FUJ00171967

Document Title:	Network Banking Internal Audit Requirements
Document Type:	Requirements Specification
Release:	Network Banking
Abstract:	This document presents the Internal Audit requirements for improving the performance of the audit solution to accommodate Network Banking and subsequent Post Office services.
Document Status:	APPROVED
Originator & Dept:	Jan Holmes (Quality & Audit)
Contributors:	Richard Laking
Reviewed By:	Richard Laking, Roger Donato, Tony Hayward, Alan D'Alvarez, Graham Hooper, Simon Fawkes, James Stinchcombe, Geoffrey Vane
Comments By:	
Comments To:	Originator (& Pathway Document Controller)
Distribution:	ICL Pathway Document Management

Ian Morrison (IDPU)	Richard Laking (IDPU)
Dave Hollingsworth (ASD)	Roger Donato (CRG)
Graham Hooper (Security)	Alan D'Alvarez (NWB PM)
David Richardson (IDPU)	Simon Fawkes (IPDU)
Geoffrey Vane (ASD)	James Stinchcombe (IPDU)
Bill Reynolds (NWB PM)	

FUJ00171967

FUJ00171967

0 Document control

0.1 Document history

Version	Date	Reason
0.1	24/05/01	Initial draft
0.2	01/06/01	Following internal review
0.3	05/06/01	Following additional work with R.Laking
0.4	18/06/01	Following review cycle. Comments from DR, RL & RD.
1.0	02/07/01	Raised to Issue following final review
1.1	06/07/01	Introducing additional EFTPoS requirements
2.0	13/07/01	Raised to Issue following final review

0.2 Approval authorities

Name	Position	Signature	Date
P. Jeram	Programme Director		

0.3 Associated documents

	Reference	Vers	Date	Title	Source
[1]	IA/REQ/004			Audit Data Retrieval Requirements (CSR+)	PWAY
[2]	SD/DES/115			Audit Data Storage & Retrieval HLD (CSR+)	PWAY
[3]	SD/DES/116			Audit Data Extraction & Filter HLD (CSR+)	PWAY
[4]	TD/DES/086			Correspondence Server Message Store Backup and Recovery for Release 2	PWAY
[5]		0.4	11/06/01	Network Banking Requirements Catalogue	PON
[6]			15/06/01	Network Banking Automation Security Requirements	PON
[7]	CR/FSP/001	1.3	24/01/01	EFTPoS Statement of Requirements	PON
[8]	CR/REP/037	0.2	22/06/01	EFTPoS Options in NWB Timeframe	PWAY

0.4 Abbreviations

Abbreviation	Meaning
ACDB	Auto Configuration DataBase
BA	Benefit Agency
CS	Correspondence Servers
CSR+	Core System Release +
DLT	Digital Linear Tape

FUJ00171967

EFTPoS	Electronic Funds Transfer at Point of Sale
FRMS	Fraud Risk Management Service
GUI	Graphical User Interface
HLD	High Level Design
IAR	Internal Audit Requirement
KMA	Key Management Agent
MSU	Management Support Unit
NBR	Network Banking Requirement
OBCS	Order Book Control Service
OCMS	Operational Change Management System
PON	Post Office Network
PON IA	Post Office Network Internal Audit
PON SI	Post Office Network Security Investigations
SSC	System Support Centre
TNT	Courier Company

0.5 Changes in this Version

Version	Changes
1.1	Introduction of Section 3 EFTPoS
2.0	No comments received

FUJ00171967

0.5 Table of content

FUJ00171967

1 Introduction

ICL Pathway is currently responding to the Network Banking Requirements Catalogue issued by PON in support of their automated network banking project. One key requirement is NBR0448.

Requirement :	NBR0448
	The implementation of the banking product on the Horizon architecture must be seamlessly integrated and transparent to the user. It must not degrade any aspect of the existing service nor must it affect the availability and functionality of existing products. Note: Except for the rearrangement of the menu hierarchy to cater for the introduction of the banking solution.
Impacted System/s:	IBM, ICL Pathway & PON

This document identifies a number of Internal Audit Requirements (IAR) for the audit solution that are required if it is not to be degraded through the addition of Network Banking service.

The Audit Data Storage and Retrieval HLD [2] states that the "…. facilities are designed to be generic and extensible, in particular any new applications introduced into the Horizon system should interface to the Audit Server ….". The design was, however, limited to those storage and retrieval volumes associated with the Horizon system at CSR+ and the current implementation reflects those volumes.

