FUJ00001945

Document Title: Audit Trail Functional Specification

Document Type: Functional Requirements Specification

Release: S80

Abstract: This document provides a specification of the Operational and Commercial Audit Trails.

Document Status: APPROVED

Originator & Dept: Jan Holmes (Programme Assurance)

Contributors: J. C. C. Dicks (Customer Requirements)

Internal Distribution: Post Office Account Document Management
S. Probert (RASD) A. Holmes (Development)
W. Mitchell (CS Security)

External Distribution: G. Potts (POL IA)

Approval Authorities: (*See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
T. Drahota (FS POA)	Joint Architecture Forum		
M. Wells (POL)	Joint Architecture Forum		

FUJ00001945

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
1.0	17/9/96	Externally published	N/A
1.1	8/10/96	Revised for BA Audit and Pathway comments	N/A
1.2	31/1/97	Revised for POCL comments and for review towards a definitive version 2.0.	N/A
2.0	19/2/97	Revised for further comments. Definitive	N/A
2.1	19/5/97	Revised for further comments from DSS, alignment with *Access Control Policy* Version 1.0, and for review towards a further definitive version 3.0	N/A
2.2	8/9/97	Revised in response to implementation questions and further comments from DSS/POCL. Further review towards a further definitive version 3.0	N/A
2.3	20/10/97	Revised for comments received during Acceptance Specification discussions and implementation progress	N/A
2.4	5/2/99	Revised to extend definition to Commercial Audit Trail and to address Horizon comments dated 1/12/98.	N/A
2.5	9/3/99	Further comments received 23/2/99	N/A
2.6	9/4/99	Changes agreed at Acceptance Review 30/3/99	N/A
2.7	26/4/99	Changes agreed at post Acceptance Review Audit Panel meeting 22/4/99	N/A
2.8	09/06/99	Removing references to DSS/BA following their withdrawal from the contract	N/A
2.9	24/06/99	Following comments received from POIA.	N/A
3.0	01/07/99	Raised to definitive. 3	CCN 423
3.1	10/11/99	Insertion of previously missing commercial audit trail details following DSS/BA withdrawal from contract	N/A
4.0		Raised to definitive. CCN. No CCN submitted; overtaken by CSR+ definition.	N/A
4.1	10/04/00	Introduction of Logistics Feeder Service (LFS), Change of name – RED :> BIMS	N/A
4.2	21/07/00	Reviewed by Brian Mooney. Document references updated	N/A
5.0	15/01/01	Raised to Approved	N/A
5.1	25/01/02	Changes to reflect Network Banking, EFTPOS and decommissioning of HAPS	N/A
5.2	12/02/02	Following internal review cycle	N/A
5.3	25/02/02	Following review comments from POL	N/A
6.0	25/02/02	Raised to Approved.	CCN 929

FUJ00001945

6.1	17/07/02	Introduce Centera and increase TMS Journal retention period from 7 years to 15 years	CP3240 CP3268
6.2	12/09/02	Remove references to Centera	
7.0	17/09/02	For Approval.	CCN 1019
7.1	16/12/02	ReduceTMS Journal retention period from 15 years to 7 years and reflect revised Schedules	CCN 1100
7.2	23/01/04	Increase pre-BI3 TMS Journal retention period from 18 months to 7 years and change Pathway references to Post Office Account or Horizon depending on the context	CP 3623 CCN 1122
7.3	09/02/04	Incorporating POA internal comments and for POL review	N/A
7.4	24/05/04	Incorporating POL review comments	N/A
7.5	09/08/04	Final PO review comments. Updated for S60 Release	CP 3507
8.0	18/10/04	For Approval	CCN 1131
8.1	20/10/04	Updated for S70/75 Release	CP 3667 CP 3368
8.2	02/11/04	Following review comments received from POA. Nil from POL.	N/A
9.0	22/11/04	For Approval	CCN 1139
9.1	16/05/05	Updated for S80 Release	CP
9.2	27/05/05	Following review comments from POA and POL.	N/A
9.3	29/06/05	Incorporating final comments from Rod Ismay (POL)	N/A
10.0	29/06/05	For Approval	N/A

0.2 Review Details

Review Comments by :	
Review Comments to :	Jan Holmes

Mandatory Review Authority	Name
Security Design Authority	Steve Probert(*v9.1)(*v9.2)
Security Manager (POA)	Bill Mitchell (*v7.2)(*v8.1)(*v9.1)(*v9.2)
Audit Development	Alan Holmes (*v7.2)(*v9.1)(*v9.2)
Commercial Manager	Hilary Forrest (*v7.2)
S80 Release Manager	Bill Reynolds(*v9.2)
S80 Host Design	Sud Agrawal (*v9.1)(*v9.2)
Post Office Internal Audit	Steve Moakes (*v9.1)
Post Office Internal Audit	Bernadette O'Donnell (*v9.1)
Royal Mail Group Internal Audit	Gary Potts (*v9.1)

