WITN04600223

Document Title: Audit Data Retrieval Requirements

Document Type: Requirements Specification

Abstract: This document presents the detailed retrieval requirements of the Horizon Audit Community for audit data collected and stored by the Horizon system. It provides further detail to support the general data retrieval requirements established in Requirements 697, 699 and 942.

Status: Draft

Distribution:

Martyn Bennett
Michelle Myles
Peter Sewell
Richard Laking
Library
Stephan Robson
Richard Laking
Harvey Potts

Author: Jan Holmes

Comments to: Jan Holmes

Comments by:

© 1999 ICL Pathway Ltd

WITN04600223
WITN04600223

0 Document control

0.1 Document history

Version	Date	Reason
0.1	16/03/98	Initial draft.
0.2	20/03/98	Addition of storage and retrieval & analysis section. Introduction of ATFS xrefs.
0.3	23/03/98	Following comments from JCCD, Ad'A
0.4	20/07/98	Inclusion of scenario information from BA Audit and POCL Audit. Also comments received from G. Lloyd.
0.5	14/12/98	Update following comments received from GR (BA Audit).
1.0	23/11/99	Raised to v1.0 to enter into PVCS Workset. No textual change

0.2 Approval authorities

Name	Position	Signature	Date
M. Bennett	Director Quality & Risk		
J. Dicks	Director Customer Requirements		
T. Austin	Director Systems		

0.3 Associated documents

Reference	Vers	Date	Title	Source
CR/FSP/006	2.2	08/09/97	Audit Trail Functional Specification	
RS/FSP/001	3.0	11/12/97	Security Functional Specification	
IA/REQ/001	0.4	16/03/98	Pathway Internal Audit Requirements	
			Contract Schedule AB04 -	

WITN04600223

Contract Schedule DA15 - Requirements

Contract Schedule PA15 - Requirements

WITN04600223

0.5 Abbreviations

AS	Audit Server
ATFS	Audit Trail Functional Specification
AW	Audit Workstation
BA	Benefit Agency
CMS	Card Management System
ESNS	Electronic Stop Notice System
LUI	Legato User Interface
PAS	Payment Authorisation System
POCL	Post Office Counters Limited
RFI	Request For Information
SFS	Security Function Specification
SMC	Service Management Centre
TED	Technical Environment Description
TMS	Transaction Management System
UT	Use Type - refers to the type of use that audit data might be put to.

WITN04600223

0.6 Table of content

WITN04600223
WITN04600223

WITN04600223
WITN04600223

1 Introduction

Business and security audit requirements for Horizon are established in the Audit Trail Functional Specification (ATFS) and the Security Functional Specification (SFS) respectively. Between them these documents form an agreed interpretation of the core requirements from Schedules AB04, DA15 and PA15 - Requirements Catalogue.

The architecture for the 'audit solution' is defined in the Audit Architecture (AA) and this identifies some basic data retrieval requirements for the data being captured and stored to form the basis of the audit solution.

This document expands further on those retrieval requirements and provides a detailed breakdown of the anticipated use of audit data by BA, POCL and Pathway Internal Audit, and frequency and expected turnaround times of requests for audit data to be provided by Pathway to BA and/or POCL Internal Audit.

WITN04600223

2 Scope

2.1 Audit Organisations

[ATFS para 1.2.3]

This document addresses the retrieval requirements for a specific audit organisations, namely the Horizon Audit Community, which consists the following :

a. Pathway Internal Audit.

b. POCL Internal Audit who undertake the POCL Auditor and POCL Emergency Manager/Audit role and through whom the POCL <C> Auditor role is exercised.

c. BA Internal Audit who undertake the DSS Auditor role and through whom the NAO Auditor role is exercised.

2.2 Current Inclusions

[ATFS para 2.1.2][ATFS para 2.2.2]

This document takes into account the contractual requirements for audit access to audit tracks as expressed in the ATFS para 2.1.2 - Audit Access to the POCL SIS Track and para 2.2.2 - Audit Access to the DSS Track.

