Document Title: Business Support Unit - RED Audit

Document Type: Audit Report

Abstract:

This document presents the findings of an audit of the function of the Reconciliation Exception Database operated by Business Support Unit.

Status: APPROVED

Distribution:

Distribution:	S. Muchow	P. Westfield
	R. Brunskill	J. Holmes
	Library	

Author: Graham Hooper (Girobank)

Comments to: Bharat Thakrar

Comments by: 29th December 2000

0 Document control

0.1 Document history

Version	Date	Reason
1.0	20/12/00	Issued for approval

0.2 Approval authorities

Name	Position	Signature	Date
Martyn Bennett	Quality Director		

0.3 Associated documents

Reference	Vers	Date	Title	Source

0.4 Abbreviations

0.5 Changes in this version

0.6 Table of content

1 Introduction

The Reconciliation Exception Database (RED) is where ICL Pathway Business Support Unit (BSU) investigate financial exceptions and arrange for any required financial charges to take place. Pathway Internal Audit asked Alliance and Leicester Fraud and Risk Management to undertake an audit of the RED function and its associated processes.

2 Scope

The audit was undertaken in accordance with the Terms of Reference (attached at Annex 1) and in conjunction with internal audit requirements as set out in requirements specification document. Specifically relevant are the requirements detailed at para 8.6.

The audit was undertaken on various dates between 1.6.98 and 19.6.98.

3 Summary of Recommendations

The audit concludes that existing state of compliance with RED Internal Audit Requirements is:

- RED-IAR1 - Met (subject to verification of procedures at HSH);
- RED-IAR2- Met;
- RED-IAR3- Met in part;
- RED-IAR4 - Not met;
- RED-IAR5- Met in part;
- RED-IAR6 - Not met;
- RED-IAR7 (i) - Not met;
- RED-IAR7 (ii) - Met in part;
- RED-IAR7 (iii) - Met in part;
- RED-IAR7 (iv) - Met;
- RED-IAR7 (v) - Met;
- RED-IAR7 (vi) - Met.

4 Specific Recommendations

Para 5.2: Current procedures for the operation of the RED facility, particularly that involving arrangements for financial settlement, are not formalised.

It is *recommended* that an operations manual be produced and that agreed recommendations from this report are included.

Para 5.3: It is anticipated that subsequent releases of the Pathway solution will increase significantly the work of the RED facility.

It is *recommended* that an investigation be undertaken to establish the likely impact on staff resources.

Para 5.5.1: Considerable BSU staff time is currently used to obtain material information required for investigations.

It is suggested that consideration be given to providing BSU with on-line, read only access to Oracle/Discover. This may help speed up resolution times - particularly in light of likely workload increases as roll out progresses.

Para 5.4**:** BSU staff have no formal job descriptions although they are aware of personal objectives.

It is *recommended* that these are developed in light of requirements emerging from the RED operations manual and used for staff appraisal purposes.

Para 5.5: RED information is provided to a number of external contacts.

It is *recommended* that steps be taken by recipients to determine the protection offered to material originated in ICL Pathway.

Para 5.1.1: It is unclear whether the current amount and detail of client confidential data recorded on RED is actually required to fulfil contract requirements.

It is *recommended* that consideration be given to establishing whether this could be reduced or eliminated.

Para 5.6.1: All RED exception cases are allocated a reference number. This is not system generated and is vulnerable to user error.

It is *recommended* that REDv3 generates a unique, sequential number automatically.

Para 5.6.2: RED report forms are updated directly to screen, changes overwrite previous information and are possible without reference to higher authority and without an apparent audit trail.

It is *recommended* that REDv3 maintains an auditable history of changes to information as the exception investigation progresses.

Para 5.7.3: On occasion, manual debit instructions have been issued by BSU staff to CCS only to be amended after financial settlement because of further investigation.

It is *recommended* that adjustment schedules are not issued to CCS until it is certain that BSU action is completed.

Para 5.7.4: The reconciliation adjustment procedure between BSU and CCS has no formal or documented certification or authorisation process.

