitised beforehand or suitably encrypted. Alternatively, DSS should be approached with a view to negotiating a dispensation allowing for the unsecured transfer of information.

4.3.4 4th line support units

A number of units provide 4th line support to the ICL Pathway system, these include AT&C, Pathway Internal Development, ISTL, Eicon, Solution Centre, Technical Direct and Escher. These units provide the software that supports the solution. The obligations of SSC to the 4th line support are summarised in CS/MAN/002 and formalised in suitable contracts between the parties.

The current status of these contracts vary: those with AT&C and The Solution Centre have been signed and represent legally binding agreements; those with Eicon and Technical Direct are under active development with completion expected by the end of 1998 *(this aspect was reviewed in November 1998)*. The support contract with Escher is maintained by Pathway Internal Development as part of an overall contract. Pathway Internal Development is committed to the contractual arrangements. All contracts form part of a series of outsourced agreements under the overall control of the Operational Service Manager.

We have been advised that SLAs only exist between Pathway and the contracting authorities; all other agreements among the suppliers are covered by either OLAs (for ICL Group companies) or formal contracts (for external companies). OLAs limit the punitive damages for non-compliance to the fees charged for the service (this is apparently consistent with ICL Group policy), while contracts with external companies transfer any penalties incurred to the third party.

In the absence of contractual agreements there is no formal route for the transference of liability or other legal restitution in the event of a failure by the 4th line to deliver the agreed service. This weakness could leave Pathway seriously exposed. Where an ICL Group company consistently fails to comply with their contracted service levels, the only practical recourse available to Pathway is to change suppliers. The SSC Manager is consequently monitoring these service levels on a monthly basis.

It is vital that the approval process for contracts with external companies is brought to a conclusion before the implementation of NR2 when SLAs and other contractually binding requirements are placed on ICL Pathway by the Authorities. It is recommended that this activity is rigorously pursued by Customer Service management.

There are no formally agreed liaison meetings with each 4th line support unit although fortnightly reviews are held by the SSC Manager with Oracle/AT&C representatives.

In general, they are held on an ad-hoc basis as and when there is something to discuss (i.e. when a high number of PinICLs are raised about bugs in software provided by the supplier). Any agreements/decisions flowing from these meetings are implemented as operational practice where appropriate. Where they are held no formal record is kept of what was discussed.

Given the impact discussions can have on service delivery and future amendments to contracts it is recommended that formal minutes are kept which, at a minimum, record what was discussed and agreed.

While SLAs, which are restricted to hardware and network monitoring rather than software-related activities, are monitored and reported via SLCA, operational level performance of the 4th line support is recorded and maintained by the SSC Manager on a discrete database. This is used to monitor deliverables, time scales and trends, and to inform discussions at ad-hoc meetings. The database collates performance statistics, which are then provided as a monthly report to SMC and to CS Managers.

Only time will tell whether these informal measures are appropriate to support the SSC. It is recommended that the situation is reviewed after, say, 6 months of NR2 operation and action taken as required.

4.3.5 Support and Release Management Process

When problems are encountered on the live system, SSC carry out the pre-authorised actions available to them including workarounds in the Known Error Log (KEL). The KEL is maintained in Microsoft Word on a fixed format template utilising pre-defined data subsets to aid completion and subsequent interrogation.

Access to the KEL is available to HSH and SMC as well as the 4th line units. SSC has a filtering mechanism for preventing access to individual KELs by the 1st, 2nd and 4th line support units if this should be considered necessary.

4.3.6 Access to Live Systems

Diagnosticians working in SSC have read access to live databases (PAS/CMS/OBCS), the CAS interface, the Correspondence Server and various NT systems. They operate on a double PC configuration, one for standard desktop activities (email, WP, Intranet, PinICL) and one for access to live systems. SSC Procedures and Testing section also have access to live systems. The live system PCs have a restricted build level, operate on a separate LAN and are encrypted.

Access at R1c is via a username and password control. However, it is not possible to attribute positively the actions of users on the system in the event of a password compromise. Further, access protocols for R1c are not auditable as no record of the access of individual users is maintained by the system. This is a serious weakness.

At NR2 it is planned that access to live systems will be via a secure ID login that uses a personal token and a password. The Personal Token will be a “Smartcard” that will generate a unique number that the system reconciles with the password. A mismatch will result in a failed login.

This proposed system is significantly more secure than that currently used for R1c and it is recommended that this is adopted for NR2.

4.3.7 Operational Change Requests

When correcting data on the live system at least two people must be in attendance. This could be two members of SSC but in practice the SSC Manager insists that, wherever possible, one of the witnesses is a person from the 4th line support unit responsible for the relevant area in which the data correction will take place. This arrangement helps avoid the "Gamekeeper/Poacher" scenario arising from the correction of data by staff who may have raised the original Operational Change Request (OCR's are covered under 4.3.7). Where complex corrections are required they are usually scripted. In practice most corrections require only quick and simple activity that it is felt does not warrant the completion of a formal script. Nevertheless all corrections made in the live environment are recorded and documents are signed by both parties and retained.

