WITN05970113

Bringing Technology to Post Offices and Benefit Payments

THE LEVEL OF INFORMATION NEEDED FOR TECHNICAL ASSURANCE - A DISCUSSION PAPER

Author: Jeremy Folkes
Authority: John Meagher
Reference: jf/21taleve.doc

Version: Issue 1.0
23nd July 1997

Contents Page

1. PURPOSE

1.1. This paper explores the issue of the "level" of visibility and information required for Technical Assurance. It is intended to promote discussion with a view to achieving rapid agreement on the correct level both within the BA/POCL PDA and with the various "suppliers".

WITN05970113

1.2. Although the paper majors on Technical Assurance, in it intended that many of the principles will be applicable to Assurance in general, including specifically the Business and Security areas within the remit of the PDA Service Development Group.

1.3. Whilst the primary supplier to the PDA is seen to be ICL Pathway (and through them, their subcontractors), there are a number of groups within both sponsor organisations which are responsible for deliverables which contribute to the success of the overall BA/POCL programme. It is therefore the intention that this paper will facilitate the achievement of a common level for information for assurance across all suppliers.

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

2. REFERENCES

The following documents are relevant to the area under discussion

[TA] - "*The Role of Technical Assurance in the PDA*"*]* - Michael Berg.

[InfoNeed] - "*Information Needs*" - Richard Hill

[UPTS] - "*Understanding Pathway's Technical Solution - Why do we need to understand Pathway's technical solution*" - Richard Hill 14th May 1997.

[SolnCon] - "*Key Solution Control Product Descriptions*" (Attachment to Andersen's paper on Solution Control).

3. BACKGROUND

The PDA Programme Management Team has recently ratified the need for Technical Assurance of the emerging Pathway solution, and a revitalised Technical Assurance function now exists, alongside assurance activities for Security and User/Business viewpoints, within the PDA's Service Development Group. This need for Technical Assurance is discussed in [TA].

A significant amount of work has already been performed within the PDA's former Design Assurance function to pull together the "information needs" of the PDA as a whole, and this has included input from a variety of sources. These needs, intentionally focused on information rather than documentation (the grouping and packaging of a sets of information into documents being less fundamental than the information itself), have been communicated to ICL Pathway [InfoNeed].

WITN05970113

4. THE NEED FOR (TECHNICAL) ASSURANCE

The PDA's need for assurance has been well discussed and documented elsewhere, and it is not intended to recite the full argument again within this paper. However, it may be useful to consider some of the key reasons for assurance:

- to minimise of risk to sponsors - major significant business/political risk are still owned by the Contracting Authorities, and contractual remedies are not sufficient to mitigate the effects of failure of the Pathway service.
- to ensure compatibility between various suppliers' solutions - the "end to end solution" includes services provided by both Pathway and a variety of other organisations - CAPS, TIP, RDP etc. Pathway are responsible to delivering to specified interfaces within the overall end-to-end solution; assurance is needed to have confidence that the pieces of the jigsaw will fit together.
- to control solution drift[1] - in addition to avoiding the risk of failure to meet the Requirements, there is a need to ensure that the supplier selection is no left open to challenge due to drift outside the scope of the procurement and/or evaluation.
- to enable "acceptance" - a number of requirements (including the so-called Non Functional Requirements (NFRs)), relate to attributes of the service rather than business functionality. Some of these can only be accepted through having a thorough understanding of the solution - an example would be requirements relating to scalability of the solution, which cannot be "proven" at Release 1 but may be accepted through the presentation of suitable models etc.
- to inform the Release Authorisation Process - we need to have an adequate understanding of the solution to be able to make an informed decision on the fitness of a Release (eg in analysing the impact of a fault, or determining the completeness of scope of testing).

5. INFORMATION AND DOCUMENTATION

In considering the level of information needed for assurance, it is useful to be aware of just what documentation is in existence or is planned to be created.

5.1. Information vs Documentation

It is important to realise that, for assurance purposes, we primarily need access to *information*, and the packaging of that information into specific *documents* is only of secondary interest (mostly for control purposes - to ensure the stability of and to provide an audit trail for information received).

[1] A separate paper is under production looking at Solution Definition and Solution Drift.

WITN05970113

5.2. The Contract

The primary documentation is that which actually forms the contract; at the technical level this is primarily the Solution Catalogue (Schedule A16), representing Pathway's response to the Requirements Catalogue (Schedule A15).

