FUJ00117508

Document Title: Audit Data Retrieval High Level Design

Document Type: High Level Design

Release: BI3 S75

Abstract: The specification of the components required to implement the audit data extraction & filtering facilities at BI3 S75.

Document Status: APPROVED

Originator & Dept: Alan Holmes, Estate Management & Secure Builds

Contributors:

Internal Distribution: See section 0.2

External Distribution:

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

Name	Position	Signature	Date
Mark Taylor	S75 Development Manager		
Bill Mitchell	Security & Risk Manager		

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	19/04/2002	First BI3 issue with details taken from SD/DES/116	CP3171
0.2		Not Issued	
0.3	29/10/2004	S75 changes. Issued for review.	CP3642 CP3721
1.0	26/11/2004	Issued for approval	

0.2 Review Details

Review Comments by:	N/A
Review Comments to:	Alan Holmes

Mandatory Review Authority	Name
System Support Centre Manager	Mik Peach
Programme Assurance	Jan Holmes*
Customer Service	Bill Mitchell
RASD Infrastructure Design	Nial Finnegan
Optional Review / Issued for Information	
ITU	Mike Berrisford
DU/Development Audit	Bryan Muir, Oddette Moronfolu

(*) = Reviewers that returned comments

0.3 Associated Documents

	Reference	Title	Source
	PA/TEM/001	Fujitsu Services Limited Document Template	PVCS
[ACP]	RS/POL/003	Access Control Policy	PVCS
[ASC]	TD/ION/011	Audit Server Configuration	PVCS
[AMAN]	IA/MAN/006	Horizon Audit Manual (BI3)	PVCS
[ATFS]	CR/FSP/006	Audit Trail Functional Specification	PVCS
[HLDEF2]	SD/DES/074	Audit Data Filtering and Extraction HLD	PVCS

[HLDSR+]	SD/DES/115	Audit Data Storage & Retrieval High Level Design (CSR+)	PVCS
[HLDGSBI3]	SD/HLD/001	Audit Data Gathering & Storage High Level Design	PVCS
[MIGCSR+]	TD/ARC/021	Strategy for CSR to CSR+ Migration	PVCS
[OPSMENU]	SD/SPE/016	Horizon OPS Menu Hierarchy: Release 2	PVCS
[ORAUT]	TD/STD/003	Host Applications Generic Procedures HLD	PVCS
[REPORTS]	SD/DES/005	BA/POL Reports & Receipts	PVCS
[REQCSR+]	SD/REQ/002	Requirement Specification for the Audit Subsystem at Release CSR+	PVCS
[REQRR+]	IA/REQ/004	Audit Data Retrieval Requirements [CSR+]	PVCS
[REQBI3]	IA/REQ/005	Network Banking Internal Audit Requirements	PVCS
[SEMR]	RS/REQ/004	Security Event Management Requirements	PVCS
[SFS]	RS/FSP/001	Security Functional Specification	PVCS
[TED]	TD/ARC/001	Technical Environment Description	PVCS
[TIVAIS]	SD/IFS/014	Audit to Tivoli Cluster Information Interface Specification	PVCS
[IAPRO]	IA/PRO/004	Audit Data Extraction Process	PVCS
[SMSD]	CS/SER/016	Service Description for the Security Management Service	PVCS

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
ARQ	Audit Record Query
AS	Audit Server
AS (B)	Audit Server (Bootle)
AS (W)	Audit Server (Wigan)
CD-W	CD-Writable (in the instance of the Audit Server/Workstation Write Once)
COTS	Commercial Off The Shelf
CS	Correspondence Server
DB	Database
DSS	Department of Social Security

FTMS	File Transfer Managed Service
GB	Giga Byte
HLD	High Level Design
Mb	Megabit
MB	Megabyte
MIS	Management Information System
NAO	National Audit Office
NFS	Network File System
OBCS	Order Book Control System
PAS/CMS	Payment Authorisation System/Card Management System
POL	Post Office Limited
RED	Reconciliation Exception Database
SLAM	Service Level Agreement Monitoring
TME	Tivoli Management Environment
TMS	Transaction Management Service
TOD	Tivoli Oracle Database

Definitions

Audit Archive — The sum of audit data written to secure storage by the Audit Servers which is available for subsequent Audit Track extraction and other recovery/extraction purposes. The Audit Archive is generated in two parts one on the Bootle campus and one on the Wigan campus. Both parts contain a copy of all audited information.

Audit Server — The system which is responsible for the gathering, archiving, retrieving and potential extraction for subsequent analysis of all audit information that is required to be retained beyond normal operational use.

Audit Data Storage — The Audit Track Gathering, and Audit Track Hoarding components of the Audit system

Audit Data Restoration — The Audit Track Retrieval and Audit Track extraction components of the Audit system.

Audit Point — Identifies a logical position in the Horizon system at which an Audit Track is generated. In reality an Audit Point is distributed across a number of locations in the system each such location is identified as an Audit Sub-Point

Audit Sub-Point - see definition of Audit Point

Audit Sub-Point — A physical point in the Horizon system from which data is gathered (see also Audit point)

Audit Track — A sequential record of activities made by a particular subsystem

Audit Track Deletion — The deletion of Audit Tracks once they have been gathered. The Audit Server is responsible for the deletion of all Audit Tracks outside of the Audit Archive.

Audit Track Deletion does not cover the removal of time expired Audit Tracks from the Audit Archive.

Audit Track Gathering — The transfer of Audit Tracks to the Audit Server prior to Audit Track Hoarding.

Audit Track Generation — The production of Audit Tracks by Horizon applications in formats suitable for Audit Data Storage

Audit Track Hoarding — The writing of Audit Tracks to secure storage in a format suitable for retrieval.

Audit Track Retrieval — The reading of Audit Tracks from secondary storage.

Audit Track Sealing — The generation and independent storage of a checksum for each file before it is subject to Audit Track Hoarding and after Audit Track Retrieval. Comparison of the before and after seals can demonstrate, to a very high degree of probability, that the Audit Tracks have not been tampered with.

Audit Trail — One or more Audit Tracks, which between them, enable an auditor to follow the treatment of related data transfers, movements or accesses by named individuals.

