Meagher, John

From: Meagher, John
To: Miller, Dave (Horizon)
Cc: Holleran, Ruth; Mohindra, Naresh
Subject: Acceptance Progress
Date: 17 December 1998 09:57

Dave

We held a meeting yesterday on the progress of the acceptance specs. The purpose was to evaluate where we were in relation to our target date of 18th December for sign off of all specs.

The meeting was attended by Pathway (John Dicks), DSS (Paul Wootton), POCL (Ruth Holleran) and Horizon (John Meagher, Jeff Austin and Tony Houghton).

As an observation, it was very helpful to have Ruth attending acting as formal 'sponsor' this allowed us to make good progress.

The currently situation is:

1) 12 specs are already agreed

2) 7 specs are at the point of agreement i.e. have agreement at the working level and now need to be formalised.

3) 1 spec - BPS Service Boundaries the 24th spec - is operating outwith the agreed time-scale and we have agreed a schedule for this.

4) 2 specs - POCL Infrastructure and Policies and Standards - have outstanding differences, are still in debate (as of last night) but I estimate these could be resolved if escalated, assuming this would be necessary

5) 1 spec - Reference Data - has outstanding differences which I estimate would not be resolved by escalation, however, I have devised an approach which may give us the assurance we need in testing and LRDP, whilst not including in the acceptance spec but still allowing us to raise acceptance incidents if faults emerge. I am working this up this morning and will advise you of progress.

6) This leaves BES. Ruth was advised by Mena not to proceed on the basis of a caveat. It is probable that Pathway would have been unable to agree any caveat that was acceptable to us anyway. We therefore advised Pathway that we were not in a position to agree the spec as written due to an outstanding dispute on the BES/PAS boundary. I felt it only fair to advise Pathway that in the event of the boundary being agreed as currently drawn (DSS agree its current position) then POCL would accept the evidence currently being nominated in the spec. This is now very urgent, we risk attracting criticism for not being able to negotiate an agreement. There are however major concerns within POCL with the risks associated with this. This needs to be advanced with utmost urgency.

I'll keep you abreast of developments.

John

RESTRICTED COMMERCIAL

Bringing Technology to Post Offices and Benefit Payments

REDEFINITION OF THE BES/PAS BOUNDARY - ADDITIONAL RISK TO POCL

Author:	Jeremy Folkes	Version: Issue 1.0 Draft
Authority:	John Meagher	25th November 1998
Reference:	jf/REDEFI~1.DOC	

Contents Page

1. PURPOSE 2
2. CAVEATS 2
3. BACKGROUND 3
3.1. Boundary Dispute 3
3.2. Requirements Viewpoint 4
3.3. The Distributed Solution 4
3.4. Historical Perspective 4
4. TWO VIEWS OF THE BOUNDARY 5
4.1. POCL View - Requirements Orientated 5
4.2. BA/Pathway View - Solution Orientated 6
4.3. Diagrammatic representation of boundary views 7
5. HELPDESK AUTHORISED TRANSACTIONS 8
5.1. Historical position 8
5.2. Disputed position 8
6. FINANCIAL RISKS 9
6.1. Where risk lies 9
6.2. Recovery 9
6.3. Cap on Liability 10
6.4. Indirect Costs 10
7. NON-FINANCIAL RISKS 11
8. RELATED ISSUES 11
8.1. Legality of the Boundary 11
8.2. Separability of BA and POCL services 12
8.3. Contractual Acceptance 12
8.4. Control, Audit and Reconciliation 13
9. SOLUTION BACKGROUND 13
9.1. Oracle vs Riposte Domains 13
9.2. Payment Authorisations vs Encashments 14

9.3. Protection of Payment Authorisations.. 15
9.4. Distributed Solution.. 15
9.5. Multiple Payees.. 16
10. CAUSES OF MIS-PAYMENT.. 16
10.1. Specific to Pathway solution.. 16
10.2. General solution failure.. 17
11. MISPAYMENT SCENARIOS.. 17
12. QUANTIFICATION OF RISK.. 25
12.1. Own Analysis.. 25
12.2. Payment Authorisation Liability.. 25
12.3. Service Levels.. 25
12.4. Pathway Actuarial Valudation.. 26
13. UNQUANTIFIED RISKS.. 26
14. CONCLUSION.. 27

1. PURPOSE

1.1. This paper aims to explore and document the issues around the additional risk placed on POCL through the redefinition of the BES/PAS boundary. It is intended to inform the debate within POCL and is therefore *not* intended for circulation to Pathway or BA.

1.2. Nothing contained within this message shall be deemed or construed as affecting existing contractual obligations between ICL Pathway, the DSS and/or POCL.

1.3. The author would like to put on record the specific assistance of Tom Patterson of Post Office IT Services for providing much useful background information on this issue, and of Janet Dore of ICL Pathway for providing verbal briefings on the BPS design.

2. CAVEATS

2.1. Because of the nature of the contract with ICL Pathway, neither sponsors nor the Horizon programme have full visibility of the Pathway solution, and Horizon have not been afforded access to Pathway's detailed design for the Benefits Payments Service. This report is therefore based on a current understanding of the design, which although believed to be correct at this point in time has not been formally validated by Pathway. It is therefore possible that additional failure conditions (and therefore risk) may exist outwith those identified to date.

2.2. To enable this work on the Boundary Issue to progress, ICL Pathway agreed, slightly reluctantly, to provide the author with access to one of Pathway's designers to enable some understanding on the design to be obtained. Unfortunately, this offer did not extend to the provision of any formal design documentation on BPS (indeed, no evidence has been seen of the existence in ICL Pathway of such full documentation[1]), and hence the process has been restricted to two "whiteboard" type sessions. To mitigate this lack of documentation, the author has created an informal "*BPS Design Overview*" document to provide a baseline for analysis, and attempts are being made to validate its contents through the Pathway designer. At the time of writing this report, a number of queries remain extant, although these are not believed to significantly alter the risk profile.

2.3. From the discussions with ICL Pathway it has become apparent that their solution has yet to reach stability and is still undergoing significant change. This is supported through examination of the latest *Service Architecture Design Document* (SADD 5.1), which appears to be at odds with the verbal descriptions from ICL Pathway[2].

2.4. A significant side effect to the lack of visibility of the solution afforded to the Authorities is that they have a corresponding lack of control over the solution at the design level. It is therefore possible that ICL Pathway can make further changes, which may affect the risk to POCL, or indeed the split of risk between BA and POCL, without our knowledge or agreement.

