Document Title: Audit Data Extraction Process

Document Type: Process

Abstract: This document establishes the process undertaken by Post Office Account CS Security Prosecution Support Section to locate, retrieve, extract, filter and prepare audit data for despatch to authorised requesters

Document Status: APPROVED

Originator & Dept: Neneh Lowther - Customer Service Security

Contributors: Jan Holmes / Penny Thomas/Bill Mitchell

Internal Distribution: Jan Holmes/Bill Mitchell

External Distribution: Jamie Henderson (POLIA) and Graham Ward (POL SI)

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

Name	Position	Signature	Date
Jan Holmes	Programme Assurance Manager		
Bill Mitchell	Customer Service Security Manager		
Dave Baldwin	Customer Service Director		

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/Peak
0.1	01/01/02	Initial draft based on CSR+ version IA/PRO/003	
0.2	15/04/02	Addition of comments and change to Fujitsu Services	
1.0	29/05/02	Approved	
1.1	17/01/03	Update to BI3 system and contractual changes	
2.0	27/01/03	Approved	
2.1	26/10/04	Addition of comments and change to internal processes	
3.0	01/02/05	For approval after review comments received.	

0.2 Review Details

Review Comments by :	
Review Comments to :	

Mandatory Review Authority	Name
Programme Assurance Manager	Jan Holmes
Customer Service Security Manager	Bill Mitchell
Audit Development	Alan Holmes
Audit Development	Brian Muir/Oddette Moronfolu
Optional Review / Issued for Information	

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001	8.0	19/12/02	Fujitsu Services Document Template	PVCS
IA/SPE/008			Audit Data Catalogue	

IA/SPE/018			Audit Data Catalogue – ADC (Consignia SIS)	
IA/SPE/019			Audit Data Catalogue (Consignia AP Clients)	
IA/SPE/020			Audit Data Catalogue (System Management	
IA/SPE/021			Audit Data Catalogue (System Management)	
IA/SPE/021			Audit Data Catalogue (Internal Audit)	
RS/MAN/010			SecureID Normal Token User Guide	
NB/MAN/002			PSS Database Manual	
CS/SER/016			Service Description for Security Service Management	

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
AW	Audit Workstation
CD-W	Writeable CD
OBCS	Order Book Control System
PIN	Personal Identification Number
Peak	Problem Management System operated by Fujitsu Services
POLIA	Post Office Limited, Internal Audit
PSS	Prosecution Support Section
ARQ	Request For Information (ARQ is synonymous with ARQ.)
TMS	Transaction Management System

0.5 Changes in this Version

Version	Changes
3.0	Updated after review comments received.

0.6 Changes Expected

Changes

Table of Contents

1.0 Introduction

The Horizon system generates significant amounts of data that is of interest to Post Office Ltd Internal Audit and other groups.
Subject to certain constraints the audit data must be made available to POLIA or other authorised groups within time scales established in the Audit Data Retrieval Requirements (CSR+) [3] and the Network Banking Internal Audit Requirements [10].

This document establishes the process for requesting audit data extractions and subsequent activities undertaken to locate, retrieve, extract & filter and prepare for despatch on behalf of authorised requesters.

2.0 Scope

Should future releases of Horizon bring about changes to the way that data is extracted this process will be updated to reflect those changes.

This process applies to ALL audit data extraction requests in respect of:

1. PSS ARQs
2. Other requests from POLIA
3. Internal Requests

Internal requests for audit data extraction will also be subject to this process. In these cases the use of an Audit Record Query (ARQ) form is optional but a Peak must be raised to the data extraction stack.

3.0 Terminology

Within this process certain terms are used which have specific meaning within the Horizon Audit Solution. They are:

Gatherer : The module responsible for collecting the audit files from the hosts, agents, correspondence servers and interface mechanisms. This module is also responsible for the application of the audit file naming policy.

Sealer : The module responsible for calculating the checksum seal of each audit data file before it is written to audit archive. This value is recalculated after data is extracted by the **Retriever** and compared to the original value when first sealed. Used to ensure data integrity during storage on audit archive.

Hoarder : The module responsible Pre-Bi3 for writing audit data files onto DLT at pre-defined intervals. From Bi3 sealer writes audit data to Centera cubes.

Retriever : The module responsible for moving audit data from the buffers where it is placed when retrieved by Centera .

Extractor : The Client/Server system responsible for retrieving data from Centera and managing Audit Data Extractions.

Centera : Online mass disk storage unit selected by Post Office Account to store and manage audit data from Bi3.

A more complete explanation of these modules can be found in the Horizon System Audit Manual [2].

4.0 Audit Data Integrity

The integrity of audit data must be guaranteed at all times from its origination, storage and retrieval to subsequent despatch to the requester. Controls have been established to provide assurances to Post Office Internal Audit that this integrity is maintained.

During audit data extractions the following controls apply:

- Extractions can only be made through the Audit Workstations, which exist at Feltham, Bracknell and the 2 Data Centres. These are all subject to rigorous physical security controls appropriate to that location. Specifically, the Feltham AWs – where most extractions will take place – are located in secure rooms subject to proximity pass access within a secured Fujitsu Services site.

- Logical access to the AWs and their functionality is controlled by dedicated Logins, password control and utilises the NT and Post Office Account security features defined in the overall Horizon security policy.

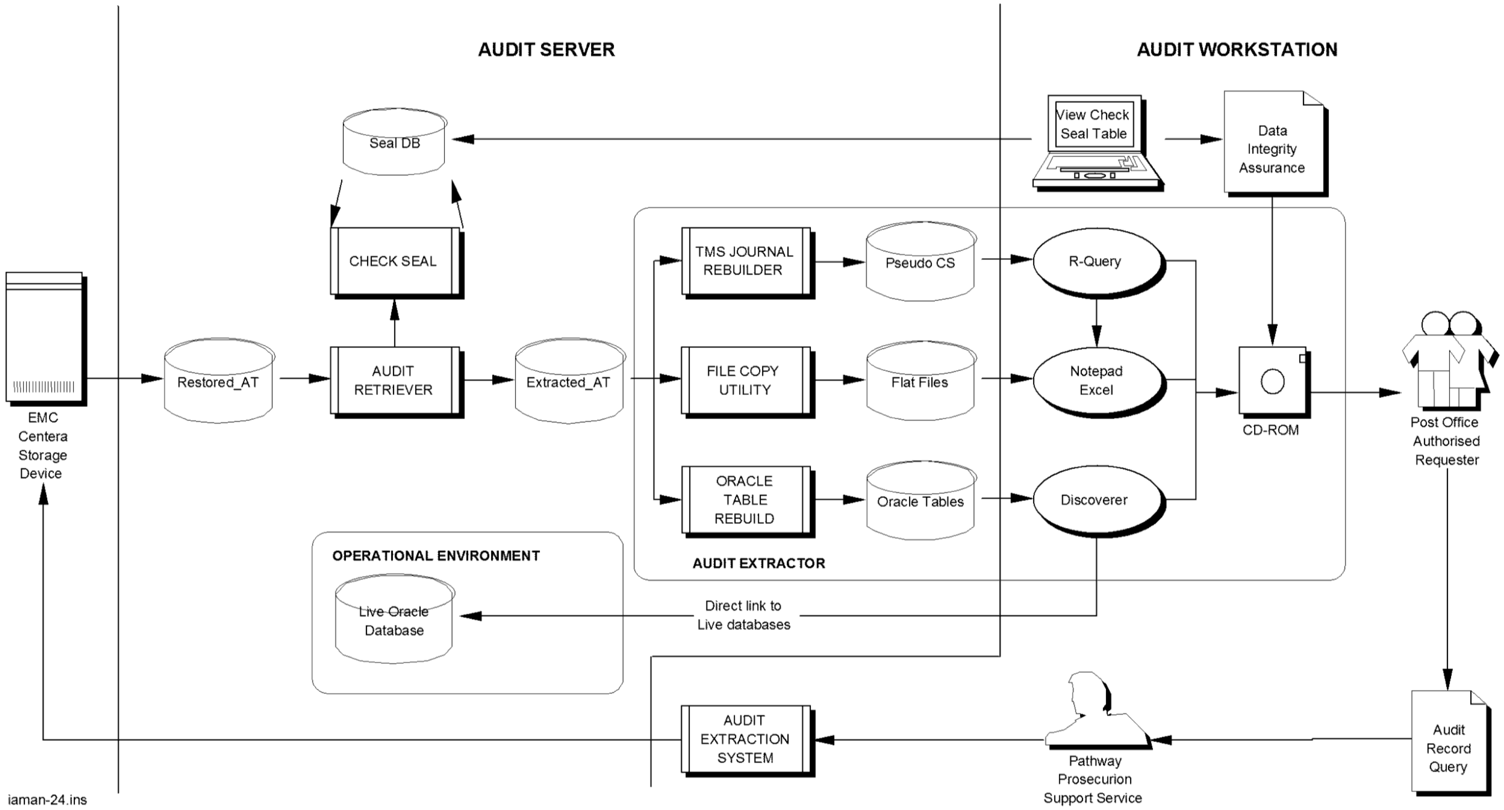
- All extractions are logged on the Audit System and supported by documented ARQs, authorised by nominated persons within POLIA. This log can be scrutinised on the AWs.

- Extractions will only be undertaken by individuals previously notified to POLIA. Currently this is limited to Post Office Account Audit and Post Office Account CS Security Prosecution Support personnel. Any additions will be notified to POLIA.

