FUJ00123758

Document Title: Audit Data Retrieval High Level Design

Document Type: High Level Design

Release: N/A

Abstract: This document describes the Audit data extraction & filtering facilities within HNG-X

Document Status: APPROVED

Author & Dept: Alan Holmes

Internal Distribution:

External Distribution:

Approval Authorities:

Name	Role	Signature	Date
Adam Spurgeon	Solution Design		
Graham Allen	Development		
Alan Holmes	Architecture		

Note: See RMGA HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

FUJ00123758

0 Document Control

0.1 Table of Contents

FUJ00123758

0.2 Figures and Tables

FUJ00123758

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	13/12/2006	Initial draft. Content taken from the equivalent Horizon document SD/HLD/002	
0.2	11/05/2007	Second draft. Includes changes resulting from comments received on version 0.1 and PCI changes CP4305	
0.3	02/02/2009	Changes resulting from review of version 0.2 Changes resulting from E2E group review of the parent architecture document ARC/SVS/ARC/0001 Changes resulting from the following CPs • HNG-X CP0157 – CP4623 • HNG-X CP0299 – CP4810 • HNG-X CP0258 – CP4751 • HNG-X CP0284 – CP4791 Extended migration coverage	HNG-X CP0157 HNG-X CP0299 HNG-X CP0258 HNG-X CP0284
0.4	14/10/2009	Clarification of Anti-Virus product used on the Audit workstation. Address comments received from review of V0.3 Addresses various Peaks (listed)	PC0184551 PC0184537 PC0188605
1.0	30/10/2009	Updated from comments received Issued for approval.	
1.1	25/03/2010	Additional facilities within the Audit extraction system to enable counter system events to be analysed and included as one of the outputs of an ARQ.	HNG-X CP0336
2.0	11/06/2010	Updated following review. Issued for Approval	

0.4 Review Details

Review Comments by :	N/A
Review Comments to :	Alan Holmes & RMGADocumentManagement GRO

Mandatory Review	
Role	Name
Solution Design	Andy Williams
Development	Gerald Barnes
Development	Andrew Mansfield
Architecture	Alan Holmes
Solution Design	David Harrison
SSC	Steve Parker
Business Continuity	Adam Parker

FUJ00123758

SV&I Manager	Chris Maving
LST	John Rogers
Optional Review	
Role	Name
Chief Information Security Officer	Tom Lillywhite
Security & Risk Team	CSPOA.Security GRO
Programme Manager	Geoff Butts
Applications Architecture	David Johns
System Qualities Architecture	Dave Chapman
Architect	Jason Clark
Security Architect	Tom Lillywhite
Test Design	George Zolkiewka
Head of Service Management	Gaetan van Achte
Head of Service Change & Transition	Graham Welsh
Service Support	Kirsty Gallacher
Service Network	Ian Mills
Data Centre Migration	Vince Cochrane
Integration Team Manager	Peter Okely
Testing Manager	Debbie Richardson
LST Manager	Sheila Bamber
RV Manager	James Brett (POL, JTT)
POL Design Authority	Ian Trundell (POL, via Document Control)
VI & TE Manager	Mark Ascott
Integrity Testing	Michael Welch
Core Services	Ed Ashford
Core Services	Andrew Gibson
Business Architect	Gareth Jenkins
Development	Graham Allen
Solution Design Architect	Sarah Selwyn
Software & Solution Design Developer	Stuart Honey
Service Manager - Retail and RMGA	Claire Drake
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001			Fujitsu Services RMGA HNG-X Document Template	Dimensions

FUJ00123758

Reference	Version	Date	Title	Source
(DO NOT REMOVE)				
SD/HLD/002			Audit Data retrieval HLD (Horizon)	PVCS
AD/DES/042			High Level Design of Common Agents	PVCS
ARC/APP/RTM/0005			Requirements Traceability Matrix for Support Services	Dimensions
ARC/GEN/REP/0001			HNG-X Glossary	Dimensions
ARC/SEC/ARC/0003			HNG-X Technical Security Architecture	Dimensions
ARC/SVS/ARC/0001			HNG-X Architecture – Support Services	Dimensions
CR/FSP/006			Audit Trail Functional Specification	PVCS
DES/APP/HLD/0020			Branch Database High Level Design	Dimensions
DES/APP/HLD/0030			Audit Data Collection & Storage High Level Design	Dimensions
DES/PPS/PPD/0035			HNG-X Audit Server (ARC) - Physical Platform Design	Dimensions
DES/PPS/PPD/0037			HNG-X Audit Workstation (AUW) - Physical Platform Design	Dimensions
DES/SEC/HLD/0002			HNG-X Crypto Services High Level Design	Dimensions
DES/SEC/HLD/0011			HNG-X Anti Virus High Level Design	Dimensions
DES/SEC/IFS/0001			HNG-X Cryptographic Applications Programming Interface Specification	Dimensions
DEV/APP/LLD/0071			Audit Data Retrieval Low Level Design	Dimensions
DEV/APP/SPG/0016			Audit Extraction Client Support Guide	Dimensions
DEV/APP/SPG/0020			Audit Server Support Guide	Dimensions
DEV/GEN/MAN/0015			Audit Extraction Client User Manual	Dimensions
DEV/INF/ION/0001			Audit Server Configuration	Dimensions
DEV/INF/ION/0008			Audit Server Migration Configurations	Dimensions
DEV/INF/ION/0009			Audit Server Schedule Design	Dimensions
IA/PRO/004			Audit Data Extraction Process	PVCS
SD/IFS/014			Audit to Tivoli Cluster Information Interface Specification	PVCS
SVM/SDM/SD/0017			Security Management Service - Service Description	Dimensions
			Extensible Markup Language (XML) 1.0	IRRELEVANT

FUJ00123758

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

0.6 Abbreviations

Abbreviation	Definition
ARQ	Audit Record Query
AS	Audit Server
ATE	Audit Track Extractor
ATR	Audit Track Retriever
ATS	Audit Track Sealer
BRDB	Branch Database
COTS	Commercial off the Shelf
CSV	Comma Separated Values
EMC	Company that supplies resilient disk technology
FAD	Finance Accounts Division
FS	Fujitsu Services
FTMS	File Transfer Managed Service
HNG	Horizon Next Generation replacing current Baseline Horizon solution
HNG-X	Horizon Next Generation – Plan X
KEL	Known Errors Log
NBS	Network Banking Service
NBX	Network Banking Service – Horizon Implementation
NPS	Network Persistent Store
NSP	Atalla Network Security Processor
NBSC	National Business Support Centre
OBC	Operational Business Change
PAN	Personal Account Number
PCI	Payment Card Industry.
PCI DSS	Payment Card Industries Data Security Standard. A set of security controls defined by the Payment Card Industry organisation.
PO	Post Office
Post Office	Post Office Limited
RAG	Riposte Attribute Grammar
RDDS	Reference Data Distribution System
RDMC	Reference Data Management Centre
RDS	Post Office Reference Data System
RDT	Reference Data Team - the Post Office and Fujitsu Customer Services teams use the RDT environment to validate and verify the reference data associated with business changes.
SLT	Service Level Target
SYSMAN	The systems management environment.
TES	Transaction Enquiry Service
TMS	Transaction Management Service. Used within the Audit system to refer to Riposte audit data.
TWS	Tivoli Workload Scheduler
XML	Extensible Markup Language

0.7 Glossary

See *HNG-X Glossary (ARC/GEN/REP/0001)*

Term	Definition
Baseline Horizon	the existing solution being re-architected
Branch	Post Office outlet identified by a unique Branch Code. Within the HNG model, a

FUJ00123758

Term	Definition
	Branch is a logical entity that can be composed of several physical locations at which business is transacted.
Cardholder Data	The PAN, Cardholder name, Service code & Expiration date information relating to a payment card
Hydra	The name given to the live Post Office Account system during that period of the HNG-X migration after the Data Centre Migration, but before the Branch Migration completes
Operational Services	Those services that are needed to run the Horizon system that are not directly supporting the Post Office business. Examples include software distribution, audit, security management etc.
Sensitive Authentication Data	The full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.), Any data element extracted from the magnetic stripe other than Cardholder Name, PAN, expiry date and service code, and Encrypted PIN blocks.