Where live data has to be manipulated an Operational Change Request (OCR) is raised. The operational procedures for altering data are covered briefly (CS/MAN/002) and require the authorisation of any one of a CS group comprising the CS Operations Manager, CS Problem/Duty Managers, BSU Manager or SSC Manager. However, CS/MAN/002 does not detail the process for updating live data, nor is there a documented procedure for maintaining an adequate audit trail of changes made to the live database.

There is a requirement for documentation that details all these end to end processes. CS/MAN/002 does not provide this level of detail and it is recommended that the document is reviewed and updated accordingly.

OCRs may be sent to SSC as an original hard copy, an e-mail, or fax. The use of both e-mails and faxes to send OCRs is considered vulnerable to exploitation. The receipt of an e-mail is not of itself proof that the OCR has been correctly authorised by one of the approved signatories (this is borne out by the observation that, in practice, OCRs from BSU are raised by BSU analysts rather than the BSU Manager). This working practice is mitigated by the fact that changes are requested by BA themselves but it is nevertheless a deviation from agreed procedure. Faxed authorities are vulnerable to the "cutting and pasting" of an authorised signature (either as a time saving practice or as a more sinister attempt to circumvent the system) and this would be potentially undetectable by SSC.

There have also been problems in the past regarding the visibility to SSC of OCRs raised by CFM and to CFM of those raised at SSC (SSC originated OCRs are held at BRA01 whereas those originated by CFM are held in Belfast). It is understood that CFM has an action to merge variants into a single electronic form which will provide independence of initiation and authorisation whilst maintaining full visibility to both parties of the work undertaken.

The OCR process is an extremely sensitive area and recent approaches from BA have added gravitas. Despite the existence of documented procedures and a standardised proforma, the current arrangements for raising OCRs are somewhat discordant, could be vulnerable to compromise and provide only a limited assurance.

In addition to the CFM action already being undertaken, it is recommended that the OCR system is standardised, with appropriate hierarchical controls, to ensure that OCRs are correctly authorised, adequately monitored and suitably reconciled.

Completed OCRs are not subject to any routine checks by the SSC Manager. No "before" and "after" images of the database are taken or retained, other than a brief description on the OCR (and a script, if completed). There is also no association or subsequent reconciliation between the OCR and the PinICL that is being fixed via the data correction. Under the current system there is therefore a limited record of what was actually done and an insubstantial audit trail should this be required at a later date.

It is recommended that:

a. Completed OCRs are subjected to a documented, % check by the SSC Manager (or designated officer) to provide some degree of assurance that procedures are being complied with);

b. A linkage is created that reconciles the OCR with its associated PinICL;

c. An adequate record is kept of the changes made to the system.

4.3.8 SSC Intranet Site

The SSC Intranet is an evolving site created, supported, maintained and managed by SSC staff to assist and inform day-to-day working decisions. Access to the site is via NT domain, controlled by username and password. The contents of the site are under constant review but currently comprise details of KELs, Change Proposals and Release Management data as well as providing access to commonly used web-sites, an SSC bulletin board and other useful information. The site is becoming increasingly important as a resource tool both for SSC Diagnosticians and other authorised users. As such it now forms a crucial element of both the SSC function and the delivery of the overall ICL Pathway solution.

In view of the importance of this site, which was developed and is being supported locally, it is essential that CS Management continually ensure that effective support is available in the long term.

4.3.9 Resource Management

The SSC functions with a very flat management structure and the SSC Manager (and to a lesser extent the Diagnosticians) operates from a position of significant autonomy. This approach is supported by the SSC Manager, who considers that any additional management layers would have the effect of insulating him from issues and problems. Whilst there are substantial advantages to be gained from this direct "finger on the pulse" approach (particularly in the technological environment in which SSC operates) it places a heavy responsibility on the SSC Manager in monitoring adequately all SSC operational and staff activities.

Succession plans exist to cover the absence of the SSC Manager and the functions of the post are documented in both the SSC Manager's Terms of Reference and in the post holder's personal objectives. Three members of SSC can provide short-term cover in the event of the manager's absence, and deputising periods are alternated between them to build a sufficient breadth of knowledge. Despite this, the level of knowledge currently vested in the present incumbent and the scope of his responsibilities may represent a significant vulnerability.

It is recommended that CS Management assure themselves that the long-term loss of the present incumbent would not affect unduly the continued function of the SSC.

All staff receive adequate training and are recruited specifically for the skills they possess. SSC specific training is undertaken "on the job" and all staff have access to both the SSC Operations Manual (CS/MAN/002), which tells them what should be done, and a Technical Environment Directory to assist them with in-house terminology. There is however little or no additional lower level procedural guidance available to staff to tell them how it should be done (although it is recognised that the investigative and intuitive nature of SSC diagnostic work makes development of this extremely difficult).