FUJ00001945

Post Office Finance	Rod Ismay (*v9.1)
Optional Review / Issued for Information	

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Vers	Date	Title	Source
RS/POL/003			Access Control Policy	PVCS
TD/STD/001			Host Application Database Design and Interface Standards	PVCS
RS/FSP/001			Security Functional Specification	PVCS
IA/MAN/003			Post Office Account Internal Audit Manual	PVCS
IA/MAN/006			Horizon System Audit Manual for BI3	PVCS
			Schedules S1, S3, S10, S15, S18, S19 & S22	POL
CS/SER/016			Service Description for the Security Management Service	PVCS
PA/TEM/001			Fujitsu Services Document Template	PVCS/BMS

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.4 Abbreviations/Definitions

Abbreviation	Definition
ACD	Automated Call Distribution
ADC	Additional Data Capture
ADS	Advanced Distribution Systems
AP	Automated Payment
APS	AP Service
BA	Benefits Agency
BdC	Bureau de Change
BIMS	Business Incident Management System
CCD	Contract Controlled Document
CCN	Change Control Note
CP	Change Proposal
CR	Change Request
CS	Customer Service

FUJ00001945

CT	Commercial Terms
CTSS	Commercial Terms Signature Sheet
CWP	Change Work Packsge
DC	Debit Card
DWP	Department of Works and Pensions
EMV	Europay Mastercard Visa
EPOS	Electronic Point of Sale
EPOSS	EPOSS Service
ESNCS	Electronic Stop Notice Control Service
ETU	Electronic Top-up
HADDIS	Host Application Database Design and Interface Standards
HSAM	Horizon System Audit Manual
IM	Inventory Management
ISDN	Integrated Services Digital Network
LFS	Logistics Feeder Service
NBE	Network Banking Engine
NBS	Network Banking System
NS&I	National Savings and Investments
OAS	OBCS Access Service
OBC	Operational Business Change
OBCS	Order Book Control Service
OPS	Office Platform Service
POA	(Fujitsu Services) Post Office Account
POL	Post Office Limited
RASD	Requirements Architecture and Strategy Design
RD	Reference Data
RWP	Request Work Package
SAP	Systeme, Anwendungen, Produkte in der Datenverarbeitung AG, German software manufacturer
SI	System Integration (Directorate)
SIS	Strategic Infrastructure Service
SLA	Service Level Agreement(s)
TES	Transaction Enquiry Service
TIP	Transaction Information Processing
TMS	Transaction Management Service

FUJ00001945

0.5 Changes in this Version

Version	Changes
10.0	None
9.3	Comments received from Rod Ismay (POL)
9.2	Comments received from POA and POL. Removal of OBCS application stream.
9.1	Inclusion of application streams introduced at Release S80
9.0	No reviewer comments received
8.2	Comments received from Gill Jackson incorporated into this version
8.1	Inclusion of application streams introduced at Release S70/75
8.0	No reviewer comments received
7.5	Inclusion of application streams introduced at Releases S60
7.4	Final updates to incorporate review comments from Post Office (M. Ferlinc)
7.3	Comments received from Alan Holmes incorporated and this version offered to POL for their review.
7.2	Change retention period of pre-BI3 TMS Journal from 18 months to 7 years brought about through CP 3623 and change Pathway references to Post Office Account or Horizon depending on the context. Tony Drahota (POA) and Mike Wells (POL) identified as Approval Authorities on behalf of the Joint Architecture Forum.
7.1	Change data retention period from 15 years to 7. Other changes to reflect the revised Schedule and Clauses of the Extension Amendment.
7.0	G. Potts (POL IA) replaced by J. Hutchinson (POL IA) Approval Authority. No other changes.
6.2	Remove references to Centera and replace with non-specific implementation media
6.1	Introduce EMC Centera as a replacement storage medium to DLT in response to POL data retrieval requirements (CP3240) and extend the retention period of Network Banking audit data from 7 years to 15 in response to POL requirement to retain data for live investigations and/or litigation support (CP3268) under R829
6.0	No changes made.
5.3	POL reviewer's comments.
5.2	Pathway reviewer's comments
5.1	Major additions; Network Banking and EFTPOS. Further changes to reflect the decommissioning of HAPS and directly linked AP Clients. Change name from POCL to POL.
5.0	Approvers changed
4.2	Approvers changed
4.1	Introduction of Logistics Feeder Service details
4.0	No changes made. Version number increased
3.1	Revised schematic for Invoicing procedure
3.0	No changes made. Version number increased
2.9	Minor amendments following feedback from POIA including a revised Commercial Audit Trail section on Invoicing

FUJ00001945

2.8	Major Surgery to remove all references to DSS and/or BA and their associated requirements following the withdrawal of the Benefit Payment Card from Horizon
2.7	Minor addition around caveats section to Commercial Audit Trail
2.6	Changes agreed at the Acceptance Review of 30/3/99 have been incorporated
2.5	Horizon comments dated 23/2/99 have been factored in
2.4	Horizon comments dated 1/12/98 have been factored in
2.3	A general overhaul to reflect agreements made in the course of Acceptance Specification negotiations and during design and development
2.2	PDA comments dated 19 June have been factored in: defining the mainstream operational Services; extending the list of keys
2.1	A further set of comments from POCL and DSS have been addressed. A number of clarifications and corrections have been made
2.0	A further consolidated set of DSS and POCL comments have been addressed
1.2	Two sets of comments from POCL have been addressed. OBCS has been added following the ordering of the service. Inclusion of raw data from CMS/PAS Help Desk ACDs and the CMS Card Production Interface. Inclusion of raw data from Horizon Help Desk ACDs. The requirement texts have been removed pending availability of Version 6 of the agreements (in preparation)
1.1	Clarification of meaning of Pathway native flat formats and removal of immediate dependencies on particular audit authority flat file formats. Correction to process of record deletions