0.8 Changes Expected

Changes
Any future revision of this document should include an additional section which details the test impact of the documented changes.

0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

FUJ00123758

1 Introduction

Within the HNG-X 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 HNG-X system is described in *HNG-X Architecture – Support Services* (ARC/SVS/ARC/0001). 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 also includes details of the changes to the Audit system required for CP4305. The only impact of this change to the Audit system is that PANs, which are classified within PCI DSS as 'cardholder Data', are no longer stored in clear text form within Audit Tracks. Thus the Audit system requires a mechanism to handle hashed and/or encrypted PANs where they form a part of retrieved Audit data.

This version of the document includes details of changes for HNG-X CP0336. As part of the data retrieval process, the archived events generated by counters at the branch are also analysed to identify any possible occurrences of problems which might adversely affect the integrity of the transaction data. HNG-X CP0336 integrates this process into the mainstream Audit retrieval applications.

This document is based upon the equivalent Horizon document SD/HLD/002.

FUJ00123758

2 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 Audit data from the Audit archive
- Seal Checking to ensure extracted files have seals intact
- Maintenance & Monitoring of Audit Record Queries (ARQs)
- Server based tools to filter high volume data
- Presentation to Auditor, tools to present data in required format
- The interfaces between the Audit server based applications restoring the Audit Tracks and the Audit Data Extraction facilities on the Audit workstation

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* (DEV/INF/ION/0001).

The scope of this HLD does not cover:

- Specification of Information Requests, this is defined in *Audit Extraction Client User Manual* (DEV/GEN/MAN/0015)
- Online access to live data to support Internal Audit
- The analysis/interpretation of Audit Tracks to provide specific Audit Trails

Minimum changes are expected to be made to the Horizon Audit applications as part of the migration to HNG-X. Specific changes which are required for HNG-X and which are covered in this document are:

- Replacement facility to analyze Horizon Riposte Audit tracks
- New facility to analyze HNG-X Branch database Audit tracks
- Changes to handle hashed and encrypted PANs as part of CP4305
- Changes to support server side filtration of Tivoli event data which is integrated in with HNG-X & Horizon branch data retrieval requests. HNG-X CP0336

FUJ00123758

3 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 HNG-X Subsystems. This HLD includes design features to interface to and support existing system features.

The Audit Architecture as defined in *HNG-X Architecture – Support Services* (ARC/SVS/ARC/0001) identifies the need to be able to cope with change as the usage of the HNG-X 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.

FUJ00123758

4 Requirements

Incoming requirements will be captured in the Support Services Topic Architecture SRS. The *Requirements Traceability Matrix for Support Services* (ARC/APP/RTM/0005) will identify where the requirement is explicitly addressed within an HLD.

FUJ00123758

5 System Overview

HNG-X Architecture – Support Services (ARC/SVS/ARC/0001) describes the overall audit system design for HNG-X. 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 Audit archive data via an Audit Workstation. The Audit Workstation is dedicated to this task.
- 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 manipulate 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 HNG-X system including:

- Post Office Counter messages and transactions
- Systems Management Facilities – primarily application, system & security events
- Database Hosts (including the Reference Data System)
- FTMS Gateways
- System Scheduler logs
- Logging of activities undertaken by support staff while maintaining the system
- NPS database audit data

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

Figure 1 gives an illustration of the major components of Audit sub-system on a single Campus. The configuration is duplicated on both the live and standby data centres.

FUJ00123758

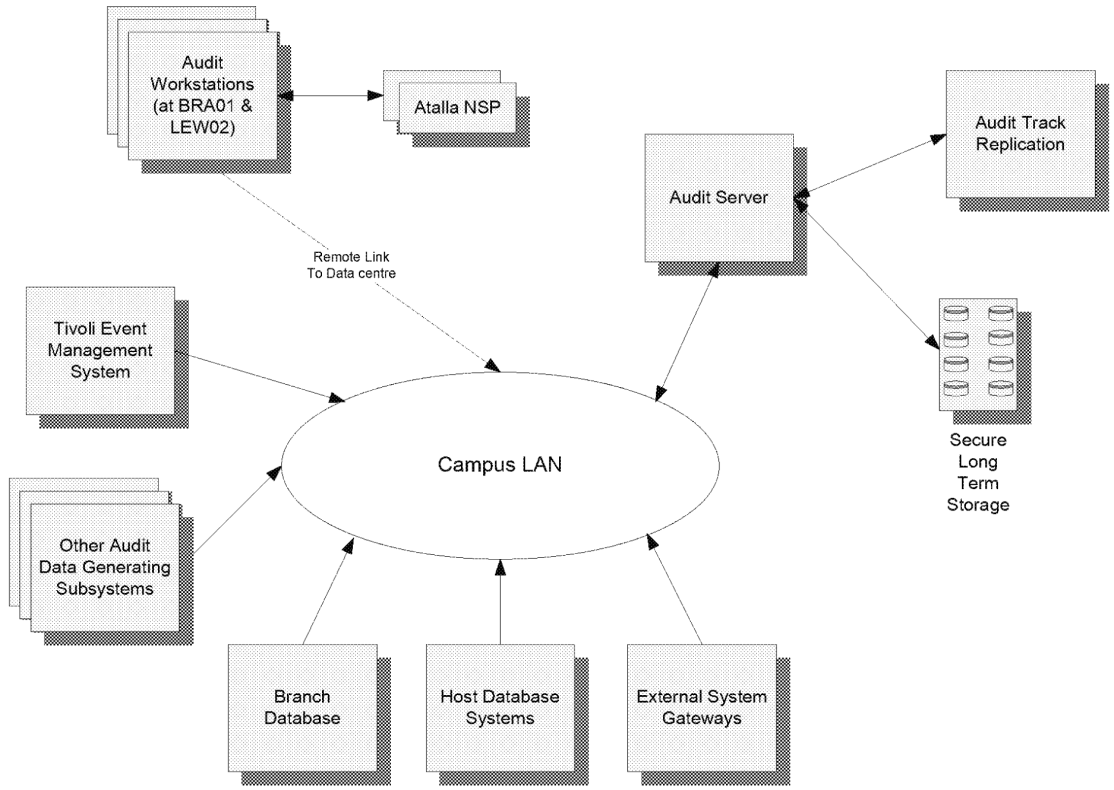

Figure 1- Audit system context

5.1 Audit Server

The Gathering & Storage components of the Audit Server are defined in *Audit Data Collection & Storage High Level Design* (DES/APP/HLD/0030).

The Audit Track Retriever component operates on the Audit server & provides support for the retrieval of data from the Audit archive when requested by the Audit extraction components.

The Audit Track Extractor component, consists of a number of utilities that extract and filter 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 Post Office counters. Transaction records relating to a specific outlet can be interrogated using a comprehensive query system. Additionally the system events logged by counters at the outlet can be analysed to determine if any problems occurred at the outlet which could cast doubt over the integrity of the transaction data.
- A utility to interrogate data which relates to Network Banking transactions. Transaction records which relate to a specific PAN can be isolated.
- 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.

FUJ00123758

- Tools to assist in the analysis of hashed and encrypted PANs which have been stored within Audit Tracks
- COTS tools to view and analyze ad hoc types of extracted data
- Tools to filter audited system events which originated from a given HNG-X or Horizon outlet plus, in the case of HNG-X, the Branch Access Layer servers.

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. The Audit workstation is dedicated to this task.

Access is via the standard user interface provided by Windows XP. A 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 filtered before files containing the relevant records are transferred to the Audit Workstation. Additional browse and filter tools will be configured on the Audit Workstation where subsequent searches/filters on files may be performed.

WordPad is provided to browse simple unstructured text files. Microsoft Office 2003 is provided to analyze other types of file. In particular Microsoft Excel may be used to perform local analysis of retrieved data.

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 HNG-X system. Instead nominated Fujitsu Services personnel will supply audit information as requested by Post Office.