Audit Track Extraction — Extraction of Audit Track information for presentation to and subsequent use by POL and by Fujitsu Services.

0.5 Changes in this Version

Version	Changes
1.0	Issued for approval

0.6 Changes Expected

Changes
Updated as a result of comments from review.

0.7 Table of Contents

1.0 Introduction

Within the Horizon system, Fujitsu Services are required to provide facilities to produce, store and present to authorised POL staff, Audit Track data in support of the security policy and audit requirements laid down for the system.

The architecture for the audit sub-system within the Horizon system is described in [TED]. This Audit Data Retrieval High Level Design Specification is consistent with that architecture.

This High Level Design (HLD) specifies the components required to provide the Audit Data Retrieval facilities together with their interfaces and functionality. The level of detail in this HLD is intended to be adequate to enable detailed design, implementation, integration and test work packages to be specified.

These Audit Data Extraction and Filtering facilities are provided for authorised Fujitsu Services staff to provide extracts of the audit data from the Audit Archive in response to information requests from authorised POL staff.

The Audit Data Extraction facilities are responsible for providing the facilities to filter, the retrieved audit tracks to the level of detail specified in the information request.

The extraction of Audit Archive data is carried out by Fujitsu Services. The facilities that are provided for the extraction of data that Fujitsu Services is contractually obliged to archive for audit purposes, will also be available to extract non-contractual audit data.

This document does not cover the on-line facilities that may be required to look at live (non-archived) data, with the exception of access to the Correspondence Server Message Store. These facilities are documented in the Horizon Audit Manual BI3, ref [AMAN].

2.0 Scope

The approach is to utilise where possible software products, already adopted or supplied with the operating systems, to access, retrieve, filter and present audit data to the requestor. Extraction is to be effected by the use of filters applied at various points in the extraction process.

This High Level Design Specification covers:

- Online extraction of data from the Correspondence Server Message Store, from any Audit Workstation
- Seal Checking to ensure extracted files have seals intact
- Maintenance & Monitoring of Audit Record Queries (ARQs)
- Presentation to Auditor, tools to present data in required format
- The interfaces between the applications restoring the Audit Tracks and the Audit Data Extraction facilities

The data that will be stored in the Audit Archive and hence the data that needs to be retrieved is defined in Audit Server Configuration, ref [ASC].

The scope of this HLD does **not** cover:

- TMS Journal Access at Outlets/Auditor Utilities as specified within Audit Trail Functional Specification, Ref [ATFS]. These are provided to POL staff only, via Riposte Desktop. Data is requested by POL via specified Reports and Functions, as defined in the Horizon OPS Menu Hierarchy: Release 2, ref [OPSMENU]. The report layouts are defined in BA/POL Reports and Receipts, ref [REPORTS]. All transactions at a Post Office can be viewed with the 'Transaction Log' facility.
- Specification of Information Requests, this is defined in Audit Data Extraction Process [IAPRO].
- Online access to live data to support Internal Audit
- Use of Audit Archive for restoration of TMS journal in support of Correspondence Server Disaster Recovery
- The analysis of Audit Tracks to provide specific Audit Trails

3.0 Design Principles

The main principle of this design is to provide the required audit data extraction and filtering facilities while minimising the impact on Applications within the Horizon Subsystems. This HLD includes design features to interface to and support existing system features.

The Audit Architecture as defined in the TED, ref [TED], identifies the need to be able to cope with change as the usage of the Horizon system develops, especially as new applications and services are introduced. Thus a significant design principle is for the Audit Data Extraction and Filtering system to be able to support the introduction of such new facilities with minimum impact.

The extraction mechanisms must provide only that data that is appropriate to the role of the requestor.

To provide facilities which can be built upon and developed to provide enhanced audit facilities for future releases.

4.0 Requirements

The requirements for the extraction of Audit Archive data are specified in the following documents:

- Audit Trail Functional Specification, ref [ATFS]
- Audit Data Retrieval Requirements, ref [REQRR+]
- Requirement Specification of the Audit Subsystem at Release CSR+ [REQCSR+]

- Network Banking Internal Audit Requirements [REQBI3]
- Service Description for the Security Management Service [SMSD]

In summary, the extraction facilities must be able to support Audit Record Queries (ARQs) in providing the relevant data for investigations, resolution of operational problems and for bulk historical information extracts. The extraction facilities do not explicitly support ARQs requesting data for proving the integrity of processing.

Extraction facilities must support extraction of the POL and Systems Management Audit Tracks as defined in ref [ATFS].

Extraction facilities must be able to cope with the specified Retrieval Frequencies and Turnaround Times, and be able to support ARQ maintenance and progress monitoring as per ref [REQBI3].

Although it is anticipated that the majority of Information Requests, to support both Investigations and Bulk Extraction, will be based on data originating from the TMS Journal, associated external interface files and where relevant database files can also be requested.

The data to be stored and hence that which must form the basis of extraction is defined in the Audit Server Configuration [ASC]

The extraction facilities must allow the auditors to extract data from one or more associated audit points, hence providing the data to support logical Audit Trails. In the absence of detailed information on required Audit Trails, there is no automated support for linking audit point data to create Audit Trail Reports.

The following documents also include requirements on the Audit Data Extraction and Filtering design:

- Technical Environment Description, Section Audit Architecture, ref [TED]
- Security Functional Specification, ref [SFS]
- Security Event Management, ref [SEMR]
- Access Control Policy, ref [ACP]

5.0 System Overview

The Technical Environment Description, [TED] describes the overall audit system design for Horizon. This section provides an overview of the design of the parts of the Audit subsystem supporting the Audit Data Extraction functions. The function of the Audit Extraction system is to

- Effect extraction of Correspondence Server TMS journal via any Audit Workstation
- Extract the appropriate records using specified extraction criteria to give a manageable number of files/records. Extracting a subset of records from an audit archive file is not provided for all file formats.
- Provide facilities to filter and subsequently browse the extracted data to meet the criteria of the 'Information Request'
- Seal check retrieved files
- Maintain & Monitor Retrievals by ARQ

The source of the data to be extracted and filtered is generated from a wide range of components of the Horizon system including:

- Correspondence Servers
- Tivoli Management Facilities
- Database Hosts (including the Reference Data System)
- FTMS Gateways

Access to the retrieval and extraction facilities is via the User Interface provided on the Audit Workstation.