0.6 Changes Expected

Changes
Comment from document reviewers

FUJ00001945

0.7 Table of Contents

FUJ00001945

FUJ00001945

1.0 Introduction

1.1 Auditor's Eye View

1.1.1 Scope

This functional specification defines the *operational* and *commercial* audit trails. These are, respectively, the audit trail associated with the operation of the services which make up the Horizon solution and the audit trail associated with that part of Post Office Account's internal commercial records to which POL's Internal Auditors or Agents may have access as set out in Schedule S3.

The operational audit trail includes that generated by the mainstream operational services and the Business Incident Management System (BIMS).

The mainstream operational services are the services making up the POL steady state applications :

- Automated Payment Service (APS) including Additional Data Capture (ADC)
- EPOS Service (EPOSS) including Debit Card (DC)
- Logistics Feeder Service (LFS)
- Network Banking Service (NBS) including NBX
- National Savings and Investments (NS&I)
- Smart Post
- Bureau de Change (BdC)
- Electronic Top-up (ETU)
- Post Office Limited Financial Systems (POL FS)
- Infrastructure Services
- Transaction Enquiry Service (TES)

The Europay Mastercard Visa (EMV) extensions to NBS and Debit Card, introduced at S70/75, while not being a mainstream operational service in their own right, do generate data that is part of the audit trail.

The BIMS provides an auxiliary audit trail that separately covers the treatment of exceptions encountered within the mainstream operational services. The audit trail associated with the mainstream services is never modified for the purposes of correction as such.

This specification also addresses, in Section 3, certain elements of Schedule3 that relate to access by POL's commercial auditors to parts of Post Office Account's own internal records and systems. These latter requirements are met through the definition and use of a *commercial* audit trial and associated audit procedure providing for access from within Post Office Account.

The TMS Journal element of the operational audit trail, and other operational support and system management elements relating to financial systems, are retained for 7 years. The remainder of the operational audit trail, specifically data relating to APS, OBCS, TIP and LFS is retained for 18 months.

FUJ00001945

Note that although OBCS and TIP are discontinued services at S80 the audit data generated up to the point of rolling out S80 will be retained under existing rules.

The commercial audit trail is retained for seven years although some records are held for the life of the contract, which may be longer than seven years.

If the technology used to hold elements of the audit trail becomes obsolete then they will be copied to the new technology to maintain continuity of access.

1.1.2 The Total Mainstream Horizon Solution

From the standpoint of the auditor, the total mainstream solution, including both the Horizon sub-systems and the source and sink subsystems, is shown in Figure A. The arrows represent the subsystem interfaces at which key auditable events occur. Horizon's responsibilities extend to the subsystems coloured green (dark lozenge) and the interfaces coloured blue (dark arrows).

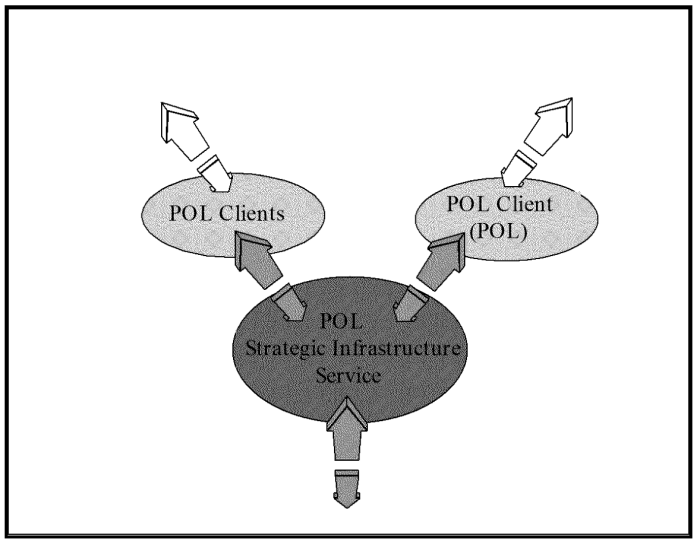


Figure A: Subsystems and principal interfaces

In addition, but not shown, are the Systems Management facilities that Horizon employs in the course of operating the hardware and software and telecommunications platforms themselves.

