WITN05970123

BA/POCL and HORIZON

A Reflection on the Past Five Years:

Lessons, Issues and Key Points

Author: Jeremy Folkes
Date: February 2000

WITN05970123

Introduction

During the last five years of the various incarnations of the BA/POCL and Horizon programmes, there has been a considerable turnover of staff within the POCL team, leading at times to a lack of continuity and certainly a loss of key knowledge and *accumulated wisdom*. This loss naturally leads to a reduction of the amount of *reliable information* on which to base decisions, the growth of *unsubstantiated rumour* about many aspects of Horizon, and a severe risk of *wheel reinvention*.

This document is intended to help to mitigate the effect of the loss of a further batch of staff. It evolved from the concept of producing a general "brain-dump" document, in addition to more usual formal handover for work-in-progress and the like.

This document has been produced for Dave Miller, the Managing Director of Post Office Network Unit, the business unit which owns Horizon on behalf of The Post Office.

Caveat

This document is not intended to be seen as attributing blame to any body or organisation, but rather as a hopefully objective learning exercise to aid both the Horizon programme and other projects in the future. This document contains much "*20:20 Hindsight*", and by its nature it may make some fairly controversial statements, but it is hoped that both will received in positive manner in which they are intended. It in written purely for internal use within The Post Office and not for circulation to outside bodies.

Specifically, this document is not intended to initiate a witch hunt against any of the organisations concerned, including Pathway. With the objective of maximising the learning opportunity, I have made reference - but without source - to information and views that I been given informally or in an "off the record" manner. It is assumed that such references will be treated with appropriate discretion.

The Author

For information, I joined the programme in early 1995, with my first major role being in the evaluation of the responses by five potential service providers to the Statement of Service Requirements, which led to three of these organisations moving forward into the Demonstrator phase. I then led one of the Demonstrator Strands culminating in the qualitative evaluation of the three suppliers, and was then involved in the ITT and Invitation to Retender process, which led in turn to the eventual award of contract to Pathway in 1996. I then undertook a variety of assurance roles during the development of the Pathway service, including being part of the Fraud & Security Group. In 1999 I was involved in the Project Emerald work in support of the government decision on the future of the programme, and latterly in work around Acceptance and Network Banking.

I left the Post Office in early 2000 to take up a post in Anshe Ltd, a Dublin-based company developing high technology software solutions for the post office marketplace. For the avoidance of doubt, this company is not directly connected with ICL Pathway or any of its subcontractors.

WITN05970123

Approach

The approach taken in producing this document has been to concentrate on issues which, in the opinion and knowledge of the author, still have the ability to affect the future of the programme and of POCL - in other words, those which still could "*bite*", or those which are in some way still "*bugging us*" - ie from which we are still suffering to some degree. By its very nature, this is highly subjective, and will tend to concentrate on areas of the programme of which I have had maximum visibility.

I have structured the document into five sections, covering:

- lessons from the past
- major inhibitors
- future risk areas and technical issues
- challenges for the future
- common misconceptions

I have also added a single sheet "key messages" section.

As one might expect, there is some inevitable overlap between these topics (for instance, an inhibitor can be reworded as a lesson to be learnt); for this reason the classifications should not be allowed to distract the reader from the points being raised.

Terminology

As the programme has moved through a number of stages, a variety of terminology has been used, including:

- Pathway, ICL Pathway etc to represent the supplier;
- programme, BA/POCL, PDA, Horizon to represent the body - sometimes joint body - charged with managing the supplier;
- contracting authority, sponsor, business etc to present POCL or BA.

I have tried to use the correct terms where possible within this paper, however a number of comments apply equally to different versions of the same body, and these terms should not be seen as being definitive or exclusive.

WITN05970123

Key Messages

It may be useful to pick out a small number of key messages that, if everything else in this paper was ignored, would still be of benefit for future projects as phases.

1. *A quality service will only result from quality software, and quality software is only produced if the right methods are followed from the start - quality cannot be retrofitted at the end of the development cycle. The laws of software development are not rewritten purely because a project is conducted on a service or PFI basis.*

   ⇨ **Ensure you have powers to assure or police a supplier's approach to quality - to ensure that the supplier "does it right"**

2. *A system or service cannot be assured purely through end-of-lifecycle "black box" testing. If you need to provide independent assurance, then you need to be able to look "into the box" and to review the various stages of the development lifecycle as they are happening.*

   ⇨ **Ensure you have the contractual rights to be able to gain assurance of the suppliers solution**

3. *Avoid premature entry to a phase - if the entry criteria are not met, then that phase's objectives are unlikely to be met, and entering that phase too soon is unlikely to help long term progress. Problems are best discovered and resolved in the earliest possible stage. Remember who won out of the "hare and tortoise".*

   ⇨ **Set entry criteria and stick to them.**

4. *The Post Office are - after a lot of blood, sweat, tears and money - in the process of rolling out an automation infrastructure of which they can be proud. Although it has had a difficult evolution, the architecture should be capable of supporting, to the characteristics needed for counters' business, a wide range of future automation. However, it would all be too easy from this point to destroy what has been achieved through misusing the architecture, eg by treating it as a set of component parts rather than as an integrated system or by forcing inappropriate technology into the solution.*

   ⇨ **Use, don't abuse, the architecture**

WITN05970123

A. LESSONS FROM THE PAST

This section documents a number of lessons which should be learnt from the problems experienced over the last 5 years on BA/POCL and Horizon. Some may only be of relevance for future projects, others may still be applicable to the current contract with ICL Pathway.

A1. "The requirements and the contract must reflect what is important to you"

Whilst this may be seen as stating the obvious, it is one where POCL were not fully successful. It is no good finding that a particular aspect of the service or how it is delivered which is of importance to you is not covered - whether this be particular service levels, or how something is done.

Example. The obvious example of this probably relates to supplier behaviour and our ability to gain assurance over the design and operation of the service. These aspects were not covered within the contract, causing some considerable problems during the development phase of the programme. [This is explored further during this document].

Example: Certain service levels which are important to POCL were omitted from the contract, this was believed to be on the grounds of cost/affordability. However, if POCL requires the service to meet certain levels, to meet their contracts with clients (for instance, for delivery of transactions for Automated Payments), then these need to be "back to backed" with those of the supplier.

A2. "Even the most obvious things should be stated if they are important"

Some attributes of the service may appear so obvious that they do not need to be stated - indeed, so obvious that stating them is almost an insult. However, if they define characteristics of the service which are vital to its success, they *should* be stated. Teasing out these attributes from the business may require some considerable effort and imagination.

Example. There was no explicit service level for the "stability" of the desktop environment. In the live trial, it became apparent that the ICL Pathway counter systems were suffering major stability problems, causing the terminals to "crash" with unacceptable frequency and have to be rebooted during office opening hours. However, the actual outage was insufficient to breach the service levels set for availability of the service, which were more aimed at managing the "mean time to repair" for hardware failures.

At the time of requirements specification, it was not envisaged that a service with these stability problems would be delivered, and therefore no explicit service level was set. During the acceptance process, a target of a maximum of 4 reboots per year per terminal was defined, and eventually met, after considerable work by ICL Pathway.

A3. "Consider the characteristics of the service in addition to the functionality"

Specification of the *functionality* of a service tends to be relatively easy to do; specification of the *characteristics* required (the "*-ity's*") for a service is generally far harder, especially in a measurable and objective way - however these characteristics will frequently have a greater influence on the overall design of the service than any particular aspect of the functionality.

WITN05970123

Unfortunately, it tends to be difficult to turn ill-defined qualitative terms (eg "*it must be secure, reliable and robust*") into measurable criteria, especially as its is natural at first sight to regard these as absolute. For instance, if you consider "*it must be secure*", how many security breaches per year would be considered acceptable - the average business manager would probably respond "*none*", although this clearly unachievable against unlimited attack resources?

There are, however, certain international standards (eg ISO 9126 on Evaluation of Software) which can be used to assist in the definition of characteristics, and for future projects we would be advised to ensure these are used when building a contract.

Example. There were major disputes between POCL and ICL Pathway regarding security, and what constituted making something "secure", especially against human frailties - eg staff not following procedures.