- Agreement has been reached with POLIA regarding their rights to witness extractions without warning or to request repeat extractions that they can witness.

- Checksum seals are calculated for audit data files when they are written to audit archive and re-calculated when the files are retrieved.

4.1 Retrieval Schematic



5.0 Overview

The process assumes that audit data has been Gathered, Sealed and written to audit archive. The five main types of files are :

a. TMS Journals from the Correspondence Servers.

b. Flattened Oracle tables output from regular OBCS database purging cycles.

c. Transaction files to and from PO systems

d. AP Client Files

e. Tivoli Event files

All file types are referenced in TD/ION/011.

The process is invoked through the receipt of an ARQ into Post Office Account CS Security PSS. Expressed in business terms, the ARQ must be interpreted into its component Audit Points and Sub-points. This then enables specific files to be identified and retrieved by the Audit Retriever, formatted as appropriate and then further Extracted against the ARQ criteria. Depending on the extraction method the data can be extracted to standard MSExcel 97 before being placed onto CD-W. The CD is then checked for despatch to the ARQ originator.

The following paragraphs present an overview of each step in the extraction process and are ordered to reflect the actual processing of a Audit Record Qu ery (ARQ) by Post Office Account CS Security PSS.

5.1 Audit Record Query

All POLIA requests for audit data must be made via the Audit Record Query form. This will contain a description, in business terms, of the times, outlets, events, items activities that the Auditors are interested in. This request has to be interpreted by Post Office Account CS Security PSS and mapped onto the Audit Points and Files described later in this document.

Internal requests (e.g. from Post Office Account investigations personnel) will typically be in the form of a Peak on the ‘Dataextraction’ stack for CS Security.

5.2 Marking Files and Tapes

Based on the above interpretation of the ARQ, as many files of audit data that are needed to satisfy the request are ‘marked’ for retrieval.

5.3 Audit Track Retriever

Polls the user area buffers and makes them available to sealer for seal verification

Audit Data Check Seal

To assure the integrity of the audit data while on the audit archive the checksum seal for the file is re-calculated by the Audit Track Sealer and compared to the original value calculated when the file was originally written to the audit archive. The result is maintained in a Check Seal Table.

5.4 Audit Trail Extractor

This is a facility that uses various tools to extract or reform the retrieved audit data in accordance with the ARQ. It also places the information onto a CD-W, or other suitable media, for despatch to the ARQ originator.

6.0 Retrieving & Extracting Audit Data

6.1 Receiving the ARQ

a) **POLIA requests** for audit data extractions must come to Post Office Account CS Security PSS in the form of an Audit Record Query. An example of this form can be found at Annex A. The ARQ may be mailed, faxed or e-mailed to Post Office Account CS Security PSS.

ARQs will only be accepted from persons fulfilling the following role or their delegate :

POL Internal Audit. Casework Manager: Tel GRO

Current names of persons fulfilling this role will be confirmed in writing by POLIA Internal Audit and held locally by PSS.

If other parts of the Post Office, or other organisations, require audit data extractions they must be channelled through POLIA to Post Office Account CS Security PSS.

Contractual limits and turnaround times for the provision of Audit Record Queries are detailed in the document CS/SER/016.

b) **Internal requests** will be in the form of a Peak, allowing the requestor's identity to be verified. Requestors should state what media is acceptable (e.g. CD-W, email of WinZipped file up to 500kB) The despatching of confidential data is bound by Fujitsu Services policy. For TMS files - also referred to as "message store" or "Correspondence Server"- they should also specify the output file format(s): text, MS-Excel or MS-Access. (See Section 8 for more information).

POLIA and Internal requests are recorded on the PSS Database (User Guide for Prosecution Support Database [12])**.** They should be logged to record the following information: Request id (e.g. ARQ no.), the date the request was received, the FAD and date range to search. Turnaround times are covered by contract as specified in the CCD CS/SER/016.

6.2 Interpreting the ARQ

It is necessary to interpret the ARQ by identifying the audit points and sub points that generated the records that are required and, through the Audit Data Catalogues [4-8], the files produced at those audit points and sub points.

6.3 Login Audit Workstation

Carry out following procedure to Login and obtain necessary shares

1. Login : *****##

2. Password : *********

3. Domain : PWYDCS

At this point the SecureID Authentication is invoked. See SecurID Normal Token User Guide [9].
Carry out the following procedure to authenticate yourself as an authorised user

1. Enter passcode : <personal 6 digit PIN and 6 digit SecureID token display>

The AW will present a blank desktop with a START icon in the bottom left of the screen. Using pull up <Programs> will reveal the extent of products available for any subsequent extraction work, as shown in Figure 1.

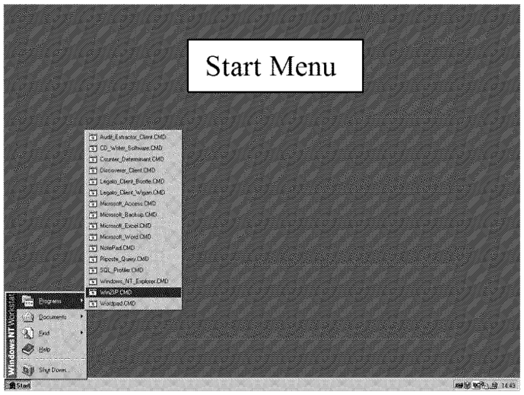


Figure 1

6.4 Preliminary Housekeeping

It is highly likely that an average ARQ will need a significant number of files to satisfy it. To avoid the AW filestore becoming clogged with hundreds of files it is strongly recommended that a working directory is established on the AW to hold all files relevant to a particular ARQ :

1. Select <Windows_NT_Explorer> from the drop down menu.

2. Set up <New Folder> as D:\audit data\ARQ Reference No.

6.5 Targeting the Data Files

At this stage of the retrieval procedure the Audit Extractor Client is used to identify and mark the files required for retrieval.

7.0 Using Audit workstations

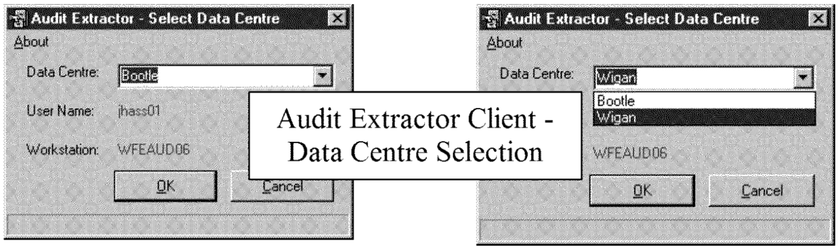
Each Audit Workstation is loaded with the following programs;

1. Audit Extractor Client
2. NT Explorer
3. RQuery
4. Roxio

An explanation of the functionality of each program is detailed in the following sections.

8.0 Extractor Client Functionality

The Audit Extractor Client is invoked from the start menu. The user will select the Data Centre they wish to work with as depicted in Figure 2. The Audit Extractor Client refers to ARQ.


Audit Extractor - Select Data Centre
About
OK
Cancel
Audit Extractor - Select Data Centre
About
Bootle
Wigan
OK
Cancel

Data Centre: Bootle
User Name: jhass01
Workstation: WFEAUD06

Data Centre: Wigan
WFEAUD06

Audit Extractor Client - Data Centre Selection

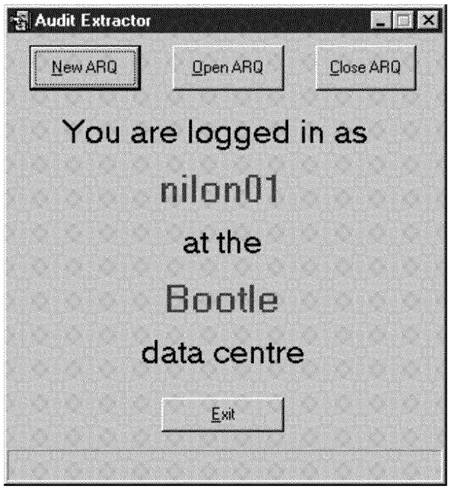
Figure 2

The Audit Extractor Client (Figure 3) has three main options;

<New ARQ> (Figure 4)

<Open ARQ> (Figure 7)

<Close ARQ> (Figure 9)

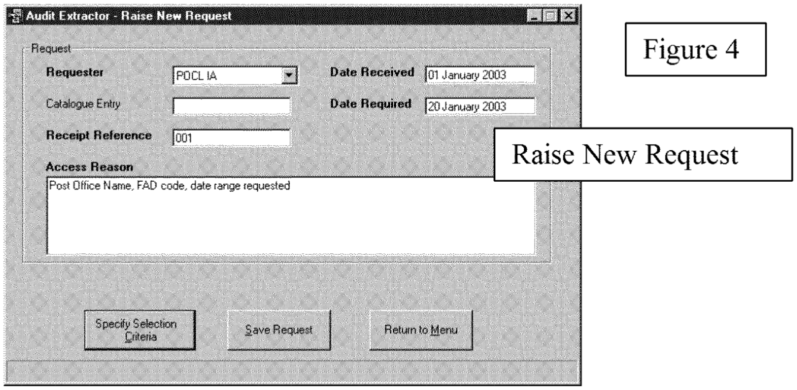


You are logged in as
nilon01
at the
Bootle
data centre

Figure3 Audit Extractor Client – Main Screen

8.1 New ARQ

This option is used to setup an audit trail for each request and to specify the search criteria identified from the ARQ form. See Figure 4.