It is *recommended* that:

- all reconciliation adjustment schedules prepared by BSU are checked against supporting evidence and formally certified as correct prior to authorisation;
- certified schedules and their supporting evidence should be submitted to management for authorisation prior to referral to CCS for invoice adjustment;
- prior to authorisation the authorised signatory should undertake a sample check of schedules for accuracy of completion and a sample of individual cases against supporting evidence (either as a percentage of the overall total or 100% if lower than an agreed de minimus level);

Para 5.7.4: There is currently no appropriate segregation of duties between exception resolution and financial settlement.

It is *recommended* that:

- the person preparing the reconciliation adjustment schedules should not be the person who certifies their accuracy;
- the person certifying their accuracy should not be the person authorising adjustment;
- the person authorising adjustment should not have prepared or certified the schedule;
- no duplication of duties should be allowed at time of absence.

Para 5.8.3: The security of the preparation, certification and authorisation process for Post Office Fallback Operations (requiring the issue of manual cashcheques to beneficiaries) is inadequate for the reasons detailed in 3.8 above.

It is *recommended* that a similar procedure is developed to ensure an appropriate segregation of duties between these exception resolution cases and their financial settlement.

Para 5.8.3: Prepared cashcheques are currently returned by CCS to BSU for issue to the beneficiary.

It is *recommended* that they be issued direct to the beneficiary by a member of CCS staff who has played no part in the preparation of the cheque. A schedule of cashcheques issued should be maintained.

Para 5.9.2: SLCA staff have access to the same information as that by BSU staff.

It is *recommended* that physical security countermeasures for the area occupied by SLCA are commensurate with that recommended for BSU.

Para 6.2: The open-plan nature of the BSU area is inadequate to protect effectively the sensitive and legally privileged information held on RED. Verbal, documentary and visually displayed information is currently at risk to unauthorised disclosure.

It is *recommended* that:

- BSU is moved to a controlled environment;
- Access to BSU should be limited by the use of AAC to BSU staff and those persons specifically authorised by its management;
- VDUs should be positioned to avoid sight by unauthorised persons;
- Its location should not permit conversations by BSU staff to be overheard;
- The BSU manager should also be provided with a similarly controlled environment.

Para 7.1: There are currently no control procedures for access to keys protecting the storage of RED information.

It is *recommended* that a key control/log procedure is developed to maintain an auditable record of key holders.

Para 7.2: BSU staff are unaware of any available protective marking system to identify the client/contractual sensitivity of RED material.

It is *recommended* that a suitable protective marking be afforded all BSU output material to denote clearly the level of protection required.

Para 7.3: Computer passwords are changed occasionally on an ad-hoc basis.

It is recommended that the RED system be designed to prompt password changes automatically at least monthly. The prompt should not be capable of user over-ride.

PIDs are not currently used in conjunction with password control and it is not therefore possible to associate input changes with the operator who performed them.

It is *recommended* that a PIN+PID system be adopted.

Para 7.5: It is unclear whether RED has an audit trail facility that permits historical interrogation of RED inputs.

It is *recommended* that the efficacy of its audit trails be established.

BSU staff are unaware of whom to contact in the event of problems with RED. It is recommended that this information is included in an operations manual.

Para 8.3: The RED report archive (containing the definitive repository of all information) is located in the same area as BSU.

It is *recommended* that this be relocated to a secure storage area away from both BSU and the back-up server.

5 System Overview

RED is where ICL Pathway Business Support Unit record, investigate and resolve financial exceptions and arrange for any required financial charges to take place. Exceptions are forwarded via the Horizon System Helpdesk (HSH) and PinICL. An explanation of the types of exceptions and the main data flows currently handled by RED are attached at Annex 2.

6 Operational Overview

BSU is a small self-contained unit that operates as part of ICL Pathway Customer Services Section. BSU currently comprises five full-time members of staff – a manager and four assistants. The latter undertake the primary initiation, recording, investigation and resolution work of RED. The duties require extensive liaison with other internal ICL Pathway sections and also with the Contracting Authorities and other external players. The unit manager provides staff line-management control and oversees the general day-to-day work, providing an interface as necessary with managers in other sections.