2.5. This study has been based upon the assumption that the delivered service is implemented as per the '*design*' as explained by ICL Pathway - it has not considered weaknesses of the specific implementation. It is of course possible that further 'features' of the solution will emerge during the test phases and during live running, and that these could affect the risk profile to POCL[3].

3. BACKGROUND

3.1. Boundary Dispute

3.1.1. A long running dispute exists between POCL and BA regarding the definition of the boundary between PAS (the Payment Authorisation Service) and BES (the Benefit Encashment Service), two components of the overall Benefits Payments Service (BPS) being provided by Pathway.

[1] Documentation may exist within Escher Group Ltd for their part of the system.

[2] SADD 5.1 Appendix B (Interfaces). The discrepancies have been flagged to Pathway's designer for confirmation and resolution

[3] Features which appear on the *Known Problem Register* (KPR) will of course be visible to POCL; POCL will therefore need to consider items on the KPR in the light of the likely outcome of the boundary issue.

3.1.2. The primary significance of this dispute relates to the liability for incorrect payments - if the error for an incorrect payment is deemed to have occurred in PAS (a BA service), then it would be for BA to recover any loss from ICL Pathway, whereas if it is deemed to have occurred in BES (a POCL service), it would be for POCL to make that recovery.

3.1.3. In addition to the issue of liability, other concerns have been raised regarding the legality of POCL's operation should they be responsible for the functionality up to the new boundary. These are considered later within this paper.

3.2. Requirements Viewpoint

3.2.1. At the time of the drafting of the original requirements set for BA/POCL, the model shared by BA and POCL was that of a Payment Authorisation Service (linked to BA (CAPS)), to which the Benefit Encashment Service at the counter would seek authorisation to make a payment. This model was based on a centralised view of the service, where authorisation would be sought from a central PAS service *at the time of the transaction.* In this environment, the boundary was clear cut, and the opportunity for dispute was small.

3.3. The Distributed Solution

3.3.1. Pathway's solution for the Benefits Payments Service is based on a unique distributed design, which, in place of real time authorisation from a central PAS, pushes payments out to offices in advance of demand, building on the strong link between a payee and their nominated office. As a result, in the majority of cases, BES needs to only seek authorisation from the locally held data, rather than having to refer to the central site at the time of the transaction. The debate effectively revolves around whether this locally held data forms part of BES (POCL service) or PAS (BA service).

3.3.2. This distributed solution has considerable advantages in terms of availability (the transaction is not impeded by loss of communications), performance (not requiring delay in remote authorisation) and cost (not requiring immediate communications), but at the expense of some loss of integrity due to potential delay in synchronisation between the distributed elements of the system.

3.4. Historical Perspective

3.4.1. It is worth noting that ICL Pathway, in their original proposal[4], contended that their PAS service comprised of three components:

[4] For example, see Pathway's *Response to the OJEC notice*, s4.4 "Benefit Payment Service", page 20 fig 3, dated 28/09/95, and/or Pathway's risk assessment dated 6.9.95.

- a Payment *Management* System (PMS)[5]
- Transaction Management Service - TMS
- the Counter Interface

and that therefore there was no physical "PAS" system as such. Unfortunately the term "PMS" gradually fell into disuse and was finally lost during a blanket change to the contract at "dropdown" in late 1996.

4. TWO VIEWS OF THE BOUNDARY

The crux of the dispute relates to the location of the boundary between BES and PAS, and specifically at what point "authorisation" is given. In very simple terms, "*who owns the functionality and data which authorises the transaction at the counter*"?

4.1. POCL View - Requirements Orientated

4.1.1. The POCL view is that PAS - as the Payment *Authorisation* Service - is responsible for authorising transactions, and that therefore BES is seeking authority from PAS at the time of each benefit transaction at the counter - and therefore that the payment authorisations held in Riposte are part of PAS and therefore are the responsibility of BA and not POCL.

4.1.2. Note that this point of view could appear to be supported by BA's stance that POCL (as an organisation) do not have the right to view these unencashed payment authorisations.

4.1.3. This POCL model therefore has an element of PAS implemented within TMS and OPS (on the POCL Infrastructure), i.e. with PAS extending down to the counter (although not necessarily visible to the clerk). This actually mirrors the situation with CMS, where some (uncontested) CMS functionality is provided at the counter, in the form of PCDF (Payment Card Distribution Facility).

4.1.4. Although the boundary at the counter could presumably be identified through detailed examination of the software (if we had access), it is not one which is easily auditable by outside parties, as it sits deep within the (so-called) BES counter application. Due to the design of the solution such a boundary would still be subject to considerable interpretation.

[5] PMS effectively represented the present Oracle domain on the central Sequent hosts - that is, what BA and ICL Pathway would now term "PAS".

4.2. BA/Pathway View - Solution Orientated

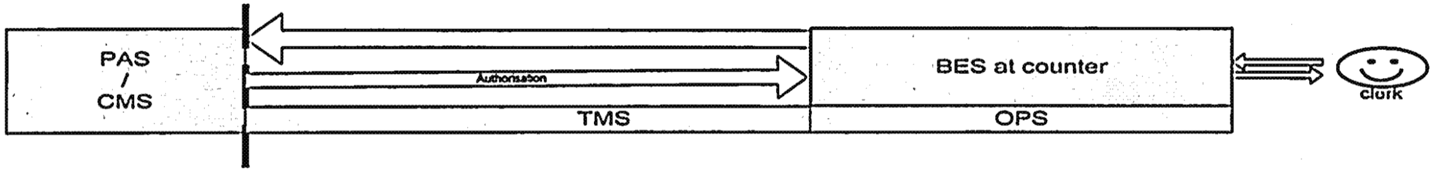
4.2.1. The current BA view is that the boundary should be drawn at the physical interface from the so-called PAS "Sequent" central host and the Riposte Agents on the TMS layer. Responsibility for payment authorisations would therefore shift from BA to POCL at the time they are passed into TMS and would remain POCL's responsibility within the POCL Infrastructure. This would include the processing of foreign payments, the functionality for which is wholly within the Riposte domain (TMS and its agents).

4.2.2. This is the location of the boundary as now proposed by ICL Pathway[6], and embodied in the *Service Architecture Design Document* (SADD), including within the *Interfaces* appendix.