A4. "Maintain clear definitions of important terms"

It is essential that key terms used within the requirements and contract are well thought through and strictly defined, and then maintained under change control throughout the live of the project. Without this control, the meaning of particular parts of the contract can be subject to widespread interpretation.

Example. The terms describing the major components of the service - TMS, OPS, PAS, BES - were not well defined and suffered from some drift; as a result the ICL Pathway usage of TMS differs from that understood and "meant" by POCL, and there was a significant dispute between BA, POCL and ICL Pathway regarding the boundary between PAS and BES (between a logical and a physical view).

Example. The term "transaction" was bastardised over time, causing some erosion of the meaning of certain requirements.

A5. "Key aspects of the solution must be embodied in the contract."

It is essential that key aspects of the solution, and in particular those on which a service provider has been evaluated, are embodied in the contract, and are therefore under Change Control. Care must be taken to ensure that "promises" and "intent" are converted into firm statements within the contract.

Example. Pathway made particular play during the Demonstrator of their highly resilient central architecture, based around 4 central sites spread over two campuses (such that any local difficulty would still leave ¾ of the equipment functioning). However, this aspect of the solution failed to be clearly translated into a "Solution" and therefore into the contract - although it did reach a lower level document - leading to dispute within the development phase when it was not implemented.

A6. "The solution cannot be fully defined by response to individual requirements"

The structure of the contract relied, for the "technical content", largely on responses (known as Solutions) to the contracting authority Requirements. However, the supplier's underlying solution is not capable of being fully defined by being a sum of the individual Solutions to Requirements. If the supplier is being evaluated on the basis of their overall solution (eg on

WITN05970123

the viability of the technical design), then this overall solution needs to be described and then maintained.

Example. This gap was identified during the Requirements phase, being plugged through Requirements 950, which called for a Solution Overview. Unfortunately, this was treated as a one off deliverable and was not maintained post award of contract, and therefore was of limited use. Service Definitions, created later in the lifecycle, mitigated this to some extent but left some part of the "big picture" still poorly defined.

A7. "Proactively manage any drift of the solution"

The service provider's solution will undoubtedly be subject to change over the life of the contract, especially during the initial development phase. A level of change is both expected and indeed desirable, as the solution develops; however it is essential to ensure that it is controlled - and in particular that it does not undermine the original procurement decision.

It may not be sufficient to operate a Change Control process in a purely reactive mode. Mechanisms should be put in place to ensure that emerging changes are *forced* into the Change Control process for consideration, rather than becoming accepted by default. Clear responsibility has to be assigned to control drift (ie to ensure compliance), with appropriate escalation processes to manage unacceptable changes in a timely fashion.

Example. Although there was a formal change control process in place, it relied on ICL Pathway to "admit" to changes and raise Change Control Notices, and obviously only operated against those features which were documented in the contract (see earlier comments). A number of changes to the solution occurred without being raised by Pathway - at least not in a timely fashion - and by the time they were formally raised were too well established to reverse, at least without causing major additional slippage.

A8. "Concentrate on the suppliers ability to deliver"

The supplier's ability to deliver the programme is potentially of greater long term importance than the particular breed of technology in use; if the technology is wrong but you have the right supplier, the supplier can modify their solution, however a bad supplier is unlikely to succeed whatever the technology.

As it tends to be easier to evaluate the solution/technology rather than the supplier's ability to deliver, the latter is frequently given less importance in evaluation activities. However, it is crucial - especially in a service contract of this magnitude - to ensure that the supplier is indeed capable to doing what they are saying they will do. A brilliant technical solution can be totally ruined by a supplier who cannot manage a programme or the key stages within that programme (eg integration, rollout etc).

Example. Despite the technological advantages of the Pathway solution, the Evaluation team raised a number of Risk Register risks against Pathway during the Demonstrator phase of the procurement - these risks relating to their ability to manage their subcontractors, to deliver etc. History has shown these underlying concerns to have been well justified, especially in the early days post award.

A9. "Do not get distracted by irrelevant or short lived standards etc"

WITN05970123

There is a danger of the procurement being distracted by debate over emerging technical or business standards which in reality have a considerably shorter "life" than the solution and contract itself - especially in a service contract. If the requirement is well defined in terms of the functionality and characteristics, then standards which only affect the "internals" - ie are not visible at the service boundary - should not be allowed to *unduly* distort the solution.

Example. The original Statement of Service Requirements (SSR) included the need for the solution to be ARTS Compliant, although existing POCL systems were not ARTS compliant. At the time of the procurement, the ARTS standards were not yet fully development and compliance was therefore not possible, and the suitability for the Post Office Counters accounting environment was unproven; over the life of the development the ARTS standards failed to have a significant effect on the industry and are now largely irrelevant. However the issue of ARTS Compliance occupied a considerable amount of time with service providers and added an unnecessary complexity to the procurement.

A10. "Do not get distracted by irrelevant technology detail"

Despite the procurement being for a service rather than a system, there has been a tendency to consider in detail aspects of the technology which do not, in the long term, affect the delivery of the service or use of solution. This consideration tends to devalue the procurement process and can undermine genuine assurance activities, as well as distracting attention from more relevant areas.

Example. The evaluation considered in some detail the specifications of the PCs being provided as counter terminals; at the time of the contract award ICL Pathway were proposing 166MHz Pentium machines, which were considered fairly top of the range. In reality, as the development has progressed, the entry level specification of PC equipment has risen considerably, and ICL Pathway are now installing 400MHz Pentium II's - indeed. We were not contracting for the supply of PCs, and although we wished to gain confidence in the viability of what the supplier was proposing (and the PCs were part of that solution), the suitability of the specification of PC was the supplier's, and not POCL, risk.

A11. "Define an assurance approach at the start"

Although a service contract should be largely policed through service levels, it is unacceptable from a business perspective to allow the service provider to "fail" - especially if such "failure" results in a significant slippage of the programme or damage to your own reputation. *Put another way, failure to deliver a quality service is a risk to the customer in addition to the supplier, and prior to the commencement of live service, service levels are of little use.*

It is therefore necessary to ensure that the contractor is "*on track*" and is not storing up problems which will emerge in latter stages of development (eg in testing phases) or worst still in live operation.

Traditionally, this could be achieved through a programme of assurance activities and stage deliverables - for instance delivery of a series of documents throughout the lifecycle, with payments or penalties tied to these events.

Unfortunately, in the PFI approach, these intermediate payment milestones tend not to exist, and as a result the service provider may take a "*leave us to it*" approach - denying intermediate visibility, and risking problems only becoming visible in the latter stages. Even if some visibility is achieved, the contracting authority may be powerless to influence the supplier. The

WITN05970123

supplier will tend to see the contracting authority's attempts at assurance as an unwelcome distraction and a cause of delay, and indeed this is what happened on Horizon.

It is therefore essential that, in a programme of this complexity, the ability to seek assurance be formalised into the contract to ensure that the risks around quality and slippage can be properly managed. This would be best achieved through a pre-defined series of reviews and deliverables, perhaps tied to industry standard criteria using ISO 9001[1], ISO 9126[2] etc.

Note that assurance work will frequently require access to supplier's documentation. This may include documentation over which the supplier may not wish the customer to have formal change rights, and where indeed it would inappropriate for the customer to dictate how the supplier should do something - but where the customer has a need to be assured that it is being done to an adequate standard.

Example. The Pathway contract did not envisage the need for "assurance" as such and did not allow the contracting authorities the ability to gain a satisfactory level of assurance during the design phase. It is now broadly acknowledged that Pathway did not follow a traditional or appropriate design approach, and that the product suffered as a result, with many problems emerging in testing and live running, with subsequent problems with slippage and rework.

A12. "Define quality assurance criteria"

Although a service contract will be largely defined in terms of the outputs, the "quality" of the software product is still important, and quality of a software product will only be achieved if it is built in from the start. It is insufficient to rely purely on output based controls - eg testing - to have confidence in the quality of the product the "how" is important, as well as the "what".

The contract should therefore encourage the service provider to take a quality approach to the development of the product; this may be achieved through insisting on the presence of and adherence to a development quality system, with some external (eg customer) visibility and audit of its operation.