Audit workstations are sited at two Fujitsu sites – there are five Audit workstations at BRA01 and two at LEW02. Each of the two Audit workstation locations has a dedicated Atalla NSP which is used, by the workstation, to decrypt PANs contained within Audit Tracks which relate to banking or payment card transactions.

5.3 Audit Archive

The Audit Archive is held on an EMC Centera, this data is replicated to the remote data centre. Audit Tracks generated on each campus are added to the local copy of the archive.

A more detailed description is defined in *Audit Data Collection & Storage High Level Design* (DES/APP/HLD/0030).

FUJ00123758

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 HNG-X system. This is intended to help reduce the knowledge that auditors need of the details of the way HNG-X 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. Due to the distributed and resilient nature of the HNG-X 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 HNG-X 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 HNG-X system and to assist the Fujitsu Services Auditors in locating the files containing the relevant data to support any particular audit activity.

FUJ00123758

6 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. These are described in the following sub-sections.

6.1.1 Audit Track Retriever

The Audit Track Retrieved is a server side bespoke application which supports the retrieval of Audit Tracks from the Audit archive.

Figure 2 identifies the main interfaces to the Audit Track Retriever (ATR)

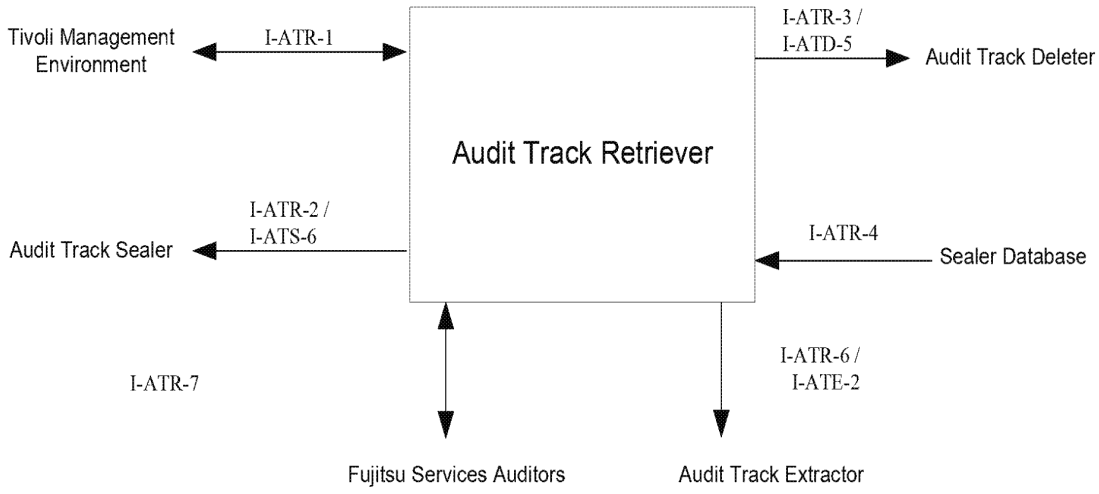

Figure 2- Interfaces to the Audit Track Retriever

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 TWS scheduling.

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

I-ATR-2 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 seal checked. Files to be seal 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.

FUJ00123758

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 to the Sealer SQL Server 2000 database. This database contains details of all archived Audit tracks held by the Audit server.

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. This deletion will occur when the relevant ARQ is closed.

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 bespoke 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 its original format, is likely to be requested in its entirety with no further extraction of specific records required. Files containing transaction data generated by Post Office Counters, due to how they are generated, may contain data associated with many outlets, are less likely to be required in their 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 date based 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 and Monitoring of Audit Record Queries (ARQs)

FUJ00123758

- Online extraction of data from the Audit Archive
- Seal Checking to ensure extracted files have seals intact
- Server based tools to filter Audit Tracks
- Workstation based tools to analyze and present audit data in required format
- Ability to copy extracted data to CD-ROM for delivery

6.1.2.1 ATE Interfaces

Figure 3 identifies the main interfaces to the Audit Track Extractor (ATE)

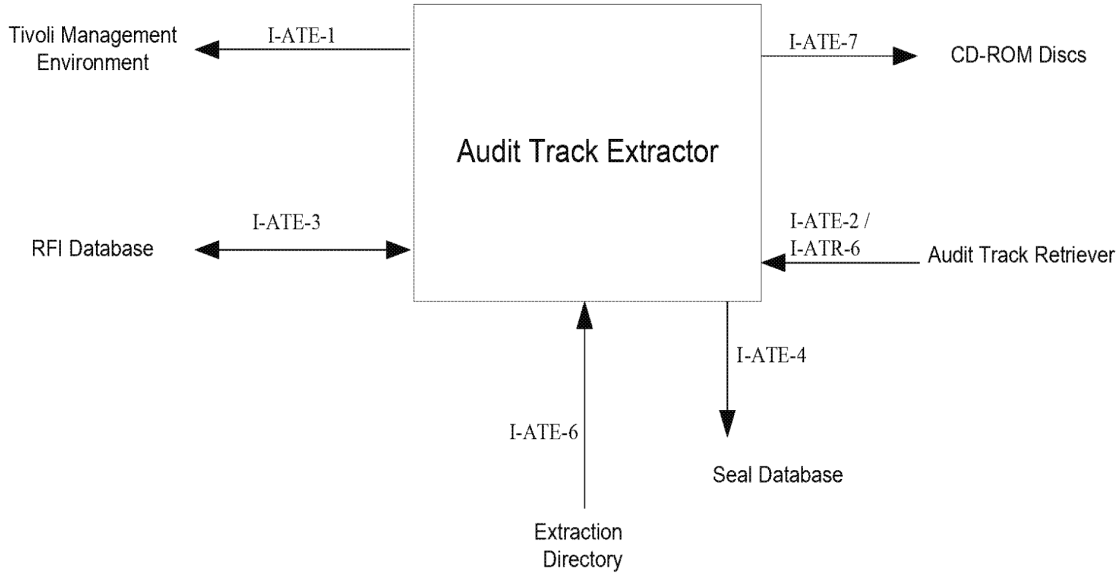

Figure 3 - Interfaces to the Audit Track Extractor

I-ATE-1 Interfaces to the system administration staff and facilities are all via the Tivoli Management Environment. This consists of remote access for administration purposes and event monitoring.

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 from the workstation applications to the SQL Server ARQ Database where ARQ and associated file information is stored. Updates to ARQ details are made from the workstation applications.

FUJ00123758

I-ATE-4 This is the interface to link to the Audit Seal Database (This database contains details of all archived Audit tracks held by the Audit server) to allow the status of Seal Checks to be interrogated via the GUI.

I-ATE-6 This is the interface between the Auditor using the tools to View and Filter data held in the extracted directory on the Audit Server. Filtered audit track data will pass across this interface.

I-ATE-7 This is the interface between the Auditor and the CD-Writer device to write analysed audit track data for use by external Auditors. This interface is implemented using standard Windows XP CD burning functionality.

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. Access to the Audit Extractor Client is provided by a Start Menu option.

The User name associated with the extractor client session is taken from the current logged on user name; there is no requirement for the user to log on to the extractor client.

The GUI will initially provide options to

- Create a new ARQ
- Open an existing ARQ
- Close an existing ARQ
- Monitor the progress of server based retrieval & analysis tasks

Details of ARQs are stored on a Microsoft SQL Server 2000 database resident on the Audit Server's local storage.

6.1.3.1 Creation of a New ARQ

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

The user will be required to enter various control information relating to the ARQ: -

- The data centre at which the retrievals are to be performed
- Requester Id, from a selection of pre-defined values comprising:
    - Other 3rd Party
    - POA Internal Audit
    - POA Other
    - POA SSC
    - POL Internal Audit
    - POL Other
    - POL Security
- Catalogue Entry - Optional

FUJ00123758

- 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.
- In the case of a retrieval of branch transaction data, specify whether system events for the branch are also to be retrieved & analyzed.
- Cancel the request

6.1.3.2 Creation of a New Fast ARQ

As an alternative to opening a new conventional ARQ, a new ARQ may be opened in 'Fast mode'. This offers a much simpler user interface & a more streamlined workflow where branch transaction data is being retrieved.

When a new Fast ARQ is opened, a single form is presented allowing the following information to be entered.