It is nevertheless recommended that CS Management periodically assure themselves that adequate procedural guidance is available. It is suggested that the measurement criterion should be whether the documentation would enable a new incumbent to operate in the function with a minimal amount of training or induction.

Pathway policy requires that all staff joining the project undergo vetting – prospective employees are required to provide proof of identity, two personal references and a self declaration regarding criminal and financial records – and are also subjected to a credit check. The policy requires that HR initiate periodic recheck by reissue of the Pathway Security Questionnaire to employees; this has not been carried out.

It is recommended that the periodic checks are carried out. In particular it is important that personnel whose positions require them to have access to sensitive functions such as amending data, be reviewed on a frequent basis to ensure that their circumstances have not changed to the extent that their continued employment could be queried by the contracting authorities. SSC diagnosticians and BSU analysts would be included under these conditions.

4.3.10 Physical Security

An independent review of physical security was carried out concurrently with this audit and a report issued (RS/REP/004a). The findings from this report are included in Annex 3 (note that the report is structured in such a way that only exceptions are reported, which convention was followed in the Annex).

The physical security of the SSC has been jointly reviewed with representatives of the Horizon Programme twice. On both occasions the existing controls were deemed satisfactory and no additional recommendations were made

4.4 Business Support Unit

The BES activities of the ICL Pathway Business Support Unit (BSU) and the Reconciliation Exception Database (RED) were the subject of an Internal Audit during June 1998 (IA/REP/007) and subsequent follow up reviews based on an agreed Corrective Action Plan (IA/CAP/002).

4.4.1 Non-BES (BPS) elements

Non-BES elements of BSU work will not come on-line until NR2 goes to live trial. The main services to be introduced at NR2 and that impact directly on BSU are EPOSS and APS with additional linkage into TPS and RDMC.

Primary Non-BES data streams will be available to BSU via the PowerHelp/PinICL systems from the first and second line support sections (HSH and SSC respectively). All HSH referrals are allocated a reference number and every incident is logged to provide a clear audit trail and a measurement against service level agreements.

Some concern was expressed about the impact of automation on workloads following NR2. Whilst BES elements have been largely tried and tested during R1c, non-BES elements are something of an unknown quantity until NR2 testing. In addition, failures of APS/EPOSS transactions are perceived as more critical than BES transactions because BES payments are generally made pending further investigation. All procedures and protocols currently in place for BES elements of BSU work will be applied to the non-BES elements. The policy and procedures for handling EPOSS/APS incidents have been documented at high level (CS/PRO/058). Lower level procedural guidance on incident handling is currently being prepared by BSU staff.

Feedback from the Contracting Authorities show that they are happy with the functionality and controls of the RED v3 database.

4.4.2 RED v3.3

RED v3.3 has been developed in response to suggestions made by BSU analysts as R1c has progressed. There is not thought to be any need to upgrade RED with the introduction of NR2 other than some minor alterations to fields.

Some concern was expressed about the adequacy of technical support for the RED v3.3 database. RED has been developed internally by BSU/CS in response to operational needs. As such it has never been considered part of the ICL Pathway operational tool set or afforded suitable priority. It is currently supported internally by BSU/CS staff, only one of whom is fully conversant with the system. This leaves it highly vulnerable to unforeseen absence or loss of pertinent staff leading to a significant risk to this element of the Horizon solution.

It is recommended that steps are taken to support and develop RED 3.3 as an ICL Pathway corporate initiative.

4.4.3 Operational Change Requests

The issuing of Operational Change Requests (OCRs) by BSU to the SSC has been formalised and is covered by procedures outlined in a joint Pathway/Contracting Authorities document (CS/PRO/058). These procedures require the authority of a BSU analyst who has individual and documented password access to the system. There is however no independent authorisation by management prior to OCR action nor is there any subsequent verification/audit by management that OCR action was appropriate.

Although OCR action is only taken following the receipt of an appropriate authority from BA (which mitigates against a lack of control in this area) it is recommended that OCRs are authorised only by the BSU Manager.

BSU monitor all OCRs and liaise with both BA and SSC to keep them informed of progress. A regular monthly "tidy-up" meeting is held with BA representatives.

4.4.4 BSU Relocation

BSU recently relocated to the first floor of Annex 2 at BRA01. Access to the building is controlled by personal token and limited to staff that work in Annex 2. Visitors are escorted at all times. Adequate and secure arrangements are in place for the control of passes. Access to the first floor CS area (which includes BSU and SLCA personnel) is controlled by an additional access control that allows entrance only to staff working in that area. BRA01's Annex 2 is suitably protected by both CCTV and an intruder detection system.