Example. We know that Pathway moved into development and coding of certain aspects of the solution - eg EPOSS and BES - without completing a formal design stage and without producing adequate formal design documentation. Significant problems therefore emerged during testing, at which time they were expensive (in time and cost) to fix, with the result that the programme suffered major slippage. We had no "leverage" through which to ensure that Pathway took a quality approach during the development phase, and therefore were largely powerless to prevent them falling into this trap.

Example. Although Pathway were committed via the contract to implementing an ISO9001 quality system, they avoided seeking accreditation for (and ongoing independent audit against) the development-related aspects until after the majority of development was complete, on the basis that the operations-related parts could not be done until the system was in steady state. This considerably undermined the usefulness of this part of the contract, and allowed Pathway to take considerable liberties with quality in the earlier stages of the programme.

[1] ISO9001 (aka BS5750) - a standard for quality management systems
[2] ISO9126 - a standard for evaluation of software products

WITN05970123

A13. "Agree a documentation set as early as possible"

It is essential that the full documentation set to be provided by the supplier to the customer - and likewise to be provided by the customer to the supplier, if relevant - is defined and agreed as early as possible in the lifecycle. This agreement should involve clarity over the content and level of detail to be provided, and the nature of the document - whether the supplier has change control rights, access rights, other restrictions, and whether the document is a one-off or is to be maintained.

Example. At least one acceptance incident, still in the process of being cleared, related to the (non-) provision of so-called third party documentation by Pathway.

Example. Because the documentation set and its proposed content was not tightly controlled, some detail was lost from one document on the intent of being moved elsewhere, only for the destination document to either never appear in the right form, or to have a different status (eg to not be generally accessible by POCL). Certain technical detail from the Functional Specification was moved to the Technical Environment Description - which was then claimed by Pathway to not be part of the documentation set accessible to POCL - rather than into the Service Architecture Design Document, and therefore became unavailable to the programme staff.

Example. The status of the "Solutions Catalogue" was a matter of disagreement between the contracting authorities and Pathway for some time - the CA view was that, as part of the contract, it should be maintained, whereas Pathway took the view that it was overtaken by lower level documentation such as the SADD. As a result, the two were allowed to get out of step, causing confusion and pain downstream when such discrepancies were discovered.

Note that this definition of documentation set needs to include the stage, within the programme, that the document will be produced - to gain the full benefit of the review. Documents are produced not for their own sake, but generally as part of an overall development lifecycle, with the document being the means of agreement or definition of one stage, as input to the next.

Example. The "Style Guide" was a document intended to define a consistent user interface for the desktop at the counter. Ideally, this document should have been produced and agreed prior to the 'cutting of code' and certainly before any release of software on live users, so that the system being developed conformed to this consistent style; in reality, this document was very much an 'after the event' statement of fact, rather than a vehicle for agreement.

A14. "Ensure that risks and issues identified prior to award are managed"

Where risks are identified against a service provider, and these are used to weight the tenders, it is then essential that the risks against the winning supplier are then properly managed. There is little point in identifying a risk as having a certain probability and certain impact, and adjusting the bids accordingly, if no process then exists to manage this risk once the contract has been awarded, ensure that the impact to the business is minimised.

Example. There were a number of risks lodged on the Risk Register against Pathway (and other suppliers) in the evaluation; these "risks" were quantified and factored into the financial evaluation. However, when Pathway were awarded the contract, there was then no formal process to take forward these identified risks to ensure that they did not adversely affect the delivery of the service - and experience has shown that a number of these risks did infact mature.

WITN05970123

A15. "Do not let fundamental issues drift"

There were a number of fundamental issues which were unfortunately allowed to "drift" and have never been satisfactorily resolved. In a programme of the size of BA/POCL, it is essential that major issues are identified and given adequate backing to be resolved before they become enshrined in folklore and become in effect unresolveable.

Example. The issue of access to design documentation for assurance purposes is a prime example of this problem. Because the issue was never resolved, a large amount of effort was expended at a lower levels in attempting to provide assurance without the tools being available for the job - resulting in a poor return on the investment and low levels of assurance (and subsequently a poor quality product being allowed into live operation).

Example. The so-called "Boundary Issue" continued unresolved for many many months, although it had potential to destabilise the entire programme (and indeed, may have prevented rollout had BPS not been cancelled).

A16. "Empower the people managing the supplier"

The "delivery authority" must be given the *authority* to deliver, that is to be *empowered* to *make decisions* on behalf of the organisation. Unfortunately, for a variety of reasons, the programme delivery authority did not enjoy this empowerment and tended to be shadowed by "the business", to whom many decisions had to be referred. This was particularly inefficient given that a number of the "*experts*" in specific domains in the organisation had been seconded into the PDA, and therefore those having to be consulted in the business had less ability to give an informed answer than those on the programme.

The perception (within POCL) of the programme being BA-dominated, and with certain POCL facing functions being staffed by BA people, did nothing to help the level of trust and therefore empowerment, and led to the creating of "*shadow PDA*" functions within the business. This in turn undermined the ability of the PDA staff in their negotiations with ICL Pathway.

A17. "Do not get distracted by short term goals"

The desire to exhibit an early "win" by implementing the 10 Initial Go-Live (IGL) offices was a major distraction for both the contracting authorities and for Pathway. This IGL system was not representative of the eventual system (in hardware, software or architecture), and it caused a number of Pathway's key staff to "*take their eye off the ball*", just to create a "*throw-away*" from which *relatively* little would be learnt. It also created a new set of problems with the go-live of the system proper, as the migration from IGL had to be managed; that system was then not starting from a "clean start".

The message here is that the political or business needs for an early pilot or demonstration of live functionality should to be carefully *balanced* against the long term effects on the main objectives of the programme. The creation of a pilot - especially one of *limited* technical or operational relevance to the end system - is likely to delay the eventual arrival of that end system still further, and may therefore jeopardise the eventual achievement of the end goal.

WITN05970123

A18. "Set entry criteria and stick to them"

Short term objectives generate an enormous enthusiasm to push forward to the next stage, although the entry criteria for that stage - or the exit criteria for the last - have not have been met. A balance has to be struck between the risk-averse "*never move forward*" approach and the *calendar-led* approach, by which a new stage starts on the planned date irrespective of the problems.

Example. On a number of occasions, Pathway entered complex and expensive test phases when the product was clearly not yet in a fit state for that phase - ie had not completed the earlier, simpler, phases. This was generally because of pressure to meet end dates, to which complex dependencies may have been attached (eg migration weekends, go live activities), however several times the effect was to cause the test phases to fail and have to be re-run, pushing out the end-dates still further.

A19. "Ensure the overall procurement strategy is reviewed, is clear and is communicated"

At times, it appeared that a clear route map for the following stages of the procurement had not been defined or at least communicated. This led to confusion and concern amongst staff and disagreement with the supplier on, for instance, what material or issues would or could be carried forward into the next stage, what state things had to be in, or simply what would be coming next.

To be fair, BA/POCL was probably a voyage of discovery for many of those involved, including those "procurement experts"[3] who had probably not had experience of anything with quite that complexity, scale or degree of government involvement (especially with two contracting authorities).

Example. Acceptance was always seen as the universal panacea - as in "it'll get caught at acceptance". However, although Acceptance had been an commonly known concept from the very start, there was a lack of clarity over how it would be run or what it would or wouldn't not pick up, and much of this was only resolved during the Acceptance stage itself.

Example. In Autumn 1995, an instruction emerged - apparently without great scrutiny - for technical and business staff to write "contract schedules" in legalise from scratch - without any form of requirements specification or even legal guidance etc. This was plainly impossible, and indeed was replaced by a several month long creation of a Requirements Catalogue. However, the abortive push into schedules, followed by much heated debate over the need for the Requirements Catalogue, wasted time and effort.

A20. "Agree consistent ground rules and stick to them"

On a number of occasions, the programme appeared to enter new phases of activity with the underlying ground rules, rules of engagement, the methods of working etc not having been designed or agreed, either internally or between the parties. As a result, a number of different methods of working tend to emerge, as people on all sides try to "*do their best*"; either one will become dominant, causing others to have to change (and possibly rework their position), or several will continue in parallel, potentially undermining each other.

[3] And including the author!