- Requester Id – See above
- Receipt Reference – See above
- Request Date – See above.
- Required Date - See above.
- Filter start & end dates – The data range for the analysis. For extraction purposes, there is an option to add extra days onto the end date to allow for where data has been gathered late.
- FAD code – the Branch Accounting code
- Whether system events for the branch are also to be retrieved & analyzed.
- The set of queries to be run against the retrieved data.
- Output Folder - The location (on the audit workstation) where the resulting spreadsheets are to be written

Once all required data is entered, the ARQ may be executed & will, in the background:

- Retrieve all the data required
- Run the requested queries
- Execute the event filters if selected
- Generate the required spreadsheets on the workstation.

Status information will be displayed on the user interface showing progress through the above phases.

If a Fast ARQ is closed before it has reached the end of its normal execution, it will not be possible to subsequently reopen it and allow it to continue. It will be necessary to close the ARQ and open a new one.

FUJ00123758

It is anticipated that the Fast ARQ approach will be usable for the majority of retrievals of branch transaction data. There will however be exceptional cases where the finer control offered by the conventional ARQ is required.

6.1.3.3 Opening an Existing ARQ

The user will be able to select existing ARQs (at a given data centre) and open them to progress file retrieval and analysis.

A list of the ARQs available at the selected data centre will be presented to the user. This list will only contain open ARQs

Once an ARQ is selected & reopened, the user is able to progress the ARQ through to completion.

Note that if an existing ARQ was originally opened as a Fast ARQ, if it is closed & reopened, no further updates may be made to the ARQ. When it is reopened the Fast ARQ form is displayed, read only with all originally entered data.

6.1.3.4 Closing and Cancelling an ARQ

The user will be able to select existing ARQs (at a given data centre) and close them, preventing any further activity on the ARQ.

A list of the ARQs available at the selected data centre will be presented to the user. This list will only contain open ARQs.

No further amendment to an ARQ will be permitted after it is closed.

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 shared Userarea filestore on the Audit Server along with other internal files relating to the ARQ.

An audit file (which is written to the Audit archive as part of the Audit servers own internal audit trail) will be produced giving the following details of the ARQ: -

- 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

6.1.3.5 ARQ Status Monitoring

The ARQ status display will show current state of all open ARQs (across both data centres). The status values shown will only relate to server based actions undertaken on behalf of each ARQ, this will include:

- Audit Track retrieval
- Audit Track seal checking
- Server based filtration & analysis

Only the status for the most recently initiated server action will be shown on the initial display. It will be possible to drill down into an individual ARQ to show additional information relating to preceding server actions.

FUJ00123758

6.1.3.6 File selection criteria

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

The *Audit Server Configuration* (DEV/INF/ION/0001) 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 within 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.
- 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, a branch FAD code. This will automatically determine the relevant Audit point / Sub-Points which contain transaction data generated by the outlet. This will require retrieving a subset of data from the audit points containing both Horizon Correspondence server data and HNG-X data Branch database data depending upon the date the branch migrated to HNG-X. See sections 6.1.3.6.1 & 6.1.3.6.2
- In the case of a retrieval of branch transaction data (i.e. where a FAD code was entered), specify whether system events for the branch are also to be retrieved & filtered.

Once the above fields have been supplied the user may initiate the search for files that match the search criteria.

6.1.3.6.1 Branch Cluster Determination – Horizon Correspondence Server Data

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 Correspondence server cluster an outlet's messages will have been created on for the requested Date Range.

For Horizon counters, 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 *Audit to Tivoli Cluster Information Interface Specification* (SD/IFS/014).

- The Tivoli Web page will be accessed from the Audit Server
- The outlet required will be provided as a six character branch Id 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.

FUJ00123758

The Audit system will require continued access to this branch to cluster mapping information for seven years after the last Horizon counter is migrated to HNG-X. The Tivoli cluster information server used by the Audit system will disappear at the end of Hydra. Until this time, the cluster mapping data will be volatile and the Audit system will require access to the dynamic data held within the Tivoli cluster information service. After this time, the data will be static and it will be imported into the Audit ARQ database. The Audit system will then look up the mapping directly from its database. See section 6.1.4.6

Within each cluster, TMS audit data is further divided into eleven separate streams based on application of a hash function to the Branch Id. There are four Correspondence server clusters, thus the set of files that need to be retrieved to contain all data relating to a branch is ≈1/44th of the total volume of TMS audit data for the period under analysis. The Branch ID hash function returns the following results:

- 'X' - for non outlet data
- [0-9] - for branch data based on the 3rd digit of the 6 digit Branch Id

The hash value is embedded in the Audit Track file names generated by the harvesting agents. This is further described in *High Level Design of Common Agents* (AD/DES/042)

This function is only applicable to data generated by Horizon Counters.

6.1.3.6.2 Branch Hash Value Determination - HNG-X Branch Database Data

An equivalent function to that described in section 6.1.3.6.1 is also necessary to limit the volume of retrieved data which originated at HNG-X outlets.

Within the HNG-X Branch Database each branch is allocated a hash value ranging from 0 to 127. This is used internally within the BRDB to partition data. The hash allocation remains constant for the life of the branch. This hash value is also used to partition the audit data generated by the BRDB. A separate audit stream is generated for each of the 128 possible hash values, each stream containing audit data for all branches which map to the hash value associated with the stream. Data within a given stream may be further partitioned, to ensure that an individual Audit Track file size is within the advisory limit for the Audit system of ≈100MB. This process is further described in *Branch Database High Level Design* (DES/APP/HLD/0020).

When the Audit retrieval system needs to retrieve BRDB data relating to a particular branch, it derives the branch hash value from the branch Id & only retrieves (from Centera) data for the correct audit stream.

The audit system derives the branch hash value, from the branch Id, by direct look up from table *brdb_fad_hash_outlet_mapping* in the BRDB.

This function is only applicable to data generated by HNG-X Counters.

6.1.3.7 File Retrieval facilities

The files that match the search criteria are displayed on the 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)

FUJ00123758

- 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 server based processing of retrieved data

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

6.1.4 ARQ Database

This section contains a brief overview of the content of the ARQ Database. For full details of the database structure sees *Audit Data Retrieval Low Level Design* (DEV/APP/LLD/0071)

6.1.4.1 Overview

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

A separate database 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 schedule.

The ARQ database will contain the following information: -

- Details of information Requesters
- Details of Requests for Information (ARQs) and their associated files and query requests
- Details of valid users of the Audit facilities
- Details of Audit points and Audit Subpoints
- Horizon FAD to cluster mapping (post Hydra)
- Client-Server interface management

6.1.4.2 Requesters Data

The data recorded in the database 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. POA, POL etc.)

Table 1 - Requesters Data

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.

FUJ00123758

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
Events filtration	Whether Event data is to be included in the analysis
Fast ARQ flag	Indicates that this ARQ is a 'fast ARQ'

Table 2 - ARQ Data

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 lists in the Retrieval User Interface.

These tables will be synchronized automatically (on a daily basis) with the Audit Server Configuration to ensure that they contain an up to date view of the system configuration.

6.1.4.5 ARQ File and Query Status

The user will be able to monitor the status of files and queries utilised to satisfy an ARQ

6.1.4.6 Horizon FAD to cluster mapping

When performing Horizon TMS data retrievals, the Audit system will require access to branch to cluster mapping information. The Tivoli cluster information server used by the Audit system will become obsolete when all SYSMAN2 functionality is removed from the solution. Until this time the Audit system will require access to the data held within the Tivoli cluster information service. After this time, the data will be

FUJ00123758

static and it will be imported into the ARQ database. The Audit system will then look up the mapping directly from its database.

The following data will need to be modelled in the database:

Field Name	Definition
FAD	Six character FAD code of the branch.
Status	The status of this branch (at the point of data import). Possible values are: NOT_FOUND – FAD not found in Oracle table. NOT_LIVE – No installation date (with no removal date) for any counters. CLOSED – Set to permanently closed by OCMS. LIVE – At least one counter is installed (with no removal date). TEMPORARY_CLOSURE – Set to temporarily closed by OCMS.
Cluster Id	Cluster id in range 1..4
Start Date	The date the branch was assigned to this cluster
End Date	The date the branch was assigned removed from this cluster. Not present if this was the active cluster at the time of data import.