1.1.3 The Strategic Infrastructure Service

The Strategic Infrastructure Service (SIS) can be analysed as a number of "visible" counter applications to which the post office clerks interface:

- EPOS Service (EPOSS) including Debit Card (DC)
- Automated Payment Service (APS) including Additional Data capture (ADC)
- Logistics Feeder Service (LFS)
- Network Banking Service (NBS) including NBX
- Smart Post
- Bureau de Change (BdC)
- Electronic Top-up (ETU)

FUJ00001945

- National Savings and Investments (NS&I)

Interfaces to POL Financial Systems running on SAP, hosted by Fujitsurunning on an "invisible" middleware messaging transport system:

- Transaction Management Service (TMS)

That is in turn supported by an operating platform distributed across a Wide Area Network containing:

- Instances of the Office Platform Service (OPS) in each outlet
- Central servers

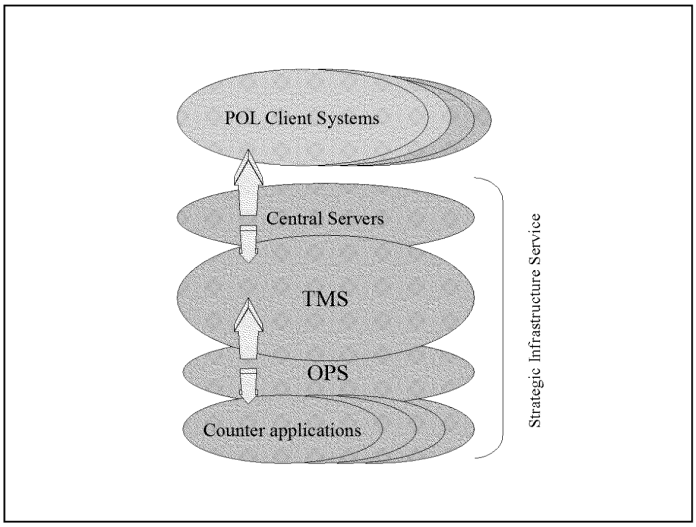


Figure B: Principal components of the Strategic Infrastructure Service

The SIS also contains a telephony interface to callers and interfaces to Systems Management functions (not illustrated).

Figure B shows the SIS components with the same interfaces remapped appropriately.

FUJ00001945

1.1.4 Other POL Clients

Figure D shows the relationship between the SIS and other POL Client systems. These client systems comprise both those that belong to the POL organisation itself and those, which belong to POL's commercial Clients, such as utilities and high street banks.

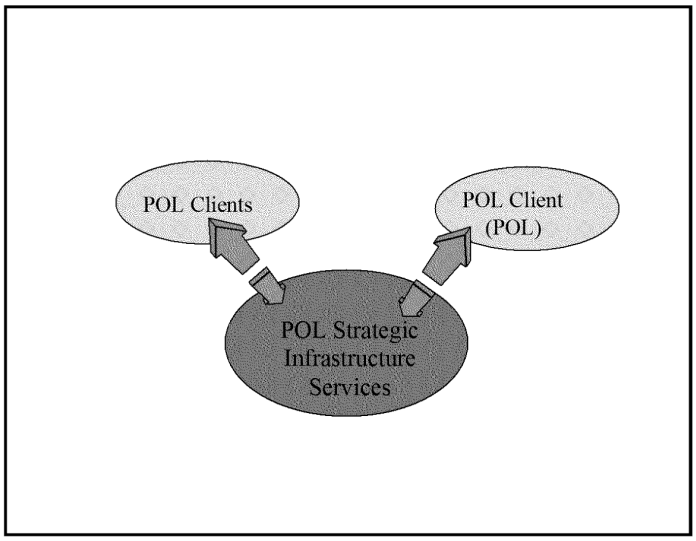


Figure D: Other POL Clients

1.1.4.1 POL In-house Systems

The POL in-house systems that interface to the POL SIS are:

- Reference Data
- SAP Advanced Distribution System (ADS) for Inventory Management (IM)
- Post Office Limited Financial Systems

The stock and cash account files are also produced within each office on paper. These signed paper records will, foreseably, represent the fiduciary record of the outlet's business.

The Reference Data system is responsible for supplying transaction steering data to Horizon. This data describes the relationships and properties of the data to be processed (typing of regions, POL organisations, outlets, Clients, items for sale, methods of payment, and transaction tokens); and the processing methods (processing and validation rules, check digits, calendars, accounting collation sequences, tax tables).

ADS is an on-line system but with a same-day level of response time. It handles orders, secure stock returns, transfers and secure stock inventories, providing for central control interfacing with Horizon's Logistics Feeder Service (LFS)

AP Clients will have direct interfaces to the POL SIS for receiving files of payment records.

FUJ00001945

1.1.4.2 POL Client Systems

This level of specification does not define the audit facilities to be made available to the audit departments of POL's Automated Payment commercial Clients. These facilities will be negotiated between POL and the Client as part of the AP Migration Plan Interface specification for each Client. It has been decided by POL that such Client systems will NOT access the POL SIS directly to provide customer and payment scheme reference data (transaction steering data). Such data will be passed through the POL Reference Data system.

1.2 Audit Trail Responsibilities and Usage

1.2.1 Responsibilities

1.2.1.1 Tracks and Trails

In the description below use is made of the terms *audit track* and *audit trail*. An audit track is a record of activities made within a Horizon subsystem for one or more of its interfaces. An audit trail is one or more such tracks. The data recorded in a trail's several tracks may represent the treatment of related transfers and processing.

In general it is possible to produce an audit track for an interface on either side of that interface, or, if the interface is itself problematic, on both sides.

It is of course a matter for POL and POL Clients to produce their own audit tracks on their sides of the interfaces to Horizon.