Figure 5.1, shows the major components of Audit sub-system on a single Campus. The configuration is duplicated on both the Wigan and Bootle sites.

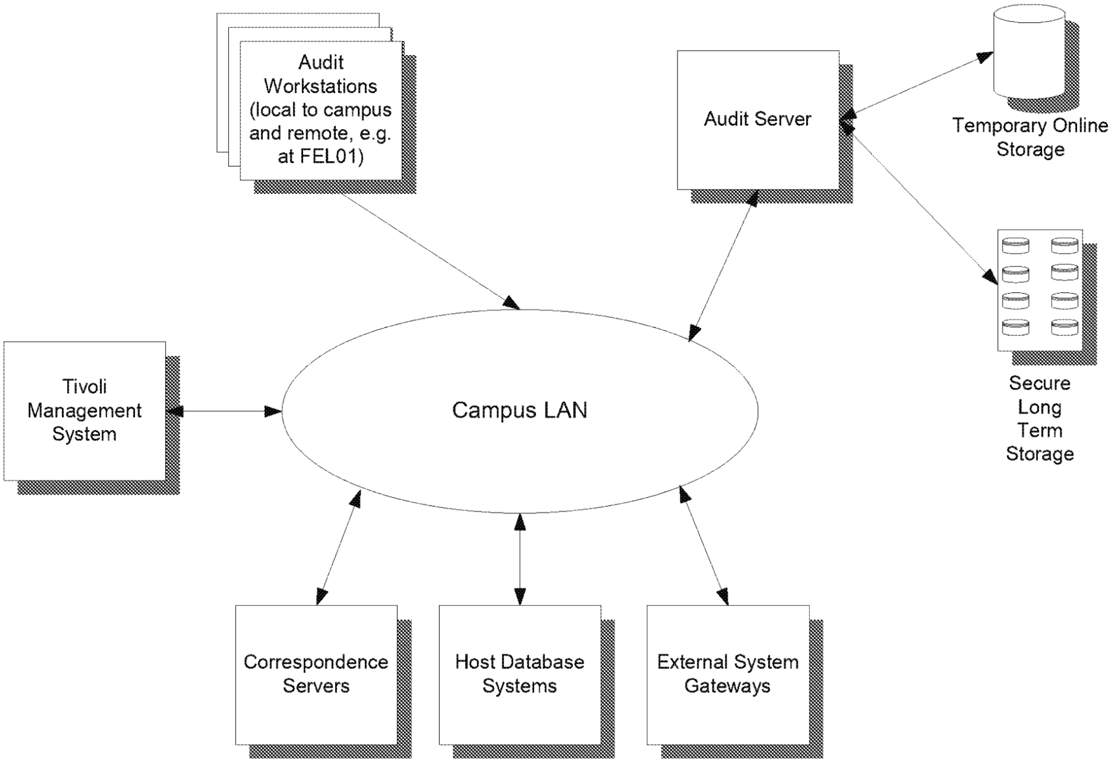

Figure 5.1

Main Components of Audit Subsystem

5.1 Audit Server

The Gathering & Storage components of the Audit Server are defined in Ref [HLDGSBI3].

The Audit Track Retriever component covers the retrieval of data from the Audit archive

The Audit Track Extractor component, consists of a number of utilities that extract data retrieved by the Audit Track Retriever component

In overview the Extraction & Filter components of the Audit Server are:

- A utility to restore audit tracks from the Audit archive
- A utility to interrogate data, which originated from the Correspondence Server Message Store. Riposte records are loaded into an empty Riposte Message Store in a form that enables the standard Riposte facilities to be used to browse it. This utility allows an outlet(s) and date range to be specified, to limit the restoration to only those records pertaining to that outlet.
- A utility to restore oracle table data that enables the retrieved data to be populated to an empty oracle database. Standard oracle tools can then be used to browse the restored data.

- A utility to manage ARQs as they progress through the retrieval & extraction processes. The data to support this facility is maintained on the Audit Server.
- COTS tools to view and filter extracted data

5.2 Audit Workstation

The Audit Workstation provides facilities for authorised Fujitsu Services staff to access the Audit Server in order to retrieve Audit Track data from the Audit Archive and to either select or prepare Audit Track data for presentation to POL or in support of internal audit activities.

Access is via the interface provided by Windows NT.

At BI3 an Audit User Interface is provided to give the User access to the applications on the Audit Server.

A Retrieval User Interface is provided to search for specific audit tracks & manage details of ARQs.

The files retrieved from the Audit Archive are stored on the Audit Server. Where necessary audit tracks will be restored and extracts performed before files containing the relevant records are transferred to the Audit Workstation. Browse and filter tools will be configured on the Audit Workstation where subsequent searches/filters on files may be performed.

Riposte QueryUK (RQueryUK) will be available on the Audit Workstation, to enquire on the Correspondence Server Riposte Message Store, or the Audit Server/Workstation restored message stores, whichever is appropriate. The user specifies the appropriate message store to RQueryUK.

Oracle Discoverer is provided to browse/query restored database tables.

WordPad is provided to browse text files.

User interfaces are provided on the Audit Workstation to the restore utilities. A detailed definition of the utilities provided is contained in section 6 below.

There will be no automated synchronisation between the Audit Data Extraction and the Audit Data filtering facilities.

The Audit Workstation supports a Write-Once CD to which selected Audit Track data for POL can be written.

POL staff will not be given direct access to the Audit Workstation to safeguard other parts of the Horizon system. Instead nominated Fujitsu Services personnel will supply audit information requested on or off-site.

5.3 Audit Archive

A copy of the Audit Archive for both the Bootle and Wigan sites is held on EMC Centera. Audit Tracks generated on each campus are added to the local copy of the archive. The locally generated Audit Tracks include a full copy of the TMS Audit Tracks generated on the local instances of the Correspondence Server machines and all other non-TMS Audit Tracks generated on the campus.