Table 3 - Horizon FAD to cluster mapping

See *Audit to Tivoli Cluster Information Interface Specification* (SD/IFS/014) and section 6.1.3.6.1 for further information.

6.1.4.7 Client-Server Interface

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

- Recover files
- File status
- Get cluster/hash Id
- Query branch transaction data
- Query NBX data
- Close ARQ
- Create ARQ

6.1.5 Extraction Tools

6.1.5.1 Uncompressing Files

Files which have been compressed at source prior to being gathered by the Audit archive will require manually decompressing prior to analysis or viewing. WinZip will be provided on the menu for the Audit workstation for this activity.

FUJ00123758

An exception to the above rule is Branch database counter transaction data which is automatically decompressed during retrieval by virtue of the PreCompress parameter in the Audit server configuration file. See *Archive Server Configuration* DEV/INF/ION/0001

6.1.6 Filtering & Viewing

6.1.6.1 Branch Transaction Data Query

This feature enables branch transaction data for a specified Branch to be analyzed using customisable queries. A set of branch transaction Audit tracks (which could contain Horizon and/or HNG-X branch database data) must have been retrieved & seal checked prior to invoking this function.

- Manage sets of user queries
- Confirm the integrity & completeness of the data
- Execute equivalent queries against both Riposte & HNG-X transaction data
- Perform System event filtration
- Import the query results into Microsoft Excel workbooks

All functionality that involves processing large volumes of retrieved audit data will be deployed on the Audit server in order to minimise the volume of data that needs to be transferred to the Audit workstation.

The facility is described in greater detail in *Audit Data Retrieval Low Level Design* (DEV/APP/LLD/0071).

This is process is summarized in Figure 4

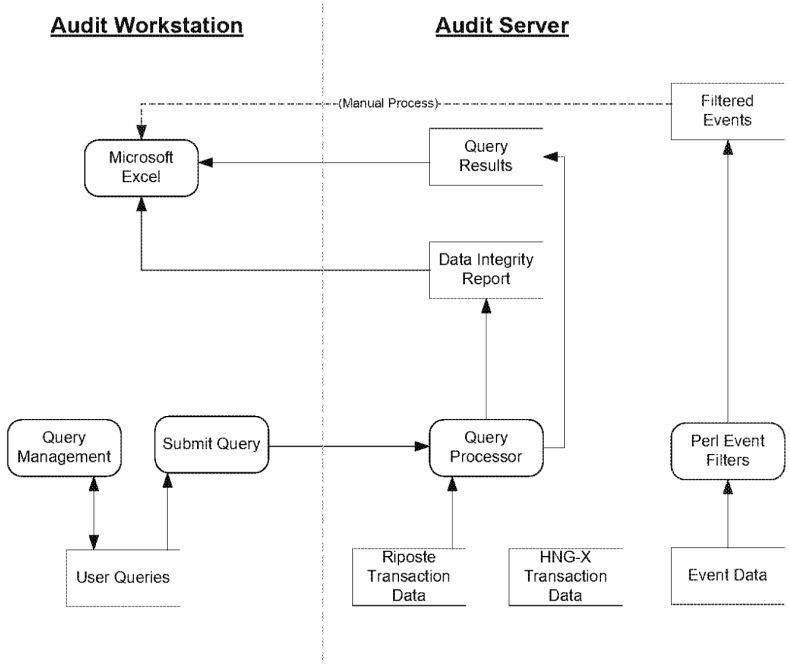

Figure 4 - Branch Transaction Query Overview

FUJ00123758

6.1.6.1.1 User Query Management

The Audit workstation will enable the user to maintain a set of queries that can be executed against branch data. The user will be able to perform the following management operations on those queries.

- Create new queries
- Save named queries to filestore
- Load named queries from filestore
- Edit queries
- Maintain a set commonly used queries which can be quickly loaded via selection from a list

The user will be able to select the location where queries are to be stored to or loaded from. Queries will, in general, be shared between all audit workstations - thus the user will typically store queries centrally.

Matched pairs of queries will be managed, one of the pair will operate on HNG-X transaction data and the other will perform an equivalent query upon Riposte transaction data.

6.1.6.1.2 Query Submission

When, as part of an ARQ, a set of audit tracks have been successfully retrieved and seal checked, the user may load a query and execute it against the audit tracks associated with the ARQ.

The query will be submitted to the Audit server based Query Processor. Execution of the query will operate asynchronously. The user will monitor progress of the query using the standard Audit Extractor mechanism used to check the status of server actions.

Queries will be automatically constrained to only return data for the single Branch Id that was used to select audit tracks for retrieval – see section 6.1.3.6.

Once the server has completed the execution of the query, the user may open the results of the query using Microsoft Excel. If required, any further analysis of the data may be undertaken using standard Excel features.

The server will also generate a report on the integrity and completeness of the source data. This will be included in the Excel spreadsheet as a separate worksheet.

6.1.6.1.3 Query Processor

The Audit server based Query Processor will accept and process Branch transaction data queries from the Audit workstation. The process will support the following functionality:

- Operate within the context of an ARQ
- Accept a query and branch Id as input
- Process both HNG-X and Riposte Audit tracks, producing separate reports for each
- Perform an initial filtration of the audit tracks
- Perform Event filtration
- Perform integrity checks on both types of audit tracks, producing summaries of the results of the check. See §6.1.6.1.3.3
- Apply the supplied queries to the filtered data, producing Excel compatible results files. Separate results files are produce for HNG-X & Horizon data.

This logical view of this functionality is given in Figure 5

FUJ00123758

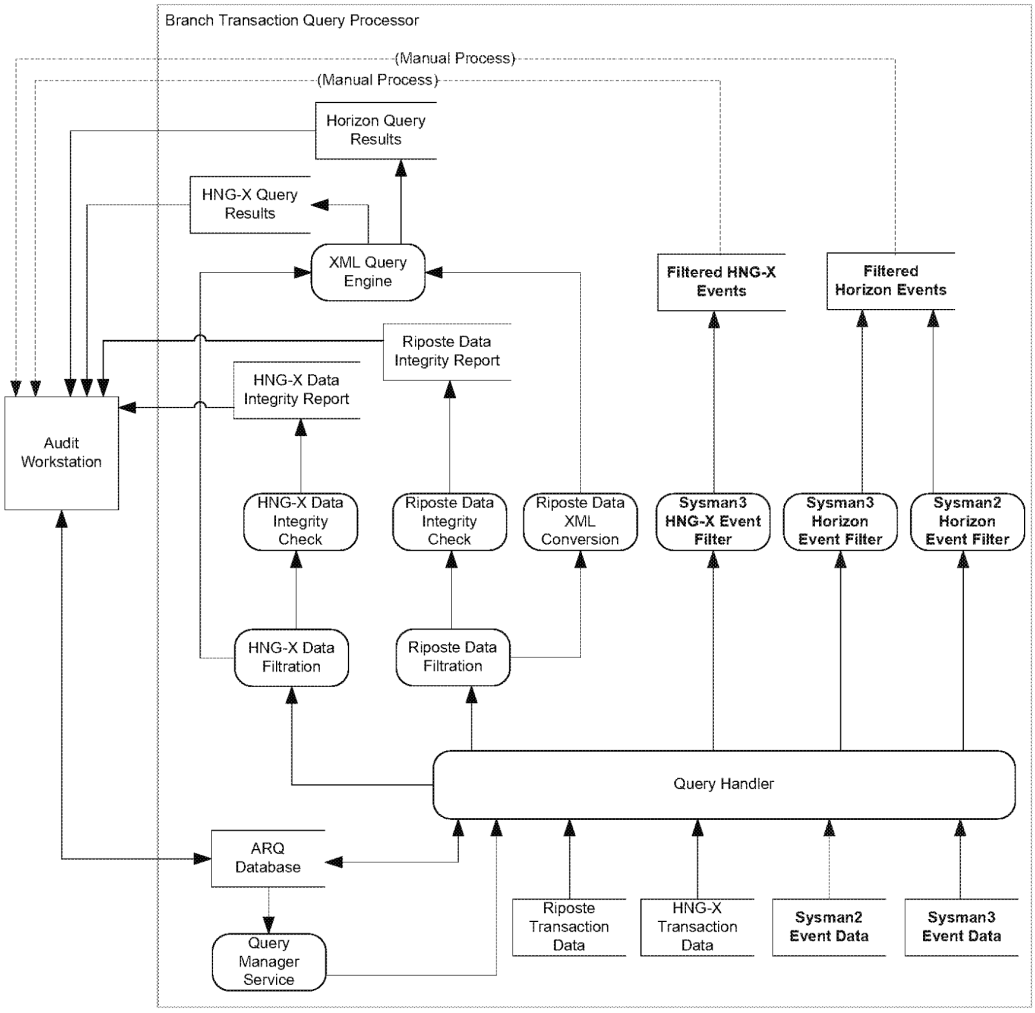

Figure 5 - Branch Transaction Query Processor

6.1.6.1.3.1 Query Manager Service

The Query manager is a windows service that monitors the ARQ database for new query requests & launches new Query handler instances to process them