1.2.1.2 TWO Tracks

The Horizon audit trail is based upon files representing the single main audit track representing the traffic running through the Horizon solution, the POL SIS. This system is Post Office Account's operational responsibility and its operating interfaces are also under its control.

As discussed above, a second audit track represents the systems management operation of the Horizon system itself.

1.2.2 Principals, Agents And Rights Of Access

The underlying policy for access control is defined in the Access Control Policy – RS/POL/003 (ACP) and the Security Functional Specification – RS/FSP/001 (SFS)

An Agent may carry out a particular audit for POL or by POL themselves. The Agents that are permitted are defined in Schedule S3.

Horizon provides for rights of access for individual roles and enforces these rights of access. Changes to these rights is via Change Control.

1.2.3 Access controls

Access controls are effected through the use of roles.

There are THREE auditor roles: POL Emergency Manager/auditor, POL auditor and POL Client <C> auditor. It may not be necessary to represent the POL Emergency Manager/auditor and POL auditor separately.

The POL auditor roles are further defined in the Horizon System Audit Manual – IA/MAN/006 (HSAM).

FUJ00001945

The POL Emergency Manager/auditor has the same access rights as that of the Manager or Postmaster. In addition, he/she may delete and create a Manager/Postmaster Role, and produce a cash account. Access as POL Emergency Manager/auditor is via initial access as POL auditor then, if required, as in the case of the Manager or Postmaster being unavailable, a further exchange via the Horizon System Help Desk to obtain a one-shot password that enables the additional Emergency Manager/auditor operations and a key reference that turns on the filestore encryption/decryption.

POL Emergency Manager/auditor and POL auditor have access to all TMS journal records.

The POL auditor has no rights to modify the TMS journal. The POL Emergency Manager/auditor is not able to modify the TMS journal, except as the auditable result of permitted operations in connection with his role as an Emergency Manager. In common with all journal updates, such permitted modifications are always in the form of appends.

The POL Client <C> auditor role when implemented will have access only to that part of the TMS journal that deals with transactions pertaining to that Client and in accordance with the Client organisation's contract with POL. The POL Client <C> auditors have no rights to modify the TMS journal.

The POL Emergency Manager/auditor has access only at the outlet. The POL auditor has access at both the outlet and the centre. All access at the centre is via the Post Office Account audit function.

1.2.4 POL usage

POL Audit functions has access to the POL SIS audit track and the Systems Management track

1.2.5 POL Client Usage

POL Client Audit functions will have access to those parts of the POL SIS track relating to that Client and subject to the Client's contract with POL (subject to paragraph 1.2.3 above)

1.2.6 Audit trail formats

1.2.6.1 Native Formats

The principle followed is that Horizon originates the audit track source data in self-describing flat files.

The format in which the TMS journal is written by Horizon operational software is that used as input to the utilities that prepare the bulk extracts for the audit authorities. That is, the native flat format is the operational format. This format is attribute grammar (keyword and value) format and is self-describing at the field level. Subsets of the TMS journal represent the data transferred toADS and POL Clients, and from RD, ADS, possibly POL Clients.

The native format of the flat files containing the data transferred between subsystems is described in file headers. They are therefore self-describing at the file level. See Host Application Database Design and Interface Standards - TD/STD/001 (HADDIS).

The logs of file transfers (control files) are in one simple format.

1.2.6.2 Custom Formats

The TMS journal native flat format is not to be further transformed.

FUJ00001945

Custom formats for other audit files may be specified at a later level of specification.

Transfer is by CDROM.

As a principle, the less transformation the better, since this preserves more of the original raw data and removes the need to qualify and maintain transforming software.

1.2.7 Audit trail retention periods

Schedule 18 establishes the retention periods for the Operational and Commercial Audit Trails. These are, for the TMS Journal element of the operational audit trail, and other operational support and system management elements relating to financial systems, 7 years. For other operational systems18 months, and for the Commercial Audit Trail 7 years or contract duration, whichever may be longer.

Operational Audit Data may be retained beyond the specified retention period if it is required to support an ongoing POL investigation, or Litigation Support by Post Office Account, as described in the CCD Service Description for the Security Management Service - CS/SER/016.

Certain archived data such as EPOSS administration functions, which contain dated internal references, will itself have an implied longevity of more than 18 months.

2.0 The Audit Tracks

2.1 POL SIS Audit Track

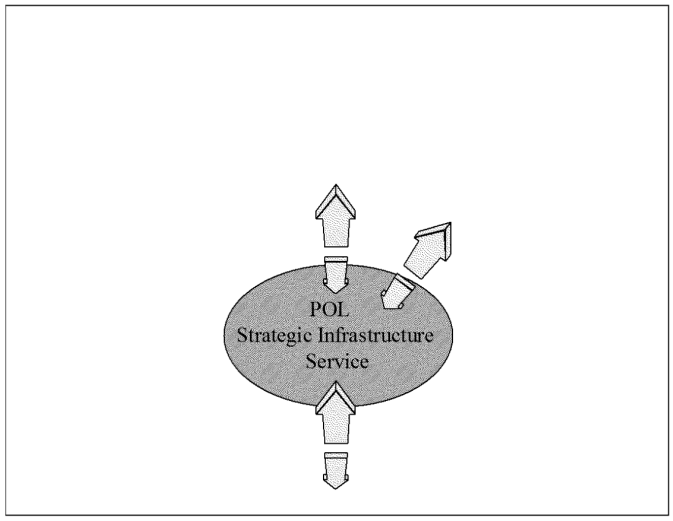


Figure E: The POL SIS track

2.1.1 POL SIS Track Content And Maintenance

The POL SIS audit track comprises:

- the TMS journal

and those POL files exchanged between the Horizon data centres:

- the Horizon System Help Desk files

FUJ00001945

- POL's own systems' files
- AP Client files
- Debit Card payment and error files

Any other intermediate file or table constructs do not form part of the track.