BSU is contained in a discrete area of the first floor and is separated from other work areas by the use of medium level acoustic screens providing suitable privacy and protection from eavesdropping. VDUs of the RED database cannot be viewed by unauthorised personnel or visitors. It is considered that BSU now operate in a suitably controlled environment.

4.4.5 Contingency Planning

Contingency procedures are being documented to support RED and the work of BSU in the event of a failure at BRA01 or of a software/hardware failure and these will be available at NR2. It is anticipated that space/terminals will be available at FEL01 with access to PAS and Discover tools.

A document (CS/PRO/060) is also being prepared by BSU that outlines a proposed clerical back-up system that provides for the recording of RED incidents with the limited issuing of subsequent reports.

Paper based reports held by BSU are being transferred to electronic archive to reduce the amount of documentation held by the section. In addition, BSU regularly archive RED data to ensure that a smaller data set is held on the system.

All live data is backed up automatically by the system on a daily basis and stored on the server ("P" Drive).

4.5 Incident/Problem Management

Incidents escalated to Service Management are reviewed in terms of a set of criteria to decide whether they should be regarded as problems. These criteria include business impact, time scales, customer satisfaction, cost, complexity and extent of the problem, security implications and the impact on other organisations. If they are accepted as problems they are recorded on a Problem Management Database and allocated to a Problem Manager, who is responsible for co-ordinating the activities involved in arriving at a solution.

4.5.1 Problem Management Database

The PinICL system is being used as the Problem Management Database. There have been problems in the past where calls have been transferred between stacks; hence Customer Service did not have a permanent record of the calls. The procedure in place now requires a copy of the record to be made and held on the Problem Management stack as a diary entry, cross-referenced to the live call. This is to be monitored by the newly appointed administrator.

The use of the PinICL system for the maintenance of Problem Management is currently under review - its analytical functionality is very limited and it does not have powerful search facilities.

These issues are being addressed and will be included in the next audit of CS.

4.5.2 Feedback

There is no procedure to ensure that the originator of a problem receives feedback. Where a PIR is produced it will fulfil this requirement, but in terms of the latest process specifications a PIR is not always required. A proposal has been put forward that written approval should be obtained from BA/POCL before a problem is closed, but this has not yet been agreed.

It is recommended that written approval is obtained from the originator of a problem in all instances, and that this is used as the authorisation for closing the problem.

4.5.3 Documentation of processes and procedures

Processes have been documented, but there are not detailed procedures that will enable a new employee to operate with a minimum of training. In particular, several requirements are stated very generally (e.g. the criteria for deciding whether a specific call should be classified as a "problem" or not), requiring a subjective judgement from the Duty Manager. This is not a major issue at present as the Duty Managers (of whom there are currently three) are suitably familiar with the project to reach consistent decisions.

It is recommended that detailed procedure documentation is prepared at the level that would facilitate consistent operation of the system by newly appointed staff.

4.5.4 Escalation of changes to future releases

There is not an effective control mechanism for ensuring that changes made to the current release of the software via PinICL are incorporated in future releases. This is under discussion but as yet agreement has not been reached, nor have any procedures or controls been implemented.

It is crucial that this issue is resolved and appropriate controls implemented – failure in this area will cost time and money and can damage Pathway's credibility.

4.6 Business Continuity

4.6.1 Rationale

A key requirement of the Horizon solution is that of business continuity i.e. ensuring that there are operational processes and procedures in place to ensure that any component failure has little or no effect on the service provided. The principal requirement in respect of the provision of contingency plans is specified in Requirement 830. This is supported by associated requirements on the provision of BPS fallback facilities and the activation of contingency payments, PCHL and HSH contingency.

Contingency planning for the Horizon solution is based on the fundamental premise that elements of the solution have been developed and designed from the outset with a substantial degree of in-built resilience (e.g. networks, servers etc. are duplicated across the estate). Contingency Planning managers therefore operate on the basis that the overall system is already low risk. As a consequence, ongoing contingency planning is focused on drawing together all existing documentation into a framework document that supplements the Security Acceptance Test Specification (RS/ACS/002) by defining in detail the actual deliverables (and methods of review and assurance of deliverables) associated with Requirement 830.

The Business Continuity Framework (CS/SIP/002), owned by the CS Operations Manager, is under active production and is aimed at achieving acceptance prior to NR2 Live Trial. It defines the methodology agreed between ICL Pathway, POCL and DSS for the handling of all aspects of business continuity. In scope, the document defines the Business Continuity Framework itself, the services covered, the contingency plan, test strategy, deliverables, deliverable schedules and a review mechanism.

The constituent elements of the framework comprise a project plan, business continuity management process, test strategy & plan and review strategy as well as the actual contingency plans. Contingency plans themselves will comprise: service definition, risk analysis/service impact and escalation contacts and contain reference to proposed contingency Operations Manuals that will eventually contain step-by-step procedures to be followed by managers in the event of an incident.