A more detailed description is defined in Audit Data Collection & Storage High Level Design, ref [HLDGSBI3].

5.4 Audit Points

An Audit Point is a logical concept introduced in this design to minimise the linkage (as seen by users of the Audit Workstation) with the physical design of the Horizon system. This is intended to help reduce the knowledge that the auditors need of the details of the way Horizon has been implemented.

The term Audit Point is used, in a number of places within this design, to refer to the logical location at which a particular Audit Track is generated, e.g. where the TMS Audit Track is generated. Due to the distributed and resilient nature of the Horizon system an Audit Point is actually realised at a number of different physical locations.

The specific locations at which the Audit Track of a particular Audit Point is generated are identified as Audit Sub-Points. An Audit Sub-Point maps onto a single sub-directory on a single component in the Horizon system. It is however possible for an Audit Sub-Point to map onto a (finite) set of such sub-directories. Where there are a number of sub-directories they will be nested beneath a single top-level sub-directory.

The files stored in the Audit Archive are named in terms of an Audit Point and an Audit Sub-Point. These logical concepts are designed to be stable across the life of the Horizon system and to assist the Fujitsu Services Auditors in locating the files containing the relevant data to support any particular audit activity. For example, all TMS journal (i.e. Correspondence Server Audit Track) files will be identified by the same Audit Point and the same Audit Sub Point will identify all files generated on the same Correspondence Server cluster.

6.0 System Components

6.1 Application Components

Audit Data Retrieval is handled by the Audit Track Retriever and Audit Track Extractor components of the Audit solution.

6.1.1 Audit Track Retriever

Figure 6.1 identifies the main interfaces to the Audit Track Retriever

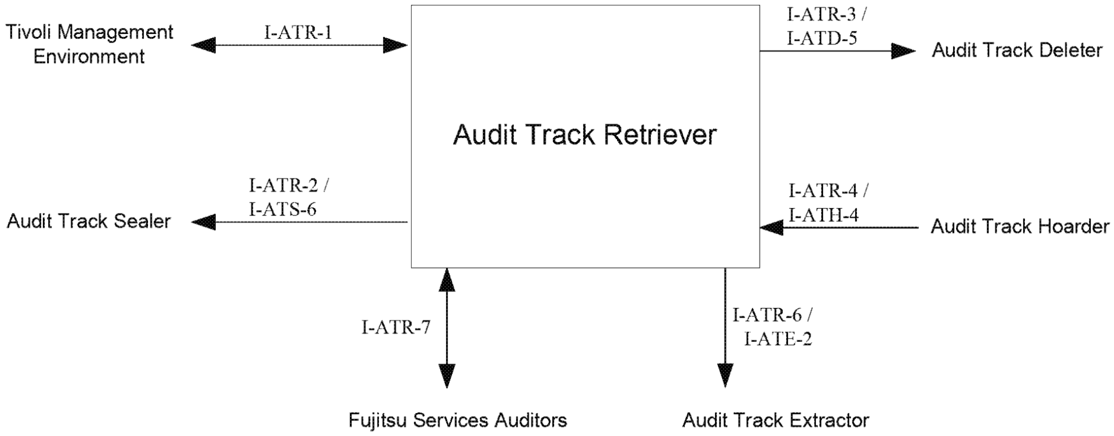

Figure 6.1

Interfaces to the Audit Track Retriever

6.1.1.1 ATR Interfaces

I-ATR-1 Interfaces to the system administration staff and facilities are all via the Tivoli Management Environment (TME). TME shall monitor the existence of the ATR and shall report as a Tivoli event any unexpected unavailability.

The ATR will be under control of Maestro scheduling.

In addition command line interfaces will be provided to start and stop the ATR outside of Maestro control.

I-ATR-2 See I-ATS-6.

I-ATR-3 For every file successfully (or unsuccessfully) retrieved from Centera by the ATR it will inform the Audit Track Deleter (ATD) of:

- The time and date of the Retrieval
- A meaningful success/failure code
- The path name file

The ATR will pass the details of the files retrieved to the ATD via an agreed directory. Details of the files will be put in a Record File in the shared directory for collection by the ATD. Each Record File must contain the details of at least one file, but may contain many. Details of retrieved files batched together in one Record File must always be held on persistent storage media (e.g. disk) and must never be over written. Record Files must regularly (e.g. every hour) be passed over to the ATD. The frequency shall be a configurable parameter. The Record File shall be a text file.

Note that this interface is to support internal logging of Audit Server activities.

I-ATR-4 This interface is effectively the Sealer SQL database

I-ATR-6 The files retrieved from the Audit Archive are placed into a directory from which the Audit Track extractor can copy the data for subsequent extraction activities. The ATE is responsible for deleting the files from this directory.

I-ATS-6 Files whose seals are to be checked are notified to the ATS via this interface. Each request is in the form of a marker file that uniquely identifies the filename of the file to be sealed/checked. Files to be sealed/checked are placed in an agreed directory. The ATS regularly checks the directory and removes the first entry and checks the seal. The ATS is responsible for removing files from the common directory.

I-ATR-7 represents the ‘Retrieval User Interface’, which Fujitsu Services auditors use to retrieve files from the Audit Archive. This interface is one part of the graphical user interface provided for Data Extraction

6.1.2 Audit Track Extractor

The Audit Track Extractor (ATE) component of the Audit solution will be implemented as a set of functions available from the Audit workstation to refine & interrogate data retrieved by the Audit Track Retriever (ATR).

The level of extraction will always be dependent on the associated Audit Record Query and the characteristics of the audit archive file containing the data being requested, e.g. an external interface Control File which has been archived in it's original format, is likely to be requested in it's entirety with no further extraction of specific records required. A TMS Journal file, due to how it is originated and the fact that it may contain data associated with all of the Horizon system applications, is less likely to be requested in its entirety.