Although the level of detail does vary considerably - in some areas it just echoes back the Requirement, in others it drills into some detail of the actual solution - this document is, in reality, of little use for assurance, except as a control against which to measure solution drift.

5.3. Documentation Required by the Contract

5.3.1. The contract requires the delivery by Pathway of certain documents at various stages within the lifecycle of the project; perhaps the best known of these is the Service Architecture Definition Document (which has evolved from the Functional Specification), however there are a number of other documents which will eventually be required to satisfy specific requirements.

5.3.2. These documents, if delivered within in the right timeframe, will support the assurance process, and indeed might provide the majority of the information required for assurance in a specific area, but assurance is not their main function - each one was originally required for a specific purpose (eg related to separability, development of new services etc).

5.3.3. Prime examples of this type of controlled document exist within Requirement 469 and 470, which require the delivery of "*OPS Technical Documentation*" and "*TMS Technical Documentation*", with the criteria that these have to "*suitable to allow POCL to procure applications which utilise OPS/TMS*". Within their solution for R470 Pathway committed to provide *"The TMS Architecture Document"*, *"The TMS API Document"* and *"TMS Hardware Specification"*. The TMS Architecture document, for instance, "*describes the overall systems architecture of TMS and the functionality of its various software sub-systems . This includes a description of the Agents which describes how Client systems utilise the TMS".*

5.3.4. If these documents do actually go to the detail to meet the criteria of "*suitable to allow POCL to procure applications which utilise OPS/TMS*", then the are likely to provide much useful information needed for assurance - it would be difficult to see how one could procure applications without detailed information.

5.3.5. Unfortunately, many of these documents have yet to be delivered, and it appears that Pathway are under no obligation to deliver them prior to the time they are needed for formal acceptance of the relevant Requirements - presumably immediately prior to acceptance at Release 1e - too late for any assurance of Release 1c and 1e.

WITN05970113

DN: Is there a common process in place for the PDA to extract all of the contracted documentation from Pathway, or is this currently down to each "Requirement Owner". When are we expected to get these documents?

5.3.6. Note that however useful these documents may be, the coverage of the solution provided by them is unlikely to be universal, given the way in which they were originally specified. However, they may form a useful baseline on which to hang the needs for assurance.

5.3.7. Early delivery of these documents would provide much needed visibility of the solution for assurance/release authorisation, and there would also seem to be advantages for ICL Pathway in reducing the risk of problems with acceptance of the related Requirements.

5.3.8. It is recommended that the PDA should explore with ICL Pathway the timetable for the provision of this documentation, with a view to obtaining it now rather than waiting until Acceptance. Although this may seem to be unwelcome extra work for ICL Pathway at this stage, this may be outweighed by the risk-reduction advantages.

5.4. Documentation Proposed for Acceptance

5.4.1. In addition to the documentation explicitly required by the contract as above, Pathway have themselves proposed a number of additional documents[2] - *Documentary Evidence* - which they would present as a means of achieving acceptance of specific Acceptance Criteria, through the mechanism of Acceptance Review.

5.4.2. By their nature, these documents may need to go to into considerable detail - although the exact level may be a matter of debate at the time of production, and could be contentious at the time of acceptance. They will need to provide sufficient evidence to allow the Contracting Authorities to formally accept the requirement that they are supporting.

DN: Not for this document, but how do we handle the question of level in these Acceptance Documents - is the onus on Pathway to satisfy us, or on us to be satisfied?

5.4.3. However, as with controlled documents required by the contract, these documents may not necessarily be produced until they are needed for their primary purposes of acceptance at Release 1e - too late for any assurance of Release 1c and 1e.

[2] These documents are proposed in the twenty or so Acceptance Specifications currently under review between Pathway and the PDA.

WITN05970113

5.4.4. Again, these documents, although providing useful information, are unlikely to give full coverage of the solution (they are, after all, based upon satisfying aspects of the requirements).

5.5. Other Documents

We are in receipt of other documents which apparently have no contractual status, but which are supplied for '*historical reasons*' by Pathway - probably the best example being the TED, or Technical Environment Description[3]. This is quite detailed in some areas (sometimes well beyond what we would need - eg down to detailed specifications of equipment), this being a feature of its prime purpose, which is not for assurance.