Audit Extractor - Raise New Request

Request

Requester: POCL IA

Date Received: 01 January 2003

Catalogue Entry:

Date Required: 20 January 2003

Receipt Reference: 001

Access Reason: Post Office Name, FAD code, date range requested

Figure 4

Raise New Request

Requester – Drop down list.

> Other *3rd party*
>
> *Post Office Account IA* (Post Office Internal Audit, ARQs are always POIA)
>
> *Post Office Account Other*
>
> *Post Office Account SSC*
>
> *POCL IA*
>
> *POCL Other*
>
> *POCL Security*

Date Received – Date ARQ received, taken from ARQ form

Date Required – Date ARQ must be completed. Use SLA target times to calculate date to be completed by

Catalogue Entry - Blank

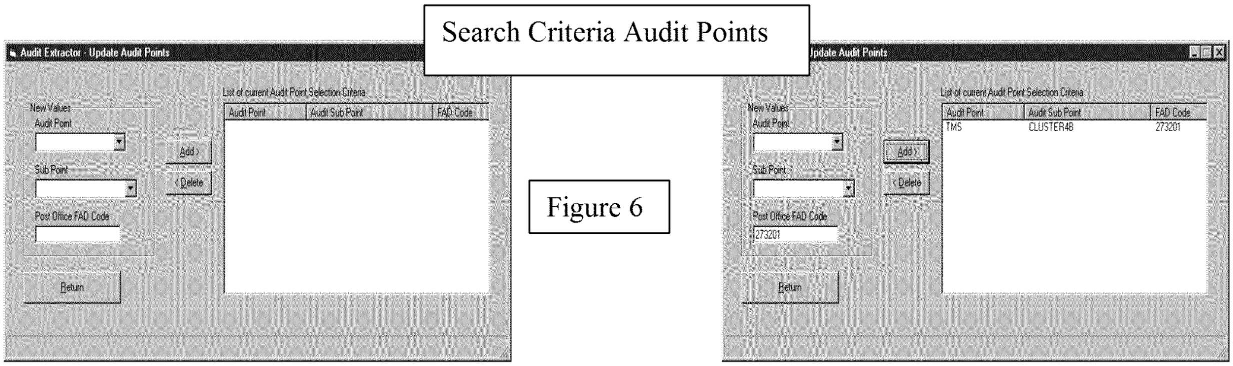
Receipt Reference – ARQ Number, taken from ARQ form

Access Reason – Post Office Name, FAD and dates specified on ARQ form

<Specify Selection Criteria> See Figure 5 below.

From Date – The first date requested on the ARQ

To Date – The last date requested on the ARQ + 2 days. This ensures if data hoarded late that all files are identified.



Search Criteria Audit Points

Figure 6

Audit Extractor - Update Audit Points

Audit Point	Audit Sub Point	FAD Code
TMS	CLUSTER4B	273201

Post Office FAD Code: 273201

<Update> See Figure 6 above.

Audit points – Used to select AP Client files and Tivoli events, etc

Subpoints – Used to narrow audit point selection

FAD code – FAD code from ARQ

<Add> - input above value and click add to enter the details

<Delete> - Select any values in List of current Audit points and click delete to remove them

<Return> - Click to return to Search Criteria Screen (Figure 5)

<Search files> – when file search completes, the 'Retriever' screen opens, see Figure 10.

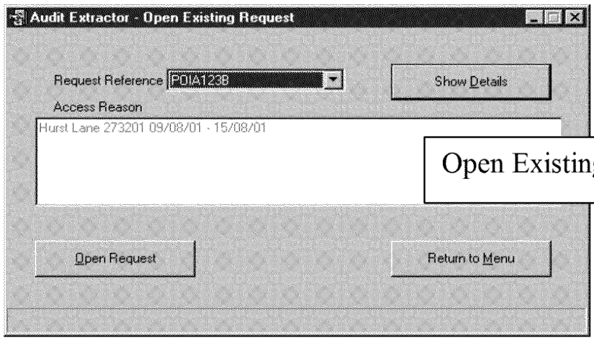
<Save selection> - saves the selection criteria

<Return to menu> – returns to main screen (Figure 3)

<Save request> - saves the request

<Return to menu> – returns to main screen (Figure 3)

8.2 Open ARQ



Request Reference: POIA123B

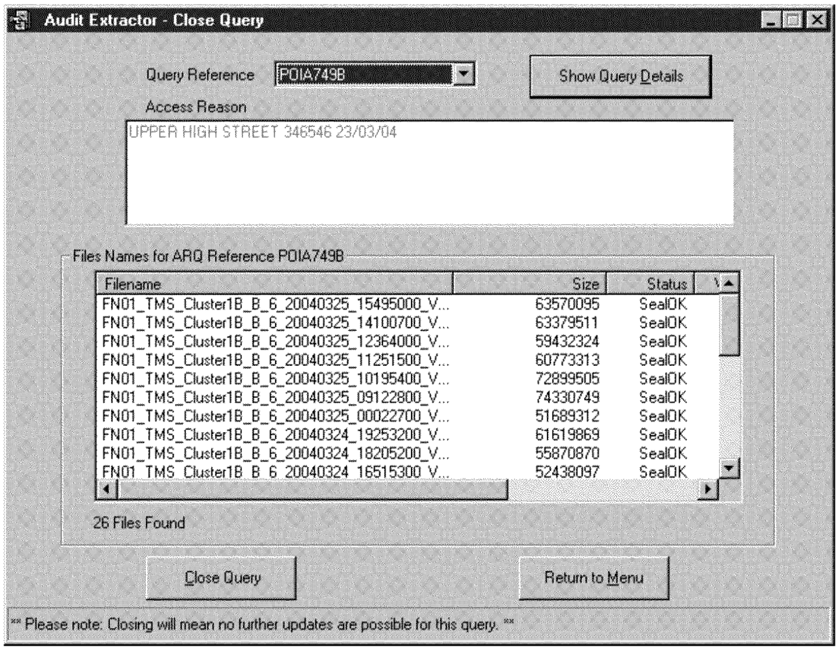
Access Reason: Hurst Lane 273201 09/08/01 - 15/08/01

Figure 7

Open Existing Request

Select the 'Request Reference' from the drop down list i.e. POIA001B

<Show Details> - Figure 8 below.



Query Reference: POIA749B

Access Reason: UPPER HIGH STREET 346546 23/03/04

Files Names for ARQ Reference POIA749B

Filename	Size	Status
FN01_TMS_Cluster1B_B_6_20040325_15495000_V...	63570095	SealOK
FN01_TMS_Cluster1B_B_6_20040325_14100700_V...	63379511	SealOK
FN01_TMS_Cluster1B_B_6_20040325_12364000_V...	59432324	SealOK
FN01_TMS_Cluster1B_B_6_20040325_11251500_V...	60773313	SealOK
FN01_TMS_Cluster1B_B_6_20040325_10195400_V...	72899505	SealOK
FN01_TMS_Cluster1B_B_6_20040325_09122800_V...	74330749	SealOK
FN01_TMS_Cluster1B_B_6_20040325_00022700_V...	51689312	SealOK
FN01_TMS_Cluster1B_B_6_20040324_19253200_V...	61619869	SealOK
FN01_TMS_Cluster1B_B_6_20040324_18205200_V...	55870870	SealOK
FN01_TMS_Cluster1B_B_6_20040324_16515300_V...	52438097	SealOK

26 Files Found

** Please note: Closing will mean no further updates are possible for this query. **

This lists the details of the request as inputted in Figure 4, New ARQ. The user can not add or update any fields.

Requester Details

- Requester
- Date Received
- Date Required
- Catalogue Entry
- Receipt Reference
- Access Reason

Selection Criteria

- From Date
- To Date

File Source Requirement

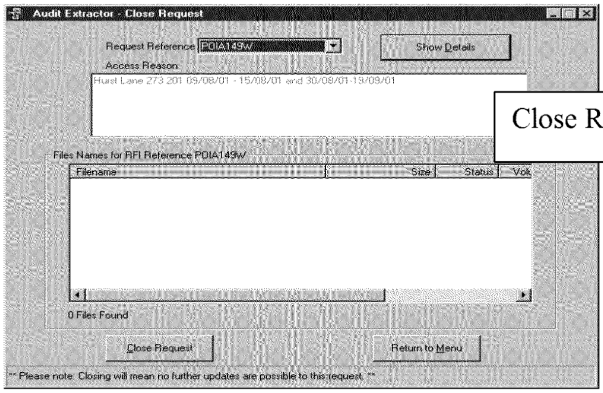
- Audit Points
- Sub Points
- FAD Code
- File Name Template

<Close> Closes 'Details' screen and returns to 'Open ARQ' screen

<Open Request> Displays Figure 10

<Return To Menu> Returns to Figure 4

8.2 Close ARQ



Audit Extractor - Close Request

Request Reference POIA149W

Access Reason

Hurst Lane 273 201 09/08/01 - 15/08/01 and 30/08/01-19/09/01

Files Names for RFI Reference POIA149W

Filename	Size	Status	Vol

0 Files Found

** Please note: Closing will mean no further updates are possible to this request. **

Figure 9

Close Request

When all work has been completed the ARQ must be closed on the Audit Extractor Client.