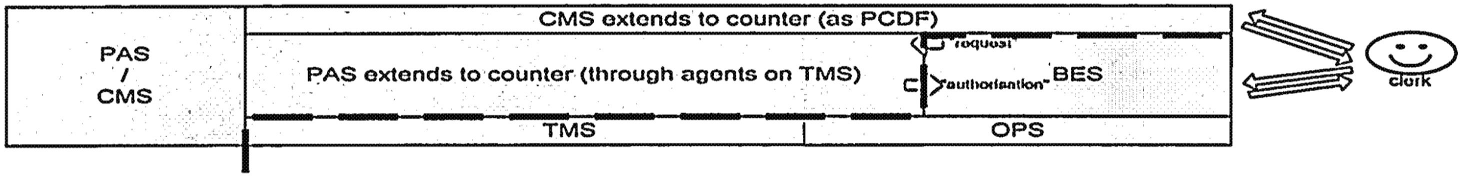
[6] To be precise, Pathway put the interface just inside the Sequent/Oracle domain, so that the loaders/harvesters would sit within the POCL domain; however, the key point is that the Oracle database would remain in the BA domain.

4.3. Diagrammatic representation of boundary views

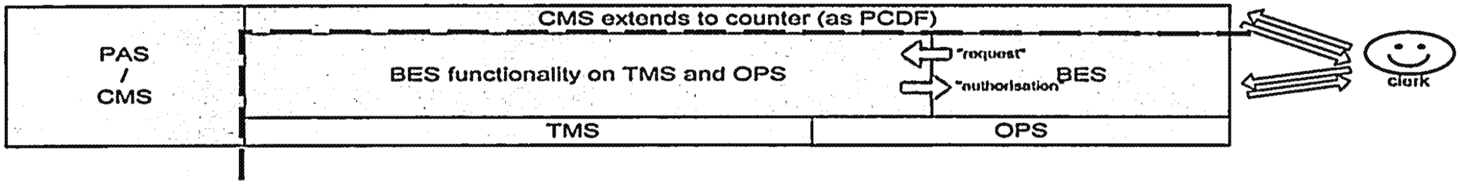
Centralised "banking model" envisaged by Requirements



Distributed Model as implemented - showing where requirements implemented (POCL viewpoint)


PAS
/
CMS
CMS extends to counter (as PCDF)
PAS extends to counter (through agents on TMS)
"request"
"authorisation"
BES
clerk
TMS
OPS

Distributed model as implemented - Pathway definition (BA viewpoint)


PAS
/
CMS
CMS extends to counter (as PCDF)
BES functionality on TMS and OPS
"request"
"authorisation"
BES
clerk
TMS
OPS

5. HELPDESK AUTHORISED TRANSACTIONS

5.1. Historical position

5.1.1. In cases of loss of either the ISDN line or counter equipment in the office (and potentially other failure scenarios), the clerk can make use of a telephone authorisation service to be able to continue making benefit payments.

5.1.2. The authorisation service is provided by what Pathway call the "*PAS Helpdesk*" or "*Payment Card Help Line*" (PCHL), using the (PAS) Oracle application running on the Sequent platform. Traditionally this has been seen as part of the PAS service, and that the authorisation call therefore crosses a BA-POCL boundary[7].

5.1.3. This in itself generates an additional complication, as it means that (if we take the BA definition of the BES/PAS boundary), a payment can be authorised from BES or PAS, i.e. from either a POCL service or a BA service. This raises the spectre of a duplicate arising from simultaneous authorisation from both sides of the boundary[8] - that is, one clerk being given authority to pay from the counter terminal, and another by the PAS Helpdesk.

5.1.4. The liability in this case does not appear to be clearly defined, even with the BA BES/PAS boundary, however it could be reasonable to assume that as two authorisations have been given by the PAS element of the service (one in advance via BES, the other in real time by the helpdesk) that this is a BA/Pathway liability.

[DN: Happy to be proven wrong it the liability is defined....]

5.2. Disputed position

5.2.1. However, the exact status of this telephone authorisation service now also appears to be subject to some dispute. It appears that it is BA's contention that this is now a wholly POCL service, although hosted on what has traditionally been known as PAS[9]. This view is now reflected, apparently at BA's behest, in the latest draft of the *Service Architecture Design Document* (SADD), although it is believed that objections have been raised by POCL.

[7] At the time (Dec97/Jan98) of debate with Pathway over the security of the office-helpdesk exchange, Pathway and BA appeared to concur with this view that the exchange cross the boundary.

[8] Note that the window for such duplicates is relatively small - of the order of a few minutes - if the system is operating as intended (see later) - as the Oracle database is updated when possible from the Riposte database.

[9] SADD 5.1 (draft) reviewed September 1998 now shows the helpdesk as sitting within the POCL Service Infrastructure rather than DSS Service Infrastructure. However, in technical terms the Helpdesk operators are accessing the PAS database, and are therefore seeking authorisation, in real time, from PAS (and not from the TMS copy of the data).

5.2.2. This change is important as it further complicates the boundary - accepting BA's contention would mean that significant POCL functionality was running on the BA side of the Oracle-Riposte or Sequent-TMS boundary.

5.2.3. This change, if allowed, would place the entire front end of the payment authorisation service into the POCL domain, and therefore the risk for inappropriate encashments via the Helpdesk would appear to fall fully to POCL and Pathway.

[DN: The SADD 5.1 does not make it clear exactly where the boundary would sit if this further change was allowed - although the Helpdesk itself would be on the POCL side, the key question is whether the data against which it is authorising is down to POCL or Pathway, and whether BA are responsible for the merging of the two streams (the Riposte and HD encashments). Taken to its logical conclusion, a large slice of the Oracle functionality would have to move to POCL.....]

6. FINANCIAL RISKS

6.1. Where risk lies

6.1.1. The risk for the majority of technical failure conditions[10] identified below are believed to fall to ICL Pathway, who as PFI service provider have the responsibility for the security and integrity of the IT infrastructure on which the service is provided[11].

6.1.2. However, these risks are generally realised through the payment of monies, authorised by the Pathway service, across the counter - in other words a payment has been made by POCL for which BA do not wish to settle. Therefore, although the risk is theoretically held by ICL Pathway, it is POCL who will initially be out of pocket.

[DN: Does a shift in boundary have any affect on the liability (between BA and POCL) for non-duplicate fraudulent transactions - eg card counterfeiting, repudiations,. etc, etc? I do not have visibility of the BA-POCL contract but I presume someone has checked for knock-ons.]

6.2. Recovery

6.2.1. From a financial perspective therefore, what is therefore primarily at dispute is that of responsibility for recovery of losses from ICL Pathway - i.e. whether the losses should be recovered by BA or by POCL.