2.1.1.1 TMS Journal

The audit archive of the TMS journal is taken daily at the correspondence server level by copying all new messages that day to audit archive media.

The TMS journal comprises records appended to the journal of each outlet within a messaging group usually in time sequence. Each group includes correspondence servers that hold a replica of the outlet. The outlet replica(s) of the journal are housekept from the front periodically to maintain a recent history to cover at least three cash account periods. The correspondence servers' replicas are similarly housekept.

The TMS journal contains the original transaction details, including its origin, when it happened, who caused it to happen, and the outcome.

2.1.1.2 Horizon System Help Desk

The Horizon System Help Desk files contain the call records from the Automated Call Distribution (ACD) system. These are written during operation and harvested daily into a flat file. A control file will be written for each such daily file.

2.1.1.3 POL Systems

These comprise:

- Those at theRD and ADS interfaces holding control records describing files being transferred
- There is no systematic value in holding separate audit copies of the raw data transferred across these interfaces with TMS because this is what the TMS journal itself represents and because the ADS transfers are selective extracts of it.

2.1.1.4 AP Client Systems

This comprises the various AP Client interfaces holding control records describing files being transferred.

2.1.2 Audit Access to the POL SIS Track

Logical audit access will be provided as follows:

2.1.2.1 TMS Journal Access at the Outlet

Views of the transactions that have taken place within a whole post office during the recent past are available from any counter or back office position within a post office, subject to the POL Auditor having appropriate access rights. This recent past period for which transaction records will remain at any workstation in the post office varies inversely with the traffic conducted by that office as a whole, but is not less than the current and two previous cash account periods, such periods being typically a week. The term "transactions" here embraces

FUJ00001945

both the serving of customers and EPOSS administration events. The journal is also used to carry certain Horizon control sequences. These are of no intrinsic interest to auditors but their retention within the message numbering means that auditors can be sure there are no missing records[1].

2.1.2.2 TMS Journal Access at the Correspondence Servers

Equivalent TMS journal data is maintained at each of the two Horizon Data Centres. These are not copies of each other but are independently derived from the same original data by the same systems. They will therefore provide a natural point of systematic reconciliation: for example, on a sample basis it is possible to compare the audit track record of the same transaction recorded in two places to verify that systems were operating consistently.

Audit records are written to audit archive media. They are presented in exactly the same way as recent records when retrieved although will be subject to filters appropriate to the selection and the audit authority for which the selection is being made. Archive records will take a longer time to retrieve, the retrieval time being in proportion to the volume requested.

If and when the TMS service provider changes, then the TMS journal will be transferred to the new provider as part of the transfer agreement. Apart from the longevity of data retention and the associations of data with post offices, these views are equivalent to those taken in the post office. It is understood that the vast majority of POL audits will be conducted within the post offices, with resort to the Correspondence Server views only where the outlet views are not available (denial, destruction) or, of course, where the historical record is required.

Access from one outlet to the data of another or to the back-history data on the correspondence servers is not provided.

Although the bulk of the TMS journal data is transferred to TIP, Schedule S18 specifies that the audit trail shall be maintained and retained by Post Office Account and protected by security measures.

2.1.2.3 Horizon System Help Desk Log File Access

This comprises simple access to serial flat file. File selection will be by date or dates. Search of the selected file will be by ordinary text search.

2.1.2.4 POL Systems Files Access

This comprises simple access to the control files, potentially followed by access to other files transferred to the TMS journal.

2.1.2.5 POL Client Files Access

This will be defined at a later level of specification.

2.1.3 Auditor Utilities

2.1.3.1 Interactive Access

Access Using Keys

[1] Improved implementation.

FUJ00001945

In both the post office and correspondence server cases audit facilities are provided to retrieve, store locally, display and/or print one or more transaction records, with the selection being based on simple keys. Key elements may be drawn from certain selected keys in the transaction records.

These key elements will be:

- one or more outlets as defined by reference data, e.g. POL Region
- stock unit
- Clerk id
- interval of time
- POL Client identity
- one or more product codes

Other specific key elements may be defined at a later level of specification in the light of experience.

The keys that an auditor may use will be in accordance with the auditor role.

Controls will be available to limit the selection to practical length. Initially this control will be set at 256 records.

Disk serial files thus produced may be saved for later local search.

Access using Standard Reports

The following table categorises and lists the operations to be supported by POL auditor and POL Emergency Manager/auditor use of EPOSS facilities, taken from notes of 17/12/96. Auditor access to such operations is a function of POL auditor or POL Emergency Manager/auditor role management. In all meaningful cases print or print-preview is provided.