Request Ref - Select reference from drop down list (ref POIA***)

Access Reason

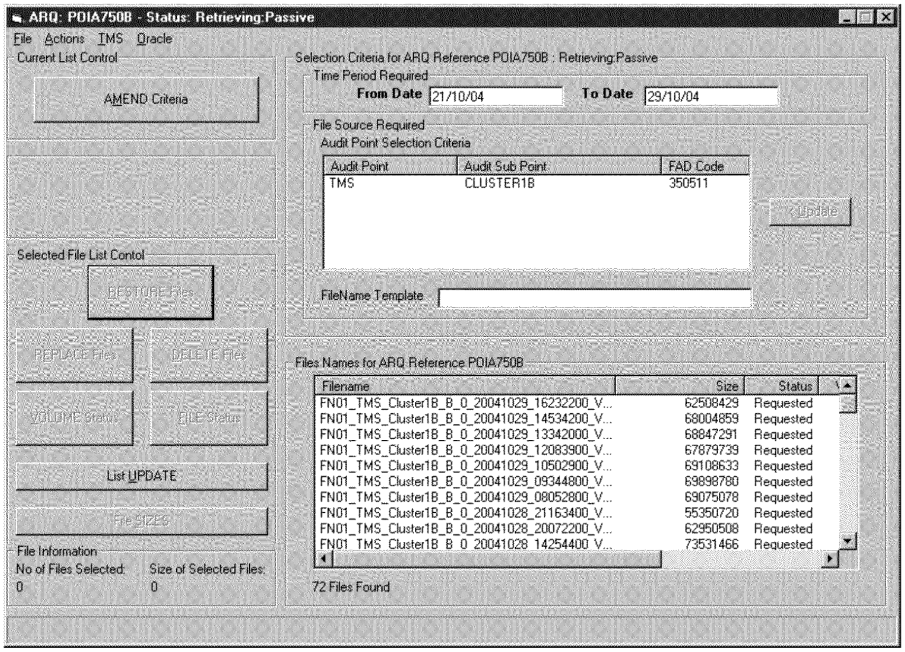
Filenames for ARQ reference POIA**

<Close Request> - once the request is closed the audit log is written to the request directory on the Audit Server, Figure 13. A copy of an example audit log can be viewed in appendix 2.

<Return To menu> - returns to Figure 4

<Show details> – Figure 8 this function displays the ARQ details as in 'Show Details' from 'Open ARQ' screen

8.3 Audit Extractor Client – Retriever Screen



Selection Criteria for ARQ Reference POIA750B : Retrieving:Passive

Time Period Required

From Date 21/10/04 To Date 29/10/04

File Source Required

Audit Point Selection Criteria

Audit Point	Audit Sub Point	FAD Code
TMS	CLUSTER1B	350511

FileName Template

Files Names for ARQ Reference POIA750B

Filename	Size	Status
FN01_TMS_Cluster1B_B_0_20041029_16232200_V...	62508429	Requested
FN01_TMS_Cluster1B_B_0_20041029_14534200_V...	68004859	Requested
FN01_TMS_Cluster1B_B_0_20041029_13342000_V...	68847291	Requested
FN01_TMS_Cluster1B_B_0_20041029_12083900_V...	67879739	Requested
FN01_TMS_Cluster1B_B_0_20041029_10502900_V...	69108633	Requested
FN01_TMS_Cluster1B_B_0_20041029_09344800_V...	69898780	Requested
FN01_TMS_Cluster1B_B_0_20041029_08052800_V...	69075078	Requested
FN01_TMS_Cluster1B_B_0_20041028_21163400_V...	55350720	Requested
FN01_TMS_Cluster1B_B_0_20041028_20072200_V...	62950508	Requested
FN01_TMS_Cluster1B_B_0_20041028_14254400_V...	73531466	Requested

72 Files Found

File Information

No of Files Selected: 0

Size of Selected Files: 0

Selection Criteria

These fields are as entered on the 'New ARQ' screen, Figure 4.

Time Period Required

From Date

To Date

File Source Required

Audit Point Selection Criteria

- Audit Points
- Audit Subpoints
- FAD Code

Filename Template

File Names for ARQ Reference POIA***

The Audit Extractor Client retrieves the following information using the search criteria inputted in the 'New ARQ' screen, Figure 4

- Filename
- Size
- Status

Current List Control

<Amend Criteria> - If the original search criteria is too narrow, select this button to re-input the search criteria and re-search for the required files. This facility is not available once files have started to restore.

Selected File List Control

<Restore Files> - Mark the files required by either holding the <CTRL> key and marking the individual files spaced throughout the range listed or select the first file in a group, hold the <SHIFT> key and select the last file to mark a consecutive group of files. Once all the required files are marked click the 'Restore Files' button to restore the files from archive.

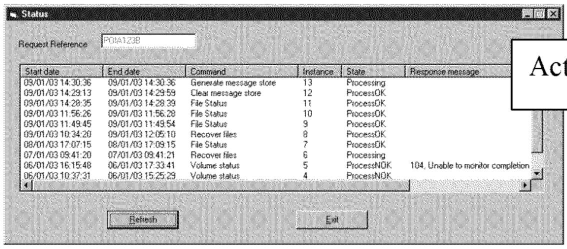
<Replace Files> - Mark the required files, select 'Replace Files' and the files not selected will be removed.

<Delete Files> - Similar to 'Replace Files' except the marked files are removed from the list.

<File Status> - this function updates the status of a set of selected files so that the user can identify progress and seal validity.
<List Update> - this function updates the audit workstation in line with the audit server

File / Close – This exits the 'Retriever' screen

Actions / Check Actions – Actions allow the user to view the status of each function/facility as detailed throughout section 9.0 of this document, thus allowing the user to identify when each process completes and if it completes successfully.



Request Reference: P0IA123B

Start date	End date	Command	Instance	State	Response message
09/01/03 14:30:36	09/01/03 14:30:36	Generate message store	13	Processing	
09/01/03 14:29:13	09/01/03 14:29:59	Clear message store	12	ProcessOK	
09/01/03 14:28:35	09/01/03 14:28:39	File Status	11	ProcessOK	
09/01/03 11:56:26	09/01/03 11:56:28	File Status	10	ProcessOK	
09/01/03 11:49:45	09/01/03 11:49:54	File Status	9	ProcessOK	
09/01/03 10:34:20	09/01/03 12:05:10	Recover files	8	ProcessOK	
08/01/03 17:07:15	08/01/03 17:09:15	File Status	7	ProcessOK	
07/01/03 09:41:20	07/01/03 09:41:21	Recover files	6	Processing	
06/01/03 16:15:48	06/01/03 17:33:41	Volume status	5	ProcessNOK	104, Unable to monitor completion
06/01/03 10:37:31	06/01/03 15:25:29	Volume status	4	ProcessNOK	

Actions Screen

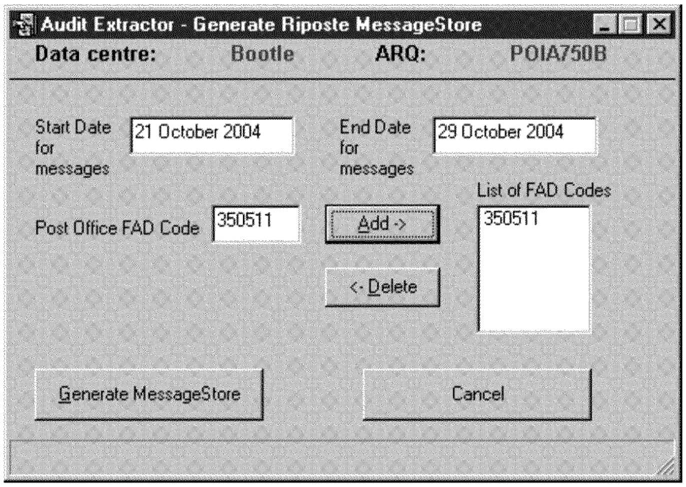
Figure 11

TMS

Once the TMS Archive files have been deposited in EXTRACTED_AT they must be 'built' into a pseudo Correspondence Server for R-Query to access. Further filtering is available to restrict the number of Outlet records that are included in the re-build activity based on the original ARQ.

Clear MessageStore – This clears the current messagestore on the audit workstation

Generate MessageStore – enter the date parameters and FAD code, as depicted below in Figure 12 and then 'Generate MessageStore' to generate the message store on the audit workstation.



Data centre: Bootle ARQ: POIA750B

Start Date for messages: 21 October 2004

End Date for messages: 29 October 2004

Post Office FAD Code: 350511

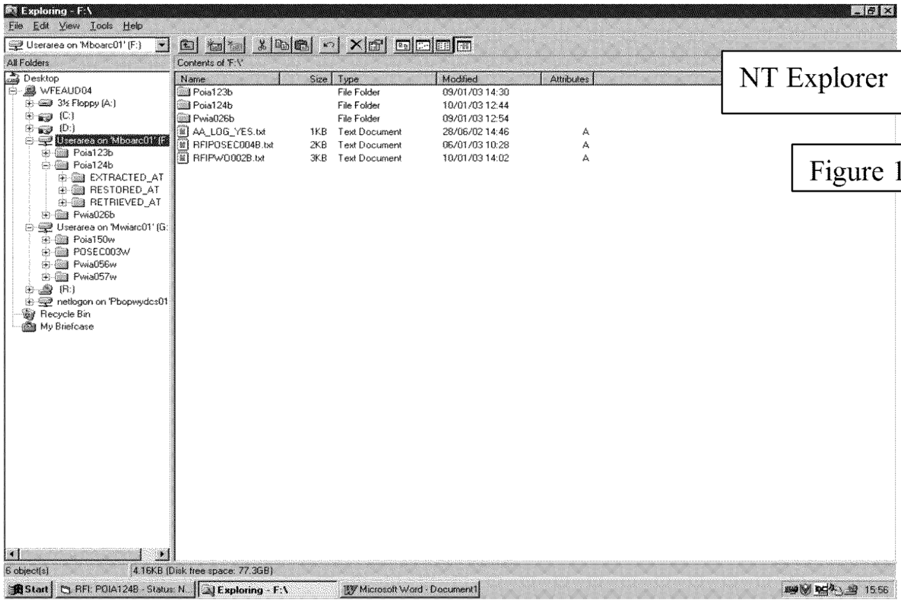
List of FAD Codes: 350511

Server MS Build – Used to generate a messagestore on the audit server. Only one workstation at a time can generate a messagestore on the audit server. This shall only be used as a last resort.

