Subject REVIEW OF HORIZON CASH ACCOUNT SYSTEM - STAGE 2

Introduction

A review of the Horizon Cash Account System was undertaken following a request from the Horizon Programme Director. The objectives of the audit were reflected in the terms of reference which were agreed with him on the 15 July 1999. A copy of these is included at Appendix A. It was agreed that the review would be undertaken in two stages and this report reflects the findings from the second stage.

> We note that a number of the observations in this report appear to fall outwith the remit of the original TOR, which had as its objective "*to confirm that the end to end reconciliation and accounting processes are free from system inaccuracies or discrepancies*".

Management Summary

POSIS Investigations at Outlets

We were extremely concerned to be informed during the review that POSIS currently do not have access to archived data from the system. Data on the system is compressed and archived after 35 days. It was originally intended that access would be gained via the Fraud Risk Management Server, which formed part of the benefits payment system and has now been withdrawn. This means the business could be in a position where it is unable to investigate potential frauds or prosecute cases due to the unavailability of critical data.

Bob Martin, External Crime Manager for POCL's Security and Investigations Executive, informed us that the issue had been raised with senior managers from the project. Les Thorpe, Investigation Manager in North East Region, advised us that Pathway had estimated the cost to re-introduce the Fraud Risk Management Server to be in the region of £180,000 with an additional fee of £1,500 per manday for performing extraction. These concerns were highlighted after a possible fraud at Grange Park SPSO which is involved in the Horizon Live Trial.

In order that the business can investigate potential fraud cases, we strongly recommend that procedures to address this major risk are put in place. These should include:

- **a documented process, with a defined point of contact;**
- **agreed timescales for the receipt of information;**
- **an agreed specification for the information provided.**

> There is considerable background to this issue, and this has been discussed in much correspondence over the past 2-3 years between Horizon and SIE. Horizon has offered to meet with SIE to discuss these concerns on a number of occasions. The following is intended to clarify the position:
>
> **Background**
>
> 1) Transaction data **in the outlet** is indeed is only held for a limited period - usually 35 days. This is for practical reasons of storage capacity and performance, and is a figure designed to give a balance between the needs of the staff (this is usually enough to enable queries to be resolved locally, if problems are identified in the weeks following the production of a cash account) and that of the system.
> 2) However, the replicated copy of this data held **at the Data Centre** is retained on-line for 90 days within the Riposte message store (in TMS); every record is written to tape, to be retained for the period for which we have contracted (usually 18 months, but extended indefinitely if specific records are needed for support of a prosecution), and to be made available to POCL under the contracted audit requirements.

3) All transactions data is of course delivered by ICL Pathway to POCL's TIP system, which in the POCL IS Strategy is seen as the "Data Warehouse". Rather than having multiple departments in POCL seeking information from ICL Pathway, the strategic approach would be for these departments to seek this data from a single POCL repository. However, we understand that POCL SIE do not view TIP as a practical source of data for their needs.

Fraud Risk Management Service

4) There appears to be some confusion here regarding the purpose and history of the Fraud Risk Management SERVICE. This was a service for which BA (only) contracted from ICL Pathway, to provide reporting on BA specific fraud patterns, related to the Benefit Payment Service, and defined in a specific BA Requirement. POCL did not contract for this (although the BA/POCL PDA Fraud and Security Group did approach various areas of POCL on a number of occasions to suggest how POCL could benefit from investing in a similar service geared to POCL's data, to no avail). **The BA FRMS was never intended to act as a means of accessing specific POCL transaction data, and indeed being a BA service the non-BPS transaction data should not have been available to BA** (for sound commercial and data protection reasons).

5) Arrangements were reached between POCL SIE and BA Organised Fraud to enable the sharing of fraud related information, including that obtained from FRMS by BA, between the two organisations, for assist in the mutual objective of managing fraud with the Benefit Payment Service. Given the demise of the BPS, the BA FRMS is no longer relevant - with the exception of one report on "out of hours transactions", all of the FRMS reports were specific to BPS, and even if the FRMS still existed there would be nothing on which to report.