5.6. Shortcomings of the Documentation Set

Unfortunately, the current documentation set currently available to the PDA, even if supplemented by the Controlled Documents required to be delivered by Acceptance, and further documentary evidence likely to be obtained to satisfy specific acceptance criteria, is unlikely to be sufficient for the needs of assurance.

6. THE QUESTION OF LEVEL

6.1. Difficulty in Specifying Level

6.1.1. The question of the *level* of visibility and of information is notoriously difficult to answer, not just within the confines of the unique environment of the PDA but in systems development generally.

6.1.2. It would be naive to assume that, with a procurement of this complexity and a solution of this size that we could easily specify that "We need an XYZ document". If we attempt to specify a level in a simple form of words - eg "High Level Design" we may appear to give a level, however in reality the term "High Level Design" would mean many different things to different people.

6.1.3. So we need to find a way through which we can set some ground rules for level without getting bogged down in terminology.

6.2. Minimum Level

6.2.1. Whilst it may be difficult to specify a required level for assurance, we can specify a "minimum" level based upon the highest in any area of:

[3] Although it seems likely that many of these informal documents will form input to controlled documents required by the contract, or will be used as documentary evidence for Acceptance.

WITN05970113

- the level of documentation used in the selection/tender process - it would be patently absurd to attempt to assure at a higher level than that at which we evaluated Pathway

- the level of controlled documentation required by the contract - if our assurance was at a higher level than the documentation that Pathway have to delivery to us at the time of acceptance, we run the risk of finding problems immediately prior to acceptance [but note that the level of this documentation varies widely]

- the level of documentary evidence proposed to facilitate acceptance - again, it would appear unworkable to expect us - in general - to accept based on evidence of a lower level than that which had been supplied for assurance.

6.2.2. In summary, this minimum could be defined as that to ensure "no surprises" for acceptance. This would appear to be mutually beneficial risk reduction approach for both ICL Pathway and the PDA.

6.2.3. The important point here is the timing of information - Pathway have every incentive to give us what we need to pass acceptance, but little to provide information in advance of then. On one hand we are having difficulty in getting information, on the other we know they have to provide (some of) it for acceptance.

6.2.4. However, inspection of the minimum level reveals that it is unlikely to be sufficient for assurance - the documentation by nature tends to concentrate on the service boundaries and interfaces (internal and external) within the Pathway service. For instance, it would appear to give very little information on the manner in which BPS actually operates, especially the complex processing within the POCL domain.

6.3. The Dynamic Nature of Level

In many respects a precise definition of level is neither possible nor desirable, as it will provide an environment which is far too rigid to be useful, with an inability to focus on the legitimate areas of risk and a danger in being swamped by unnecessary information.

The depth to which the assurance activity needs to explore will, by nature, be fairly dynamic, depending on a combination of two major factors:

- the business risk of a particular area "not working" (eg sponsor business risk should the ICL Pathway coffee machine fail is low, but should the ability to maintain time synchronisation fail the risk may be high)

- the perceived technical risks in this area (eg certain well known, tried and tested products may be "low risk", whereas a totally bespoke component providing a mission critical function may be "high risk").

WITN05970113

It should be noted, however, that the perception of risk - and therefore the level of information required for assurance in a particular area - may be subject to modification over time; it will evolve either as a result of experience (eg a period of live running may have an effect either way, depending on the results) or of what is found during the assurance activity itself.

An example of the latter category would be say where the performance of a particular business function was being addressed. High level information provided by a supplier, eg that detailed modelling has been performed, may provide sufficient confidence to avoid the need for further information; the corollary is that if there is no evidence of modelling then the assurance activity may force the need for a greater level of detail.

The exact level required for any particular area is best left to the professional judgement of the assurance teams, reflecting their experience and knowledge, and the outcome of the assurance activities. This is in fact the approach suggested by Pathway in some areas of testing, where they have a similar problem with specifying depth, and also the approach used to good effect during the demonstrator/evaluation phase of the programme.

7. MEANS OF DEFINING LEVEL

We are therefore faced with the need to find a means of defining a level, against the backdrop of the acknowledged difficulties of so doing; the only concrete thing have can establish is a "minimum" level based on documentation we either have or will receive.

In this situation, two (possibly complementary) approaches exist - to define the level through defining our need, or to define the level in terms of existing documents.