[10] Liability for non-technical failure - eg error in the fallback authorisation exchange - is less clear.

[11] Authorities Agreement, Clause 808 - Liability. This includes "*copied, altered or forged cards, unauthorised access to the Service Architecture, hacking*" but subject to Schedule B08 *Benefit Encashment Fraud.*

DN: Is this overly simplistic?

6.2.2. In financial terms, this can be viewed as a cash flow issue, in that the party responsible for recovery may have to stand the loss until such time as it can be recovered. Settlement is believed to be due on a quarterly (13-week) basis from ICL Pathway, and therefore (in undisputed cases) the recovering party may have to fund sums due for an average of 13/2= 6.5 weeks.

[DN: Believe POCL could recover costs of funding from Pathway - lost interest etc]

[DN: Does this shift affect the ability to recover incorrect payments from customers? In other words, if BA cease to have any responsibility for payment authorisations once they have crossed to TMS, will POCL and/or Pathway have any means of extracting duplicate payments from a BA beneficiary. What is the effect on investigations and prosecution - if the fraud is now occurring within the POCL service?]

6.3. Cap on Liability

6.3.1. There is, however, an upper limit of liability on Pathway of £200M, pooled between POCL and BA, in the agreed proportion of £80M POCL to £120M BA. It is presumed, however, that this split between the two Authorities was agreed against a particular understanding of the BES/PAS boundary, and that this split may be viewed as inappropriate (at least by by POCL) should they take on larger element of the risk on BPS.

6.3.2. In the case of this pool becoming exhausted during the term of the contract, further sums would become unrecoverable and full liability for risk would fall to BA or POCL depending on the boundary location. At this stage the location of the boundary would therefore become of primary importance.

6.3.3. Should the liability then fall to BA, they have the option (at least in theory) to attempt to recover overpayments from beneficiaries directly. POCL, however, having no direct relationship with the beneficiary, does not have this option without the active support of BA.

[DN: Does POCL-BA contract cover recovery of overpayments?]

6.4. Indirect Costs

6.4.1. In addition to the direct costs - whether related to delayed recovery of mis-payment or, post-cap expiry, funding of mis-payments, of potentially greater significance are the indirect costs of having to manage mis-payments. If the boundary shifts to POCL's disadvantage, it is assumed that these costs will be significantly increased.

6.4.2. Given that the average payment authorisation of the order of £65, it is quite possible that the costs of handling the investigation of a mis-payment could outweigh the actual value of the original payment.

7. NON-FINANCIAL RISKS

7.1. Although this paper, by design, is focused on the direct financial effects of mis-payment within the Benefit Payment Service, a shift in boundary may open up other, softer, non-financial risks to POCL, including:

(a) lack of public confidence in POCL's services

(b) poor customer perception

(c) poor staff perception

(d) poor client perception, etc etc

7.2. In reality, the ownership of non-financial risks around customer perception and satisfaction may be irrelevant, as it will be "the service" which is getting the publicity, and that POCL, as the front end to this service, will suffer any consequences wherever the actual liability sites.

[DN: Are POCL at any risk of legal action from a customer if that customer is denied monies as a result of mis-operation of the BPS - especially if POCL now have responsibility for a significant part of PAS?]

8. RELATED ISSUES

8.1. Legality of the Boundary

8.1.1. It has been suggested that POCL would be acting outside their legal powers if they adopted the boundary now being suggested by BA and Pathway. In particular, it may be possible that POCL could be construed as operating as a bank, outwith the defined Post Office Powers, if it accepted the revised boundary position.

[DN: Need a view from expert on Post Office Powers (eg Legal Services)? If it were true that this is outwith Powers, this could be a deciding factor]

8.2. Separability of BA and POCL services

8.2.1. Requirement 736[12] specifies that the BA and POCL services should be capable of separation. In the context of this issue, these means that the BA part of BPS and the POCL part of BPS should be separable - in other words that PAS and BES should be separable.

8.2.2. From Pathway's viewpoint, they have specified the boundary at the simplest point for separation - at a physical interface between two computer systems. Although this interface is complex, it is on the face of it considerably more "separable" than that if we consider PAS to extend to the counter. For example, it would be hard to imagine being able to re-tender for PAS but not for BES in the case where PAS and BES are both running over TMS and OPS and are both represented within the Counter Application[13].

8.2.3. If, however, the fallback helpdesk is deemed to be part of BES and not PAS, and the boundary moves further back into the Oracle domain (including the main database tables), this physical separability would be destroyed. This may be a key point in influencing ICL Pathway over this additional shift in boundary.

8.3. Contractual Acceptance

8.3.1. The dispute over the location of the boundary is currently restricting progress on the agreement of the PAS and BES Acceptance Specifications. Currently, the BES Acceptance Specification contains a large number of "PAS" requirements, that is requirements which state that *"PAS shall..."*, as the contracted functionality is actually performed in (what they call) BES - and indeed, within that document, Pathway have stated in the Acceptance Specifications that "*Comments relating to the inclusion of PAS functionality within BES are not addressed, because these would entail changes to the contracted Pathway Solution*".

8.3.2. The POCL position is that these criteria, as they relate to PAS requirements, should be located in the PAS specification; BA are believed to be content for the criteria stay in the BES ATS, however, they would also like corresponding criteria in the PAS ATS to test that the Services are separable. ICL Pathway have stated that it is not possible to do this, as the criteria only have to be tested (accepted) once.

[12] **Requirement 736 - Benefit Payment Service - CMS: Logical Separation between CMS, PAS, and POCL Infrastructure**
"*The CONTRACTOR shall ensure that a logical separation is maintained between CMS, PAS and POCL Infrastructure Services and shall have in place a detailed interface specification agreed between the CONTRACTOR and DSS to support this.*"

[13] **In reality, however, the BA supported boundary, if placed at some point within the Sequent platform, may have dubious separability.**

8.4. Control, Audit and Reconciliation

8.4.1. Wherever the boundary is located, if POCL have responsibility for data within the solution then they will require the correct tools and means to be able to discharge that responsibility. If POCL now become responsible for Payment Authorisations within the Riposte domain, then it is likely that they will require a number of controls, including:

(a) to ability to audit and reconcile across the interface between the BA domain and the (new) POCL domain. This may require additional functionality in both domains, plus the agreement of BA to participate in such reconciliation (and agreement of BA to POCL having access to this data).

(b) the ability to be able to determine the total value of outstanding Payment Authorisations within the (new) POCL domain.[14]

(c) the ability to control and assure the design of the authorisation elements of BES.