6.1.6.1.3.2 Query Handler

The Query Handler manages the processing of the query. It is responsible for:

- Accepting the initial request
- Maintaining the status of the process in the ARQ database
- Differentiating Riposte & HNG-X audit tracks
- Manage the subsequent processing of the data

FUJ00123758

As HNG-X and Riposte audit data will be fundamentally different in both structure and field naming, each query will be composed of two parts – a Riposte and a HNG-X version. The correct part of the query will need to be passed to the query engine according to the type of audit track being processed.

The end user will not need to be aware of the Horizon – HNG-X migration date of the branch in question. The system will determine this by querying the Branch database and retrieve the appropriate type of Audit tracks.

When retrieving data relating to branch transactions, the retrieval system must potentially retrieve both Horizon & HNG-X Audit tracks for the branch & date range specified if the query dates span the branch migration to HNG-X. The date that a Branch migrated from Horizon to HNG-X is available in the Branch database.

6.1.6.1.3.3 Data Integrity Checks

The following integrity checks will be applied to the data

- Completeness of data – contiguous message sequence numbers
- Integrity of individual messages
    - For Riposte data the message CRC should be checked
    - For HNG-X data the message signature will be verified

Separate Riposte & HNG-X summaries of the results of the integrity checks are generated. They should detail:

- Summary of the message sequence runs broken down by counter Id. This should include start & end date/times and start & end message sequence numbers. Any gaps in the message sequence runs must be highlighted.
- Summary of messages that have failed individual message integrity checks

Any failure of the data integrity checks will not prevent subsequent execution of the query. The audit workstation user will be warned of the failure via the server process status notification mechanism.

6.1.6.1.3.4 Riposte XML Conversion

Riposte audit tracks will be Riposte Attribute Grammar (RAG) format. In order that a common query engine may be used, they will be converted to XML format. The following considerations need to be made during this conversion.

Valid XML element names must conform to the following:

```
NameStartChar ::= ":" | [A-Z] | "_" | [a-z] | [#xC0-#xD6] | [#xD8-#xF6] | [#xF8-
#x2FF] | [#x370-#x37D] | [#x37F-#x1FFF] | [#x200C-#x200D] | [#x2070-#x218F] |
[#x2C00-#x2FEF] | [#x3001-#xD7FF] | [#xF900-#xFDCF] | [#xFDF0-#xFFFD] |
[#x10000-#xEFFFF]

NameChar      ::= NameStartChar | "-" | "." | [0-9] | #xB7 | [#x0300-#x036F] |
[#x203F-#x2040]

Name          ::= NameStartChar (NameChar)*
```

The rules for RAG attribute names are less restrictive – They can be comprised of any printable characters excluding those in the set {whitespace | ':' | '.' | '<' | '>' }. Thus some RAG objects will need to be renamed during conversion.

Valid data within an XML document consists of characters in the following range:

```
#x9 | #xA | #xD | [#x20-#xD7FF] | [#xE000-#xFFFD] | [#x10000-#x10FFFF]
```

FUJ00123758

There are isolated examples within existing Riposte data where RAG attribute values contain non-printable control characters outside of the above range. These cannot be represented within XML content, but should be represented in a textual form (e.g. _xnn_;)

See W3C document *Extensible Markup Language (XML) 1.0* IRRELEVANT for further detail on the rules for creating well formed XML documents.

6.1.6.1.3.5 XML Query Engine

The XML Query Engine must provide at least the following functionality:

- Identification of individual fields within a message via a path specifier
- Enable a subset of fields within a message to be selected for output
- Meaningful column headings can be included in the output
- Can handle mixed message types
- Awareness of the following basic data types
    - String
    - Numeric
    - Date
- Output can be sorted on selected fields. The sort process should be type aware
- Supports the following expression types which are used to specify which messages are selected
    - Existence of a field within a message
    - Type aware comparisons using the following operators ({'==', '!=', '<', '<=', '>', '>='}. Comparisons can be against fields or typed literal values
    - Grouping of selection sub-expressions via parentheses to alter the order of evaluation

6.1.6.1.3.6 Event Filters

The Event filters are implemented as Perl scripts. Perl provides a sophisticated regular expression implementation that is capable of filtering on complex criteria. A script based solution has been chosen as it allows the filters to be more readily adapted to include or exclude particular events as required.

The scripts operate by filtering out all events originating from counters at the branch under investigation, then excluding a set of known to be benign Horizon and benign HNG-X events. The resulting sets of events are written to the output file in CSV format. These files can then be manually copied to the Audit workstation and examined using Excel.

There are two sources of Tivoli event audit data, the Horizon OMDB (Sysman2) and the HNG-X EDS (Sysman3) database servers. The format of the audit files produced by these two servers is very different & each needs to be processed by its own filter script.

Note that although Horizon counter events will normally appear in the OMDB audit subpoint, once the branch has had its branch router installed, events from the branch go up the Sysman 3 EDS route. Thus when filtering events for a Horizon branch, both sources of audit data must be searched.

FUJ00123758

6.1.6.2 View / Filter Other Audit Track

The extraction of other (than Branch transaction) 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

6.1.6.3 NBX Transaction Journal Filtering / Viewing

This feature enables high volume Network Banking transaction journals to be searched for entries related to a user specified PAN.

With the introduction of CP4305 into the solution, the NBX journals will no longer contain the PAN in clear text. Instead there will be an encrypted version of the PAN and, in a separate field, a securely hashed version of the PAN. Historic NBX Audit Tracks which are held in the Audit archive will continue to hold the PAN in clear text form.

To enable filtering of NBX transaction journals, they must first be retrieved to the Audit server using the standard Audit Track Extractor. At the point they are extracted from the NPS, the NBX audit tracks are partitioned using a hash function based on the PAN associated with the transaction - 64 separate streams of audit data are written. The hash value is embedded in the Audit Track file name generated by the NPS harvesting process. Thus, assuming a full clear text PAN is available, it is possible to only retrieve the subset of Audit Tracks that contain transactions relating to the required PAN.

The hash function that is currently utilized on Horizon is:

(PAN MOD 64) + 1

which yields results in the range 1-64.

With the introduction of CP4305, the full PAN is not available thus an alternative function is applied to the hashed version of the PAN:

(RIGHT(PAN, 3) MOD 64) + 1

A given retrieval will need to evaluate both possible hash values & retrieve both the corresponding streams of audit data.

Even allowing for this partitioning of data a 30-day enquiry will involve searching a large volume 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.

The workstation application will accept a single PAN number (either in clear or hashed form) as input, calculate the NBX journal hash values and retrieve the relevant NBX journal streams. Once the NBX Audit Tracks have been retrieved and seal checked, 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 server based application will perform a simple line based search for occurrences of the PAN string in the retrieved Audit Tracks. It will 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.

If a hashed PAN was originally entered as input, then only records that contain the hashed version of the PAN can be located. If a clear text PAN is entered, which is expected to be the norm, the search will locate records which contain either the clear text form (originating from pre CP4305 audit tracks) or the hashed form.