Oracle / Build Table – Allows the user to rebuild Oracle back up files in the Oracle format.

Unzipping Zipped Flat Files - It is strongly recommended that files to be unzipped are transferred from the AS to the AW in their zipped state and unzipped on the AW. This can produce space savings of the order of 90%.

9.0 NT Explorer



```
Desktop
  WFEAUD04
    3½ Floppy (A:)
    (C:)
    (D:)
    Userarea on 'Mboarc01' (F:
      Poia123b
      Poia124b
        EXTRACTED_AT
        RESTORED_AT
        RETRIEVED_AT
      Pwia026b
    Userarea on 'Mwiarc01' (G:
      Poia150w
      POSEC003W
      Pwia056w
      Pwia057w
    (R:)
    netlogon on 'Pbopwydcs01
  Recycle Bin
  My Briefcase
```

Name	Size	Type	Modified	Attributes
Poia123b		File Folder	09/01/03 14:30	
Poia124b		File Folder	10/01/03 12:44	
Pwia026b		File Folder	09/01/03 12:54	
AA_LOG_YES.txt	1KB	Text Document	28/06/02 14:46	A
RFIPOSEC004B.txt	2KB	Text Document	06/01/03 10:28	A
RFIPWO002B.txt	3KB	Text Document	10/01/03 14:02	A

6 object(s) | 4.16KB (Disk free space: 77.3GB)

NT Explorer

Figure 13

NT Explorer is used as a tool for viewing files associated with an ARQ. As each new request is logged on the Audit Extractor Client using 'New ARQ' a directory will be created on the audit server for which the request was initiated from. Each directory takes the Audit Extractor Client ARQ Reference i.e. POIA****. This main directory holds the sub directories; Extracted_at, Restore_at and Retrieved_at. The main directory includes a txt file named using the Audit Extractor Client ARQ reference. This files contains details of each process initiated through the Audit Extractor Client. NT Explorer allows a window to view these files and directories.

10.0 Introduction to R-Query

R-Query is an interrogation tool used to extract data from a Correspondence Server. It has powerful SQL type features, which are used to define the extraction scenarios and the ability to output the results to standard MS-Office utilities.

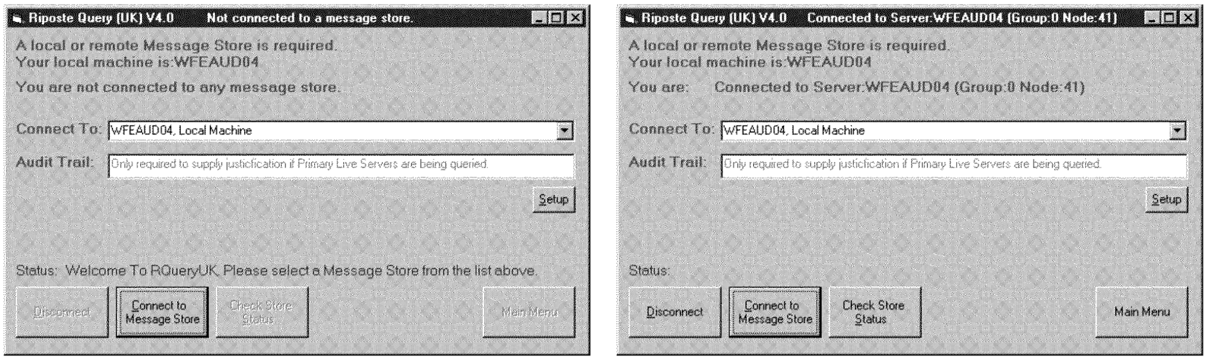
It is a vital element in the Audit Workstation tool set and requires that a Correspondence Server exists on one of the Audit Workstations or Servers. Details on how to achieve this pre-requisite can be found earlier in this procedure.

10.1 Invoking R-Query and Connecting to a Correspondence Server.

The Riposte Query initial screen is invoked from the start menu.

Figure 14

Riposte Query Initial Screen



Riposte Query (UK) V4.0   Not connected to a message store.

A local or remote Message Store is required.
Your local machine is:WFEAUD04
You are not connected to any message store.

Connect To: WFEAUD04, Local Machine

Audit Trail: Only required to supply justicfication if Primary Live Servers are being queried.

Status: Welcome To RQueryUK. Please select a Message Store from the list above.

Riposte Query (UK) V4.0   Connected to Server:WFEAUD04 (Group:0 Node:41)

A local or remote Message Store is required.
Your local machine is:WFEAUD04
You are: Connected to Server:WFEAUD04 (Group:0 Node:41)

Connect To: WFEAUD04, Local Machine

Audit Trail: Only required to supply justicfication if Primary Live Servers are being queried.

Status:

Connect to – The user selects the workstation/server for which the message store exists

Audit Trail – User is only required to justify use of servers

<Disconnect> - disconnects any connection from current workstation to messagestore

<Connect to MessageStore> - ‘connect to’ and ‘audit Trail’ are to be specified before connecting

<Check Store Status> - details of message ranges in the rebuilt message store.

<Check for Gaps>

<Main Menu> - Connects to the main RQuery Screens as detailed in the following sections.

10.2 RQuery Main Screen.

This consists of 7 tabs.

Select Cols – Used to select attributes required for output to excel etc.

Where – Used to enter search criteria i.e. date range and FAD code

Order By – Used to specify sort criteria when output to excel

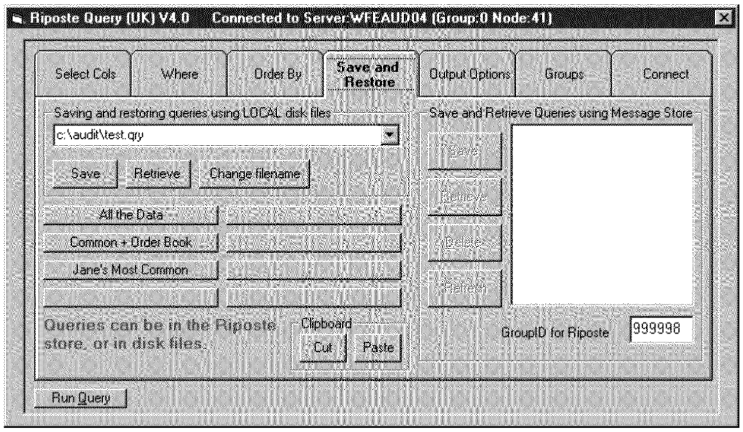
Save and Restore – Used to load and save Query

Output Options – Used to specify file and MS product to export data to.

Groups - Used to specify PAN or STAN identifier

Connect – Used to connect to Messagestore.

10.2.1 Save and Restore - Restoring Retrieval Scenarios



Riposte Query (UK) V4.0 Connected to Server:WFEAUD04 (Group:0 Node:41)

Saving and restoring queries using LOCAL disk files: c:\audit\test.qry

Queries can be in the Riposte store, or in disk files.

GroupID for Riposte: 999998

Save and Restore

Figure 15

The <Save and Restore> dialogue provides the opportunity to restore scenarios that have already been scripted for further use.

SCENARIOS FOR RE-USE EXIST AT TWO LEVELS:

Those that are associated with the current Correspondence Server.

Those that have been saved to an external file or Catalogue.

Scenarios associated with the Correspondence Server exist only while that particular CS exists. If the user believe that an extraction scenario is likely to be re-usable it's as well to remember that unless the scenario is saved to an external file it will not be available if a new CS is built for another retrieval exercise.

Use these steps to re-use scenarios associated with current Correspondence Server.

Go to 'Save and Retrieve Queries using Message Store' window.

Select <Refresh> to list all scenarios associated with the current Correspondence Server.

Highlight the required scenario and select <Retrieve>.

OR

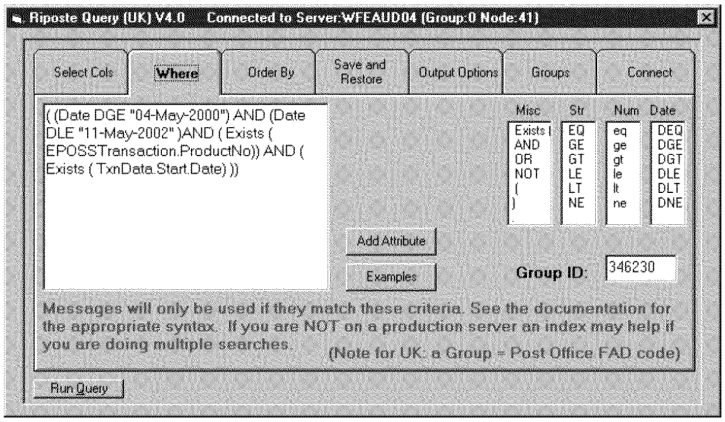
Use this step if retrieving scenarios from the Catalogue.