[DN: If the boundary is accepted as per BA, then the relevant bodies in POCL will need to work up their control requirements for this new responsibility.]

9. SOLUTION BACKGROUND

Although it is not intended to involve the reader in the full details of the Pathway solution, there are a small number of key concepts of which some knowledge may aid the understanding of the discussion of the modes by which mis-payments can be made.

9.1. Oracle vs Riposte Domains

9.1.1. Physically, the ICL Pathway solution is implemented in two fairly discrete domains:

[14] According to the latest draft of ICL Pathway's *Solution and Service Reconciliation* document (CR/REP/011 dated 23/10/98 version 0.3), some additional functionality is being developed by Pathway for "*PAS Additional Monitoring*" to perform such a check between domains, although the full version of this will not be available at NR2 and its suitability to provide the control POCL would require has not been assessed.

(a) Oracle: central "hosts" with applications written in Oracle and running on Sequent hardware. This includes the central PAS/CMS functionality and the fallback helpdesks. The Oracle domain consists of a single physical database on a managed central site[15] and given proper implementation, leaves little scope for lack of integrity.

(b) Riposte: a distributed system covering both the central TMS layer and the office layer, implemented on Escher's Riposte message replication architecture running on NT boxes. This database is spread between central NT Correspondence Servers and the terminals in the office, with synchronisation between the various instances on a "*eventual, best endeavours*" basis, however due to the distributed nature of the solution over a fallible wide area network, some inconsistencies can occur at any particular point in time.

9.1.2. Although there is natural tendency to equate Oracle with PAS/CMS and Riposte with BES, the crux of boundary issue is that (in POCL's view) PAS extends into the Riposte domain.

9.2. Payment Authorisations vs Encashments

9.2.1. Authorised Payments from CAPS are translated, by the Oracle functionality, into Payment Authorisations which are passed to the Riposte domain. The counter application (whether viewed as PAS or BES) authorises against these Payment Authorisations messages.

9.2.2. When an payment is made and committed, an Encashment message is written to Riposte. It is the presence of this Encashment message which prevents further encashment and effectively renders the Payment Authorisation marked as "paid"[16]. More pertinently, the absence of the Encashment message for any reason allows the Payment Authorisation to be reused[17].

9.2.3. This concept is crucial as it encompasses much of the reason for the importance of the boundary dispute. A single message, written at Encashment, prevents further use of a Payment Authorisation. The dispute could, maybe slightly simplistically, be distilled to a consideration of ownership for the Encashment message, which in effect has dual uses - one to record payment, and one to prevent further payment.

[15] Note that only one central site is "live" at any one time as far as providing Oracle host functionality; the second site is on warm standby and can take over live running after a short delay if required, but that then becomes the single "live" site.

[16] Additional functionality writes additional messages to mark other instances of the Payment Authorisation as being unavailable for collection, but the principle is the same.

[17] Subject, of course, to stop notices, expiry dates and other business rules

9.3. Protection of Payment Authorisations

9.3.1. Payment Authorisations within the Riposte domain of the ICL Pathway solution are "digitally signed" using strong cryptographic means, in a manner which means that undetected modification of a Payment Authorisation record is extremely unlikely[18]. For the purpose of this paper we can assume that the details of a Payment Authorisation record, including the amount and card details, cannot be modified once properly signed at the centre.

9.3.2. This protection, however, does not in itself protect against the 're-use' of a signed Payment Authorisation, and in particular against the repayment through separation from the cancelling Encashment record.

9.4. Distributed Solution

9.4.1. The ICL Pathway solution is based on the Riposte message replication architecture. A key benefit of the architecture is that is designed for "real world" scenarios where a permanently available wide area network is neither achievable or affordable. The distributed solution is a trade-off of integrity for availability, based on the importance of the ability to pay benefit without the immediate reliance on communications links to a central site.

9.4.2. The system is therefore designed to be able to withstand the loss of communications to the centre; in other words to withstand a (temporary) delay in the transmission or replication of data between the outlet and centre. Although giving considerable benefits in availability (and performance and cost), this opens up the risk that a payment could be made against "out of date" data, or that multiple payments can be made against separate copies of the same data item.

9.4.3. This may be best illustrated in the context of a "failed stop" - if the ISDN line to an office is down, a payment could be made in an office although that payment has already been 'stopped' by BA centrally, due a delay in the stop message getting to the office. The stop message will eventually reach the office, but after the payment has been made.

9.4.4. In the centralised model, all authorisations would have to be sought from the centre (and therefore the failed stop would not exist as such), however no payments could be made if the communications were unavailable.

9.4.5. In summary, the distributed model, in order to give high availability, gives rise to the risk of some types of mis-payments, through a combination of:

[18] This protection, of course, relies on the correct operation of the software in checking the signature, and the correct storage and handling of the public and private keys.

- *delay in replication* - that is, data has been successfully introduced into the Riposte message store (RMS), but due to natural latency or failure of the infrastructure does not achieve replication in time to prevent a business failure

- *use of local copy of data* - that is, using a local copy of data, which may be "out of date" is used in preference to checking with some remote copy of the data.

9.5. Multiple Payees

9.5.1. An additional complication is the handling of multiple payee scenarios within the Pathway solution. Where two or more customers are permitted to pick up an Authorised Payment, functionality within the Oracle applications explodes the payment into a number of separate Payment Authorisations, linked by Payment ID, and passes each one of these across the BA-positioned boundary. Functionality in the Riposte domain is designed to prevent more than one of these Payment Authorisations from being paid, although in certain scenarios this can fail.

9.5.2. It has been suggested that if the Riposte domain authorises payment against more than one copy (i.e. if the linkage mechanism fails), this would be a BA liability, as BA have passed the multiple versions over the boundary to POCL.

9.5.3. In reality, examination of the solution shows that the functionality which is responsible for marking off the multiple versions is similar to that employed in handling foreigns. Although the author does not have sight of any discussions between BA and POCL over the liability on this point, it does appear inconsistent for liability to be assigned in a different way for this case.

[DN: Has this been explicitly agreed? If we conceded this boundary issue, I would feel uncomfortable about assuming we were not conceding the multiple payee case]

10. CAUSES OF MIS-PAYMENT

Due to the nature of Pathway's solution, we can categorise failure into two broad types - those that occur due to the distributed solution, and those which would occur in any generic solution. Although the two categories are fairly clear cut, it is of course possible for a failure in one to open up a risk in the other. For the purposes of this analysis, the failure are classified into four classes, Classes A, B, C and D.