6) If POCL did wish to establish its own FRMS, geared to POCL's data (and therefore not restricted to only BPS-related activities), this could of course be done, and Pathway would undoubtedly be willing to provide this service. However, this would be a new requirement, and would need to be funded. Note the distinction here between a full FRMS, with sophisticated data mining and reporting tools, aimed at detecting patterns etc, and simple access to transaction data, which FRMS was never intended to provide.

Audit Access to Transaction Data

7) A documented process has been established between POCL and ICL Pathway for access to historical audit information from Pathway's central systems, under the auspices of the requirements on Audit (Requirements 699 and 829), using a "*Request for Information*" (RFI) procedure. This process involves the exchange of the RFI and data between nominated individuals in the audit domain, believed to be (originally) Hilary Stewart and (now) Chris Paynter of POCL National Audit, and Jan Holmes of ICL Pathway's Audit team. All requests from POCL would therefore need to be fed through the nominated POCL audit contact. The process is documented within the *Horizon System Audit Manual (IA/MAN/004*) This process was exercised during acceptance, but Pathway report that apparently no "live" RFIs have yet been processed by this route.

8) We understand that in the case of Grange Park SPSO the request did not follow the correct route and therefore was legitimately refused. There may be an improvement opportunity here in ensuring that those who require such information are fully aware of the correct route. [BSM 19990803001 refers].

Requirements specific to POSIS and/or SIE

9) The contract with ICL Pathway does not include any requirements relating to reporting tools specifically for Investigations staff. During the development of the *Access Control Policy* (*RS/POL/0003)* the needs for auditors and investigators were included within the role defined as "*POCL Auditor*" in that policy, represented by National Audit, and the combination of local access (using the Auditor office role) and access to the audit trail (as per the above RFI process) was we understand considered adequate.

10) If SIE require more sophisticated functions, including covert access to specific views on data within the office (eg complex reporting on the financial position in the office, copies of reports produced in the office, etc), then this would potentially not fall within the definition of "audit

access" and would be seen as a new requirement by ICL Pathway, to be introduced by Change Request. We are aware that SIE have held discussions on this directly with ICL Pathway, around additional "fraud control" requirements. Any such new requirements would have to be introduced via the Change Control process.

Bob Martin also advised us that Security and Investigation Executive (S&IE) had requested an expert witness statement from Pathway to support a prosecution and this had been refused on the grounds that there was no contractual requirement. John Cook advised us that there is a contractual requirement for Pathway to ensure that the system meets the requirements of the Police and Criminal Evidence Act. **There is a need for Pathway to agree with S&IE and Internal Audit how this requirement will be met, as well as the procedures for obtaining this evidence when needed for prosecutions.**

The requirement (R829.1) is actually that "*The CONTRACTOR shall ensure that all relevant information produced by the Service Infrastructure at the request of POCL shall be evidentially admissible and capable of certification in accordance with the Police and Criminal Evidence Act (PACE) 1984, the Police and Criminal Evidence (Northern Ireland) Order 1989 and equivalent legislation covering Scotland.*".

An outstanding Acceptance Incident (370 - LOW), exists against the POCL requirement, on the assertion by POCL that Pathway should product a witness statement to support prosecution. This AI revolves around the interpretation of "*ensure that all relevant information is evidentially admissible*" - POCL's view is that to be admissible it will need to be supported by witness statements etc; Pathway have stated that they will "*provide PACE statements as necessary to support a fraud prosecution*", but that "*the work required to produce draft witness statements*" is not within the scope of the requirement and will be done once POCL raise a Change Request.

This issue has been handled with Pathway by Bob Martin and Paul Harvey of SIE. The Acceptance Incident is still open, and its resolution would appear to primarily be a commercial issue.

[Note that the Benefits Agency had similar requirements (R741 and 780) covering their aspects of the service mirroring the above section, however these had a addition clause reading: "*The CONTRACTOR shall provide certification in accordance with the Police and Criminal Evidence Act 1984, PACE(NI) Order 1989 (and equivalent Scottish legislation) when necessary for a proposed prosecution to demonstrate that the Service Infrastructure was operating within normal parameters at time of an alleged offence.*" . This additional clarifying clause was lost at the time of the withdrawal of BA (at contract codification), but in any effect it (strictly) only referred to PAS and CMS, both BA services, even prior to BA withdrawal. Attempts were made to get this clause inserted into the codified agreement to apply to POCL, but without success].