A resilience and recovery strategy for all aspects of the service has been prepared and is documented in TD/DES/31.

4.6.2 Status

The project plan is owned jointly by ICL Pathway, POCL and DSS and is being reviewed at regular monthly meetings between the tripartite. The Group is currently developing the Business Continuity Management Process (CS/PRD/031) and defining what could trigger a business continuity event. These scenarios are being mapped into developing contingency plans.

A list of business critical areas and their owners have been identified and these will appear in the Operations Procedures Plan for NR2.

Assurances are being obtained from CS managers that suitable and sympathetic plans are being developed/completed in their respective areas and that they are in a position to respond adequately to possible contingency events. Subsequent reports have shown no serious shortfall in arrangements. Similar assurances are being obtained from Business Continuity Managers in companies providing service support to ICL Pathway.

A number of POCL initiated E2E walkthroughs have been undertaken in order to identify potential gaps in procedure. Some good value observations have been made and these are being taken forward by the tripartite group where they consider there is cause for review.

A technical integrity test plan has also been prepared and test reports have been produced. These have identified areas for further consideration. Three quarters of all issues highlighted from the tests have already been resolved to the satisfaction of all interested parties. All tests have been run against data volumes expected at NR2 and these have fully demonstrated the capability to cope during live trails.

4.6.3 Conclusion

The strategic approach adopted is sound and extensive documentation exists. Potential problems have been identified, documented and scheduled into action plans. Liaison amongst the interested parties is well established and issues are jointly owned and resolved. Business Continuity Managers are satisfied that they have the right people doing the right thing in the right places at the right time.

4.7 Management Information

Management Information Systems under the control of Customer Service comprise facilities for monitoring Pathway's compliance with contracted Service Level Agreements, and for tailoring reports to meet the needs of both Pathway management and the Authorities.

4.7.1 Reliance on Key Personnel

The calculation and comparison of actual performance against contracted service levels involves a complex set of calculations, the standards of which are currently held on a set of spreadsheets, which are loaded into the data warehouse to facilitate the conformance calculations. There is adequate short-term cover for staff absence. Due to the complexity of the volumetrics model, however, the MIS Team Leader responsible for the project has significant autonomy, and there is no alternative member of staff capable of immediately taking over the project in the event of the present incumbent's untimely departure.

While the present incumbent is a person of proven ability and integrity, it must nevertheless be recognised that this situation places Pathway at risk. It is recommended that this risk is mitigated by detailed documentation describing the model in terms that will facilitate another person's taking over the project without a phased hand-over.

4.7.2 Timeliness of information

When requests are made for ad-hoc reports, access must be gained to the Data Warehouse in order to obtain data in respect of encashments done or to enquire on calls made to CMS/PAS. The Data Warehouse does not hold archived data; if the data required is older than 26 weeks a request must be made for the required data to be loaded; data manipulation is then carried out using Business Objects. When data needs to be loaded from archive, DW is unable to supply the required data in time for Pathway to meet the SLA. This will be exacerbated if the 26 weeks is to be further reduced, as has been proposed.

It is essential that a solution be found to enable Pathway to meet the SLA – data must be delivered in a time frame that allows enough time for the analysis and reporting required.

4.7.3 System Testing

System testing has covered the operation of the Data Warehouse batch schedule jobs relating to the MIS applications in MIS0101. SLAM receives its data download after these calculations, and calculates the conformance figures. This function has not yet been tested.

It is imperative that the calculations performed by SLAM are tested to ensure that the reporting and monitoring of conformance figures is reliable.

Due to the complexity of the model that relates service level agreements to performance achievements, the system testers do not understand the model sufficiently to test the operation of the MIS system effectively.

It is recommended that MIS staff prepare a set of input data and expected results for use when testing the operation of the MIS system – both initially and when any changes are made.

4.7.4 Documentation of Processes and Procedures

Processes have been documented, but there are not detailed procedures that will enable a new employee to operate with a minimum of training. For present operations this has been partially mitigated by ensuring that, for every operational function, each responsible person has a backup.

It is recommended that detailed procedure documentation is prepared at the level that would facilitate consistent operation of the system by newly appointed staff.

4.7.5 SLAM

At the time of the audit staff running SLAM were experiencing problems with the stability and speed of response time of the application. They also reported errors in the reports being produced. Since then Oracle Express has been upgraded, which has apparently alleviated some of these problems. A workshop was held recently and included representatives from Testing & Integration and AT&C. An action plan has been agreed to address the outstanding issues. Outsourcing will be able to correct some of them for NR2 (this will be done by 1 March to allow Testing and Integration sufficient time to test and validate the changes); the balance will be held over for NR2+.