6.1 Data Classification

The work of BSU involves extensive live handling of client confidential/personal data relating to DSS Benefits Agency (BA) customers. This information is designated by HM Government as “Restricted” and is covered by the provisions of the Data Protection Act (DPA) 1984 (including the requirements of the European Union Data Protection Directive 1995), the Social Security Administration Act 1992 and by a general duty of confidentiality as per the contract between ICL Pathway and the Contracting Authorities. Protection sufficient to prevent the unauthorised compromise of sensitive information is therefore required to satisfy extant legislation, maintain customer confidence and avoid reputational damage. BSU also handle quantities of information (both in written and electronic format) relating to internal ICL Pathway matters that, in the commercial interests of the company, warrant a degree of protection from unauthorised compromise.

A significant amount of client confidential material is held on RED (ie. information relating to identifiable, living individuals) and as such, requires suitable and costly countermeasures to prevent compromise and comply with relevant legislation. BSU consider that this level of customer data is often irrelevant to the efficient resolution of cases and, in general, adds little positive value to their work. Further, the holding of such information may expose ICL Pathway to the spectre of subject access requests under the DPA. Whilst it may be that this information could be/is currently used by ICL Pathway for other purposes (or is required by the contracting authorities), consideration should be given to reviewing whether the current amount of client information recorded on RED is appropriate or necessary.

6.2 Current Procedures

There are currently no formalised procedures for the day to day running of the unit although staff have ready access to both high level documentation and the advice of the unit manager. They are also aware that an operations manual is being produced. Operational procedures have been developed on an ad-hoc basis according to the demands of the work. BSU staff report no known occurrence of a breach of security but would bring any such incident immediately to the attention of the unit manager.

5.3 Staff Resources

Four assistant staff are currently allocated to BSU/RED and are generally interchangeable across all functions (one member is currently allocated to SLA to work on developing RED v3). There is therefore an in-built flexibility in the event of expected/unexpected staff absence. They cope easily with the current volumes of work generated under r.1.2. Based upon current volumes (and assuming current software-fix status) there will be a significant increase in exception referrals following r.2. and programme rollout across additional benefit groups and Post Offices. The full extent to which this impacts on BSU is yet to be determined but may affect significantly the number of staff required - particularly in view of the aggressive exception resolution timescales contained in the SLA.

5.4 Knowledge/Skills

BSU staff are experienced and, in the absence of specific instruction, have adopted a common sense approach to the work. Informal case conferences are held, knowledge is shared and details are committed to paper as and when required. No formal investigative training has been undertaken by staff but case-based reasoning is used to build up expertise and, as a result, analysis skills have been developed. In the main, this approach appears to have worked well. BSU staff have developed a section identity, are committed to the work and are fully aware of its sensitive nature. They have no formalised job descriptions but have been set personal objectives for appraisal purposes.

5.5 BSU Interfaces

There is no hierarchy within BSU and all staff liaise on a demand-led basis in order to get the work done. They enjoy good relations with both internal and external contacts. Main daily internal interfaces are with other Customer Service sections (for SLCA/MIS issues), Fraud Risk Management, Business Process section, SSC Bracknell and CCS (Finance). Main daily external interfaces are with BA/CAPS Exception Service, POCL at Chesterfield, BA/POCL at Lisahally and PCHL at Bootle. BSU also attend monthly meetings with Horizon Programme representatives. BSU is totally reliant upon the integrity of the information with which they are supplied and have no control over the security subsequently afforded any RED data issued to external contacts (i.e. Horizon Programme, BA and POCL). The direct BSU/RED interface with CCS involves a manual data flow whilst that with SLCA is on-line.

BSU spend a considerable amount of time during case resolution contacting SSC by telephone to obtain material, non-client sensitive, information relating to transactions under active investigation (dates, times, amounts etc). As roll-out progresses and exception volumes rise, the amount of staff time spent on the telephone obtaining this necessary information will increase quite substantially. It is therefore suggested that consideration be given to providing BSU staff with on-line, read only access to Oracle/Discover to enable them to obtain information direct. This would speed up overall times for resolution of cases and free up resources for other work.