The current implementation, shown at Annex A (Archive and Storage) and Annex B (Retrieval and Extraction), has functioned reasonably well since it was 'switched on' and any failures have been recovered within acceptable timescales.

However, it is clear that the current implementation is operating at its limits and will not, in its current guise, continue to meet the new, increased operational requirements brought about by Network Banking. Section 3 of this document identifies a number of limitations, system and operational, which are being tolerated now but will, unless addressed, cause the audit solution and ultimately the Horizon system, to fail.

The Requirements in Section 4 are raised as Pathway Internal Audit requirements to satisfy Network Banking and have been given a prefix of IA to differentiate them from any requirements placed by POCL in any of their Requirements Catalogues

Section 5 identifies a number of issues surrounding these requirements and any proposed solution to meet them.

2 Related Network Banking Requirements

The following requirements, extracted from the Requirements Catalogue [5], are directly related to the internal requirements identified in this document.

FUJ00171967

Requirement :	NBR0016
	All transactions must be fully auditable, including abandoned transactions (I.e. after a [R] Request has been generated)
Impacted System/s:	IBM, ICL Pathway, LINK & PON

Requirement :	NBR0441
	An audit trail of all transactions and events (including abandoned ones) must be maintained. This has to be in conformance with Banking Standards, Post Office Counters Information Security Policy and a Code of Practice for Post Office Information Security Systems.
Impacted System/s:	IBM, ICL Pathway, LINK & PON

Requirement :	NBR0443
	Data held in outlets can be accessed to enable PON and Consignia audit requirements to be met. Also assistance has to be provided by Suppliers during the life of the contract and for 6 years afterwards to allow information to be accessed to fill obligations to supply information for parliamentary, judicial or administrative purposes;
Impacted System/s:	IBM, ICL Pathway

Requirement :	NBR0445
	The confidentiality, integrity, validity and completeness of data has to be maintained throughout e.g. storage, processes and transmissions, including during periods of service failure and recovery from service failure;
Impacted System/s:	IBM, ICL Pathway, LINK & PON

Requirement :	NBR0446
	In the case of any criminal investigations and prosecutions the audit trail and other information required has to be retained for the duration of the investigation and prosecution. In addition information has to be in accordance with PACE.
Impacted System/s:	IBM, ICL Pathway, LINK & PON

Requirement :	NBR0315
	Access to archived transactions (I.e. over 3 months old but within 7 years) must be available within 24 hours of any request
Impacted System/s:	IBM, ICL Pathway

Requirement :	NBR0444
	On notification of an audit reasonable access to the audit trail and the facility to interrogate the trail shall be supplied to the auditors;
Impacted System/s:	IBM, ICL Pathway, LINK & PON

Requirement :	NBR0459
	The system must be able to support the transaction volumes detailed in version 1.0 of the spreadsheet 'JC BB external sheet 1.00'. This includes hourly peak loads, weekly loads and take on rates. In summary, the system should be capable of supporting; * 29 million NB transactions in year 2002/2003 * 270 million NB and UB transactions in year 2003/2004 * 532 million NB and UB transactions in year 2004/2005 * 638 million transactions in years 2005/2006 and 2006/2007
Impacted System/s:	IBM, ICL Pathway, LINK & PON

Assumption :	NBR0461
	It is assumed that the infrastructure required to support increased online transaction volumes is in place and operational prior to the go live of the Network Banking Release
Impacted System/s:	IBM, ICL Pathway, LINK & PON

FUJ00171967

Requirement :	NBR0057
	The E2E service must support projected workload volumes (including peak throughputs)
Impacted System/s:	IBM, ICL Pathway & LINK

The following Requirement is audit related but not directly to the audit solution.

Requirement :	NBR0442
	Access must be provided to any additional material required to support the records e.g. premises, facilities, services, documentation, information (magnetic or otherwise), staff, procedures and timesheets and other data used directly as a basis for charging.
Impacted System/s:	IBM, ICL Pathway & LINK

3 Related EFTPoS Requirements

EFTPoS is an additional service that is being introduced within Network Banking timescales and will be enabled through the NWB service. Requirements have been defined and these will have an effect on the audit solution in two main areas, transaction volumes and retrieval requests.

Current estimates for transaction volumes assume ~50Million when fully implemented. It is anticipated that the transaction files sent to the Merchant Acquirer on a daily basis will be included in the overall Pathway Audit Archive.

Retrieval requirements are not quantified but have been identified as required.

While each of these requirements is small in comparison to the main Network Banking requirements they act to exacerbate the current situation and reinforce the need to make the improvements identified in this document.