There is no contingency plan for MIS systems – they depend on recovery of the Data Warehouse in the event of a DRP being invoked. The relevant SLA requires that Pathway report conformance data to the Authorities within five working days after the end of a reporting period; the average time needed to run the reports is between two and four days. Since the reporting dates are a calendar month apart, and the Data Warehouse SLA on disaster recovery is 48 hours, it is felt that the exposure does not warrant the cost of implementing other contingency arrangements.

4.8 DSS Services

The BA Services delivered by Customer Service comprise the Payment Card Help Line located at Girobank, Bootle; Card and PUN production by DLR Card Systems; Temporary Tokens by DLR Secure Printing and the distribution of Cards, PUNs and TTs by Royal Mail.

4.8.1 Card and PUN Production

This activity is effectively controlled through the Card Production Management Strategy (CS/STR/003). Version 0.1 dated 07/08/98 was reviewed and it was agreed that it required a final review and approval.

It is recommended that this document is reviewed for content and accuracy and updated to reflect the approaching NR2 position. It should be approved and issued.

There is a wealth of lower level documentation to monitor stock values and production schedules and these are reviewed at the monthly progress meetings with De La Rue. There are also agreed procedures in operation at DLR covering the handling of 'spoiled' cards during production. In addition the DLR security procedures are overlaid with Pathway specific requirements and these were audited by Pathway during 1997. However, the monthly meeting review is not supported by any other form of periodic verification of stock values by Pathway, nor has there been any recent site or security auditing taking place.

The role of DLR in the Horizon solution is critical and it is recommended that Customer Service introduce regular stock validation exercises with DLR. It is also recommended that the processes and security measures in place at DLR are audited prior to the NR2 production increases.

4.9 POCL Services

The POCL Services delivered by Customer Service comprise the Horizon System Helpdesk at Stevenage, the Service Management Centre, also at Stevenage, and the management and control of the Field Engineers responsible for equipment repairs and replacement in the Outlets.

4.9.1 Horizon System Helpdesk

The activities of the HSH are governed by a large number of documents headed by a single document, the Helpdesk Document Structure Overview (CS/ACS/014). Version 1.0 dated 22/07/97 was reviewed and while the content was comprehensive it did not include references to the Payment Card Helpline - the complementary BA Helpdesk - and its approval date suggests that it warrants a thorough review.

It is recommended that this document is reviewed for content and accuracy and updated to reflect the approaching NR2 position.

The lower level documentation was comprehensive and the approach for removing any subjectivity in the initial problem analysis by Helpdesk Operators impressive. Escalation is controlled by the Helpdesk itself and the direct involvement of the Duty Manager occurs once penalty limits have been reached. This appears to be too late in the cycle as some time will be required for the Duty Manager to take control of the situation by which time penalties might be in force.

It is recommended that this aspect of the problem escalation process is reviewed with a view to advancing the direct involvement of the Duty Manager.

4.9.2 Service Management Centre

The SMC operate as the 2nd line support to the HSH and is involved in the diagnosis and resolution of known problems through the application of the 3rd line Known Error Log. Concern was expressed during the audit about SMC's readiness for NR2 and the anticipated increase in calls once more Outlets come on-stream based on their ability to deal with calls within the required SLAs. It was suggested that calls are being passed through to SSC for action that should have been cleared as 'known errors' by SMC.

Appropriate action to address this issue has been recommended earlier in this report.

4.9.3 Review Process

The review process for POCL (and BA) Services operates at three levels:

a. Internal CS Review, which identifies potential or actual hotspots for action either internally, directly with the supplier or via the Horizon Service Management Review Forum.

b. With the supplier where specific SLA issues are dealt with.

c. At the Horizon Service Management Review Forum which is the overarching body, chaired by POCL, that monitors the operation of all aspects of the Horizon service.

Meetings are minuted and where SLAs are not being met recovery plans established and monitored. Plan DSP/PLA/HH/001 v1.4 dated 17/8/98, which relates to contingency arrangements for the Horizon System Helpdesk, was reviewed and it was noted that some action dates were being moved without adequate explanation. The most extreme example was one which slipped from 03/98 to 10/98 with no supporting text.

It is recommended that when action dates are moved in the Recovery Plans some justification text is added to provide an audit trail of changes for subsequent review.

4.10 Communications

4.10.1Liaison With Other Pathway Groups

Liaison with other CS areas is effected mainly by a combination of established regular management meeting and other ad-hoc meetings arranged as and when operationally required.

The active detection of real or attempted fraud is not currently a specific responsibility of the SSC, BSU or Incident/Problem Management. Nevertheless, they are considered to be in an ideal position to spot anomalies which may indicate fraudulent activity or other malpractice at the Counter Outlets.

There have been a couple of occasions where Customer Service staff have become aware of spurious activity and, in the absence of a formal referral mechanism, have provided an ad-hoc report to the CS Problem Manager. Customer Service recognise the value of such referrals, are sympathetic to the needs of Fraud Risk Management and will do what they can to assist when incidents arise. They are not however trained or resourced to provide this service.