Locate stored scenario from the Catalogue via <Change filename> button to browse as required.

At this stage the user will have retrieved the scenario complete with the parameter setting used on the last retrieval activity. If the user want to change any of the parameters they will need to go to the <Where> tab.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown.

10.2.2 Where - Changing Retrieval Parameters



```
( (Date DGE "04-May-2000") AND (Date
DLE "11-May-2002" )AND ( Exists (
EPOSSTransaction.ProductNo)) AND (
Exists ( TxnData.Start.Date) ))
```

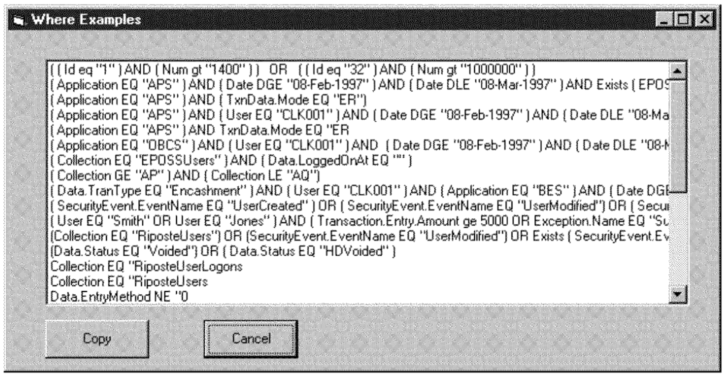
Group ID: 346230

Messages will only be used if they match these criteria. See the documentation for the appropriate syntax. If you are NOT on a production server an index may help if you are doing multiple searches. (Note for UK: a Group = Post Office FAD code)

Where Screen

Figure 16

Note that the current version provides significant amounts of assistance with regard to the structure of the query statement. An 'Examples' button (see Figure 17) allows search parameters to be retrieved and tailored (e.g.):



```
( ( Id eq "1" ) AND ( Num gt "1400" ) )   OR   ( ( Id eq "32" ) AND ( Num gt "1000000" ) )
( Application EQ "APS" ) AND ( Date DGE "08-Feb-1997" ) AND ( Date DLE "08-Mar-1997" ) AND Exists ( EPOS
( Application EQ "APS" ) AND ( TxnData.Mode EQ "ER")
( Application EQ "APS" ) AND ( User EQ "CLK001" ) AND ( Date DGE "08-Feb-1997" ) AND ( Date DLE "08-Ma
( Application EQ "APS" ) AND TxnData.Mode EQ "ER
( Application EQ "OBCS" ) AND ( User EQ "CLK001" ) AND  ( Date DGE "08-Feb-1997" ) AND ( Date DLE "08-M
( Collection EQ "EPOSSUsers" ) AND ( Data.LoggedOnAt EQ "" )
( Collection GE "AP" ) AND ( Collection LE "AQ")
( Data.TranType EQ "Encashment" ) AND ( User EQ "CLK001" ) AND ( Application EQ "BES" ) AND ( Date DGE
( SecurityEvent.EventName EQ "UserCreated" ) OR ( SecurityEvent.EventName EQ "UserModified") OR ( Secu
( User EQ "Smith" OR User EQ "Jones" ) AND ( Transaction.Entry.Amount ge 5000 OR Exception.Name EQ "Su
(Collection EQ "RiposteUsers") OR (SecurityEvent.EventName EQ "UserModified") OR Exists ( SecurityEvent.Ev
(Data.Status EQ "Voided") OR ( Data.Status EQ "HDVoided" )
Collection EQ "RiposteUserLogons
Collection EQ "RiposteUsers
Data.EntryMethod NE "0
```

Where Example Screen

Figure 17

(Date DGE "29-May-2000") AND (Date DLE "01-Jun-2000")

for all dates between 29 May-1 June 2000.

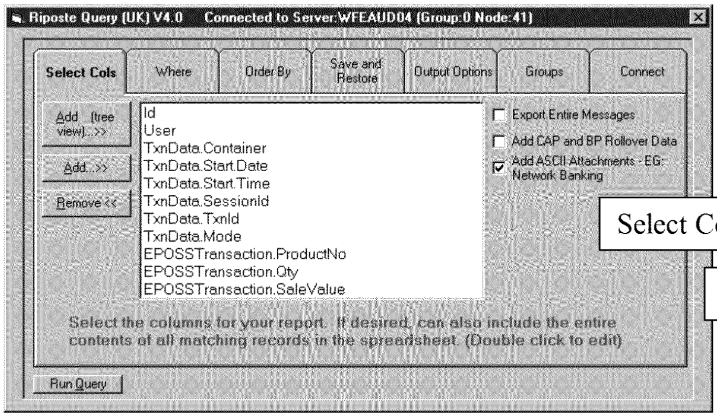
Date DEQ "31-May-2000"

for this day only.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown. If the user want to change the TMS fields that will be visible following the retrieval they will need to go to the <Select Cols> Tab.

Note: Riposte Query can only work with one FAD code (GroupID) at a time. It will need to be run separately for each Post Office, remembering that by default it may delete the previous output file

10.2.3 Select Cols - Selecting TMS Fields for Display



Riposte Query (UK) V4.0 Connected to Server:WFEAUD04 (Group:0 Node:41)

Id
User
TxnData.Container
TxnData.Start.Date
TxnData.Start.Time
TxnData.SessionId
TxnData.TxnId
TxnData.Mode
EPOSSTransaction.ProductNo
EPOSSTransaction.Qty
EPOSSTransaction.SaleValue

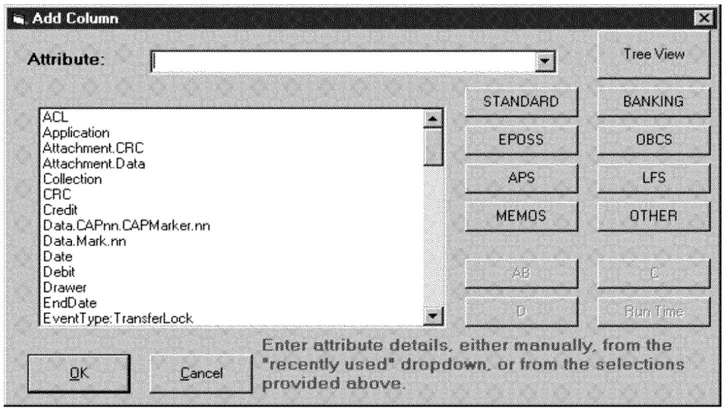
☐ Export Entire Messages
☐ Add CAP and BP Rollover Data
☑ Add ASCII Attachments - EG: Network Banking

Select the columns for your report. If desired, can also include the entire contents of all matching records in the spreadsheet. (Double click to edit)

Select Cols Screen

Figure 18

Note that the current version provides lists of available fields per Horizon application which can be selected by highlighting and pressing <Add> or <Add (tree view)>. See Figure 19 below. Alternatively to reduce the numbers of fields displayed highlight the field in the window and press <Remove>.



Add Column

Attribute:

ACL
Application
Attachment.CRC
Attachment.Data
Collection
CRC
Credit
Data.CAPnn.CAPMarker.nn
Data.Mark.nn
Date
Debit
Drawer
EndDate
EventType:TransferLock

Enter attribute details, either manually, from the "recently used" dropdown, or from the selections provided above.

Add Columns

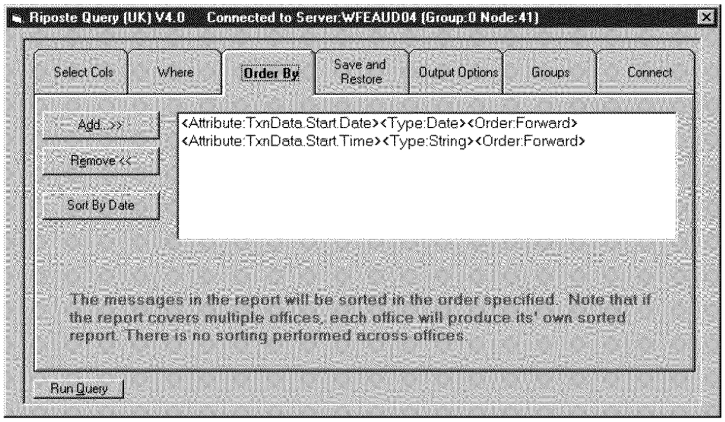
Figure 19

If the user want to retrieve the entire message for a given selection parameters <Remove> all entries in the window and put an 'x' in the <Export Entire Messages> field.

Optionally a field "Add CAP and BP rollover data" or "Add ASCII Attachments – EG; Network Banking" can also be checked.

The user may now want to choose how the results of the retrieval will be presented. To do this go to the <Output Options> Tab.

10.2.4 Order By Tab



```
<Attribute:TxnData.Start.Date><Type:Date><Order:Forward>
<Attribute:TxnData.Start.Time><Type:String><Order:Forward>
```

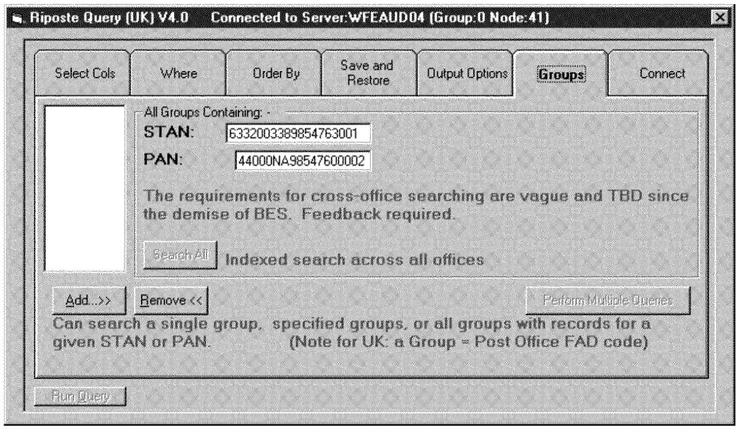
The messages in the report will be sorted in the order specified. Note that if the report covers multiple offices, each office will produce its' own sorted report. There is no sorting performed across offices.