Clearly, a process does need to be agreed between POCL SIE and ICL Pathway for the commissioning of PACE certification, statements and court appearances.

Transaction Processing

During the course of the review we were made aware of concerns that Transaction Processing had regarding the level of errors generated by Horizon outlets and the impact on operations with the roll out to further outlets. This is because the level of Class and Pivot errors are well above the expected levels of a 195 and 110 per week respectively. Currently the average weekly number in the six weeks to 14th July, the latest date where accurate data is available, is Class 415 errors per week and Pivot 192 errors. Only the Pivot errors appears to be showing a reduction.

TP were also concerned at:

- the work involved in correcting outlet cash accounts following the resolution of problems caused by incorrect carry forward figures and the discrepancies between receipts and payments;

- the legal implications of manual alterations to computerised cash account by Subpostmasters in the event of a court case.
- a problem with the analysis of Benefits Agency transactions in the first week following implementation of Horizon. The Migration Management software only allows 2 lines for the analysis of Benefits Agency transactions. The Agency attach great importance to the detailed analysis of payments into different types of pension and allowance as each type is subject to Parliamentary approval. We understand that a manual process has been put in place to provide this information. However, this process was not followed for 2 offices during the Live Trial rollout of 24 offices.

We confirmed that TP were raising incidents in all appropriate cases. **There is a need to ensure that the volume of work arising from the correction of errors is taken into account when assessing an acceptable rate of roll-out for the new system.**

> The error rate being experienced by TP is one of the statistics included within the weekly Horizon "*Management of the Live Environment*" report from BSM (specifically section 3 *"Transaction Processing"*). This information is an input into the Release Authorisation process and should inform debate on the acceptable rollout rate.

Logged Incidents

We reviewed the latest log of incidents raised with Business Service Management (BSM), and noted that the number of cases classed as open has risen from 17 to 19 since Stage 1 of our review, with one case being closed and three new ones being opened.

All individuals responsible for resolving incidents were however aware of the need to resolve issues prior to full National Roll out. The target date for all but two incidents to be resolved was on or before the 23rd August. The two remaining incidents were only minor and not software related.

Audits at Outlets

The number of outlets audited has now risen to approximately 20, with no problems being encountered in verifying assets on hand at the time of audit. The concerns identified regarding POSIS investigations at outlets, could also affect the ability of the Network Audit Team to investigate shortages and poor accounting. In addition several other issues relating to Network Audit have been identified:

- the user history log and user event log which would be useful tools for auditors do not appear to be working. When reports are requested the screen freezes and the system has to be re-booted;

> These functions should indeed be present and available to the auditor. However, there have been general problems with system stability (being progressed under Acceptance Incident 298) which have affected a number of functions, potentially including these reporting tools.
>
> (BSM are unaware of any specific faults reported with the use of this functionality)

- the Horizon System Helpdesk were unable to provide a one shot password for one outlet we visited despite the Network Auditor going through the correct process to obtain one. The auditor was then dependant on the Subpostmaster to provide information from the system.

> The one shot password mechanism is indeed designed to allow access by auditors and the like without being reliant on the co-operation of the Subpostmaster. This mechanism, including the associated manual procedures, is in fairly frequent use and BSM are not aware of any underlying problems. This would appear to be a one-off failure of the process. We are aware of one (single) case in early August where the auditor ran out of time due to delays in provision of the password.

We have registered these findings as incidents with the Service Management helpline.

Other Coverage

We reviewed the information gathered by BSM in relation to time taken to balance, receipts and payments balancing and the level of support provided and noted no reason for concern.

Conclusion

There is a need to ensure that the problems relating to the audit trail for S&IE investigations and demonstrating that the system meets the requirements of the Police and Criminal Evidence Act have been impact assessed as incidents and are considered by the Acceptance and Release Authorisation Boards if not satisfactorily resolved. In addition, it will be necessary to consider whether the current level of cash account errors will affect the accuracy of settlement with clients, when considering the rate at which the system should roll-out.

We would again like to thank all managers and staff for there time and assistance in the undertaking the review. Please do not hesitate to contact me or the Senior Auditor for the review Gary Potts, GRO GRO, if you have any queries or require further information