10.1. Specific to Pathway solution

10.1.1. This category describes those conditions which are a feature of the ICL Pathway implementation of the Benefits Payments Service specifically on a distributed architecture, with a design aimed at high availability.

10.1.2. Analysis has shown that we can subcategorise these conditions as follows:

(a) Class A - perfect world - where the system is operating at 100% availability, but where mis-payment is allowed by the design in certain conditions.

(b) Class B - real world - where the software and central systems are operating as they should, but where certain of the distributed elements of the infrastructure are unavailable (eg ISDN lines, office equipment)[19].

(c) Class C - system failure - where certain elements of the central systems are failing to operate at full performance, although individual software components are still operating to some degree of specification.

10.2. General solution failure

10.2.1. This category is intended to cover those cases where the system does not operate as per design, and does not specifically relate to the distributed design - examples could be:

- where some software fault exists which just pays out the wrong amount of money
- where a telephone authorisation results in the wrong amount being paid
- where an attacker manages to circumvent security controls and modify data within the system
- where an Authorisation/Encashment is not properly on the system due to user or system failure during the encashment.

These general failures are considered to be Class D.

11. MISPAYMENT SCENARIOS

11.1. This section attempts to define the mis-payment scenarios which are exposed by the boundary shift - in other words, scenarios which are considered to exist and be POCL's liability in the both boundary positions (and where the level of risk is now changed between positions) are not shown. Where it is not clear whether this is new risk, the list errs on the side of caution and includes the item but with a shaded background.

[19] The exposure from such failures is highly dependent on the time to detection in addition to the time to fix. The time to detection of an ISDN failure will be dependent on the ability of ICL Pathway to pro-actively manage the 'network' and to educate of users to report faults in a timely fashion.

11.2. The assignment of liability is based on the author's understanding of the contract and has not been validated by ICL Pathway, POCL or BA. Given the nature of this dispute, it is likely that different interpretations could be put by the different parties.

11.3. In attempting to assign frequency, a simple random distribution of failure has been assumed - in particular, no attempt has been made to model any opportunistic change in customer behaviour to target, for instance, offices with certain types of failure; likewise, no attempt has been made to model the effect of detection and recovery as means of deterrence of such behaviour. Likewise, intentional denial of service attacks (which increase the probability of Class B or Class C failure) have not been modelled.

11.4. The list of scenarios is arranged by Class, as defined in the previous section.

11.5. The following volumetrics and assumptions have been used within the table:

- Payments per day - 6M payments, £400M
- Secondary payees - £7.3M per day out of £400M daily[20] (1.8%)
- ISDN availability - ~99.75%, assumed occurs as one failure of 5 working hours per year, plus 0.5% of calls unsuccessful due to congestion etc.
- Helpdesk transactions - assume 2000 per day
- Riposte replication - assume average 7.5 minutes for synchronisation to occur (random distribution 0-15, ignoring effect of priority messages and centre-outlet calls).
- Oracle-Riposte synchronisation - assume average 5 minutes for synchronisation to occur (encashment harvesting, loading of HD authorisations)[21]
- LAN failure - consider 1 hour per year per terminal
- Working days - 305 per year[22]

11.6. Note that risk of actually making an incorrect payment - especially due to delayed replications (Classes A-C) - is highly dependent on customer behaviour. Although a payment may be theoretically available for collection, the risk is only realised if a customer does try to collect a payment, at a point when in theory none is supposed to be due.

[20] Note from Colin Oudot to Ruth Holleran, Aug98

[21] SADD 5.1 B2.4 refers to 5 minute poll interval.

[22] Workload Brief, table 1.1

Class	Condition	How occurs	Frequency	Impact
A	Lack of synchronisation between Oracle and Riposte domains	The Oracle and Riposte domains provide authorisations autonomously (Oracle for helpdesk, Riposte for automated use at the counter). Updates from Oracle to Riposte TMS and Riposte TMS to Oracle are processed by an agent running at 5 minute intervals. Update between Riposte Office and Riposte TMS on average 7.5 minutes. Duplicates are possible as: • a helpdesk authorised transaction can take say 15 minutes to reach the nominated office and prevent duplicate payment • a nominated office transaction can take say 15 minutes before it reaches the Oracle tables to prevent payment *Note that the liability for this form of duplicate is unclear, as the two authorisations are on different sides of the boundary!* *If PAS HD became POCLs, then this risk would appear to fall wholly to POCL.*	Risk of accidental double payment low - in normal operation customer or proxy would have to attempt second payment within 15 minutes. Pathway estimate 2000 HD transactions per day. Requires customer to deliberately choose to represent card. Risk - low	Duplicate payment.
A	Synchronised encashment in same office	Two customers attempt to collect the same payment at the same time at different counters in the same office - if extremely well synchronised it may be possible for both to be authorised and paid.	Very low - requires precision timing due to the additional checks now added by Pathway.	Duplicate payment.
B	Lack of synchronisation between Oracle and Riposte domains (Office link down)	The lack of synchronisation between the nominated office Riposte domain and the Oracle domain can increase from 15 minutes to the length of an ISDN outage.	Assume ISDN 99.75 availability, so 0.25% of time ISDN unavailable. Model as one failure for 5 working hours per year per office.	Duplicate payment.

Class	Condition	How occurs	Frequency	Impact
B	Duplicate between foreign and nominated office (ISDN down)	Loss of ISDN link between nominated office and centre results in foreigns being authorised against Correspondence Server without reference to nominated office.	ISDN availability 99.75%. Assume 8% foreigns on 6M transactions, therefore 2400 per day performed without check.	Duplicate payment.
B	Duplicate between foreign and nominated office (Congestion)	Failure of ISDN call to nominated office from centre results in foreigns being authorised against Correspondence Server without reference to nominated office.		
B	Duplicate between secondary payee and primary payee (ISDN down)	Loss of ISDN link between primary payees nominated office and centre results in secondary payee being authorised against Correspondence Server without reference to primary payees nominated office. *[May be considered to be BA risk as two Payment Authorisations sent over the "boundary"]*	ISDN availability 99.75%. Assume 2% secondary payee on 6M transactions, therefore 300 per day performed without check.	Duplicate payment
B	Duplicate between secondary payee and primary payee (Congestion)	Failure of ISDN call to primary payees nominated office from centre results in secondary payee being authorised against Correspondence Server without reference to primary payees nominated office. *[May be considered to be BA risk as two Payment Authorisations sent over the "boundary"]*		
B	Failed stop (next day)	Loss of ISDN link between nominated office and centre results in payment being made despite stopped	Assume 5000 next day stops per day. Assume 0.25% unsuccessful due to ISDN failure => 12.5 per day. Low	Payment of stopped authorisation
B	Failed stop (urgent)	Loss of ISDN link between nominated office and centre results in payment being made despite stopped	Assume 5000 urgent stops per day Assume 0.25% unsuccessful due to ISDN failure => 12.5 per day. Low	Payment of stopped authorisation