The different levels of filters to achieve extraction of required data are

- File Identification, by Audit Point, using data from ARQ and Audit Server Configuration
- Extraction of a subset of audit tracks from a set of audit points file using defined extraction criteria
- Filtering (post extraction or post retrieval if no further extraction took place) using tools appropriate to the format of the extracted file

The functionality provided will comprise of: -

- Management database to contain ARQ information
- Tools to reconstruct a message store on he Audit server or workstation from retrieved TMS files, expand files stored in compressed format and reconstruct Oracle tables from retrieved files in Oracle format
- Functions for viewing & filtering data produced from the ATR and further extracted by the provided tools and additional the online Correspondence Servers (Interactive Retrieval)
- Ability to copy extracted data to CD-ROM or floppy disk for delivery

6.1.2.1 ATE Interfaces

Figure 6.2 identifies the main interfaces to the Audit Track Extractor

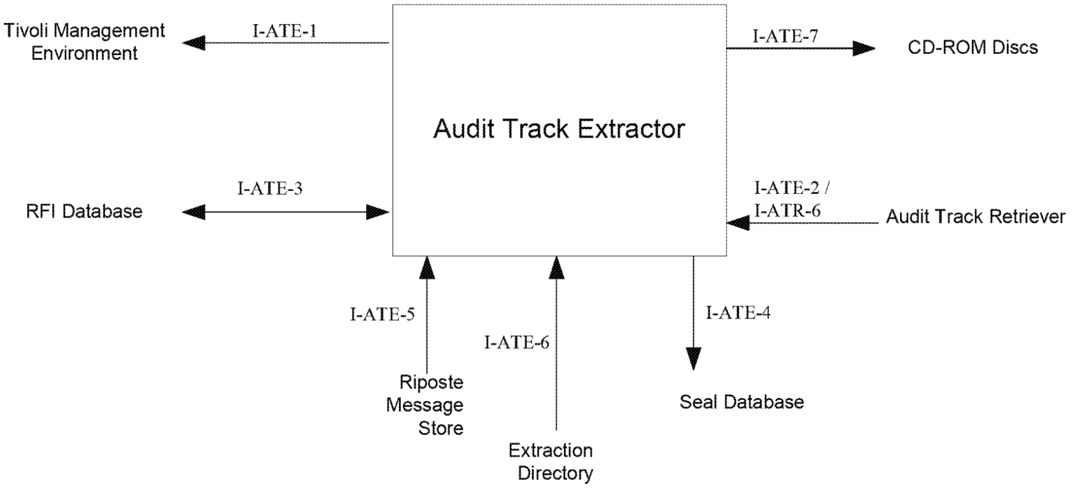

Figure 6.2

Interfaces to the Audit Track Extractor

I-ATE-1 Interfaces to the system administration staff and facilities are all via the Tivoli Management Environment (TME).

I-ATE-2 (**I-ATR-6**) the files retrieved from the Audit Archive are placed into a directory from which the Audit Track extractor can copy the data for subsequent extraction activities. The ATE is responsible for deleting the files from this directory.

I-ATE-3 This is the interface to the ARQ Database where ARQ and associated file information is stored via the GUI

I-ATE-4 This is the interface to link to the Audit Seal Database to allow the status of Seal Checks to be interrogated via the GUI.

I-ATE-5 This is the interface between the Auditor using RqueryUK to access the Live Correspondence Server message stores to extract data, and the pseudo rebuilt message store located on the Audit server or workstation

I-ATE-6 This is the interface between the Auditor using the COTS tools to View and Filter data held in the extracted directory on the Audit Server

I-ATE-7 This is the interface between the Auditor and the CD-Writer device to write data for use by external Auditors. This interface is implemented using Easy Creator CD.

6.1.3 Audit Extractor Client

The Audit Extractor Client application that will reside on the Audit workstations handles the selection, retrieval and recording of the usage of Audit Data.

Audit Record Queries will be in an agreed defined format, with the minimum information required being that which will allow an Audit Archive file to be identified.

ARQs will be specified as per Horizon Audit Manual (BI3), Ref [AMAN].

The ARQ GUI on the Audit workstation will enable management of ARQs and their associated files and provide access to the tools to extract data

The GUI will provide options to

- Create a new ARQ
- Open an existing ARQ
- Close or Cancel an ARQ
- Select files for retrieval
- Monitor the progress of requested files

6.1.3.1 Access

Access to the Audit Extractor Client is provided by a Start Menu option. Invoking this option presents an initial connection screen.

The initial connection screen enables the user to: -

- Select which Data Centre to connect to.
- The screen also identifies the Username and the Audit workstation id

6.1.3.2 ARQ Selection

After selection of a Data Centre the ARQ selection screen will be presented.

This screen of the application provides functionality to: -

- Open an existing ARQ
- Create a new ARQ
- Close an ARQ
- Exit
- The screen also identifies the user name and the data centre to which the application is currently connected

6.1.3.3 Creation of a New ARQ

When an ARQ is received by it should be registered at the Data centre for which the extraction is to be performed by using the create ARQ function.

This option is invoked from the New ARQ button on the ARQ selection screen.

Using this screen, the user will be able to enter: -

- Requester Id, from a drop-down menu of pre-defined values comprising:
  - Other 3rd Party
  - Pathway Internal Audit
  - Pathway Other
  - Pathway SSC
  - POL Internal Audit
  - POL Other
  - POL Security
- Catalogue Entry - Optional
- Receipt Reference – Requester reference
- Request Date – The date the request was received.
- Required Date – The date that the information is required.
- Access Reason – Explanatory text

On completion of the above fields the user will be able to: -

- Save the ARQ, which will result in generation of a new ARQ Id
- Specify details of the files required to satisfy the ARQ.
- Quit and return to the previous screen

6.1.3.4 Opening an Existing ARQ

The user will be able to select existing ARQs and open them to progress file retrieval and also monitor the progress of the ARQ file retrieval.

This option is invoked using the ‘Open ARQ’ button on the ARQ selection screen.

A dropdown list of the ARQs available will be presented to the user to select the required ARQ. This list will only contain OPEN ARQs

Once an ARQ is selected the user will be given options to: -

- View details of the ARQ, which includes the selection criteria
- Open the ARQ, which allows file selection an monitoring
- Quit and return to the previous screen

6.1.3.5 Closing and Cancelling an ARQ

The user will be able to select existing ARQs and close them, preventing any further activity on the ARQ.

This option is invoked using the 'Close ARQ' button on the ARQ selection screen.