2.3 Current Exclusions

[ATFS para 2.3.2]

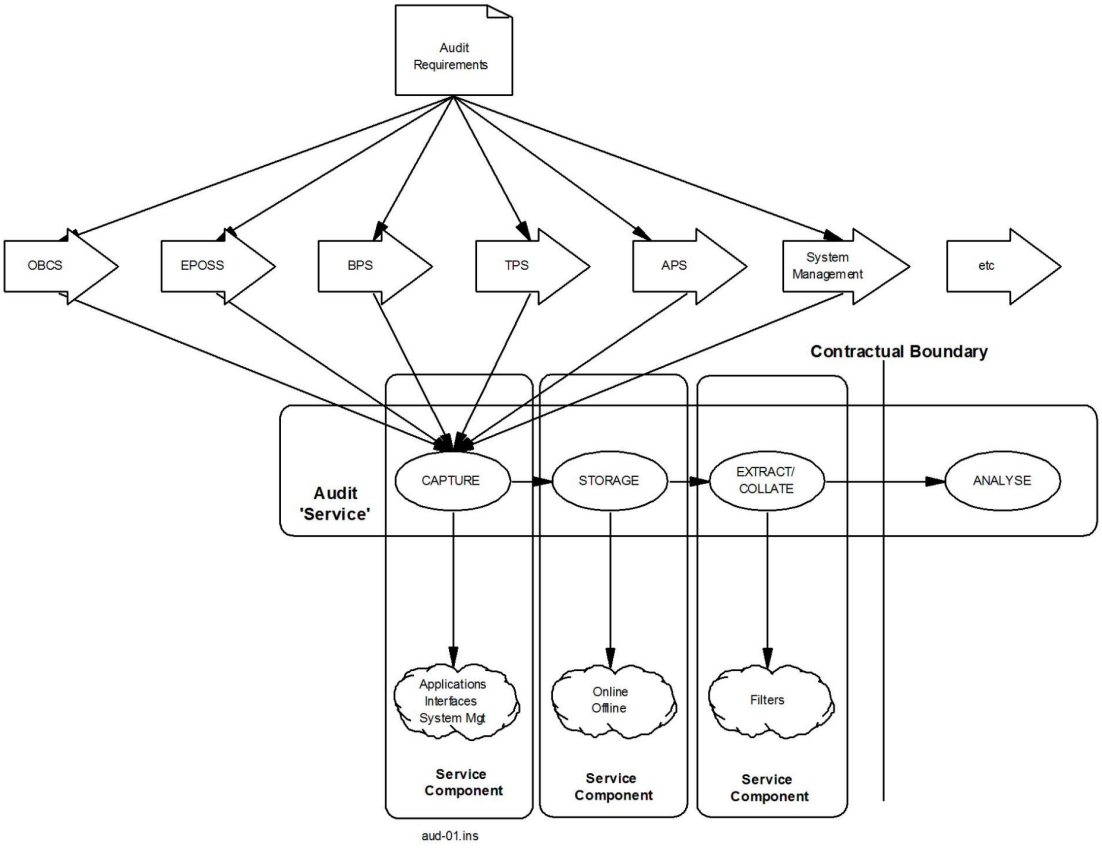
This document does not cover (yet) the retrieval requirements for system management data harvested through Tivoli. Thus the requirements expressed in the ATFS para 2.3.2 - Audit Access to the System Management Track are not dealt with here.

The identification, harvesting and management of Security Events is not covered by this document.

WITN04600223

3 Audit System Schematic

At its simplest the Horizon Audit Solution can be represented by the following logical diagram.



This identifies four key elements :

a. Data Capture.

This is the phase where the data identified in the ATFS and AA are captured by the various applications and utilities that comprise the Horizon solution.

b. Data Storage

This is the phase where the data are stored, either online or off-line, for a period of time defined in the ATFS. The method, sequence and timing of the storage activity are all essentially driven by the subsequent use of the data identified in this document.

c. Data Extraction and Collation

This is the phase where the data is accessed by Pathway personnel in order to extract elements of it for subsequent despatch to BA or POCL Internal Auditors. The data may also be used by Pathway personnel during regular System Audits or during Investigations.