The following EFTPoS requirements, extracted from the Statement of Requirements [7], are directly related to the internal requirements identified in this document.

EFT7	• Support for up to 50M EFTPoS transactions and the authorisation volumes specified by end of year 2. (N.B. See Section 9.3.4. for note on the effect of Authorisation Floor Limits).

EFT18	• Refused authorisations are recorded in the Data Warehouse for recording and reporting purposes.

EFT24	• Use of daily Hot Card File when operating floor limits, (see 4.2.2). However, if the impact on transaction times is negligible and the system design is simplified, the HCF may be cross referenced even when no floor limits are in use.

The following 'Industry Standard Requirement', also to be found in [7], is relevant to the Audit Solution.

FUJ00171967

ISR8	Access to historic information during data retention periods. Chargebacks can be instigated up to 180days after transaction date for Visa schemes, (120 days for Switch). Consequently transaction data must be accessible during these periods.

4 Current Limitations

4.1 Non-Audit Use of Audit Server

The Audit Server is used as a back-up server for a number of key servers within the Horizon system. These include the Correspondence, ACDB, OCMS and KMA Servers. This secondary usage was first introduced in TD/DES/086 : Correspondence Server Message Store Backup and Recovery for Release 2 as a secondary use for the Audit Server that had, at that time, spare capacity.

There are a number of issues with this arrangement :

a. Now that full data volumes are being experienced there are pressures on the schedule to be able to complete all CS backups in time for the primary Audit Solution work to take place.

b. The number of Legato drives (6 per site) was as per the original Audit Solution design [2]. No increase in numbers was made to accommodate the CS backup work.

c. The contention for DLT drives exacerbates the DLT handling issues .

d. The full impact of increases in audit data volumes on the backup activity is not known.

The advent of Network Banking and the experience to date suggests that the use of the Audit Server for non-audit work should be reconsidered and a dedicated solution put in place.

This problem is mitigated through the introduction of a fully automated tape silo.

4.2 Broken Audit Trail

We have experienced the complete loss of the TMS Journal element of the audit trail covering a six-day period from 8th – 14th August 2000. The problem stems from a DLT failure at both sites for the same period of time. It was exacerbated by TNT managing to lose the Wigan tape that was being sent to FEL01 for more detailed analysis. The Bootle tape was sent to Vogon, data recovery specialists, for analysis who confirmed that they would be able to recover some, but not all, of the data. The odds of two DLTs simultaneously failing in the same place in two separate locations must be very high but they did and as a consequence Pathway is technically in breach of contract.

The cause of the failure is not known. However, since 1998 it has been pointed out that the continued manual handling of DLTs increases the risks of accidental or deliberate loss of or damage to tapes and that the introduction

FUJ00171967

of automated tape silos at he Data Centres would mitigate against this (and other) risks.

Evidence obtained during a recent OBCS audit shows that DLTs are not being used and cycled as expected resulting in potential over-use of tapes.

While it is true that this has no direct relationship with Network Banking the increase in transaction volumes and associated retrievals will exacerbate the tape handling problems that are being experienced.

4.3 Escalating Retrieval Requests

The current Archive and Storage implementation of the audit solution is a balance between the cost of storage and the frequency with which data has to be retrieved.

The Audit Data Retrieval Requirements [1], generated with the help of Post Office Internal Audit (and, at the time, Benefit Agency Internal Audit) identified that the number of retrievals that they anticipated requesting would be in the tens per year. Based on this a DLT based solution was implemented.

Since then two further categories of retrieval request have emerged :

a. Retrievals in support of internal support requests, usually made by MSU or SSC. The SSC requests have diminished greatly since they introduced their own rolling 6 months support data store. MSU requests are exceptional and only occur when they cannot source information from the Data Warehouse.

b. PON Security Investigations. This group require data to support their investigations and ultimately prosecutions for fraud. Originally they did not express any requirements for access to audit data so were not taken into account. Historically they were to obtain their data from the Fraud Risk Management Service (FRMS), a BA service that disappeared when BA withdrew from the contract. They are now the main requesters for audit data and have stated, but not substantiated, a continuing need for ~500 retrievals per year.

The debate surrounding the PON SI requirements has been escalated back to the Contract and both sets of solicitors have been involved. Following meetings in May 2000 and March 2001 a letter has been sent to PON accepting that Pathway will perform 50 retrievals per rolling 12-month period. Although accepted at the March meeting, attempts to get agreement to CCN759, which would change Requirement 699 to reflect this, have been rejected. The situation remains unresolved.