A dropdown list of the ARQs available will be presented to the user to select the required ARQ. This list will only contain OPEN ARQs

Once an ARQ is selected the user will be given options to: -

- View details of the ARQ, which includes the selection criteria
- Close the selected ARQ.
- Quit and return to the previous screen.

Once this is done no further amendment to the ARQ will be permitted, although it will be possible to View the details.

It is the responsibility of the User to ensure that they have completed extraction and filtering of retrieved files before they close an ARQ.

When an ARQ is closed ALL of the data files retrieved for the request will be deleted from the Userarea filestore on the Audit Server along with other internal files relating to the ARQ.

A text file will be produced giving the following details: -

- Basic details of the ARQ
- A list of ALL files associated with the ARQ and their seal status
- A list of All of the actions taken by the user to complete the ARQ

6.1.3.6 File selection criteria (Retrieval User Interface)

The information on the ARQ is used to determine the required files to be retrieved from the Audit archive store

The Audit Server Configuration, Ref [ASC], specifies the Audit points and sub-points known to the Audit system. This enables the user to translate the User specified data from the Information Request into a set of file selection criteria. There is no automated support for the translation process.

The required Data is specified on the File Selection screen invoked for a New ARQ and when a request to amend selection criteria is made for an existing ARQ

The following selection criteria for file selection are required:

- A single Date Range (From Date and To date) in which the required files were collected by the Audit system.
  It should be noted that files and data are not always available to the Audit system for some days after their creation date.
  In the case of TMS journals it is possible for an outlet not to synchronise with the Data Centre for several days and thus TMS data generated at the counter will not be available at the Correspondence Server until synchronisation takes place. The Non-

polled offices report held in the Audit archive is available to the Auditor to determine (manually) whether such a condition has occurred at the end of the date range for the offices in consideration.

- Optionally, a selection of Audit Points and Audit Sub-Points.
  This selection to be controlled by lookup lists of all the available points.
  In the case of Audit Sub-Points the list is to be restricted to those related to the selected Audit point.
- Optionally, a file name template may be supplied. This allows the user to restrict the search to file names that match the pattern entered. Wild cards may be included in the supplied pattern using the * character.
- Optionally, an office FAD code. This will automatically determine the Correspondence Server Cluster(s) that the FAD belongs to and add the relevant Audit point / Sub-Point to the selection criteria (See 6.1.3.6.1)

Once the above fields have been supplied the user may: -

- Initiate the search for files that match the search criteria
- Save the current search criteria
- Quit and return to the previous screen

6.1.3.6.1 Cluster Determination (Retrieval User Interface)

Because of the volumes of TMS files, it is a requirement to retrieve only those files relevant to the Outlet. This necessitates being able to establish which Cluster an Outlet's messages will have been created on for the requested Date Range.
Note: the introduction of OCMS (Operational Change Management Service) changes the concept of Cluster /Outlet mapping. Prior to OCMS an Outlet would reside in a single cluster throughout its lifespan.

This information will be provided by a Tivoli Web service. This returns historical Cluster information for an Outlet. The interface to this view is defined in [TIVAIS].

- The Tivoli Web page will be accessed from the Audit Server
- The outlet required will be provided as a six character FAD Code (i.e. without the trailing check digit)
- The utility must provide ALL of the Correspondence Server Clusters in which the Outlet has resided together with the corresponding date ranges

From the Tivoli provided information the Cluster Determinant component will determine the required Audit Sub-Points for the requested date range.

6.1.3.7 File Retrieval facilities (Retrieval User Interface)

The files that match the search criteria are displayed on the Main ARQ screen once a search has been initiated

This screen provides all of the functionality to manipulate the files associated with an ARQ

The following facilities are to be provided: -

- Restore a selected set of files from the Audit archive to the Userarea of the Audit Server
- Check the status of a selected set of files (i.e. where they are in the retrieval cycle)
- Delete a selected set of files from the ARQ
- Replace the files for the ARQ with a selected set (i.e. delete all but)
- Amend the search criteria which will remove the file list associated with the ARQ and present the user with a file selection screen
- Add files which will effectively widen the search criteria and produce additional files on the list
- Allow the user to Monitor the progress of any actions being carried out for the ARQ
- Provide menu options for the generation of a TMS message store and Oracle tables

Once a file has been retrieved it needs to be automatically passed onto the ATS (for seal checking)

6.1.4 ARQ Database

6.1.4.1 Overview

The ARQ database (aka RFI database) will be a SQL Server Database.

A copy will be held on each Audit Server with data only pertaining to ARQ requests handled by that server.

The database will be regularly backed up as part of the Audit Server backup

The ARQ database will contain the following information: -

- Details of information Requesters
- Details of Requests for Information (ARQs) and the associated files
- Details of valid users of the Audit facilities
- Details of Audit points and Audit Subpoints
- Client-Server interface management

6.1.4.2 Requesters Data

The data recorded for each requester will be: -

Attribute	Description

Requester Identity	Identifies the Requester of information.
Telephone No	The telephone contact number of the requester
ARQ Prefix	The prefix to be part of the unique number generated for each ARQ. This will aid identification of ARQs by different requesters
Organisation	The organisation to which the requester belongs (e.g. Fujitsu Services, POL etc.)

As it is expected that data in this table will be relatively static maintenance will be via direct access to the table using standard Microsoft SQL Server tools.

6.1.4.3 ARQ Data

The Data recorded for each ARQ will be: -

Attribute	Description
ARQ Reference	A unique generated reference number for the ARQ constructed from the ARQ prefix for the requestor and a sequential numeric suffix
Operator Id	The identity of the Auditor performing the ARQ taken from the Logon information for the ARQ GUI
Requester ID	The identity of the requester entered by the user from the dropdown list presented to the user when creating an ARQ
Receipt Reference	The requesters reference for the ARQ, input by the user
Access Reason	Textual Details of the ARQ input by the User
Catalogue Entry	Reference for the Auditor to relate to the manually held ARQ catalogue
Date Received	The date on which the ARQ was received, input by User
Date Required	The date by which the information is required by the Requester, input by the User
Status	The status of the ARQ which is maintained automatically by the system
Selection Criteria	Details of the Audit Data selection criteria as input on the Request for Information screen defined under the ATR facilities in [HLDSR+]

6.1.4.4 Audit Points and Sub-Points

Tables of valid Audit Points and sub-Points will be held in the ARQ database to be utilised for the provision of dropdown list in he Retrieval User Interface.