7.1. Defining Level by Need

7.1.1. One approach to the definition of level is to base it purely on the "need" - in particular around a set of key characteristics to be assured, including for instance:

(a) confidentiality, integrity, availability (the traditional CIA security model)

(b) performance

(c) resilience

[This list is not intended to exhaustive - there are other dimensions, such as migration and contingency which also need to be considered].

7.1.2. However, there is also a need to have confidence that the service, at the basic level, "works" - that the service will operate as desired. This requires general, higher level

WITN05970113

information, not allied to specific key characteristics, in addition to the detail, and therefore it would not be appropriate to limit the coverage to just these specific items.

7.1.3. The need approach gives a useful indication of the scope and depth if considered against the provision of assurance on an "end-to-end"[4] basis within the ICL Pathway solution - for this we would need to be able to track the flow, storage and processing of data from its entry to the Pathway domain to its exit. This is likely to require visibility of detailed design documentation (including message flows, file stores etc), at level sufficient to identify individual data items.

7.1.4. A variation on the definition of level through need to it shift the onus on the level from the PDA to ICL Pathway - that ICL Pathway need to provide sufficient information to demonstrate that their solution is "fit for purpose", rather than for the PDA to have to seek out information. This model is similar to that being employed for Acceptance, where Pathway have every incentive to demonstrate, though documentation evidence provided for Acceptance Reviews, that they have complied with the relevant Acceptance Criteria.

7.1.5. It is recognised that Assurance (and Release Authorisation, as one of its drivers) is not given the same coverage in the contract as Acceptance, and that any shift of onus would therefore need to be the subject of negotiation by the PDA with ICL Pathway, presumably at CNT level.

7.1.6. In reality, the issue here is one of timing - assurance is an ongoing activity, with one of its purposes being to inform the Release Authorisation process. With the revised, multiple release, implementation approach, we are likely to have at least two releases to authorise (1c and 1e) before Acceptance (at the end of the trial of 1e). Information at the right level is needed now to inform Release Authorisation; although Pathway may not wish to provide this now, they are contractually committed to provide information[5] of a *broadly similar* nature and level for Acceptance.

7.2. Defining Level by Analogy to Existing Documents

7.2.1. Another approach is to define a *typical* level by analogy to existing Pathway documentation of which we have had either formal or informal visibility, whilst noting that the level required for assurance is going to be dynamic, as discussed earlier.

7.2.2. The obvious advantage of this method is that it turns otherwise abstract concepts into something concrete for discussion; there are also issues of practicality in that if we pitch our initial information needs at the level of existing documentation which could, subject to commercial negotiation, be provided to us, this is likely to be seen

[4] Note this is restricted to "end to end" within the Pathway solution, as opposed to the higher level/wider scope "end to end" of the emerging Solution Control function.
[5] Recognising of course that acceptance and authorisation (and assurance) are different activities, and the spread of level of documentation required within the Acceptance Criteria is wide.

WITN05970113

as less of a threat (in terms of effort/timescales) to ICL Pathway than if we are seen to be requiring a whole new set of documentation.

7.2.3. Note that here we are trying to suggest a *level* through comparison with existing documents; we are not suggesting that *scope* of these actual documents is sufficient - although we have seen a fairly wide variety of documents, they do not in any way provide full coverage of the solution.

7.2.4. Candidate documents for this exercise would include such as the "High Level Design" (HLDs) for each of the sub-systems, the emerging message definitions for BES, and the like, however without a full understanding of the documentation set that Pathway have planned (or are planning, as part of their recent review activities), it is difficult to make much practical use of this approach.

8. CONCLUSION

This paper has explained some of the difficulties with specifying a level for the information required for assurance, however it has suggested that as an absolute minimum we need that level achieved during the selection process, together with that due to be delivered to us for acceptance, either as part of a controlled document or as documentary evidence.

It is suggested that the only sensible approach is to define the level through *the need to assure* the high level characteristics (for example, but without limitation security, performance, resilience etc) and the fitness for purpose of the service.

However, this approach in itself is unlikely to be successful unless some incentive is put on ICL Pathway to provide information of an adequate level to allow informed assurance to take place - for instance to allow Release Authorisation to take place. This model is far closer to that proposed for Acceptance, effectively mirroring, albeit in an informal way, the provision of "documentary evidence" for Acceptance Review.