Where access to the outlet itself is not possible, as for example when an outlet has been destroyed by fire, equivalent access might be effected by visit to a correspondence server centre or by restarting the outlet at an auditor centre or a replacement centre.

Category	Report
POL Auditor	
Outlet asset verification	Cash account for selected week
	Interrogate Transactions
	Daily summaries
	Cash on hand
	Stock on hand
	Rems in and out
	Suspense account
	History of losses and gains
Stock unit asset verification	Counter balances
	Internal transfers

FUJ00001945

Role verification	Statement of users
Collateral verification	Order books on hand
POL EmergencyManager/Auditor	
Role management	Delete/create users
	Statement of users
Restatement or unexpected loss	Cash and stock declaration
	Rem out
	Current cash account transactions
	Daily summaries
	Cash account
Effect transactions	Any transaction normally available to the Postmaster

2.1.3.2 Bulk Access Using Keys

Bulk access is provided via the Horizon Data Centres only. A utility is provided to produce bulk selections according to the role of the auditor and in the custom magnetic format specified by the audit authority to which he belongs. POL Client audit authorities may require different formats from those used by POL but Post Office Account proposes that they be required to use the Horizon native flat format directly. Clearly, subject to the terms of POL's contract with a POL Client, the data accessed will be limited to that pertaining to that Client.

Retrieving Operational Audit Data in support of POL requests is described in the CCD Service Description for the Security Management Service – CS/SER/016.

In the event that the audit function requires direct, personal and extempore access to the actual TMS operational journal then this access will be by attendance at a Post Office Account location and will be supervised by Post Office Account staff.

2.2 Systems Management Track

2.2.1 Systems Management Track Content and Maintenance

The track is made up of audit events for the particular domain in question. In the Horizon solution all events are generated within domains and eventually transferred to the Tivoli Event Management Server.

Within these domains events are collected by Tivoli Agents and transformed into Tivoli Events. On non-NT platforms the Tivoli Agent role is performed by an equivalent agent function within the local systems management facility appropriate to the platform.

These non-NT platforms are:

- SUN Servers, whose events are notified directly
- Network Devices, such as routers, whose events are mediated by HP OpenView

Audit events comprise:

- System Events, which include Security Events

FUJ00001945

- Status Reports
- Software Distributions

System Events are gathered from all domains, and Status Reports and Software Distributions from all Windows NT domains.

Tivoli provides extensive event management facilities including central display, sorting and filtering before viewing, for example, all operations initiated by a particular operator. These facilities are accessed via a PC-based Tivoli Desktop available to the Fujitsu Services Systems Management functions located in Stevenage and Lytham St Annes and connected via the Horizon WAN to the master Tivoli Management Region, or hierarchic level that is at Bootle.

These Tivoli Events are extracted from the Tivoli Event Management Server and archived using the standard Archive Service. Filters are used to remove unusable operational events before archiving. Archiving is in Comma Separated Variable (CSV) format.

2.2.2 Audit Access to the Systems Management Track

2.2.2.1 Interactive Access

Archived data may be restored from CSV format and viewed using native Tivoli facilities.

2.2.2.2 Bulk Access

This will be facilitated as follows:

- The Tivoli events will be archived daily
- Analysis can be either by Notepad-type browsing the archive file or by importing from CSV format into a database or editor of choice.

FUJ00001945

3.0 The Commercial Audit Trail

The commercial audit trail is defined to comprise material, held in either magnetic forms or definitively on paper, to which POL has access.

3.1 Magnetic Records

These comprise copies of certain Operational Support records that POL receive as part of the Service, and those parts of Post Office Account's internal commercial records to which POL have access.

The track making up the magnetic commercial audit trail is the Business Incident Management System (BIMS)

3.1.1 Business Incident Management System (BIMS)

BIMS is freestanding from the mainstream Pathway Solution. It is a record of the activities undertaken by the Pathway Customer Service Management Support Unit to make necessary adjustments to transactions, typically to effect accurate reconciliation.

3.1.1.1 Data Retention Requirements

Schedule 18 establishes the retention periods for the Operational and Commercial Audit Trails. These are, for the TMS Journal element of the Operational Audit Trail 7 years and 18 months for all other elements, and for the Commercial Audit Trail 7 years or contract duration which may be longer.
For these purposes BIMS is deemed to be part of the Operational Audit Trail ..

3.1.1.2 Audit Access to Operational Support Records

Access is obtained via the procedures contained within the HSAM.

3.2 Manual Records

These comprise Post Office Account records that are held definitively on paper to which Post Office Ltd have access.

3.2.1 Included Items

The scope of this list is restricted to items of significance to POL.