WITN04600223

d. Data Analysis

This is the final phase and is carried out within the BA or POCL domain using data provides from the Extraction and Collation phase. It is outside the contractual boundary and as such Pathway has no responsibility for its conduct. It is shown here primarily to complete the audit solution but also as an acknowledgement that Pathway Internal Audit will itself carry out analysis activities of audit data.

WITN04600223
WITN04600223

4 Approach to Defining Retrieval Requirements

[ATFS all]

The purpose of defining retrieval requirements is to inform the archiving process as to how data will be requested by BA, POCL and/or Pathway Internal Audit in the future and under what circumstances.

The base requirements are established in the ATFS and while this identifies the contractual obligations it does not establish the detailed working requirements. To arrive at these, discussions have been held with POCL and BA Audit Managers to understand precisely :

a. What they want the information for.

b. When and how often they expect to ask for it.

c. How quickly they expect to receive the information once requested.

d. Selection criteria that they expect to be able to use.

e. How they expect the information to be presented to them.

This specification presents the results of those discussions along with any specifically identified by Pathway's own Internal Audit function.

WITN04600223
WITN04600223

5 Use of Audit Data

The ATFS and AA use the term 'audit data' to cover any data that is being retained by Horizon to satisfy contractual requirements. Although there may be a significant number of organisations and departments requiring access to the collected data its use by the Audit Community is limited to three Use Types (UTs) :

a. Use Type 1 : Proving Integrity of Processing.

b. Use Type 2 : Investigation Support.

c. Use Type 3 : Bulk Extraction.

5.1 Proving Integrity of Processing (UT1)

To prove the integrity of a process during a regular System Audit. This will use data that is available on the day(s) that the audit takes place and establishes no special requirements for collection, storage or retrieval. Audits of this type are likely to be run or led by Pathway Internal Audit.

5.2 Investigation Support (UT2)

To provide information to support investigations or help resolve operational problems. 'Investigations' is used in its broadest sense and does not limit itself to fraud. Any Request For Information (RFI) is likely to be associated with a specific business event, eg. An encashment, a card authorisation, an outlet, a beneficiary. It is anticipated that the majority of this type will be based on the TMS Journal, or will use it as a start point.

5.3 Bulk Extraction (UT3)

[ATFS para 2.1.2.6.2]

To provide historical 'chunks' of information for further analysis by POCL or BA at their convenience. RFIs for this type are likely to have broader time scope, eg. All encashments for this outlet between these dates. It is anticipated that the majority of this type will be based on the TMS Journal although BA and POCL may also request information from other files (PAS, CMS, ESNS, etc).

WITN04600223

6 Retrieval Frequency

6.1 UT1 - Integrity

Requests for this usage will be influenced by two factors :

a. The planned Internal Audits for the Horizon system.

b. The potential to have to conduct special audits of this type in the event of prolonged failure of the process.

Generally these will be requested on an ad-hoc basis.

6.2 UT2 - Investigation

Difficult to anticipate as retrievals will be on the basis of investigations being conducted. One way to deal with this imprecision is to streamline and automate the process from RFI to delivery as far as possible.

6.3 UT3 - Bulk

BA and POCL's expectation is that between 6 and 10 RFIs each would be made for bulk extraction during the year. Other requests would be for copies of PAS/CMS/ESNS files held.

WITN04600223
WITN04600223

7 Turnaround Times

7.1 UT1 - Integrity

Essentially this usage is to prove the integrity of processing. Thus examples of known inputs will be required along with the corresponding expected outputs, and any major transformations shall have to be demonstrated to have worked correctly. As long as the extraction can be turned around during the audit this will be considered acceptable.

7.2 UT2 - Investigation

48 hours was felt to be generally acceptable. Normal access mode will be via the archive tapes or read-only access to the live Oracle tables.

7.3 UT3 - Bulk

BA suggested 3 to 4 months as their audit plan is agreed at the beginning of the year although they anticipate some clarification nearer the start of each audit. POCL would also be based on a plan although their notice period would be shorter. However, between 1 and 2 weeks from RFI to delivery of bulk extract was considered acceptable. Normal access mode will be via the archive tapes.