Given the potential of Customer Service to assist in this area it is recommended that SSC and Problem Management open a formal dialogue with FRM to establish how they could contribute more fully to the general anti-fraud effort and formalise an agreed referral procedure. The procedures established by BSU (CS/PRO/027) should be used as a reference.

5 Annex 1 - Terms of Reference

1. Audit Aims

The audit will provide assurances to ICL Pathway Customer Service Director about the policies, procedures and practices of Customer Service, with particular regard to New Release 2 and the impact on CS that the implementation of that Release will have.

2. Objectives

2.1 To ensure that CS policies, procedures and practices exist and support those of ICL Pathway and the delivery of an efficient and effective service to both BA and POCL.

2.2 To ensure that the CS organisation is capable of supporting the imminent release of New Release 2 to the existing automated estate and the NR2 increment (+~100 outlets).

2.3 To assess the degree of readiness and preparation for National Rollout and the impact of the increased estate on current organisation and resources.

2.4 To assess the effectiveness of internal controls in particular areas of the CS organisation:

a. System Support Centre.

b. Non-BES elements of Business Support Unit & RED.

c. Incident and Problem Management.

d. Business Continuity.

e. Management Information production.

These activities are all located at BRA01.

2.5 To assess the effectiveness of the management of services supplied to CS as part of the Horizon solution:

a. Horizon System Helpdesk at STE09.

b. Payment Card Helpline at Girobank Bootle.

c. System Management Centre at STE09.

d. De La Rue Card Technology at Tewkesbury.

e. De La Rue Secure Printing at Dunstable.

Member(s) of the audit team may visit the service supplier if concerns are raised about the quality of service received or the state of the relationship.

2.6 To review the communication channels in place between CS and other parts of ICL Pathway and the exercising of those channels.

3. Exclusions

The BES activities of the Business Support Unit and the Reconciliation Exception Database will not be included as they were the subject of an Internal Audit during June 1998 and subsequent follow-up reviews based on the agreed Corrective Action Plan.

However, the current status of the RED CAP will be reported as part of this audit, especially where the move to BRA01 affects changes made following the June audit.

4. Dates

The audit will start during week commencing 23rd November and complete before Christmas 1998 with a final report to the Customer Service Director, ICL Pathway.

5. Approach to the Audit

The nature of the CS operation and availability of audit resource means that it will not be possible to complete the audit in a two-week block. Rather a series of interviews and site visits will be conducted at mutually agreed dates at the location where the work is carried out.

The available procedural documentation will be scrutinised and used to structure interviews where the emphasis will be on confirmation that procedures are successfully deployed and complied with.

It is understood that a series of Operational Readiness Reviews are taking place within CS. Where an ORR has been completed the outputs and action lists will be used as inputs to the audit.

Every effort will be made by the audit team to minimise interruption to the normal work of the Department although this has to be tempered with the need to complete the audit within the required time scales.

6. Audit Resources

The following members of the Quality and Risk Management Directorate will be involved in this audit:

Jan Holmes	:	Pathway Audit Manager [*]
Stanley Loam	:	Internal Auditor [*]
Barry Procter	:	Pathway Security Manager

David Groom	:	Pathway Quality Manager
Graham Hooper	:	Alliance & Leicester Internal Auditor [*]

[*] Full time members.

7. Reporting

At the conclusion of the audit a draft report will be produced and discussed with the auditees. Corrective actions will be agreed and documented in a Corrective Action Plan. A final report will be produced and distributed to members of the Customer Service and Quality & Risk Management Directors only.

Further distribution will be at the discretion of the Customer Service Director.

8. TOR Distribution

Steven Muchow	:	Customer Service Director
Martin Riddell:	Operations Manager	
Paul Westfield:	Information Services and Processes Manager	
Peter Burden	:	Support Services Manager
Mik Peach	:	SSC Manager
Martyn Bennett	:	Director of Quality and Risk Management

Audit Team Members

6 Annex 2 – Current Status of the BSU CAP (IA/CAP/002)

007/1 Procedures between BSU and Contracting Authorities currently being prepared to cover all aspects of reconciliation incident handling. Lower level procedures are documented in CS/PRO/055.

007/2 Assessments of incident volume and the likely impact on staff resources post NR2 continue. Precise requirements are difficult to gauge until EPOSS/APS incidents are reported and analysed during live trials. A regular working review of the size, percentage and type of exception transactions continues. BSU will have access to Discover tools at NR2.

007/3 Job descriptions have been written for all members of BSU. These will however be subject to ongoing review in light of changes reported during the tail end of R1c and those in NR2.

007/4 BSU have trialled a "non names" approach in reports and this has been successful.

007/5 Status as per IA/CAP/002. Documented in CS/PRO/055.

007/6 Specification produced and REDv3.3 now contains adequate functionality to maintain an auditable history of changes made to information. No amendment to previously entered data is possible.