Class	Condition	How occurs	Frequency	Impact
B	Recall and reissue	Loss of ISDN link between nominated office and centre results in recall failing to be applied before the payment is made; the reissued version is then also available for payment.	Assume 8000 recalls and reissues per day => 20 per day. Low (Has occurred in R1c due to network failure)	Duplicate payment
B	Delayed Encashment Notifications	Loss of ISDN link in middle of a foreign or secondary payee transaction can cause the EncashmentNotification to be delayed and for any Hold to expire before it arrives. The encashment can therefore be repeated in this window. *For secondary multiple payees, could still be BA responsibility?*	V Low	
B	LAN failure	Loss of replication between terminals could result in duplicate payment. *[Note some evidence that Pathway may prevent this, however not known whether this means that that terminal would be considered "out" for SLA etc purposes]*	Pathway's claim LAN failure v low.	Duplicate payment.
B	Change of Nominated PO when nominated office link down.	If the nominated PO link is down, it will not receive messages cancelling that the nominated office for the specific customer. However, a new office will be enabled as that customers nominated office, and both will therefore make payments against local data until the former nominated offices re-synchronises with the centre.	3000 ChNPO per day from CAPS.	Duplicate payment.

Class	Condition	How occurs	Frequency	Impact
B	Disk failure	An encashment, although properly committed to the local disk in an office, could be "lost" due to equipment failure prior to replication to the centre, and therefore a payment could be repeated. (Risk low as dual disks in single position office, multiple terminals otherwise. Operational procedures require that "lost" transactions be recovered from receipts) *[This is viewed as a new risk as if the failure occurs it is the "PAS" functionality re-authorising the payment. It therefore seems as if the recovery process is serving BA by recovering the authorisation as well s POCL by recovering the encashment]*	V Low	Duplicate payment
C	Slow running TMSAuthorisation agent	There are certain central agents which, if not running in a timely fashion, would fail to distribute EncashmentNotifications to cancel other copies of a paid Payment Authorisation. *Liability is messy here, as this affects both foreigns and multiple payee scenarios.*	Depends on Pathway's system management capability.	Duplicate payments
C	Slow running Harvester/Loader agents	There are harvesting/loading agents, which if not running in a timely fashion, would fail to maintain synchronisation between Oracle and Riposte domains, and therefore increase the window for duplicate authorisations. *Liability also messy, as it affects the Riposte-Oracle boundary. BA would choose, probably correctly on their logic, to put the Agents into the POCL domain as elements of TMS.*	Depends on Pathway's system management capability.	Duplicate payments
C	Failure of inter-site replication	If the Riposte replication between Bootle and Wigan fails, it would be possible for authorisation for foreigns and secondary multiple payees to be	Should be low (redundant links etc) but depends on Pathway's system management capability.	Duplicate payments (many)

Class	Condition	How occurs	Frequency	Impact
C	Arrival of multiple payee authorisations on different day	If different copies of a PaymentAuthorisation for multiple payees arrive on different days and one is encashed before the remainder have arrived at the centre, later copies may not be marked off.	Low - enough lag in system	Duplicate payments
C	Duplicate between foreign and nominated office due to failure of gateway agent	Failure of the Redirector agent in the office could cause a similar effect to ISDN failure, where requests for verification of payment status may not be available.	Depends on Pathway's system management capability	Duplicate payment
C	Duplicate between secondary and primary office due to failure of gateway agent	Failure of the Redirector agent in the office could cause a similar effect to ISDN failure, where requests for verification of payment status may not be available.	Depends on Pathway's system management capability	Duplicate payment
D	Lost transactions / Incomplete Transactions	The Pathway solution fails to correctly record that an encashment has taken place, and therefore leaves the authorisation "live" for further use. This can occur if the transaction is not properly completed at the counter, or when various forms of failure occur.	Depends on whether R1C design weaknesses corrected. R1c experience ranges from 0.6% at peak to 0.03% after software fixes applied. If persists at 0.03% this could result in	Duplicate payments.
D	Misheard helpdesk call	Incorrect amount could paid through miscommunication between helpdesk and clerk (eg mishearing £14 for £40). BA settle on the authorisation (apparently) given by the HD. *[Appears that this is already considered to be a POCL liability and is therefore not "new" - certainly would appear to become fully POCL responsibility of PAS Helpdesk shifts to POCL]*	2000 helpdesk transactions per day	Payment of incorrect amount, inability to recover any of amount.

Class	Condition	How occurs	Frequency	Impact
D	Spoofed helpdesk call	Clerk could be tricked into making a payment against false authority, or could make a payment without getting authority from PCHL. *[Appears that this is already considered to be a POCL liability and is therefore not "new" - certainly would appear to become fully POCL responsibility of PAS Helpdesk shifts to POCL]*	Deliberate action	Payment of unauthorised amount (potentially large).
D	Date change	If the terminal date is reset to some past time, it would be possible for expired Payment Authorisations to be rejuvenated and repaid.	Low. Specific controls in Riposte theoretically prevent excessive clock changes.	Duplicate or expired payment (many)
D	Rogue software	An insider manipulates the service to allow additional payment.	Cannot quantify - may relate to a Pathway failure to implement adequate security controls or quality controls	Potentially large.
D	Hacking of TMS/OPS platforms	An outsider manipulates the service to allow additional payments.	Cannot quantify - may relate to a Pathway failure to implement adequate security controls.	Potentially large.
D	Unpredictable failure	The system could fail to operate as per design (eg through a software error, and make incorrect or unauthorised payments in an unpredictable manner.	Cannot quantify	Potentially large.

12. QUANTIFICATION OF RISK

In this section we will try and assign some quantification to the risk. By nature of the lack of available information, this should be seen as providing "high level" steers rather than massive detail.

12.1. Own Analysis

12.1.1. Our own analysis, based on the identified and quantifiable mis-payment conditions outlined in the last section, suggests that under *normal* running (ignore any deliberate attack) the risks of mis-payments are low, although they will occur.