5.6 Casework (RED Forms/Reports)

Casework referrals are generated either by receipt of documents by internal courier/mail, faxes (i.e. CBOS reports) or on-stream via PinICL at SSC Bracknell. A summary of the main exception data-flows into RED is at Annex 2. RED report forms are raised on the RED system for all exception incidents and these form the basis of ongoing live exception cases. A copy of a typical RED report is attached at Annex 3. The number of exception referrals varies on a day-to-day basis from nil to seven. Mondays generally see busier traffic. The live load fluctuates and BSU staff could not provide an estimate. RED is currently operating on RED v.2. BSU/SLCA staff are in the process of developing RED v.3.

All exception cases are allocated an incident number on RED forms by BSU staff. The RED system does not do this automatically. There is therefore a possibility that the same number may be allocated to more than one referral or that sequential numbering is not maintained. This could lead to confusion and future reconciliation problems.

RED forms are updated directly on screen as resolution work progresses. Changes to existing data are possible without prior referral to a higher authority. The RED system has no attendant audit trail facility and subsequent entries overwrite historical information. The integrity of the data it contains therefore relies solely upon the honesty of its operators and the veracity of ad-hoc management checks.

RED reports can be printed at any time either as a status report for ongoing cases or as a final report once exception resolution has been satisfactorily concluded. Every exception reported to BSU results in the generation of a form and a hard-copy report. Final reports detail the reason for the reconciliation exception, the conclusions of the subsequent investigation and recommendations for further action (e.g. for software fixes). RED reports therefore play an important role in influencing changes to programme procedures. Final RED reports also provide the vehicle by which manual debit/credit instructions, as appropriate, are referred to CCS.

RED reports have three informal status levels – ongoing cleared and closed.

- <u>Ongoing:</u> cases that are the subject of active enquiry;
- <u>Cleared:</u> cases that have been resolved the satisfaction of all parties and any required software fixes have been identified;
- <u>Closed:</u> Information from cleared cases has been used to update exceptions knowledge, any credit/debit action has been completed and cases have been put away.

5.7 Manual Debit/Credit Instructions

The BSU manager reviews all cases where resolution requires the issue of manual debit/credit instructions by CCS. BSU staff report that they hand a hard copy of the completed RED report to the manager together with any available supporting evidence. After due consideration the manager agrees manual debit/credit action and advises BSU staff to refer to CCS for invoice adjustment.

There is no formal guidance on what the precise procedure should be. In practice, the BSU manager agrees action verbally and BSU staff then create a schedule of cases requiring adjustment. These are then E-mailed to CCS with a request for adjustment.

CCS is the sole invoicing point for ICL Pathway. CCS prepare a summary reconciliation settlement form and scheduled payments are invoiced generally on a monthly basis. After their action, CCS return a copy of the schedule and associated invoice number to BSU for their records. BSU record the invoice number on the associated RED report and print a copy of the RED report for filing. CCS retain securely a copy of schedules and invoices for audit purposes.

The system has caused some reconciliation problems in the past. On one occasion a manual debit instruction was actioned by CCS, only to be amended later by BSU who had, in the interim, established that no adjustment was in fact appropriate. To avoid the recurrence of such an overpayment, CCS now check the status of schedules with BSU prior to final invoice action. However, as programme rollout progresses and payments increase this will become impractical.

The CCS manager also expressed some concern that there is no way of knowing whether the schedules have been prepared correctly. The schedules contain neither an accuracy certification nor a management authorisation. Under the existing system there is no evidence of an appropriate segregation of duties or of a documented certification/authorisation procedure. The BSU manager is, in effect, by-passed. Credit/Debit schedules are prepared by BSU staff and, following cursory endorsement, are then returned to them for referral to CCS. It is therefore possible for invoice amounts to be amended before final referral to CCS.

5.8 Manual Cheque Payments to Beneficiaries

Exception resolution of Post Office Fallback Operations (Ref: IA/REQ/001 – Para 8.1.2) can result in a requirement to issue a manual cashcheque payment direct to the beneficiary negotiable at a nominated Post Office. This procedure has been used only twice and BSU staff are somewhat uncertain of the required procedure.