007/7 Status as per IA/CAP/002. Documented in CS/PRO/055.

007/8 Status as per IA/CAP/002. Documented in CS/PRO/055.

007/9 Status as per IA/CAP/002. Documented in CS/PRO/055.

007/10 Status as per IA/CAP/002. Documented in CS/PRO/055.

007/11 Status as per IA/CAP/002. Documented in CS/PRO/055.

007/12 Status reported at para 4.4.4.

007/13 Status reported at para 4.4.4.

007/14 Key procedure documented at 4.4.5. A purge of unnecessary documentation has been undertaken. Key documents have been identified and are now stored electronically on the BSU server.

007/15 Status as per IA/CAP/002.

007/16 REDv3 allows password control at clerk and managerial levels and prompts regular password changes utilising NT security protocols.

007/17 REDv3.3 contains drop down initials field within each RED update action. However, the absence of a password + token access protocol means that each input to RED cannot positively be attributed to the operator.

007/18 Status as per IA/CAP/002. Specification for RED audit trail produced.

007/19 All RED reports now stored in electronic format on server. No paper records are now kept.

7 Annex 3 – Summary of SSC Security Review

A review of the security aspects of the SSC at Bracknell was undertaken concurrently with the audit of Customer Service. Findings raised in that report, which was issued as RS/REP/004a, are appended here for convenience.

7.1 Scope

The IT Security audit concentrated on four aspects of the controls required in a live support environment: Anti-Virus, Cryptographic key handling, Business Continuity & Data Protection.

7.2 Anti-Virus.

Members of the SSC operate dual workstations in compliance with the ICL Pathway Access Control Policy; one for use on the live network, the other for 'regular' office applications and access to the ICL corporate network.

7.2.1 Office Desktop

Due to a recent change in the provision of ICL Pathway I.T. services, for the purposes of virus detection and prevention, the SSC is no longer a member of the Pathway 'domain' which provides automatic virus software update.

Since the change in anti-virus software provision, a loose arrangement has evolved whereby individual staff members download the 'current' version of Dr Solomon's AV software. This is not a formal arrangement and is not enforced.

7.2.2 The Live Network

RS/REQ/012 - 'Group Definitions for the Secure NT Build Release 2' describes the software to be made available to each group operating on each NT platform. No AV software is mentioned in this document or any of the secure NT build documents. As a result, no AV software is present on any of the NT workstations accessing the live network.

It is recommended that:

- *The group responsible for the provision of ICL Pathway I.T. services takes steps to ensure they can provide the SSC with automatic, monthly updates of the Dr Solomon anti-virus software.*
- *All relevant documents and builds are modified to incorporate Dr Solomon anti-virus software and a strategy is agreed for its regular (monthly) update.*

7.3 Cryptographic Key Handling

During Release 1c, the Manager of the SSC was issued with a subset of the live cryptographic keys but no operating instructions were issued.

The keys are retained securely and are under the sole control of the SSC Manager. At no time have they been in danger of loss or compromise.

It is recommended that:

- *The SSC Manager is nominated as a formal Cryptographic Key Custodian.*
- *He is issued with a complete set of cryptographic keys for appropriate releases.*
- *He receives a set of Cryptographic Key Operating Instructions for appropriate releases.*

7.4 Business Continuity

The SSC provide third line support behind the HSH and the SMC, both of which operate out of Stevenage 09 and neither of which yet have adequate business continuity arrangements for long term site or service unavailability.

Whilst the HSH and the SMC contingency arrangements are out of scope for this audit, the burden on the SSC in their absence would be untenable.

No formal, documented business continuity arrangements currently exist for the SSC. It is anticipated that in the short term (up to four working days) relevant SSC experts would relocate to Feltham and work from there on PC's configured from existing build scripts. Thereafter, application support would revert to the appropriate development team.

It is not clear how SSC staff operating from Feltham would gain access to the live environment.

It is recommended that:

- *All elements of CS with access to the live service (SSC, BSU, OTT and Reference Data Support) are included in the existing business continuity exercise owned by the CS Operations Manager.*
- *Given the sensitivity and importance of their work the SSC need to consider the human elements of contingency too - their staff complement is small but they are highly skilled in specialist areas.*

7.5 Data Protection Act

Members of the SSC have received formal Data Protection Act training from the ICL Commercial & Legal Group and appear particularly sensitive to the requirements around non-disclosure.

Doubts remain about the awareness of the various groups and companies on whom they depend for fourth line support.

Recommendations arising from this part of the review, which have already been addressed earlier in this report (section 4.3.3), were:

- Contracts with providers of fourth level support are modified to incorporate the New European Union directives on Data Protection.

- An explicit definition of ‘personal data’ is formalised, particularly where an obscure combination of fields may reveal personal data in a way that is not immediately obvious.