Update of these tables when there is a revision to the Audit points and/or Sub-Points defined in ASC will be carried out automatically on a daily basis to ensure that the list represents the latest view of the Audit Server Configuration.

6.1.4.5 ARQ File Status

The user will be able to monitor the status of files selected for extraction to satisfy an ARQ

The file selection screen will show the filename, status, volume and whether the volume is online.

Update to the status will at user request.

The file status and the meanings are as follows.

Status	Meaning
Displayed	The file has been presented as a candidate for retrieval as it meets the selection criteria entered
Requested	The file has been marked by the user as required for the ARQ and retrieval has been requested
Restoring	The file is in the process of being restored
Restored	The file has been restored from the Audit Archive and is awaiting processing by the Audit Track Retriever (ATR)
Restore Failure	The file has failed to restore
Waiting Seal Check	The file has been processed by the ATR and is awaiting seal checking. The file is available to the Auditor in the EXTRACTED_AT directory
Seal OK	The file has been processed by the ATR and the seal has been checked and is correct. The file is available in the EXTRACTED_AT directory and is now ready for further extraction and/or delivery
Seal Failure	The file has been processed by the ATR and the seal has been checked but a difference has been found in the value indicating possible data corruption and/or tampering
Unknown	It has not been possible to determine the status of the file retrieval

6.1.4.6 Client-Server Interface

Tables to manage the client-server interface between the Audit workstations and the Audit server. These tables will support the following client-server functionality:

- Recover files
- File status
- Clear message store
- Generate message store
- Get cluster Id
- Close ARQ
- Create ARQ

6.1.5 Extraction Tools

6.1.5.1 Restore TMS Files to Message Store

To enable filtering of TMS Data the TMS files must be extracted into a pseudo Correspondence Server located on the Audit Server or Audit Workstation.

Locks will be introduced such that only 1 ARQ at a time may use an Audit Servers message store. The Audit workstation Riposte Messagestore should be considered as the prime messagestore.

The utility to produce the messagestore will be invoked from the ARQ GUI and run on the Audit Server to which he user has connected rebuilding the message store on either the Audit workstation from which the request has been issued or the Audit Server handling the ARQ

The user will be able to specify

- The Date range for which messages are required
- The FAD codes for which messages are required with an option of ALL
- Whether the existing message store should be cleared prior to running

A separate option will allow the User to clear down the Audit Server messagestore to reclaim space after completion of an ARQ

6.1.5.2 Correspondence Server Rebuild Utility

The utility is required to process ALL of the TMS files (recognised by filename format) in a given directory, inserting relevant information into the Correspondence server dependent on the input parameters

The Utility will have the following interfaces and capabilities: -

- The utility must have a command line interface and be able to be invoked from a Command session

- The utility must be run on an Audit Server
- The directory where the TMS files are stored must be a parameter
- The utility will only process files which match the TMS file name format
- The utility must be able to accept a single date range for extraction to allow messages which fall into the range to be extracted (subject to FAD validation)
- The utility must be able to accept a file of FAD codes, with an option to have a single line specifying ALL
- The utility will extract the messages from the specified files based on the extraction criteria and populate the message store on the Audit Server or Audit Workstation
- Successful or unsuccessful completion of the extraction and reload needs to be notified to the User.

6.1.5.3 Clear Messagestore Utility

The utility will clear down the Audit Server or Audit Workstation Message Store and produce a message store containing only license details.

The utility must have the following interfaces and capability.

- The utility must have a command line interface and be able to be invoked from a Command session
- The utility must be run on an Audit Server
- The utility MUST only operate on the message store contained on an Audit server or Audit Workstation
- The utility must leave the Riposte service running after use

6.1.5.4 Restore Oracle Tables

To enable subsequent filtering and searching files, which contain Oracle, table must firstly be restored to an Oracle Database.

The utility must be invoked from the ARQ GUI on the Audit Workstation

The Audit Archive files will be restored to an oracle database using a utility that accepts input parameters of filename, user details etc, and uses them in addition to the DDL information contained in the Data Mapping Directive records of the archive file to create an oracle table and populate it with the table data from the archive file.

Restoration will be effected by the generic ‘RESTORE’ module, as specified in [ORAUT] running on the Audit Server,

6.1.5.5 Uncompressing Files

Files which have been compressed prior to being copied to the Audit archive will require uncompressing prior to filtering / viewing.

WinZip will be provided on the menu for the Audit workstation for this activity.

6.1.6 Filtering & Viewing

6.1.6.1 Message Store Filtering / Viewing

Extraction of Data must be possible from both the Live Correspondence Servers (Interactive Retrieval) and from the reconstructed message store on the Audit server or Audit Workstation.

These facilities are provided on the Audit Workstation using the RQuery facility available on the Menu

6.1.6.1.1 Interactive Retrieval at Data Centre (Correspondence Server)

Interactive Retrieval at the Data Centre is allowed to facilitate Emergency Access to the Transaction Message Store on the Correspondence Server. The Audit Archive will normally be accessed but the CS Message Store can be accessed where the turnaround time for retrieving the required data from the Audit Archive is unacceptable.

Authorised Fujitsu Services staff will carry out the retrieval & filtering of data.

The use of the CS is only appropriate where the data required is within a given time range, because messages are only held on the CS for a certain number of days. The time limit varies for different application transactions and there is an overall limit of 37 days. Details of the retention period for different messages may be found in the relevant Attribute Grammar catalogues

6.1.6.1.2 Filter Restored Message Store

RqueryUK is to be used to further filter messages in the restored message store.

The data from the Information Request is used to specify a new RqueryUK enquiry or matched to an existing enquiry.

There are preformatted RqueryUK fields to accept the Date From, Date To and Outlet required. All other Filtering Criteria are specified based on EPOSS Attribute Grammar.

Messages that match the filtering criteria are extracted from the message store to file. The current facility extracts filtered messages to an MS Excel File.