WITN05970123

In the tripartite relationship between BA, POCL and Pathway, this was even more stark, as the approach taken would depend on whether a BA or POCL-ite happened to be leading an activity.

A21. "Never underestimate integration"

One of the reasons behind the amount of slippage in ICL Pathway's plans for delivery appears to have been an underestimation of the time and effort needed to integrate the various parts of the solution into a single, end to end, operational system. Obviously this interrelates with problems with the design methodology, lack of appreciation of requirements complexity etc, but also stands on its own as a valid criticism. There were numerous cases where integration appeared to be a "*last minute*" activity, assumed to be going to take very little time to perform, which in reality took a considerable amount of time and effort and had significant effect on downstream activities.

Our own experience - from projects such as ALPS - goes to support the message that Integration, especially of diversely developed components - is non-trivial and high risk, and therefore needs to have adequate time allowed in any plans.

A22. "Beware of outsourcing business functions to a purely IT company"

ICL Pathway are, by their nature, an IT services company; although the initial Pathway consortium did consist of other companies, they were still primarily IT orientated, with little experience of either the Post Office business or the Benefits Agency business. Where specialists were involved, it appeared that at times - presumably for cost reasons - they were kept at arms length and their input was restricted.

As a result, much time had to be spent "teaching" the IT services company about POCL and BA and the fairly unique models under which they work; given that both POCL and BA had existing information technology expertise, there was at times something rather perverse about having to bring a new set of information technology people up to speed. There is perhaps a sub-message here about whether it is easier to bring IT people up to speed with a business rather than business people up to speed with IT.

However, the key point here is that we were - especially in the BPS days - buying a business service from ICL Pathway - which included much non-IT content, and certainly needed business as well as IT input. Much as the contracting authorities were criticised - with some justification - for wanting to look too much at the technology, there is some evidence that the supplier was over keen on the technology rather than the business need.

WITN05970123

B. MAJOR INHIBITORS

B1. Two contracting authorities.

The existence of two contracting authorities (BA and POCL) with different agendas and approaches, with one of the authorities also being a subcontractor of the other, led to major difficulties, and caused much confusion with mixed messages being fed to the supplier and back within the two customer organisations.

This inhibitor has been discussed in great detail elsewhere and will not be pursued here.

B2. Design approach

It is now generally acknowledged[4] that Pathway did not follow an appropriate design and development approach, especially in the early days of the programme, through a combination of a lack of appreciation of the complexity of the service requirements and a misguided but heroic attempt to meet impossible early timecales. Once they had gone so far down this route, it was then very difficult for them to pull back to a position of stability and to adopt a quality approach, without admitting to massive and politically unacceptable slippage.

Example. It appears that no overall formal design document existed for the Benefit Payment Service in the early days of the project, despite it being a highly complex[5]; individual specifications, each to different standards, had been generated for some aspects of the service (eg the PAS/CMS Oracle work, and the TMS Agents) and Escher was developing the front end BES code, with little documentation provided to Pathway. As a result, considerable problems were experienced in integrating these three parts of the end-to-end BPS system, with major design flaws only emerging in the latter stages of testing, when these parts were first interconnected.[6]

Example. Late in the development of the Benefit Payment Service (probably mid-late 1998, when POCL were attempting to resolve the "boundary issue" with BA), we attempted to obtain design documentation on the overall operation of BPS, in particular the split between BES and PAS, and specifically the messaging between the counter and centre for BES/PAS. It became apparent at that Pathway did not themselves have an clear and validated message definition, and that much knowledge was purely retained in the heads of their key staff. This key interface had evolved apparently without any formal validation or documentation held by Pathway; at the time of our enquiry Pathway were attempting to retrofit design documentation to this product, and were still uncertain about certain aspects of the functionality.

B3. Naive development approach by Pathway

Pathway's approach to development was, at times, naïve, especially around the handling of exceptions and errors. Most seasoned development staff will freely admit that a considerable amount of effort has to be put into error and exception handling, especially in systems which have to maintain financial integrity in a hostile environment (a category into which post offices would fall). Unfortunately, Pathway did not appear to have in place the necessary processes to ensure that errors and exceptions would be suitably handled, at times appearing to favour the "*it won't happen*" approach. Of course, in a system with 20,000 sites, 20,000 communication

[4] Eg Project Mentors report "*serious problem in the way in which ICL Pathway have developed the system*".
[5] BPS's complexity stems from some demanding business rules - especially around proxies, agents, foreign encashments etc - implemented on the highly distributed architecture provided by Riposte.
[6] Eg Recall and Reissue functionality in PAS/CMS had to be re-written due to mismatch with front end design.

WITN05970123

lines, 40,000 terminals and 70,000 users, almost every form of failure WILL happen - and the design has to be cognisant of these failures.

Example. The build of counter system submitted to Live Trial was not immune to power failure or interruption during the Cash Account production process; a failure at this stage would cause accounting integrity to be lost, with certain figures being doubled up in future reports.

Example. Transactions were lost on the boundary between the "Riposte" and "Oracle" domains, where the Oracle validation rules differed from those implemented in the Riposte world. Although this possibility was predictable (and indeed, had been flagged by the POCL assurance team), processes and procedures were not put in place to handle this exception condition. (This failure contributed directly to the AI376 reconciliation Acceptance Incident).

B4. Lack of understanding of the architecture

The development of applications was, especially in the early period (but probably extending by two years) of development, hampered by a lack of understanding and appreciation of the architecture and in particular the characteristics of Riposte. In hindsight, this is hardly surprising, as the technology was new in the UK, and requires a different mindset to that of conventional architectures.

As a result of a lack of understanding of Riposte, and an apparent lack of input being sought from those who did have the understanding (such as those in Escher Group[7]), applications, and in particular EPOSS, had a very troubled early life, with a considerable amount of rework being required to make it fit for purpose.

B5. Assurance and Documentation etc

The refusal by Pathway to give access to design documentation - generally under the excuse of protecting their IPR, but at times this concealing the lack of adequate documentation - prevented the PDA and its successors from providing the level of assurance that was expected by the sponsors.

As a result of the lack of visibility, a number of problems emerged (to us) only at the end of the development lifecycle, with greatly magnified effect on cost, timescale and quality. Had a documented design been made available to open review at the appropriate time, we would (hopefully) have had the opportunity to discover evidence to support our concerns and therefore have a means of influencing Pathway back onto "*the straight and narrow*".

Due to the nature of the contract, Pathway did appear - unfortunately - to be within their rights to deny this access, as the necessary provisions did not exist; this led to the position where teams were set up within the PDA to provide Assurance of the Pathway solution, without them having the means of discharging this need. This "*responsibility without authority*" led to decisions being made on poor quality information on, for instance, the readiness of the product at particular milestones, and allowed Pathway to fall into self inflicted traps in cutting corners in their design process. Although this may be viewed as them "*shooting themselves in the feet*",

[7] It appeared that Pathway were attempting to "go it alone" with minimal use of Escher on applications such as EPOSS and APS, as a means of reducing their costs with Escher. We know that EPOSS, for example, eventually needed to be "*Escher-fied*" (at some considerable expense) to put right the resultant deficiencies.

WITN05970123

it had negative considerable effect on POCL, and we therefore had legitimate (although contractually unsupported) interest in preventing this self-damage.

B6. Inability to control quality

We had no means of controlling the quality of the product being developed by Pathway for use in provision of the service - although this quality (or lack thereof) would have a significant effect on the delivery of the operational service. As a result, very poor quality product was delivered into both end-to-end test phases and into live operation, with faults then being corrected during these phases - with obvious effect on both progress and user perception etc.

B7. Over reliance on testing

For a variety of reasons, the programme - both Pathway and POCL - have become over-dependent on the use of "testing" as the primary means of assuring quality. As any good textbook on software quality will testify, quality is only achieved by building the right processes into the entire development lifecycle, and cannot be "retrofitted" in testing.

As a result, product entering test phases was found to be in poor condition, requiring much rework and retest, extending the duration of testing and so delaying the availability of the service. Likewise, the product entering live service exhibited a far higher level of fault than might be otherwise expected, with a significant number of problems not having been detected in testing.