FUJ00123758

6.1.7 PAN Hash Calculation

The Audit workstation contains a function than enables the user to calculate the CP4305 PAN Hash value for a given clear text PAN. This is utilized by the Audit workstation when searching for transactions which relate to a specific PAN.

The user will be able to invoke this function as a free standing feature within the workstation application or implicitly when querying NBX data using a full clear text PAN (see section 6.1.6.3.)

The PAN hash function is specified in *HNG-X Crypto Services High Level Design* (DES/SEC/HLD/0002) §3.2.1.

The PAN hash calculation is performed using the HNG-X Crypto API (See DES/SEC/IFS/0001). This API will be utilized directly from the Audit Workstation Visual Basic applications.

6.1.8 PAN Decryption

The Audit workstation contains a freestanding feature than enables the user to decrypt a single encrypted PAN. This is utilized when query has returned Hashed PAN & encrypted PAN data, and it is necessary to positively identify the PAN in question.

The PAN decryption function is performed using the HNG-X Crypto API (See DES/SEC/IFS/0001). This API will be utilized directly from the Audit Workstation Visual Basic applications. The Crypto API requires access to an Attalla NSP, which is locally connected to the Audit workstation subnetwork.

The Audit user may need to decrypt PANs which go back up to seven years, thus the key server must contain up to seven years of historic PAN decryption keys.

Usage of the PAN Decryption feature will be included in the Audit server audit trail.

Note that it is not possible to turn a Hashed PAN back into clear.

6.1.9 Data Delivery

Data will be delivered to the requester by CD-R media. CDs will be burnt using the standard Windows XP CD writing feature.

The user must ensure that the Seal Checking has completed successfully before extracted data is further processed and/or passed to the requestor.

FUJ00123758

6.2 Distributed Application Services

Figure 6 show the distributed application interfaces between the components of the Audit system

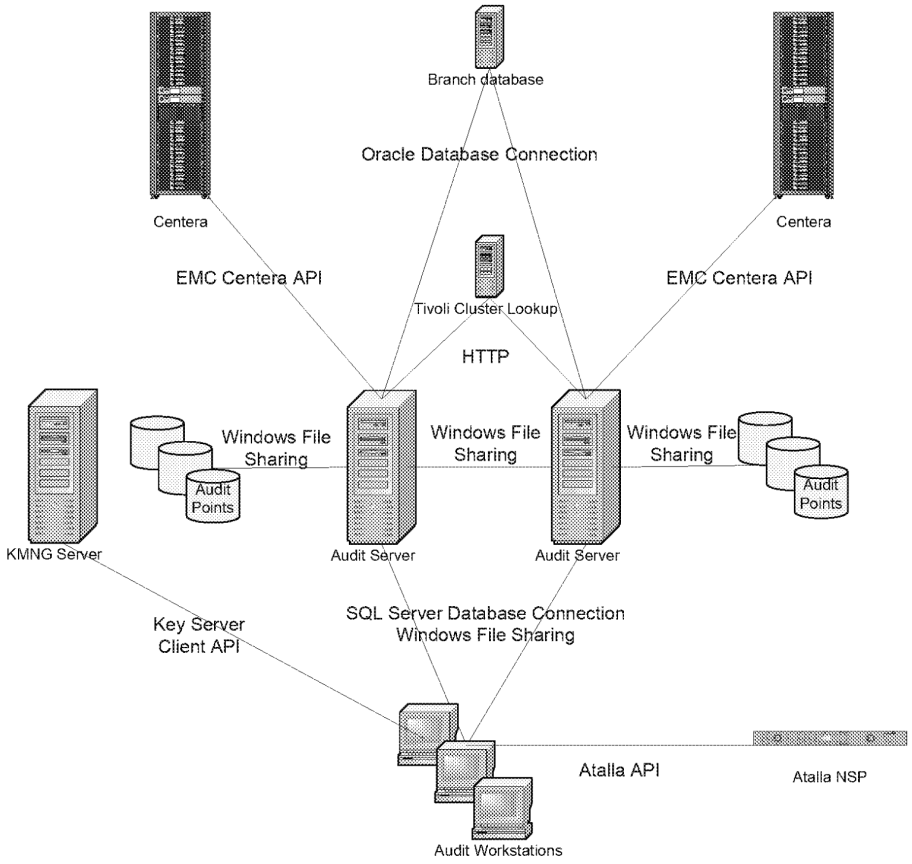

Figure 6 – Audit Distributed Application Interfaces

The ARQ SQL Server 2000 database is used to support client-Server communication between the Audit workstations & servers. Service requests are initiated by writing to interface tables in the database. The client monitors the progress of server actions via status tables in the database.

The Audit servers access the EMC Centera units using the EMC Centera API.

The Audit workstations access the Atalla NSP and the KMNG Server using the HNG-X Crypto API (See DES/SEC/IFS/0001). .

The Tivoli cluster lookup service is used to determine which Correspondence Server cluster a particular branch belonged to at a particular point in time. This is only relevant to Horizon Riposte transactions, but access to this data must be maintained for the 7 years that Riposte data exists in the Audit archive. The cluster lookup service will be retired once Sysman2 components are removed from the solution. At this point the cluster look up data will be imported into the Audit system and accessed directly.

FUJ00123758

6.3 Networking Services

The Audit Server will use the standard HNG-X network services. Figure 7 shows the networked interfaces between components of the Audit system. All application services utilise TCP and/or UDP on a predictable set of ports.

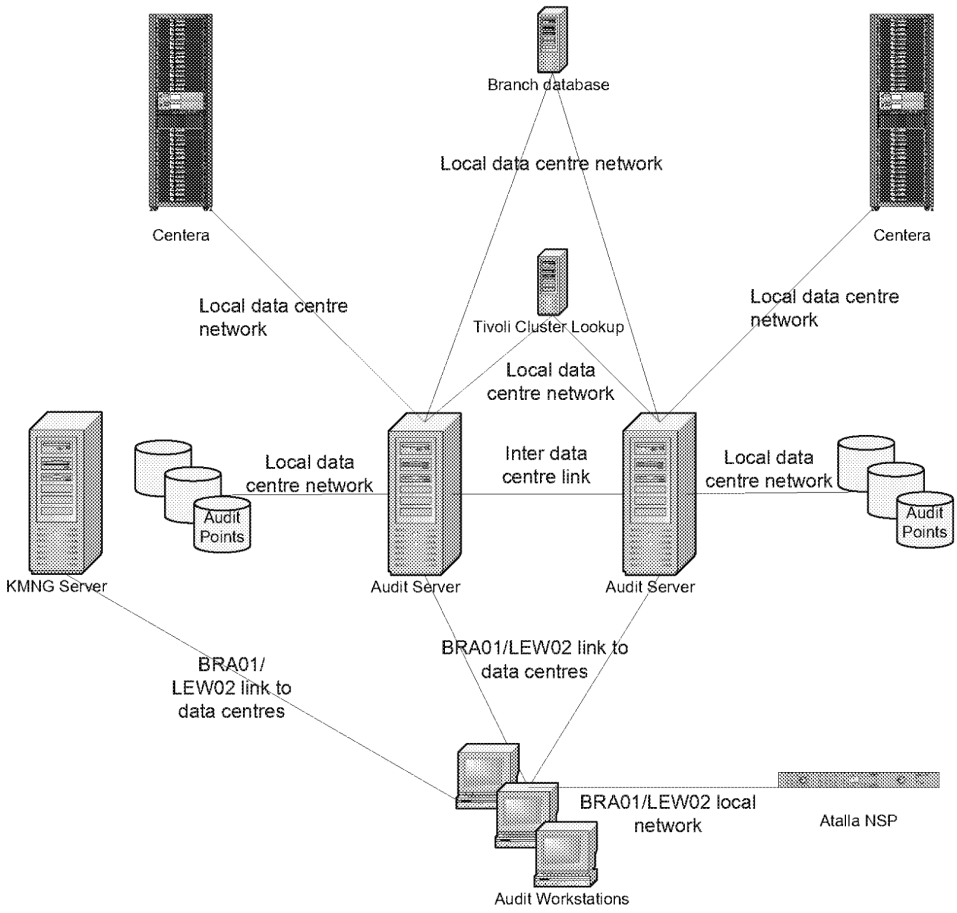

Figure 7 – Network Services

The Audit system can move large volumes of data around the network. On a peak day, it is estimated that the audit system will gather 10 GB of data at the active data centre. This data will flow as follows

1. Local data centre network - HNG-X systems ➔ Audit server 1
2. Local data centre network – Audit server 1 ➔ Centera 1
3. Inter data centre link – Audit server 1 ➔ Audit server 2
4. Local data centre link – Audit server 2 ➔ Centera 2

In addition, during Hydra, the following additional flows will exist

1. Bootle/IRE11 link - Horizon systems ➔ Audit server 1
2. Bootle/IRE19 link - Horizon systems ➔ Audit server 2
3. Inter data centre link – Audit server 2 ➔ Audit server 1

FUJ00123758

During Hydra, a peak load of 35GB per day will flow from Bootle ➔ IRE11 and Wigan ➔ IRE19. The volume of this traffic will decrease as the HNG-X counter rollout progresses.