Order By

Figure 20

Selecting the parameter "Sort By Date" is recommended to ensure ascending time sequence (where appropriate).

10.2.5 Groups Tab



All Groups Containing: -

STAN: 6332003389854763001

PAN: 44000NA98547600002

The requirements for cross-office searching are vague and TBD since the demise of BES. Feedback required.

Indexed search across all offices

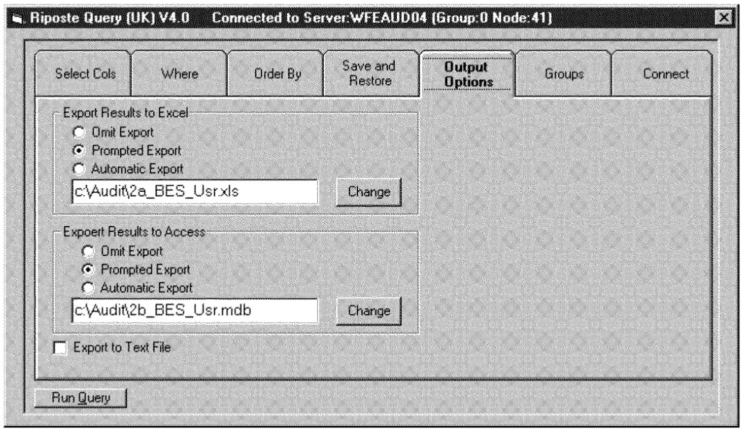
Can search a single group, specified groups, or all groups with records for a given STAN or PAN. (Note for UK: a Group = Post Office FAD code)

Groups

Figure 21

The Groups tab on the R-Query tool is used to specify PAN search criteria.

10.2.6 Output Options



Export Results to Excel
○ Omit Export
● Prompted Export
○ Automatic Export
c:\Audit\2a_BES_Usr.xls

Expoert Results to Access
○ Omit Export
● Prompted Export
○ Automatic Export
c:\Audit\2b_BES_Usr.mdb

☐ Export to Text File

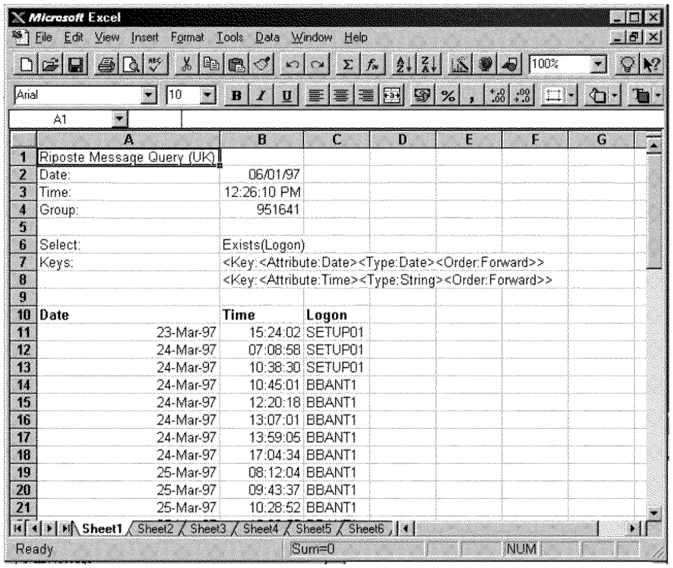
Output Options

Figure 22

By default an Excel spreadsheet is created (default name when selected: C:\Audit\2a_BES_Usr.xls). In the current version there is also an option to export to an MS-Access database (default name when selected: C:\Audit\2b_BES_Usr.mdb) and a text output file.

If the user want to export the retrieved message to either an Excel spreadsheet or an Access database then enter 'x' in the "Export Results to Excel/Access, Prompt Export" field.

Using the template.qry file found in d:\audit data gives the report format as shown below



	A	B	C	D	E	F	G
1	Riposte Message Query (UK)						
2	Date:	06/01/97					
3	Time:	12:26:10 PM					
4	Group:	951641					
5							
6	Select:	Exists(Logon)					
7	Keys:	<Key:<Attribute:Date><Type:Date><Order:Forward>>					
8		<Key:<Attribute:Time><Type:String><Order:Forward>>					
9							
10	**Date**	**Time**	**Logon**				
11	23-Mar-97	15:24:02	SETUP01				
12	24-Mar-97	07:08:58	SETUP01				
13	24-Mar-97	10:38:30	SETUP01				
14	24-Mar-97	10:45:01	BBANT1				
15	24-Mar-97	12:20:18	BBANT1				
16	24-Mar-97	13:07:01	BBANT1				
17	24-Mar-97	13:59:05	BBANT1				
18	24-Mar-97	17:04:34	BBANT1				
19	25-Mar-97	08:12:04	BBANT1				
20	25-Mar-97	09:43:37	BBANT1				
21	25-Mar-97	10:28:52	BBANT1				

Excel Output

Figure 23

Details of the query statement used will appear on the spreadsheet and this provides the evidence to POLIA of the search criteria used, in other words, how their ARQ has been interpreted.

10.3 Running the Query

Normally the user would not actually execute the retrieval scenario until such time as they had built the query statement (the Where tab), selected the fields (Select Cols) and chosen the output medium (Output Options). However, at any time in this sequence they can run the query statement by selecting <Run Query> using the button on the "Save and Restore" tab.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown.

Once this has been done an intermediate screen will be displayed, allowing the file format to be confirmed – select the <Excel> or <Access> buttons or the "text" icon, as appropriate to commence loading the package and complete the data transfer. This will also allow the data format to be checked on-screen.

Note: In the case of very large Correspondence Server files spanning a number of days, an error may be generated on trying to save an Excel file. This will be because the maximum number of rows (records) has been exceeded. Should this occur, the range of dates should be covered, say one or two days at a time, and a number of output files generated.

In rare cases it will theoretically be possible to produce a text output file that is too big to be read by Wordpad. Should this occur, a possible response is to produce output files for a smaller range of dates, or to initially create data as an Excel working file which can be 'Save As' "Text, OS/2 or MS-DOS".

It is good practice to check that all output files can be opened before they are copied to floppy disk or CD-W for onward transmission.

11.0 Data Retrieval – Missing Day

If while retrieving data for an ARQ there is no data retrieved for a day, or a sequence of days (but not all days) duplicate retrieval of data for those missing days from the other server to ensure consistency.

If both servers are consistent, re-run R-Query using *templateMissingDay,rft* from the day before to the day after the missing day.

The spreadsheet is sorted by ID and Number

Check that the number sequencing is contiguous from day to day - normal, automatic housekeeping events, both during the early hours, and at the end of the normal working day, will be present.

If the numbering system is contiguous, it means that there is no sales activity records absent. If in doubt, call Audit Support to verify.

Save the spreadsheet to the ARQ directory and name using the missing day(s) as the title.

Select *Readme for missing day.frt* (if not on audit station use from Janes Directory on Bootle) and complete and save to ARQ directory.

Both should be sent to POL along with the normal ARQ data.

Example - ARQ 464

12.0 Data Retrieval – No Records Found

In the event that during R-Query a message of ‘No Records Found’ is presented for a series of days, it may be that the outlet has been assigned to the incorrect cluster in Horizon. Another symptom of this error is that only two files are brought forward when connecting to the store, and checking for gaps.

Contact SSC in BRA01, Tel GRO Mobile GRO

Ask him to check which cluster the outlet should be assigned to. If it is incorrect in Horizon the Audit Support team should be advised.

Until the necessary changes are made in the system a manual selection of the cluster will be necessary. To connect to the correct cluster follow these steps:-

1. Start a new query in Horizon

2. Specify dates required and select ‘update’, as usual

3. DO NOT enter FAD code into the ‘PO FAD Code’ box as usual

4. Under ‘Audit Point’ select ‘TMS’

5. Under ‘Sub Point’ select correct cluster ie ‘Cluster 1B’ or ‘Cluster 1W’ depending on the server already selected

6. Return, in the ‘FileName template’ box type:

FN01_TMS_CLUSTERXX_X_X_*

CLUSTERXX – type the relevant cluster code ie CLUSTER1B

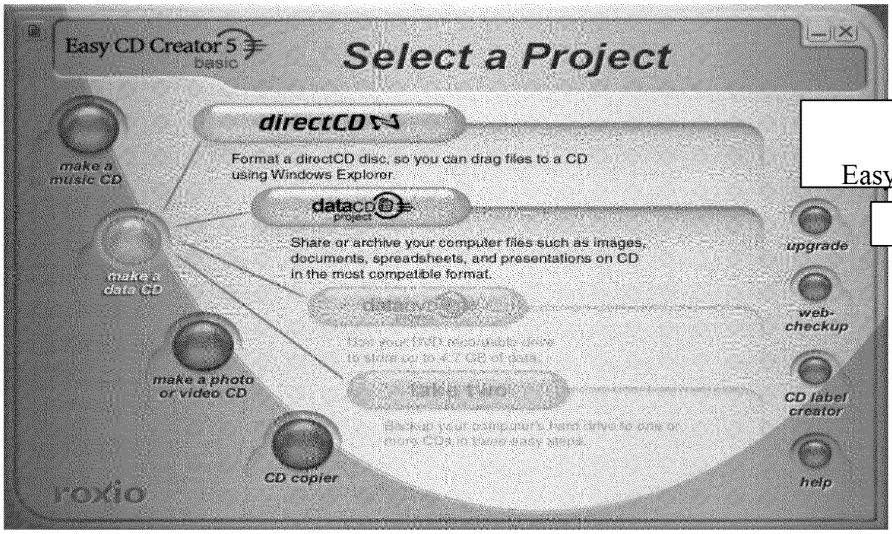
Third X – CLUSTERXX_X – type W or B depending on server chosen

Fourth X – CLUSTERXX_X_X – type number displayed on original ARQ request which resulted in ‘No Records Found’ from ‘Filename for ARQ Ref POIA…’ ie “FN01_TMS_CLUSTER1W_W_6 – this number should also correspond with the third number of the FAD code.