3.2.1.1 Invoicing

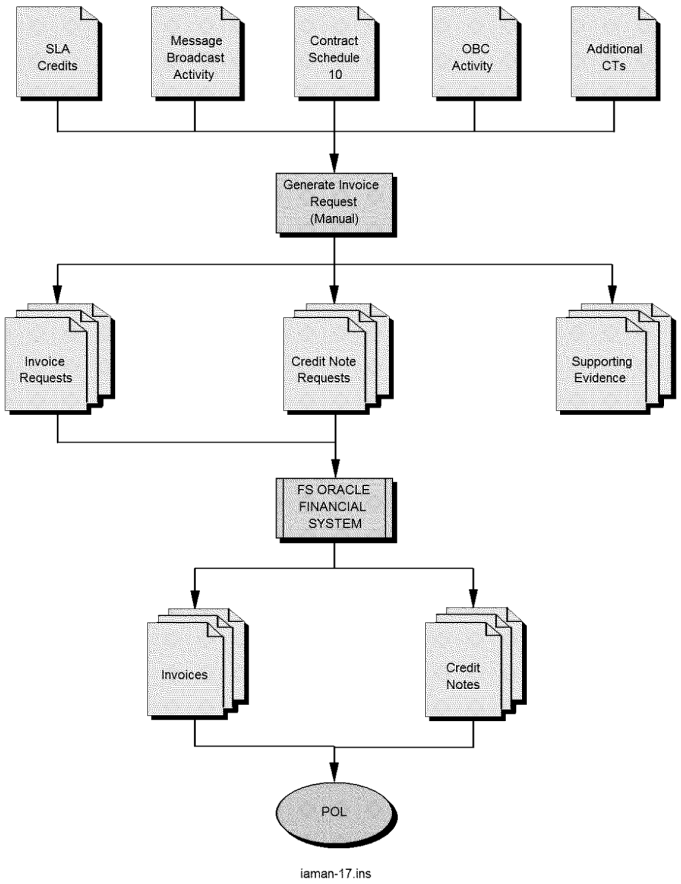
System Overview

All invoices raised under the Agreement are processed through the Fujitsu Services Oracle Financial System.

FUJ00001945

Schematic

The following diagram shows the main data flows within the Invoicing process.



Data Input Streams

Contractual Data

Operating Fee during operating period.

SI Commitment Fee during period.

CCN Service at Annex C to Schedule 10

Manual Data

Debit Instructions from BIMS.

Credit Instructions from BIMS.

These are manual notifications that are applied to the Invoice during its production cycle. (There is, currently, no identified occurrence that might cause a BIMS Instruction to be raised but it is included for completeness.)

Additional CCNs (Monthly)

FUJ00001945

OBC Invoice (Quarterly) – Schedule 19

Message Broadcast (Monthly)

SLA Credits (Monthly) – Schedule 15

Additional CTs executed by CORE along with corresponding Credit Note for any CORE already pre-paid through SI Commitment Fee.

Property Charges

Availability Fee

Changes to Contractual Data

Changes to any element of the Contractual data can only be achieved through formal negotiation between the two parties.

Output Stream

The invoicing suite of documents consists of the following :

- SI Commitment Fee Invoice
- Operating Fee Invoice
- Credit Note for service credits.
- Credit Note for CORE already pre-paid through SI Commitment Fee.

Data Retention Requirements

Schedule S18 establishes the retention periods for the Commercial Audit Trails as 7 years or contract duration which may be longer..

3.2.1.2 Change Control Documentation

Change Control is an agreed process, through which changes to Horizon are defined, notified, impacted and costed, authorised and controlled. Documentation that falls into this group include :

Change Requests (CR)

Change Proposals (CP)

Commercial Terms (CT)

Commercial Terms Signature Sheet (CTSS)

Change Control Notes (CCN)

Request for Work Package (RWP)

Change Work Package (CWP)

Documents that are output from the process and which represent the audit trail of proposed changes and their outcome form part of the Commercial Audit Trail.

Retention: Contract life or seven years whichever is the greater.

3.2.1.3 Special Assistance Invoices

Schedule 22 enables Post Office Account to charge for costs incurred in assisting POL with audit activities following contract termination. Records relating to time spent and expenses will be maintained on a case by case basis.

FUJ00001945

Retention: Contract life or seven years whichever is the greater.

3.2.1.4 Development Activity Invoices

Where development activities are entered into under the terms of the revised contract invoicing will be in accordance with Schedule 10.

Retention: Contract life or seven years whichever is the greater.

3.2.1.5 Contracts with Sub-Contractors

Access is limited to contractual and service related arrangements.

Retention: Contract life or seven years whichever is the greater.

3.2.2 Excluded Items

The following items are outside the scope of 'Records' as defined in Schedule 1:

- Financial arrangements with Post Office Account sub-contractors.
- Financial and employment arrangements with Post Office Account employees, both direct and contract.
- The Post Office Account Business Case.
- General accounting information including funding.
- Reports from and to Fujitsu Services HQ or Fujitsu Group, Japan.

There may be other documents or records that are subsequently added to this list.

3.2.3 Caveats

There are two caveats that apply to the above lists:

- Special access to records not identified as 'included' may be granted on a case-by-case basis, subject to request and approval at the appropriate level.
- The scope of access to records identified as 'included' must be agreed as part of agreeing Terms of Reference for an audit as described in the Joint Working Framework described in the Post Office Account Internal Audit Manual (IA/MAN/003) and HSAM.

It is possible that records and/or documents will be identified during an audit that were not included in the original Terms of Reference. Post Office Account Internal Audit will facilitate the release of these records and/or documents through the appropriate channels subject to the records not being on the 'Excluded' list.