12.1.2. However, this statement has to be considered alongside the dangers of either deliberate interference with the service or of some other failure of the service pushing it outside the parameters of normal running.

12.2. Payment Authorisation Liability

12.2.1. An average of (say) £200M payments will pass through the service each day (£1B per week) - either as payment authorisations being passed to the Riposte domain, or as Encashments flowing back to the Oracle domain. Estimates of the unencashed payment authorisation sitting within the Riposte domain at any point in time are of the order of £500M[23]

[DN: Can the commercial people help here - this seems low - we must have a view from funding angle as to the rate of pickup?]

12.2.2. An alternative approach is to consider the total value of Payment Authorisations - encashed or otherwise - which will be sitting within the Riposte domain at any point in time[24]. Given a 100-day retention period, this could be of the order of £40B. This figure would, of course, a significantly larger if the archiving mechanism within Riposte were to fail (and therefore potentially all Payment Authorisations that had ever existed within Riposte had to be considered).

12.3. Service Levels

12.3.1. Pathway are committed to an SLA[25] of "*no more than 0.1% of Transactions shall result in errors*", "*total value of errors outstanding shall not exceed £1m.*" , and "*100% of all errors shall be cleared within 5 days*". These would suggest a possible acceptable (in contract terms) error rate of 3,000 per day.

[23] Estimate from Tom Patterson briefing notes to sponsors on Accounting and Reconciliation, eg 3 June 1998.
[24] This is on the rationale that a Payment Authorisation is cryptographically protected against modification, but that this protection does not prevent "re-use".
[25] DSS Agreement - Schedule D08 "*PAS Service Levels*" section 4 Accounting and Reconciliation.

[DN: Presumably this SLA would still apply if much of the functionality ceases to be BA and moves to POCL? Need a contractual view.]

12.3.2. Given an average payment amount of £65, and an assumption that these errors are now fully within the POCL domain, as a result of the boundary shift, this would suggest that without breaking the SLA, errors could related to some ~£200k per working day, or say £1M per week. This level would, of course, quickly exhaust the £80M liability cap.

12.4. Pathway Actuarial Valuation

12.4.1. It is understood that ICL Pathway have quoted[26] a figure of £6M per year as their actuarial valuation of the risk; this figure is that which will therefore be included within their financial accounts.

12.4.2. Given the £80M cap and a 7 year contract, this figure would fall within the cap, however with limited headroom. It is not known whether the actuaries had full visibility of Pathway's design, development methodology, track record, etc at the time of provision of these figures.

13. UNQUANTIFIED RISKS

13.1. It is important to note that the "quantifiable" risks outlined in previous sections could be dwarfed by risks which on which a single figure cannot be assigned. These relate not to identifiable one-off failure conditions, but to the effect of events such as some catastrophic failure of the benefit payment service, such that unauthorised payments are made to customers (eg all previous payments repeated[27]), through either failure or deliberate attack.

13.2. Such risks of course exist in all such systems, although it could be argued that a complex distributed system offers more scope for such events and less ability to control, than say a (lower availability) central solution.

13.3. Risks would normally be controlled through a combination of strong control over the whole project lifecycle, from design through development, test and implementation, and live running. Unfortunately, within the constraints of the contract and relationship with ICL Pathway, we have not been able to provide assurance of these controls. No rigorous application design assurance has possible (indeed, this study has probably given us the best insight to date into the BES design), and the testing

[26] Verbal report of statement by Tony Oppenheim to CAPS Project Board, circa March 1998. The full scope referred to by this £6M is not known.

[27] In reality, some quantification could be made - as earlier we have tried to estimate the total number of unexpired Payment Authorisation records - but this becomes increasingly less scientific.

strategy is focused towards white-box, positive testing rather than an adversarial, black box approach.

13.4. Note also that the quantification above is based on random, unintentional, failures, rather than specific, targeted, criminal activity. It would obviously be possible to manipulate the service, either through opportunistic use of genuine failures, or by deliberately inducing failures, to cause significantly higher numbers of mis-payments. The level of such loss is gated by the ability of ICL Pathway and the Authorities to detect and respond to such events and in the success or otherwise of investigations and prosecutions.

14. CONCLUSION

14.1. Although this paper started out with the aim of trying to identify the financial risks on POCL of accepting the revised boundary position, it is now clear that the issue is significantly larger than one of a pure financial cost. In taking on responsibility for much of PAS, POCL would be shouldering potentially the largest slice of risk within the BPS and for a significantly complex design over which it has had little control.

14.2. Examination of the BES design shows that, if the system works according to that design and is not subject to deliberate attack or misuse, the number of mis-payments should be low. However, due to the complexity of the system and the manner in which it has been constructed, the number of mis-payments could be dramatically increased if the infrastructure was deliberately targeted or should some major system failure occur.

14.3. The financial risk becomes significant once the liability "cap" approaches exhaustion[28]. However, at the point when which such exhaustion seems likely, POCL may have little control over the service and little choice but to continue with its operation.

[DN: What if we accept this boundary position, and the £80M liability, and after 2 years find that £60M has been eroded? At this stage we do not have ability to "turn it off", but we could not afford to continue. How do we gain control?]

14.4. Before POCL make any decision to accept this revised boundary position and the financial risks associated therein, it is recommended that a number of other areas need to be considered, including:

(a) check that POCL are legally permitted to act in this role

(b) consider how the risk/liability can be shown in the PO/POCL accounts

[28] In reality, one would want to retain headroom for at least one single catastrophic failure.

(c) ensure that the revised boundary is fully and explicitly defined in technical teams (as this analysis has shown that this new boundary is not without ambiguities) and that its effect on the remainder of the ICL Pathway contract is understood.

(d) consider what financial control mechanisms POCL require to be able to manage this risk, including to be able to quantify the liability at any period in time.

(e) consider what business controls can be implemented to allow timely detection of some significant failure of the solution (eg by monitoring transactions volumes or cash supply)

(f) consider what additional verification and validation of the Pathway solution is needed to be able to control their risk (this could include requiring a full and open design review of the solution, in a traditional design assurance manner).

(g) consider what additional control POCL require over the Pathway solution to maintain this position (given that much of the risk is beneath the detail of the contractual documentation, how do we ensure that they do not change the risk profile to suit their commercial needs?)

(h) consider that rights POCL requires to be able to prevent losses if the service proves to make a large number of mis-payments (noting that the SLA is unlikely to be an adequate control). What rights would be need to have to force major design changes?