A copy of the appropriate RED report (containing details of the reconciliation differences) is prepared by BSU staff and handed to CCS together with an accompanying letter for issue to the beneficiary. The accompanying letter contains the associated RED incident number. A cashcheque is then prepared by CCS and this is given back to BSU for issue to the beneficiary. The process has been documented by CCS and a copy is attached at Annex 4. An appropriate and secure procedure has also been developed by CCS for the receipt of any refunds from beneficiaries resulting from overpayment cases.

The procedure for physical storage, retrieval, writing and authorisation of the actual cashcheques by CCS was investigated and was found to be both secure and auditable. *The requirements of RED-IAR7(iv, v and vi) are therefore met.*

The process of certification and authorisation by BSU of the RED mandate is however inadequate for the same reasons outlined at paragraph 5.7.4. In addition, it is inappropriate that completed cashcheques are returned to BSU for despatch to the beneficiary – this should be done by CCS staff. BSU record the cashcheque details on the associated RED report and keep a separate photocopy. A formal schedule of all cashcheque payments to beneficiaries should be maintained by CCS to provide a single, accessible and auditable record of all payments. *Overall the requirements of RED- IAR7(i) are not met. The requirements of RED-IAR7(ii and iii) are met in part. The requirements of RED-IAR3 are met in part.*

5.9 Information flow to SLCA

Another flow of information from RED is to the Service Level Contract Administration Section (SLCA) physically located away from the Customer Services area. SLCA undertake the monitoring of all RED reports to establish performance against agreed contract service levels. Information from relating to four main RED SLAs are subsequently included in daily reports to senior management or in monthly reports via Service Performance Review.

In addition to any hard copy information provided to them by BSU, SLCA has independent on-line access to the RED system and also to information held in the Data Warehouse. SLCA staff therefore have access to the same RED information that BSU staff do. A member of BSU staff is currently working with SLCA staff to develop RED v.3 and, in his absence, a member of SLCA provides cover.

The area occupied by SLCA has operating AAC that allows access only to SLCA staff.

A few of the recommendations made in this report to improve the integrity of the RED database have already been identified by SLCA and are being addressed in RED v.3.

7 Physical Security

7.1 Location

BSU operates in an office area located at ground floor level adjacent to the access road to the main site car park and within the boundary of the site perimeter fencing. BSU is sited within an open-plan area that is also occupied by over 30 staff of varying grades from other Customer Service sections. A number of small offices have been constructed on one side of the main office area. These are of plasterboard stud-partitioned construction and have floor to ceiling glass windows that border the main office area. The BSU manager occupies one of these offices, which he also shares with managerial staff of other Customer Service sections.

7.2 Access Control

The area is protected by swipe-card automatic access control (AAC) at its two entrances and by passive infra-red intruder detection. The system however currently allows access to all ICL Pathway staff, not just Customer Services personnel. This presents a significant risk to information held by BSU. In addition, the AAC is not supported by the use of additional PIN protection and there is therefore a further risk from misplaced or stolen AAC tokens. Staff who cease to work for ICL Pathway have their AAC tokens recovered which prevents subsequent entry to the area.

7.3 Privacy

BSU itself is not physically separated from other customer service work areas although some effort has been made to provide segregation by the use of low-level acoustic screening and the arrangement of filing cabinets. This is however largely cosmetic and provides little or no privacy. Staff from other customer service sections frequently pass along the corridor by BSU and sometimes engage staff in conversation. BSU confirm that whilst other staff are aware of the sensitive nature of BSU work they have no authority or need to know.

The VDUs of the RED access database (on which reconciliation exception work is undertaken) can be overlooked both from this corridor area and from above the acoustic screening and filing cabinets surrounding the unit. In addition, the VDUs could, theoretically, be overlooked from the windows adjacent to the car park access road. Any such attempts would however be unlikely and would probably be noticed by other Customer Service personnel. There is no signage on adjacent windows that would indicate the nature of the work undertaken.

7.4 Counter-eavesdropping

BSU staff often discuss information of a sensitive nature both between themselves and with clients on the telephone. The siting of the unit affords no protection against both deliberate and accidental eavesdropping by other members of Customer Service staff. The use of higher-level acoustic screens would do little to improve the situation and would also affect adversely the level of natural daylight reaching adjacent office areas. Work is never discussed outside the confines of the unit (i.e. in the cafeteria).