7.4 Emergency Option

[ATFS para 2.1.2.2][ATFS para 2.1.2.6.2]

These turnaround times carry an underlying caveat that there should be an emergency option whereby direct access to the Correspondence Server can be achieved from the dedicated Audit Extraction Workstation at Wigan or Feltham.

WITN04600223

8 Selection Criteria and Data Sources

8.1 UT1 - Integrity

Driven by the system audit being carried out and limited to proving processing integrity of that part of the system.

Whatever files are available to substantiate or prove the processing integrity will be used.

8.2 UT2 - Investigation

These RFIs are most likely during 'investigations', be they for fraud, audit or problem resolution. As such they are going to be targeting a specific business event or linked events. In many respects they will use the same selection criteria as UT3 but with a much narrower spread of dates.

8.3 UT3 - Bulk

These will be bulk extracts with the selection criteria being generally date delimited. The selection criteria will be driven by the archiving storage index mechanism.

WITN04600223

9 Indexing Options

9.1 TMS Journal

Assuming that the 'Day1 Archive' approach proposed in the Audit Architecture is adopted, and based on the way that Riposte updates the Correspondence Server from the Counters, the Archive Index is expected to be :

<Date>	{Based on Day1 Archive}
<Time>	{Based on periodic capture by CS}
<Outlet>	{Riposte then captures by Outlet}
<Activity>	{Random depending on Counter activity}

Thus organisations and departments requiring TMS based enquiries will be expected to word their RFIs in the following way :

Between <this date> and <that date>

and for <this outlet> or <all outlets> or <this group of outlets>

tell me about this <event>.

Clearly the broader the range between <this date> and <that date> the larger the extraction is likely to be. Additionally the greater the degree of criteria combination the more likely the impact on performance.

9.2 Other Files

The assumption is that the primary Archive Index will be <Date><Time>.

WITN04600223

10 Audit Data Exclusivity

10.1 Principle

[ATFS para 1.2.2]

The ATFS establishes the contractual position vis Principals, Agents, Mixed Data and Rights of Access to audit data. Although no mention of specific mechanisms is made in the ATFS, apart from in the context of Tivoli and the System Management track, the practicalities of satisfying this requirement means that a filtering mechanism will have to be introduced to ensure that neither POCL, POCL <C>, NAO nor BA sees data that they should not.

From POCL and BA's perspective this general rule may be overridden where one or both organisations agree that the other can act as their agent.

10.2 Access Matrix

	POCL SIS Audit Track	**DSS Client Audit Track**	**System Management Track**
DSS Use/View [ATFS para 1.2.4]	Benefit and card related parts of the TMS journal	Full	Full
POCL Use/View [ATFS para 1.2.5]	Full	POCL calls to PAS Help Desk	Full
POCL <C> Use/View [ATFS para 1.2.6]	POCL <C> parts only	Nil	Nil
NAO Use/View [ATFS para 1.2.7]	Benefit and card related parts of the TMS journal	Full	Full

The filtering should be applied only when necessary suggesting that the time to do this is at retrieval and not storage. This will require a definitive statement from POCL and BA of which elements of the audit data is exclusive to each party and what is not. A statement is also required with regard to the other organisations identified in the ATFS. Only then can appropriate filters be made available to the retrieval mechanism.

WITN04600223
WITN04600223

11 Data Storage Options

The archived data must be written on the selected medium (DLT) so that subsequent retrievals can be carried out as effectively as possible and the resultant archive tapes are secure. There appear to be two options, by source stream or by date.

11.1 By Source Stream

Files from a single source are archived on a single tape with each days file(s) being added to the current DLT. This results in a single contiguous collection of files from a single source, for example the TMS Journal or ESNS Control Notice Files.

11.1.1 Retrieval Issues

This approach is beneficial if an RFI results in information being retrieved from a single source.

11.1.2 Security Issues

Archiving by source stream could result in archive tapes being held on campus until such time as the tape is full. For low volume streams, eg ESNS Control Notice Files, this could be days, possibly weeks.