A related problem was the premature use of "end to end" test phases - these phases are characterised by running high cost, long duration, and being unwieldy for debugging, compared with earlier test phases. The enthusiasm - by Pathway and others - to show visible progress and enter into these later phases had the net effect of delaying the readiness of the product; a classic "*hare and tortoise*" effect.

B8. Benefit Payment Service dominated by BA

The programme team assuring the Benefits Payment Service, and in particular those parts interfacing with POCL (BES and parts of CMS) was dominated by Benefits Agency staff who did not have the requisite knowledge of POCL business and procedures. Although there were some excellent POCL staff involved, they were at a relatively junior level and their views were at times dominated by the BA staff.

Given that BES and the counter elements of CMS would have accounted for over 30% of the transactions performed at the counter, and the level of financial risk involved in these transactions, POCL were very exposed by not managing to exert adequate control of this area.

B9. Lack of clarity over POCL requirements for EPOSS

The original requirements for EPOSS (eg in the SSR) were very high level, far more so than any of the other services. At the time there was at least one view in the business that they wanted "*anything but ECCO*", and that the requirements were intentionally non-proscriptive to allow the suppliers freedom to propose imaginative approaches.

WITN05970123

However, as the EPOSS package is basically the automation of existing business and accounting rules, which the business has not been prepared to or able to change, the suppliers were, in reality, always going to be constrained to an modern-day ECCO like product (generalised to support all offices, rather than just Branch Offices). Likewise, the requirement for detailed transaction data to be supplied to TIP - and indeed the shape of that date - further defined the shape of the EPOSS product.

It proved extremely difficult to embody these business and accounting rules in a single consistent document which could be provided to Pathway, and for Pathway to then confirm these rules back to POCL[8]. The situation was then further complicated through the need for many of these rules to be data driven, and therefore the need to an interface to the POCL Reference Data System (RDS).

B10. Overall automation programme not managed as such

For BA/POCL or Horizon to succeed, it would both require the success of the Pathway element and the success of the various connected systems and services - including the in-house POCL systems such as TIP and RDS.

Unfortunately, there was a lack of a strong overall programme management function (and related assurance function) to bring these various components parts together into a coherent programme, and indeed at times there appeared to be competition and blame between various projects.

[This problem is now hopefully being resolved with the introduction of the Automation Directorate within PONU etc]

B11. Distance between "the programme" and "the business"

Unfortunately, for a variety of reasons, "*the programme*" grew to become a separate entity from "*the business*", with at times a lack of trust and understanding between the two, undermining those PO staff on the programme and causing duplication of effort back within the business.

Additionally, the fact that the programme was split across a number of sites, with the main site (Terminal House) not having PO email, LAN, Intranet or telephone systems, caused increased isolation from those in the business.

B12. Lack of continuity of staff

The POCL side of the programme has suffered, with a few notable exceptions, from considerably less continuity of staff than that achieved by Pathway. This lack of continuity has affected both the programme itself and those contacts within the business fronting the programme.

This lack of continuity has been caused, at least in part, by a lack of succession planning, an over-reliance on contractors and consultants, and general difficulties in retaining staff in a highly pressured and at times demoralising environment. It also shows the difficulty in

[8] Indeed, such a exchange of Business Rules/Assumptions document for effect of reference data on EPOSS as finally completed during the Acceptance Process in late-1999

WITN05970123

having a project based environment running for a period of some 5 years - far in excess of any "normal" project.

B14. Security and Risk Management

One specific area of dispute with Pathway throughout much of the life of the programme was that of Security; despite the inclusion of general security standards, and the provision to Pathway during the bid process of the full set of relevant security standards, Pathway took a very narrow view of security on Horizon at an early stage (concentrating on encryption and cryptography, to the exclusion of other important areas, such as access control, physical security, and human aspects of security).

In a way, the problems with security are just a microcosm of the problems experienced elsewhere with both the design approach by Pathway and the ability of the PDA to provide assurance. Pathway attempted to fix a 'design' prior to carrying out suitable analysis of requirements - either analysis of the explicit requirements such as compliance with standards, or more subjective requirements around minimisation of risk. This 'design' included, for instance, the choice of data centres, apparently without regard to the specific physical security requirements.

Although these problems were identified at an early stage, the personalities involved, and the fact that Pathway were managing the security aspects under a different umbrella from other characteristics of the service, led to this being a major flashpoint on the programme, with accusations (shown by independent review to be unfounded) *of "Complex and Demanding Security Requirements"* being introduced at a late stage, and of *"Constantly changing requirements"*.

Unfortunately, a number of these security issues were only resolved by being pushed *"to the wire"*, both at various Release Authorisation points and at Acceptance.

[It is encouraging to note, however, than the technical security development work for CSR+ has been brought into the mainstream of development and has been done to a far higher standard]

WITN05970123

C. FUTURE RISK AREAS

This might be considered the "*sleeping dogs coming back to haunt you*" section - it contains areas which are future risks to Horizon - either areas where we know of a deficiency which isn't causing pain at this moment but is likely to cause some problem downstream, or where we have insufficient proof that a previous problem area is under control and fear it may cause problem in the future.

C1. Maintaining and building knowledge of Horizon

As a result the combined effect of the level of access we have to Pathway's design, and the loss of staff and contractors, the business now has a fairly low level of knowledge on the capabilities and characteristics of the Horizon service, and in particular the more technical aspects of the system.

Although it may be argued that under the current contract we do not need detailed knowledge (it being a service contract managed under SLAs etc), experience has shown that to manage risk we do need to take a more active interest in the service; once we move into future products developed, especially those developed on a Time and Materials basis, we will need considerably greater insight, and this cannot be obtained overnight.

C2. Risk transfer back from ICL Pathway

There is a genuine risk that we may, unwittingly, be taking back risk from ICL Pathway due to our actions when dealing with them - for instance, if the Post Office starts exerting undue influence over the architecture, or starts dictating specific items of technical detail. Some of the approaches which have been proposed for the forthcoming Network Banking product might fall into this arena - for instance if we exert influence over ICL Pathway to "misuse" the architecture, we may end up taking back considerable risk in other areas (eg from Pathway being unable to meet certain service levels or having to modify service levels).

At first sight this "*risk*" may seem to be at odds with the recommendations throughout this paper concerning assurance; however, this need not be seen to be a contradiction - assurance is about getting confidence that the supplier is "*doing it right*", without necessarily dictating the contents. The danger is where we start to dictate a solution - rather than just wanting confidence that the solution is being sensibly designed.

C3. Specification of future products

We had undoubtedly had problems in the past with specification of products - whether it be constructing a clear specification for (say) the generic APS product, or coming up with a clear set of business rules for products such as EPOSS.

There is a risk that our ability to specify future products will severely constrain our ability to bring those products to market - irrespective of how efficient the ICL Pathway (or third party) development process may be. We need to develop efficient processes to ensure that we can specify - but not overspecify - the business rules of future products, without unduly constraining the implementation, and to be able to agree these specifications with the minimum of delay.

WITN05970123

Example. Much has been made of the perceived inability for Pathway/Horizon to meet the required business timescales being claimed for Network Banking. However, despite the passage of many months since a Network Banking product was first discussed, there is still no clear product specification available to take to Pathway against which they could work/quote - and given that serial nature of these activities, this is effectively lost time. There is a danger that we are distracted by 'sexy technology' at the expense of adequately managing the work of requirements and product definition.

C4. Security, Fraud and Liability

Although considerable work has been done (albeit after the difficult start outlined earlier) to ensure the security of the underlying IT system on which the service is based, and this should stand POCL in good stead for the introduction of new products, there is a risk that attention is focused on the technical IT aspects (eg cryptography) at the expense of ensuring the fraud resistance of the business product - which of course includes far more than purely the system elements.

There is probably little additional scope for fraud introduced by the "day one" Horizon products - APS being an existing inpayment product, EPOSS being an implementation of existing business and accounting rules etc - however this may not be true for the introduction of new services, such as those in the banking sector, especially involving outpayments.

The risk here is that in considering the technology and the IT system, sight is lost of the need to ensure the overall *fraud resistance* of the transaction, and where any liability for fraud sits. It is obviously vitally important to have clarity over whether liability sits and to control (and make cost provision for) that part of the liability which is considered to be part of POCL's responsibility. This may involve introducing fraud risk management systems, reward schemes, education schemes etc, in addition modifying the design of the transaction itself.