The bulk of Audit data (by volume) is generated by the Branch database. This data will be made available to the audit system by an overnight extract taken shortly after 01:00. Thus the audit system will utilise the local network quite heavily during this period.

Replication of audit data must take place when the audit system is quiescent. This is scheduled to take place after the Audit backups have completed. During this period the audit system will be heavily utilising the inter data centre link. This may require some traffic management on the network to avoid the Audit replication traffic flooding the link.

If the Audit server is in recovery mode (i.e. it has been out of action for a period of time) it will put a considerably higher load on the network than stated above.

6.4 Platforms

The Audit servers run in an Active/Active configuration. They are housed in the BladeFrame.

The Audit servers will run Windows Server 2003 Standard Edition.

The Physical Platform Design for the Audit server is *HNG-X Audit Server (ARC) - Physical Platform Design (DES/PPS/PPD/0035)*

New Audit workstations will be provisioned running Windows XP.

The Physical Platform Design for the Audit Workstations is *HNG-X Audit Workstation (AUW) - Physical Platform Design* (DES/PPS/PPD/0037)

FUJ00123758

7 Systems Management

7.1 Monitoring

The Audit applications use standard Windows event logging to record application events. Events are classified using the standard mechanism and are marked as Information, Warning or Error as appropriate.

The SYSMAN3 Event Management system is responsible for analysing this event stream and taking suitable action.

The Audit gathering system automatically manages the availability of free local disk space to hold temporary copies of Audit Tracks. If the amount of free disk space falls below a given threshold, the gathering system will suspend until sufficient free space becomes available. This is normally an automatic process as other audit processes secure Audit Tracks and delete the local copy.

7.2 Schedule Requirements

The audit system is dependent on the HNG-X system scheduler to manage its operation. The scheduler is used to:

- Detect fatal application failures & raise alerts
- Schedule (run and shutdown) individual Audit application processes
- Manage the cross campus replication of Audit Tracks
- Manage the Audit server backups
- During Hydra, manage the failover state of audit gathering processes

The Audit system schedule requirements are fully documented in *Audit Server Schedule Design (DEV/INF/ION/0009)*

FUJ00123758

8 Application Development

The Audit retrieval system is developed using the following development tools and technologies

- Microsoft Visual Studio 6.0
  - Visual Basic 6.0
  - Visual C++ 6.0
- Microsoft SQL Server 2000
- Windows Scripting Host
- Microsoft Internet Explorer
- Microsoft Office 2003
- ActivePerl V5.10

FUJ00123758

9 System Qualities

9.1 Availability

The gathered Audit data held on an Audit Server is held on a RAID 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 failure of a single Audit server will not significantly impact the processing of ARQs.

The Audit system is unavailable for retrieval purposes while the audit system backups are taking place. These backups are scheduled into an overnight slot.

Multiple Audit Workstations are provided to mitigate against the loss of a single workstation. The primary Audit workstations are sited at BRA01; alternative workstations are available at LEW02.

9.2 Usability

Where users are required to interact with the Audit Server such interactions are carried out, from the Audit workstation. The Audit Extractor Client is used to initiate retrieval of Audit tracks and to submit queries for execution. Standard facilities provided by COTS software including Windows XP standard tools are used to access the Audit server Userarea share.

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 on the workstation allow other activities to be progressed while waiting for the longer term ones to complete.

The HNG-X Audit Extractor Client will allow multiple queries, each associated with a different ARQ, to be submitted from a single workstation.

9.3 Performance

The implementation must enable the ARQ turnaround times defined in *Security Management Service - Service Description* (SVM/SDM/SD/0017) to be met.

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 upon a logical grouping of data using Audit Points. 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.

When retrieving and querying branch transaction data, the time required to process a given ARQ should not exceed that required by the equivalent Horizon feature. This is necessary to achieve ARQ turnaround targets.

The interface to the HNG-X branch transaction data Query Processor will be integrated into the Audit extractor client, this will minimise the number of user interactions required to fully process an ARQ which relates to PO branch transaction data.

Staff availability may impact on the achievement of ARQ turnaround times.

Access to the Audit Atalla NSP will be manually initiated and infrequent. There are no performance constraints.

FUJ00123758

9.4 Security

Data retrieved using the Audit system is often used for litigation support purposes and is presented as evidence in court cases. A number of measures are necessary to ensure the integrity of the data generated by the retrieval process.

As Audit tracks are retrieved from the archive, they are seal checked (by re-application of the MD5 message digest function) to ensure that the source data has not been tampered with while it was stored in the archive.

Only authorised users may access the Audit workstation applications. Authorised users are required to log on to the workstation using two factor authentication & the HNG-X Identity Management system. An Active Directory group named AUDIT_USER will be created with the rights required to utilise the workstation applications. Authorised users will be added to this group.

User Log/On events are included in the Windows event log. Users are allocated to a specific role which enables them to access the Audit databases.

All retrievals of audit data are performed using the Audit Extractor Client, and all such user actions are themselves audited. It is not possible for users to access the archive by any other means.

Audit workstations and Atalla NSPs are located in secure areas. Only authorised users are given physical access to these areas.

The standard HNG-X Anti-Virus solution (Sophos) will be installed on the Audit workstation. See *HNG-X Anti Virus High Level Design* (DES/SEC/HLD/0011).

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 additional extraction and filtering facilities need to be developed for other (non branch transaction) audit data.

FUJ00123758

10 Migration

Further details of Audit system migration, including details of the changes required at each migration phase, is given in *Audit Data Collection & Storage High Level Design* (DES/APP/HLD/0030)

10.1 Audit Workstations

New Audit workstations will be provisioned using Windows XP in line with the HNG-X platforms architecture requirements.

The existing Audit client applications must be ported to run under the Windows XP environment. It is expected that the majority of client applications will run unchanged on Windows XP. This will entail an initial development team exercise to check the compatibility of the existing client applications with Windows XP & to identify & resolve any issues encountered.

A new workstation build must be developed based on Windows XP, Microsoft Office 2003 and the updated applications.

Two of the current Horizon workstations will be retained at least until all Horizon counters have been migrated to HNG-X. This is in case any existing ARQs require further work (say for a court case) and will enable the original tool set to be used. This introduced a requirement that Riposte services continue to be available on the HNG-X Audit server until all Horizon Audit workstations are decommissioned.

It will be the responsibility of the users of Audit workstations to backup any data that they may have stored on the workstations prior to migration of the platforms.

10.2 Audit Servers

The Audit servers will be upgraded to Windows Server 2003 in line with the HNG-X platforms architecture requirements.

The existing Audit server retrieval application components must be ported to run under the Windows Server 2003 environment. It is expected that the majority of such applications will run unchanged on Windows Server 2003. This will entail an initial development team exercise to check the compatibility of the existing client applications with Windows Server 2003 & to identify & resolve any issues encountered.

At the end of the Hydra phase of the migration process the data held within the Tivoli cluster information service will be imported into the Audit system ARQ database. See section 6.1.4.6.