11.2 By Date

Files from all sources are collected and written on as many DLTs as are required to accommodate a single day's archive.

11.2.1 Retrieval Issues

This approach is beneficial if an RFI results in information being retrieved from a variety of sources for a single day. However, bulk extraction RFIs with a broad range between <Start Date> and <End Date> could require a large number of archive tapes to be loaded to satisfy the RFI.

11.2.2 Security Issues

Archiving by date will ensure that the archive tape(s) is(are) available for securing off-campus at the earliest opportunity.

11.3 R1c RFI Experience

To date there has been limited experience of RFIs from POCL or BA Auditors. The current Post Implementation Review has resulted in five RFIs, all of which have a <Start Date> to <End Date> primary key running against the TMS Journal with the following spreads :

a. Extraction 1 : <22/12/97> to <30/01/98>.

WITN04600223

b. Extraction 2 : <R1c start date> to <extraction date>.

c. Extraction 3 : <22/12/97> to <30/01/98>.

d. Extraction 4 : <17/11/97> to <30/01/98>.

e. Extraction 5 : <22/12/97> to <30/01/98>.

WITN04600223

12 Extraction Scenarios

Both POCL and BA Internal Audit have identified, as far as possible, the nature of extraction scenarios that they are likely to request. These are presented below and will be added to as further work is conducted by those groups.

12.1 BA Audit Scenarios

[Note from Les Buckett (DISA) to Jan Holmes]

"….. the 80-95% of data extractions are therefore likely to be either :-

(1) time and case history driven

ie. Between <start date> and <end date> tell me all about "these cases"

However, it is the definition of "these cases" which is a little more difficult to define as the criteria for this may involve :-

- selected NINOs
- selected DSS Agencies (eg. War Pensions, Northern Ireland)
- selected Benefit Types (eg. ChB, IS, JSA)
- selected PO outlets

An example of a typical scenarios may therefore be :-

Between <start date> and <end date>

and for <these NINOs> or for all <Benefit Type Customers> dealt with at <these outlets>

show all audit events related to them as a chronological trail.

Taking a card issue as an example; this would demonstrate when the CAPS notification was received by Pathway, when De LA Rue were asked to produce the card and PUN, when they actually produced and despatched it, when the Customer came into the Office and collected it, and which PO clerk was involved.

(2) time and transaction driven

ie. Between <start date> and <end date> tell me all about "these transactions"

"these transactions" being related to business events. This, however, would again involve :-

- selected NINOs
- selected DSS Agencies
- selected Benefit Types
- selected PO outlets

An example of a typical scenario may therefore be :-

WITN04600223

Between <start date> and <end date>

and for <these NINOs> or for these <Executive Agencies> dealt with at <these outlets>

show all instances of <payments made>

Conclusion

The solution required will need to be flexible enough to allow a variety of input parameters to be supplied. ie rather than having to specify <events> up front it would be preferred to have the facility to enter any <event> of interest as the need arises.

12.2 POCL Audit Scenarios

[Letter from Hilary Stewart to Jan Holmes ref 98t307/00 dated 15th July 1998]

"The following outlines some of the typical data extractions which may be required by POCL audit functions from the Horizon system :-

Typical Events

Below is a list of some of the more typical events that we consider would be used to filter data from the Audit Archive server :

- Outlets
- NINO
- Clerk ID
- Date <between X and Y>
- Time <between X and Y>
- Transaction/Encashment ID <Receipt Number>
- Client ID (in relation to EPOSS clients etc.)
- Encashment/Transaction value

Extraction Types

We consider at this stage it will be impossible to outline all of the potential combinations that may be required for extraction. However, as previously discussed, as requests are made a catalogue of the more common request will be developed. We also assume that there is no time limit to the number of files that can be applied to each extraction.

Simple

example - Between <Date X> and <Date Y>
and for <Outlet Z>
show all instances of transactions on NINO 123>

Complex

example - Between <Date X> and <Date Y>
for <all outlets>

WITN04600223

show instances of <encashments values > £n>
for customer ID <NINO>"