A key area of weakness is Pathway's sometimes over reliance on the correct operation of manual procedures - eg by our 70,000 counter users - to manage fraud. We should design transactions to be resistant to fraud *despite* these users, rather than relying on these users.

C5. Data Protection

Concern has been raised in the past regarding the effects of the Data Protection Act 1998 on both POCL and specifically on Horizon; for instance some advice was given in the past that the DPA98 could be interpreted as requiring each subpostmaster to be individually registered under the DPA. This interpretation also suggested that the subpostmaster had a direct relationship with the POCL client, due to the "thinness" of the involvement by POCL themselves in the transaction.

Various Post Office experts domains (Legal Services, PO DP Officer etc) were involved in discussions regarding the DPA, and it is presumed that some formal position was adopted, but it is unclear how sustainable this would be under the effect of change.

Some care does need to be applied, especially with the automation/re-engineering of future transactions, to ensure that we remain within the bounds of the DPA.

WITN05970123

C6. Some technical capability still to be proven

This section outlines a number of technical areas which it would be wise to "watch", although they are not the subject of any outstanding Acceptance Incidents. They should not be taken as predictions of things which are yet to go wrong, more as a list of possible areas of weakness which could "*trip us up*" in the future, especially as the number of offices increases at the planned rollout rate up to the target full population.

There is an argument, based on the same principles as used to justify, albeit not to great effect, the need for assurance during development, that states the need for ongoing assurance during the live operation of the service and associated system. We do not appear to have any contractual basis to seek such involvement, however we may wish to negotiate with Pathway at the relevant time to seek some confidence that these issues are indeed under control.

C6.1. Software Distribution

The distribution of new version of software to the field is an area which ICL Pathway have been shown to have some difficulty in the past (see AI372), especially in the handling of the "tail" of offices which, after a number of days/weeks of trying, have still not received or installed the new version.

It is probably a "fact of life" that software distribution to 40,000 terminals on 20,000 ISDN-connected user-controlled sites is going to be problematic, but there is much which can be done through proactive management of the distribution process, handling of problem offices etc, to minimise the risks. The size of the problem is obviously related to the number of live offices.

The introduction of CSR+ - which of course is not a *single* release of software, but a series of fairly major events with VPN and Riposte upgrades as well as application software - will be a significant challenge, given the likely size of the estate at the point, and we should press for (and use) full visibility of the upgrade activity, to minimise the risk to the Post Office.

C6.2. Effect of replication delays/failures

The Riposte message replication paradigm is one which guarantees (with obvious exceptions) that a message will eventually be replicated, but not the timescale in which that will be done. Although in normal circumstances, in-office replication should be done within seconds and office-centre replication in 15 minutes, under failure or overload conditions this figure could rise dramatically. Applications therefore need to be aware that replication may not be instant, and handle these cases accordingly; it is this scenario which severely complicates the End of Day (EOD) processing within APS and EPOSS.

However, as a result of the proper handling of slow replication - ie the effect should be benign - these delays these scenarios can go unnoticed (and therefore unfixed, if there is some underlying problem) for a period of time.

WITN05970123

It remains to be seen how effective the system management functions in Pathway are at detecting and resolving problems of this nature. Faults in this category would include LAN failure and terminal failure in the office, ISDN failure, etc.

C6.3. Communications Failure/Poll Failure

In the early days of operation, Pathway were not detecting offices which were failing to communicate with the Data Centres - eg due to faulty ISDN connections, or the master terminal being disconnected or down, etc - and as a result one office went a period of something like 10 days without passing its data to the centre.

Although additional functionality was apparently added to aid the detection of such problems (in effect these can be treated a special case of the slow replication issue above), the ability for Pathway to handle these failures in large volumes - such as those that may be experienced at national rollout - is unproven. The point here is not that failures occur - they obviously will, with a large distributed network of sites - but how quickly the failures can be detected and fixed, to minimise the reduction of service and other risks in the office.

C6.4 Integrity during failure conditions

We were unable, during the development phase, to gain assurance of Pathway's approach to exception and error handling or to get visibility of any detailed failure analysis work that they had performed; indeed, we believe that no formal failure analysis was done and that Pathway relied extensively on general test activities to gain confidence in the system.

There is therefore a risk that, during live running, failure conditions will emerge which are not appropriately handled by the system; as time goes by these should be increasingly rare, and may (for instance) rely on multiple concurrent failure.

Again, to minimise the risk to the Post Office, we would be wise to ensure we seek full explanation of failures that occur, whether or not they have major business impact.

[The following example has been struck through as subsequent knowledge shows that this is handled internally by Riposte, although this was not clear to the author when the report was written. However, the general point about ensuring integrity during failure condition is still valid. JF July 2022]

~~*Example. There is a feature of Riposte known as non-atomic replication; this is the feature where a set of messages are committed atomically (ie in an all-or-nothing manner - for example a customer session at the counter) but are then replicated in a non-atomic fashion (ie at a particular point in time only part of the set will have reached a particular node). The window for such a scenario is generally small, but a failure at the right point could extend this to be considerably more visible. Problems can occur if applications reading these messages do not ensure that the full set of messages making up a session are present.*~~

C6.5. Scalability

Although much work has been done by ICL Pathway to manage risks on the scalability of the Horizon system, and they will undoubtedly be continuing to manage the risk through detailed monitoring over the ramp up of offices and transactions during the

WITN05970123

rollout, the live operation of the system at final volumes is unproven, and Horizon does represent by far the biggest Riposte implementation ever undertaken to date.

We should ensure that we are tied into ICL Pathway's monitoring work and are fully sighted on any problems and risks that emerge.

C6.6. Performance over time

We should be aware that the performance of computer systems can degrade over time, for instance as disk systems become full or fragmented, and as archiving activities kick in. Additionally, we have already suffered from one failure (the Correspondence Server Indexing Problems) which only occurred some 120 days after the system went live, when a particular set of archiving functionality was first exercised.

Again, we should ensure that we have a handle on ICL Pathway's monitoring and management of the system.

C6.7. System Management

ICL Pathway's ability to detect and manage certain failures in the system is as yet somewhat unproven; although we have assurances from Pathway on a number of issues, evidence that failures would indeed be detected and responded to (rather than just logged and ignored) will only come from live running.

There are a number of scenarios discovered through the Technical Assurance work which give examples of possible failures:

- agent lag - where an agent fails to keep up with arrival rate of transactions
- sleepy agents - where an agent has "gone to sleep" and is not processing data
- security alerts (eg attack on a system)
- widespread network failure (eg major Energis loss)
- failover between sites

[Bob Booth is our expert in these areas and has access to the previous Technical Assurance work]

WITN05970123

D. CHALLENGES FOR THE FUTURE

Although the basis "job is done", there are still a number of significant challenges for The Post Office in the use of and future development of Horizon.

D1. Management of future development

The majority of the development work on Horizon to date has been performed under so called "PFI rules", with Pathway taking a high level requirement and working at arms length from POCL (with the previously described difficulties in providing assurance). Although this leaves substantial risk with POCL (over the late arrival or poor quality of the product), the major financial risk over the cost of development is largely with Pathway.

For developments outwith the current scope of the contract - generally post-CSR+ - we will have the option of proceeding with development either on a fixed price basis, or engaging Pathway on a Time and Materials (T&M) basis. In either case, we are going to need to be in a position to evaluate and validate the estimates of the cost and, in the T&M case, to manage the spend by Pathway of our money.

Our experience from the initial products shows that Pathway's development approach has been far from efficient, with insufficient up-front investment in quality design leading to expensive back-end loading of test and correction activities. Although we have been hit by this (in delays etc), once we move into a T&M basis we would be paying directly for this sort of problem. *Put bluntly, when it was Pathway's money it was theirs to waste, but once it is ours we may wish to ensure it is spent more efficiently.*

If therefore we do move into T&M and therefore take on wider financial risk, we will need to manage Pathway far more closely, and this should include forcing them to take a more structured approach to design and development, with adequate up front design and assurance work.

We will also need to put in place considerably enhanced project management capability, if we are to manage and track a development activity of this size.