7. Complete data extraction as usual

Creating CDs

Roxio Easy CD Creater is used to copy the ARQ requested information on to CD-R, for despatch to POLIA.



Format a directCD disc, so you can drag files to a CD using Windows Explorer.

Share or archive your computer files such as images, documents, spreadsheets, and presentations on CD in the most compatible format.

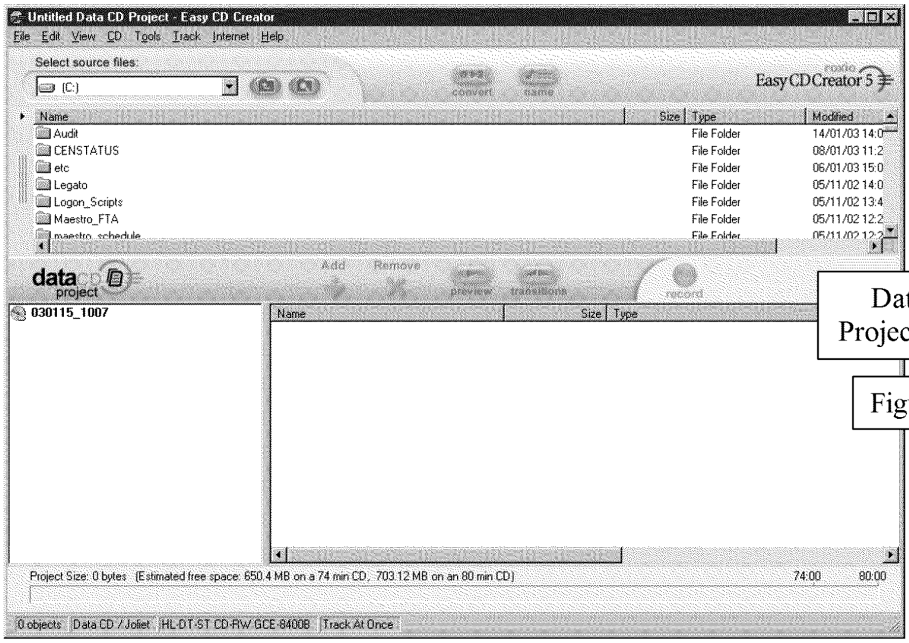
Use your DVD recordable drive to store up to 4.7 GB of data.

Backup your computer's hard drive to one or more CDs in three easy steps.

Roxio –
Easy CD Creator

Figure 24

To launch CD Creator inserts a new CD-R in to the CD writer. This will launch the main screen (Figure 24) The user selects "Make a Data CD", then "Data CD Project" this initiates the Data CD – Easy CD Creator Screen Figure 25.


Untitled Data CD Project - Easy CD Creator
File Edit View CD Tools Track Internet Help
convert
name
roxio
EasyCDCreator 5
data CD
project
Add
Remove
preview
transitions
record

Select source files: (C:)

Name	Size	Type	Modified
Audit		File Folder	14/01/03 14:0
CENSTATUS		File Folder	08/01/03 11:2
etc		File Folder	06/01/03 15:0
Legato		File Folder	05/11/02 14:0
Logon_Scripts		File Folder	05/11/02 13:4
Maestro_FTA		File Folder	05/11/02 12:2
maestro_schedule		File Folder	05/11/02 12:2

030115_1007

Name	Size	Type

Project Size: 0 bytes (Estimated free space: 650.4 MB on a 74 min CD, 703.12 MB on an 80 min CD) 74:00 80:00

0 objects | Data CD / Joliet | HL-DT-ST CD-RW GCE-8400B | Track At Once

Data CD
Project Screen

Figure 25

From here the user selects the source file from the drop down box. The source file should be held on the D:\ under Auditdata\ARQ***. The files will appear in the top window, the user will then drag and drop the required files to the lower window. All CD's will be recorded as 'Closed' to prevent any further data being added to the CD. The CD-W shall be passed to CS Security and checked for viruses after the data has been written to it and before sending it to Post Office Ltd.

In order to adopt 'best practice' processes all data retrieval completed by Security Department staff is to be checked by another prior to despatch. These notes contain the fundamental checks required.

A copy of the original request received from Post Office Limited and the resultant CD will be passed to the checker. The following initial checks should be made:-

- The FAD code has been ticked as checked on the ARQ form
- The written details on the disk reflect the requirements of the ARQ
- The detail of the retrieval has been recorded on the ARQ form

Open the CD, the following checks should be made:-

- The transaction and event files cover the timeframe requirements of the ARQ
- Open the transaction spreadsheet and check the timeframes match the requirements and that the first and last day of the request are present
- Check Group, at the top of the spreadsheet, and FAD number on ARQ form are the same
- Select sheet 2 and check the FAD number listed in column 1 is correct
- She files used cover the timeframe plus 2 days
- 'Size of Gaps' equals 'None'
- Close transaction spreadsheet and open events spreadsheet
- Again, check FAD number and timeframe(s)
- Logon is present at the top of the data retrieved for the first day of the ARQ timeframe requirement (be aware some reports are produced automatically and can be present prior to log on)
- Log off is present at the bottom of the data retrieved for the last day of the ARQ timeframe requirement – if a day(s) is missing check whether day(s) falls on a Sunday or Bank holiday
- Duplicate audit details to those recorded on sheet 2 of the transaction spreadsheet are also held on the events spreadsheet, select sheet 2 and perform a similar check
- Close events spreadsheet
- Retrieval data is held in both 95 and 97 formats
- Open Readme first file and check correct ARQ number has been entered and that personal details and anti-virus information is correct
- Close all spreadsheets and open Access database

- Ensure all data has been recorded and select own name from the drop down 'Checked by' list
- Initial ARQ form as checked and pass back to originator

13.0 Despatch of Audit Data

The audit data is despatched to POLIA contact using Royal Mail Special Delivery. This ensures that a receipt is provided to Post Office Account confirming delivery.

The Prosecution Support Database must be updated to record the date that the extraction activity was started, completed and posted.

14.0 Appendix

Appendix 1 ARQ Form

Appendix 2 Example audit log

Appendix 1

AUDIT RECORD QUERY

Originator:	Post Office Ltd Security Casework Manager P O Box 1 Croydon CR9 1WN	**Date:**	dd/mm/ccyy
Telephone:	GRO		

Witness Statement (delete as applicable)	YES/NO	**REF NO.**	ARQ ####/00

Information Requested			
Date range:		**Post Office**	Name and FAD
GENERAL DESCRIPTION / FORMAT REQUIREMENTS:			
Specific Details:	(PAN or equivalent identifier)		
Signed		**Date**	**dd/mm/ccyy**

FUJ00176265

Appendix 2

```
Log for closed ARQ: POIA149W
          ================================


ARQ created by: jhass01
ARQ Closed:     09/01/03 15:01:44

Actions:
--------
Instance: 5
CommandUsed: Get cluster ID
ErrorCode: -12
Error message: Failed to open the CLUSTER ID file.
StateID: ProcessNOK
Started At: 06/01/03 16:07:54
Ended At: 06/01/03 16:08:41
Generated by: rlaki01

Instance: 4
CommandUsed: Get cluster ID
ErrorCode: -12
Error message: Failed to open the CLUSTER ID file.
StateID: ProcessNOK
Started At: 06/01/03 10:27:07
Ended At: 06/01/03 10:27:23
Generated by: jhass01

Instance: 2
CommandUsed: Get cluster ID
ErrorCode: -12
Error message: Failed to open the CLUSTER ID file.
StateID: ProcessNOK
Started At: 06/01/03 09:55:49
```

```
Ended At: 06/01/03 09:56:04
Generated by: jhass01

Instance: 1
CommandUsed: Get cluster ID
ErrorCode: -12
Error message: Failed to open the CLUSTER ID file.
StateID: ProcessNOK
Started At: 06/01/03 09:49:37
Ended At: 06/01/03 09:50:23
Generated by: jhass01

Instance: 0
CommandUsed: Create directory structure
ErrorCode: 0
Error message: No error message held.
StateID: ProcessOK
Started At: 06/01/03 09:48:48
Ended At: 06/01/03 09:48:59
Generated by: jhass01



Files and status of files used by: POIA149W
================================================
This ARQ did not utilise any files.
Total number of files utilised: 0
```

14.1.1

14.1.1.1 Heading 4 Style

14.1.1.1.1 Heading 5 Style