The information can then be displayed, tabulated and written to CD for the requestor.

Enquiry templates will be maintained by the user.

6.1.6.2 View / Filter Oracle Tables

Oracle Discover product will be used to view restored archive data. Table Views can be specified to filter table data as required.

Discoverer will be accessible from the menu on the Audit Workstation

6.1.6.3 View / Filter Other Audit Track

The extraction of non-TMS data will be via the filters, views, and search facilities provided with COTS tools. Different filtering facilities need to be configured on the Audit Workstation, to allow the filtering of the restored data to the level requested on the ARQ.

A text-based utility, MS Word's WordPad, will be used to view and search the retrieved files if required.

Windows Explorer also has the capability to search for data strings in many files

6.1.6.4 View / Filter SQL Database Trace Files

SQL Server Profiler will be used to view the SQL trace logs output from SQL server databases. The file extension (.txt) of these files must be manually changed to an extension of .trc to make them compatible with SQL Profiler prior to opening.

SQL Server Profiler will be accessible from the menu on the Audit Workstation

6.1.6.5 NBX Transaction Journal Filtering / Viewing

To enable filtering of NBX transaction journals, they must first be retrieved to the Audit server using the standard Audit Track Extractor. The NBX audit tracks are partitioned using a hash function based on the PAN associated with the transaction. Thus selective retrieval is possible by using the Filename Template feature of the Extractor to identify the subset of Audit Tracks that contain transactions relating to the required PAN.

Even allowing for this partitioning of data a 30-day enquiry will involve searching approximately 1Gb of data. This is too large to transfer to the Audit workstation so a process running on the Audit server will filter this data for records containing the required PAN. A freestanding application, which runs on the Audit workstation, will be provided which performs the following functions:

- Accepts a PAN number and ARQ number as input, calculates the NBX journal hash value and presents the user with the Filename Template string to be cut and pasted into the relevant input field in the Audit Track Extractor.
- Once the NBX Audit Tracks have been retrieved, the application will initiate an Audit Server process to filter the retrieved files for entries containing the required PAN. The workstation application will monitor the progress of the server process and report its success or failure back to the end user.

The corresponding server based application will:

- Accept a PAN and ARQ number as input

- Perform a simple line based search for occurrences of the PAN string in the Audit Tracks in the ARQ directory.
- Produce an output file on the Audit server, containing records that contain the PAN string.

The auditor may then copy the output file back to the Audit workstation, reformat it as appropriate, and submit it to the requestor.

6.1.7 Data Delivery

Data will be delivered to the requester by CD-R media or Floppy Disk for very small volumes (less than 1.4 Mb).

Easy Creator CD will be installed on the Audit workstations accessible from the menu to allow the copying of extracted data to CD.

The user must ensure that the Seal Checking has completed successfully before extracted data is passed to the requestor.

6.2 Distributed Application Services

6.3 Information Management

It is the responsibility of user to manage the movement of data to and from the relevant directories for extraction, retrieval and analysis. Data extracted for an ARQ will be deleted from the Userarea on closure of an ARQ. Any data moved by the Auditor to other locations will NOT be automatically managed.

The Seal Check result must be confirmed before audit data is passed over to the requestor.

6.4 Networking Services

The Audit Server will use the standard Horizon network services.

6.5 Platforms

Appendix B of ref [HLDSR+] defines the hardware requirements of the Audit Server and the Audit Workstation. They will be based on the standard secure NT builds. Detailed implementation work may require modifications to the standard build.

7.0 Systems Management

The Audit Server and the Audit Workstation will be managed via Tivoli, and will be based on the standard Tivoli NT build.

8.0 Application Development

User Interface on Audit Workstation to allow access to NON-COTS Audit Server Applications

ARQ GUI to provide access and maintenance facilities for then ARQ Database

9.0 System Qualities

9.1 Availability

The Audit Data held on an Audit Server is held on a mirrored disk configuration so that a single disk failure will not result in loss of the data.

A given ARQ may be processed on either Audit server. Thus temporary loss of single Audit server will not significantly impact the processing of ARQs.

Multiple Audit Workstations are provided to mitigate against the loss of a single workstation.

9.2 Usability

Where users are required to interact with the Audit Server such interactions are carried out using standard facilities provided by COTS software including Windows NT and Tivoli.

Some of the activities require relatively long elapsed times, e.g. recovery of Audit Tracks from secure storage, to complete. The Windows based facilities provided by the COTS allow other activities to be progressed while waiting for the longer term ones to complete.

The file selection requires a large degree of User Interaction and an understanding of the Audit Archive File formats.

9.3 Performance

The implementation must meet the turnaround times defined in [SMSD]

Clearly the broader the date range the larger the extraction is likely to be. Additionally, more complex extraction criteria will have a greater impact on performance.

The file identification process is largely a manual process and will rely on the translation of the end-user view of the data to an Audit View of the data, which is based on physical directories. If a large number of files have to be retrieved, which potentially contain the information required, it may take a long time to locate the exact file(s) wanted. Staff availability may impact on the achievement of turnaround times.

9.4 Security

As defined in Audit Storage & Retrieval HLD ref [HLDSR+], section 8.4.

9.5 Potential for Change

- When detailed Audit Information Requests and Audit Reports are specified by, POL and POL Clients, detailed analysis can be carried out to determine
  - If specific extraction and filtering facilities need to be developed for non-TMS audit data.
  - The detailed extraction parameters required for TMS data, prior to filtering by RQueryUK

- All CSR+ changes require assessment in terms of how the data needs to be retrieved for audit requirements. This may impact extraction/filtering and storage facilities.

10.0 Migration

N/A

11.0 Solution Implementation Strategy

N/A

12.0 Costs Risks and Timescales

1. The architecture of the Audit Server and its HLD support the retrieval times specified in Audit Data Retrieval Requirements, [REQBI3], not those specified in Audit Trail Functional Specification, [ATFS].
2. Although the Audit Server has been sized to cope with BI3 workloads there is a risk that the actual implementation will require a more powerful platform to be introduced post BI3 if there should be any significant increase in the workload due to new applications (e.g. Network Banking).