D2. Controlling and assuring quality

Related to the above is the issue of how we ensure the quality of the product delivered by Pathway - and how we gain confidence in that quality. Whether or not we are taking the financial risk for development failure, we are still at risk from the delivery of poor quality product - and experience has shown that a testing-centric approach is insufficient to ensure quality (as indeed, the past 40 years of software development history has proven).

The challenge is to get into a position with Pathway where we can obtain adequate assurance of the quality of the product, without acting as a hindrance, and without taking on inappropriate responsibility for the design (given that this is a service contract) and therefore risk.

WITN05970123

D3. Designing products to exploit the architecture

The Pathway solution for Horizon is "novel", in that the Riposte based paradigm is radically different in many respects from a conventional 'counter automation' system. The solution has many advantages in the post office environment, but those advantages will not be exploited unless the design of products - and by this we mean business design, not purely technical - is cognisant of the architecture.

Put another way, if attempts are made to implement products in a "traditional way" - ignoring what the architecture can do best - we will end up with, at best, an inefficient use of the investment, and at worst, products which fail to perform to the required levels, or only perform at significant extra cost.

What is required is sufficient knowledge of the architecture and what it can be done to be injected into the early decision making process - preferably at the stage when products are being discussed with clients. This is not to say that products should not meet fully client requirements, but when discussing options it is essential to have a handle on the feasibility - and implications - of particular business designs.

Example. An example may be that of on-line vs off-line; the Horizon architecture can handle on-line, but (as with most systems) off-line transactions will generally be cheaper and provide greater availability; it would therefore be sensible to ensure that only those transactions which really need on-line capability use it. Those designing products at a business level with clients may therefore wish to avoid suggesting use of on-line for cases where it isn't necessary.

D4. Reducing lead times

Horizon has acquired, not surprisingly based on the experience of the initial development, a reputation for imposing a massive lead time on new developments. Much of this related to the complexity of the initial fated Benefit Payment Service product, plus the sheer scope of the infrastructure development; however as at the time of writing (Jan 2000), it is unlikely that any major new product could be delivered for at least 18 months.

However, the "sales-speak" of, for instance Escher, supported to *some* degree by experience from other users of the product[9], suggests that new desktop applications and agent software can be developed in a matter of days.

Of course, there is a massive leap to be made between coding up a new application and actually getting a new product out into the field in a fit state for 20,000 offices to use - there is an entire product lifecycle, from product design/specification, through agreement of commercial terms, design, development, testing, trialling, rollout, training, plus production of procedures etc etc.

Pathway would, with some justification, suggest that one major inhibitor to the fast introduction of new products is the time taken for POCL to develop and agree a stable specification for products, and the lengthy decision making process to handle any clarifications and changes.

[9] Eg. An Post claimed to have developed and implemented complete new products in periods as short as 3 months on a similar platform, albeit in a radically different commercial environment.

WITN05970123

The over-reliance on testing, rather than proactive assurance earlier in the lifecycle, has led to the introduction of some very lengthy and unwieldy test activities, which again does nothing to allow the rapid introduction of product.

D5. Keeping on top of the service (managing risk)

For all the reasons discussed earlier, regarding the Pathway approach, the inability to provide assurance, et al, it is essential that we ensure that Pathway are taking all necessary action to keep the service up and running, without subjecting PONU and its clients to undue risk etc.

There is of course a view, undoubtedly shared by Pathway, and supported to some degree by the contract, that we should manage Pathway primarily via the contracted service levels etc, however experience shows that we need to take a rather more proactive approach in the management of the service. This may be seen as an admission that the service levels are inadequate on their own to manage the service, and in some respects this is true.

However, the contract does support a number of monitoring activities, such as access to helpdesk information, and involvement in the software distribution process, and we should use these to the full.

Example. The Correspondence Server Indexing Problem, which occurred in September, apparently first became apparent in live running, as a decision had been taken by Pathway not to exercise certain archiving functionality in the test environment - a decision which was not made visible to POCL, and through the lack of ability to perform assurance related to a feature not known to POCL. This problem caused considerable operational problems (affecting the distribution of reference data) and the final solution took several months to be implemented (although interim measures were put in place sooner).. Much of the detail of this incident, and the risks that Pathway were taking, only became apparent after considerable questioning of Pathway by technical staff from Horizon - it was not "volunteered" by Pathway. This is a case there Pathway's risk taking had a severe impact on POCL, although POCL were not involved in the decision making process (and where the impact did not breach service levels).

-

D6. Sell Horizon internally

One of the largest challenges which confronts PONU is to "sell" the Horizon service internally within the Post Office. It is hardly surprising, after the delays, government decisions, changes etc, that there is a general lack of confidence and belief in Horizon, however the rollout is now going ahead, the infrastructure is up and running, and at least 10% of the network is installed - and significant volumes of business are flowing through Horizon. In other words, the message should be "*it's been hard work getting here, but we are now here*".

What would be the biggest disaster now is, despite the costs paid (financially and otherwise) by The Post Office and the efforts put in by its staff, if the organisation lacks a belief and desire to use Horizon and to build on it, and so fails to reap from the massive investment which it has made.

WITN05970123

D7. Avoiding ruining what has not been achieved

PONU and Pathway are now in the process of rolling out a service and underlying systems which, although they may have had a "difficult birth", is something of which they now should be proud - it has come on great bounds in recent months, and is becoming a more stable, robust and popular part of our business.

There is a danger, however, that the inappropriate use of the infrastructure - eg by attempting to dramatically '*bastardise*' the architecture - will have a disastrous effect on what has been achieved; to coin a phrase, "*to snatch failure from the jaws of victory*". This is not to deny progress or changes in business requirements etc, but rather to suggest that care is taken not to destabilise something which has taken a lot of effort (including POCL effort) to get to the state it has eventually reached.

D8. Avoiding being told it can all be done in 6 months elsewhere

There is already a tendency for observers to suggest that an alternative solution to Horizon could be procured , developed and implemented in a very short timescale, using new technology and a new supplier. Although it may be attractive to be seduced by such stories, experience shows that the development and deployment of a robust, industry strength infrastructure, on which to mount reliable and secure business applications, is not achieved across a network of 20,000 offices without a lot of effort and time.

By Pathway's own admission, only something like 30% of their development efforts were put into application development - the remaining 70% has gone into the "*under the waterline*" work on the infrastructure, system management, secure etc, and we have no evidence to suggest that an alternative supplier, working to the same requirements, would not find a similar split.

D9. Challenge the business requirements

To ensure that we get the best value from the Automation Programme, we should and must review the high level business requirements and confirm that they are still valid - and consider these requirements against the costs (in financial and operational terms) of their delivery. This may involve some fundamental challenge to the "design"; if the requirements are valid they will stand up to the challenge, but they should at least be challenged. Although it may be "too late" to change the Horizon requirement at this stage (the system having been built), it may inform future procurements and to reduce cost at the back end.

Example. The requirement for each and every individual transactions to be delivered from Horizon to TIP, at the detailed level, has caused considerable surprise to many observers. However, the flow of such data - a transaction record for a 1p stamp sale - has significant cost, both in terms of Pathway's systems and in its storage and use by back end systems; this cost is likely to be significantly more than if just summary information was produced in the office and sent to the centre. The justification for detailed records for all transactions has been generally stated as the desire to be able to operate "data warehousing" functionality at the back end, however this would still appear to be a long way off, and of limited use. Alternatives, such as sampling of data, plus in-office summarisation, could appear to meet the business need. The point here is that we should challenge each requirement on a "cost benefit" basis, to ensure that a requirement is indeed cost effective.

WITN05970123

D10. Prepare for the next contract

Perhaps the biggest challenge to face the Post Office will be how to handle the end of the contract and the (presumed) re-tendering for a future automation contract, coupled with the migration from the old to the new at that point.

There are many lessons from this contract, some reported in this paper, which should would be applied to any future procurement for automation.

D11. Additional peripherals

Addition of extra peripherals to the counter is always going to be an expensive activity, due to the multipliers involved - not only the cost of the peripheral itself, but any survey and modifications and installation work, on top of the development costs themselves.

We should therefore plan very carefully before adopting any products which may require additional peripherals - both to establish need and to ensure maximum flexibility/suitability (ie payback) of any new device.