The office used by the BSU manager is also shared by his immediate manager and one member of his staff from the IS&P area. Sensitive discussions between BSU management and staff, and telephone conversations with external parties are therefore vulnerable to eavesdropping. In addition, the BSU manager has a PC that is used amongst other things to record and access sensitive MIS information. This is vulnerable to overlooking by unauthorised persons. Sensitive hard-copy documentation handled by the BSU manager (ie. E-Mail printouts and hard-copy RED reports provided by BSU staff) are similarly vulnerable if left unattended.

In view of the findings detailed above *the requirements set out at RED-IAR4 are not met.*

8 Information Security/IT Controls

8.1 Physical Data Storage

Hard-copy casework and files are generated, processed and stored within BSU. These can contain details relating to identifiable individuals and information of a commercially sensitive nature. They are stored in lockable filing cabinets to which all staff have access. Staff report that they lock files away at the close of business and secure keys. There are however no formal key control procedures and staff do not maintain a key log. There is therefore no auditable facility for determining physical access to files or documented contingency arrangements.

When available space is exhausted in the main filing cabinets, RED reports closed by BSU are transferred to an archive in an adjacent area.

It is intended that all records of exceptions handled, investigated and resolved by BSU and recorded on RED will be retained for a period of not less than 7 years. Staff are aware of this requirement. RED information provided to SSC will be similarly retained. *The requirements of RED-IAR2 will therefore be met.*

8.2 Clear Desk Policy

An informal clear desk policy has been adopted - the aim being to lock away all paperwork before the close of business. There are however no formal document control procedures and BSU staff are not aware of any protective marking system used within ICL Pathway to visibly designate sensitive personal or commercial information.

8.3 PC Access Control

Access to computer based systems, including RED, is controlled with each member of BSU having a specific alphanumeric password. Staff report that they do not share each other's passwords nor do they write them down. Staff are aware that passwords should be changed regularly but in practice this only happens occasionally. *The requirements set out at RED-IAR5 are therefore only partly met.*

Personal identification devices (PIDs) are not currently used in conjunction with password control. It is therefore not possible to directly associate input changes with the operator who performed them. *The requirements set out at RED-IAR6 are therefore not met.* Screen savers are used and in general are set at about three minutes although there are no set rules for this. Passwords must be re-entered after this time in order to re-gain access to the system.

8.4 Disposal arrangements

All unwanted hard-copy outputs from BSU are disposed of as sensitive waste. This is shredded in a machine adjacent to the section. It was however noted that the top of this machine was stacked with documents awaiting shredding from other Customer Service sections. There may therefore be some risk of compromise unless material is shredded immediately.

8.5 Data Back-Up

Information is backed up nightly to a central server physically located away from the Customer Services area. Staff did not know whom they should contact in the event of a forgotten password, system malfunction or other contingency but assumed that they would have access to a system administrator should such a problem occur. Staff were unaware whether any audit trail facility operated with non-PAS systems.

8.6 Security Compliance

The BSU manager undertakes random checks on the general state of security within the unit and summarily checks every RED report before issue. These procedures are not however formalised or documented. Checks are undertaken on statistical information provided for SLCA purposes and are included in monthly operational review documents for other MIS/management purposes.

9 Contingency Arrangements

Data held on RED is backed up daily to a server located away from the BSU area. Hard-copy RED reports are also held externally by other sections in ICL Pathway and also by the contracting authorities. There exists therefore alternative access to records in the event of loss of data through fire/flood etc. at BSU.

BSU staff are interchangeable in the event of absence and they ensure that there is always at least one person in attendance at all times. This is done informally although the BSU manager oversees the arrangements.

In the event of an emergency a GSM mobile phone is available to any member of BSU staff when working away from the office. Digital GSM phones offer adequate protection from eavesdropping via scanners.

The RED report archive is located in the same area as BSU. In the event of a disaster (fire/flood etc.) all electronic and paper RED records might be lost. It is therefore recommended that the RED paper archive is relocated to secure storage outside the immediate Customer Services area.