Possible new peripherals which can be envisaged include:
- customer side PINPads (eg for banking transactions)
- contactless smart card readers (eg for public transport applications)
- Security Access Modules (SAMs) (retailers smart cards) (eg for Mondex etc)
- passbook printers (eg for banking transactions).

Example. The original Automated Payments project, back in the mid-90s, was highly distracted by the need to modify the design to allow use of the Schlumberger smart key product. This "need" caused considerable slippage, rework and delay, for what appeared to be very genuine business reasons, however in reality only relatively few terminals have ever used their Schlumberger capability and we are not, for instance, taking this forward onto Horizon. In hindsight, the decision to implement Schlumberger was not cost effective.

D12. Capacity Management

Any system, and the Pathway system behind Horizon is no exception, will have limits on capacity - there will become a point when it is not possible to add further functionality, transaction or traffic without significant upgrade. Although we have no reason to believe that the counter kit itself has any specific limits which are likely to affect our plans, the central systems may have greater scope for constraint, due to the funnelling effect.

Pathway are well equipped with a scalability strategy and the system is technically scaleable, but there are of course costs involved with any scaling. The costs tend to depend on the size of the increment needed - if one extra box is needed alongside an existing set of 30, the cost may be small, if one extra box is needed alongside some massive single machine, the cost may be large.

Given that we are likely to have to pick up the cost of scaling under certain conditions (eg if forced by new products), we need to have some means of predicting when upgrades might be needed; such modelling will need information and co-operation from ICL Pathway. One result of such modelling is that, at some point, we might decide not to implement some "heavy"

WITN05970123

product as it may dramatically restrict our ability to implement - or at least force up the cost of implementing - other products downstream.

These considerations are unlikely to be relevant in the first 2-3 years; they are, however, potentially important in the last 2 years of the contract, depending on what strategy is to be followed for its replacement or ongoing use.

[The other way of looking at this is to require a "resource budget" to be submitted with an new product - this may influence the design of the product - eg away from all on-line - to minimise the impact on the available resources]

WITN05970123

E. COMMON MISCONCEPTIONS

This section outlines a number of common misconceptions about Horizon which appear to circulate, unfortunately with some apparent authority, within PONU and the wider Post Office.

E1. "It can't do on-line"

Perhaps the most common misconception around the Post Office regarding Horizon is that the infrastructure is unable to handle real time or on-line transactions. In reality, the infrastructure should be quite capable of handling on-line work, both back to the Pathway's data centres and further into client (eg banks) systems is required. Indeed, both the current OBCS service does, and the old BES service did, use on-line for foreign transactions (those away from a customer's nominated office) to access centrally held data; additionally at (at CSR+) the Automated Payments Quantum product uses a "near time" paradigm, with data being delivered within 30 minutes, to meet a specific business need.

What is true is that Pathway's design for Horizon chooses to use an off-line, local processing paradigm where possible, for a variety of genuine reasons:

- higher availability (reliance on WAN only where strictly necessary)
- higher performance (avoiding delays with comms/central processing)
- ability to use lower cost network (on demand ISDN rather than a permanently on-line private network)

all of which are obviously of benefit to the Post Office (directly or indirectly).

Where on-line is needed - eg for on-line authorisation to an external system - the infrastructure supports the concept of a "priority message" which forces an on-line connection.

There is, of course, an upper limit on the number of on-line transactions that could be supported on this infrastructure - *if*, for instance, we mandated that *every* transaction, including stamp sales, had to be performed on-line, the infrastructure in its current form would not be able to cope - and would need to be replaced by a (potentially considerably more costly) permanently on-line system, with all the problems of availability and performance that would bring.

There are two factors to consider when introducing large amounts of on-line traffic to the solution:

- as the amount of traffic increases, the capacity of the central systems (eg incoming communications links, routers and servers) will need to increase; if in-extremis you increased towards 100% on-line, you would require considerable capacity (at considerable expense), potentially reaching a level of on-line transaction processing potentially far exceeding even the biggest financial services systems. We have no evidence to suggest, however, that these systems could not be scaled to support relatively low levels (comparatively) of on-line traffic suggested for Network Banking etc.
- the commercial advantages of using ISDN (low fixed cost, but a charge per call) against a private circuit solution (high fixed cost, no call charges) will obviously diminish as the amount of on-line traffic increases. As the traffic does go up, it may be economically sound to convert certain offices - and noting the massive variation of traffic between offices in the current PONU network, it will only be certain - to a private circuit solution. Pathway currently have an option to use Frame Relay, and one would expect it to be commercially

WITN05970123

attractive to cut those high throughout offices over to this technology should our on-line requirements increase dramatically. Note this is just a change of communications medium - the use of Riposte as the messaging product would not be invalidated.

The key point here is that the "constraint" is the use of a switched network rather than, pre se, the use of Riposte; in Ireland, for instance, where Riposte was first used, An Post have been performing on-line banking transactions for their DNS equivalent using Riposte for some years - although this was originally over X.25 rather than ISDN.

E2. "The solutions isn't relevant now that BA have gone"

There is another common misconception that the solution was heavily focused towards the BA requirements for the Benefit Payment Service, and that now that requirement has gone, it is no longer relevant.

Although it is true that much of Pathway's application development effort was focused on the BA requirements, perhaps to the detriment of the POCL only applications, the underlying post office infrastructure has not been designed specifically for the BA requirement, and is just as relevant for the POCL now as it was.

The underlying Riposte product, on which much of the solution is based, is indeed sold specifically to the post office marketplace (not the benefit payment sector) and is in use - or being implemented in - a number of post offices worldwide, most of which do not have the UK benefit payment requirement (and indeed, a number of which have heavy banking requirements).

E3. "We wouldn't pick this solution again"

This statement has been made a number of times - that if we were selecting a post office automation technology again and now, we would not choose the same solution - and in particular the same Riposte based solution.

Obviously, without defining what requirements we might have if we were going out for new solution, or understanding the commercial issues at the time, it would be impossible to say what we might or might not choose, however there are many aspects of the current solution which would probably still be of importance to the Post Office - for example:

- low communications cost
- reduced availability on on-line networks
- ease of use/no local management

etc.

For the purpose of this misconception we should draw a clear distinction between the "*technical solution*" and the "*service provider*". If we are to be objective we should be careful to understand what failures have been due to the technology and what are due to the supplier (the integrator). To put this in context, in addition to Escher and the Riposte product, both Energis and Oracle provide major parts of the solution, and indeed are both major suppliers in their own right to The Post Office.

WITN05970123

E4. "It can't talk to outside systems"

This is another misconception that has arisen in recent months as the Post Office considers options for Network Banking. In reality, Horizon already interfaces to a number of Post Office systems - RDS, TIP, HAPS, to the Benefits Agency ESNCS system - and in coming months will link to SAPADS and to a variety of Automated Payments clients. Additionally, prior to the withdrawal of the Benefits Agency, it supported a complex interface, with both batch and more immediate traffic, to the BA's CAPS systems.

The Horizon system was architected - in line with the then Post Office Counters IS Strategy - around the concept of offices connecting back to a central "switch" (the TMS or Transaction Management Service), with links onwards from there to other systems. This arrangement has considerable advantages from the point view of security, control and system management, and indeed mirrors that in use in the financial services industry.

What Horizon is not set up to do is to allow links from individual office terminals directly to a variety of third party systems - in much the same way that (say) a bank ATM will not connect directly to every bank whose card it may handle, but rather connects to the bank's central switch, from where onward communication would take place. The introduction of links directly from individual offices to a variety of external systems would have significant implications for configuration and system management, availability, security, reconciliation etc, and ought not to be entered into lightly.

E5. "Delays were due to problems with the technology"

The various reviews that have been performed on the project, both internally and externally[10], have supported the view that the major delays on the programme were not due, per se, to any problems with the underlying technology, but were rather due to the supplier's approach and underestimation of the complexity of the requirement (linked to the specification of that requirement).

This is not to say that Pathway have not found the use of the specific technology challenging, and that it has not been without problems, but we have little evidence to support the view that the primary cause of slippage or overrun has been down to the underlying technology.

[10] Eg. HM Treasury Independent Panel report July 1998, stated that "the programme is technically viable".