4.4 Extraction Process Restrictions

Apart from the limitations of DLT handling at the Data Centres, one of the major limiters to the number of retrievals that can be serviced is the extraction process itself and the architecture of the audit server and workstation.

There are two stages to the retrieval process :

FUJ00171967

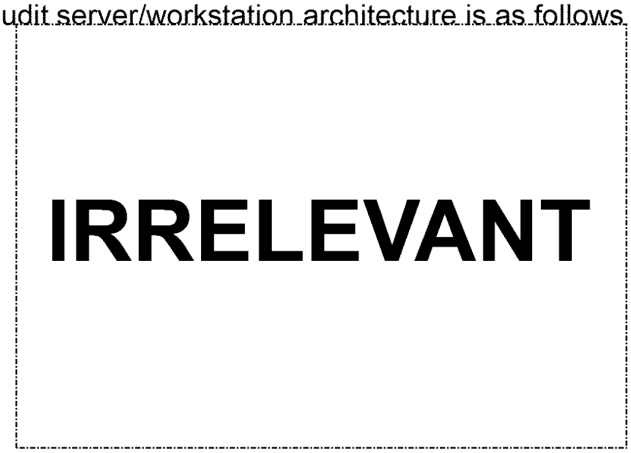
a. Stage one is where data files are retrieved from the DLT and placed into directories on the audit server.

b. Stage two is where the relevant records are extracted from the files on the audit workstation, analysed and written to CD.

For non-TMS files the transition from stage one to stage two is usually achieved by dragging the files across the network. However, for TMS Journals it is necessary to filter out the required Outlet code(s) and date range(s) by generating a pseudo Correspondence Server. This work has to take place on the audit server and it is not possible to run more than 1 such filter exercise concurrently.

This restriction is having an effect on the throughput of retrieval requests that are taking considerably longer than originally anticipated.

The current audit server/workstation architecture is as follows :



The workstations at Wigan and Bootle exist for resilience purposes and anticipated use by North based audit staff. In reality these have never been used in anger and one could be moved to Feltham to provide a dual capability. However, the need to run the filtering activities on the audit server mitigates against any real benefit being derived from this arrangement.

4.5 Conclusion

When implemented and accepted in July 1999 the audit solution was considered to be satisfactory and capable of meeting anticipated workload and transaction levels at CSR+. The Audit Data Storage and Retrieval Design [2] clearly states that limitation.

The completion of rollout and arrival of Network Banking and Universal Banking will bring about significant increases in transaction traffic and likely numbers of retrieval requests. Adding these factors to the current difficulties could lead to further deterioration and ultimately collapse of the audit solution.

FUJ00171967

5 Network Banking Internal Audit Requirements

5.1 Introduce Automated Tape Silos

IAR #001 : Introduce automated tape silos at the Data Centres to improve the efficiency of data retrievals and mitigate against DLT handling risks.

The potential for the introduction and use of tape silos has been the subject of an earlier correspondence culminating in CP2084 raised on 6th July 1999 for a feasibility study into the use of an automated tape silo for the audit server. The user justification was primarily risk based identifying the following key risks :

a. Accidental or deliberate mis-handling of DLTs at the Data Centres.

b. Accidental or deliberate loss of DLTs.

c. Accidental or deliberate damage to Legato drives through increased manual loading/unloading of DLTs.

d. Industrial action/non co-operation by ISD.

e. Potential for unacceptable delay in the audit data retrieval activity on behalf of the customer.

In the event the work was not completed and a Feasibility Report was not produced.

Of the five risks identified 3 have already manifested themselves, two (a. & b.) evidenced by the break in the audit trail described in Para 3.2 and one (e.) in Para 3.4. The arguments for introducing tape silos for the audit server are now stronger than ever and would go a long way to mitigate the impact of larger audit data volumes and increased retrieval requests.

Related NBR Requirements :	NBR0441	NBR0445	NBR0315
	NBR0448	NBR0444	NBR0459
	NBR0461		
Related EFT Requirements :	EFT7	EFT18	EFT24
	ISR8		

5.2 Remove Non-Audit Work on Audit Server

IAR #002 : Remove non-audit related work from the Audit Server.

The Audit Server is used to backup Correspondence and other Servers at the Data Centres. This secondary use causes schedule congestion, unnecessary DLT handling at the Data Centres and can impede the retrieval of audit data if not completed before the start of the normal working day.

The increased volumes introduced with Network Banking will exacerbate this problem.

Related NBR Requirements :	NBR0459	NBR0315	NBR0461

FUJ00171967

Related EFT Requirements : EFT7 ISR8

5.3 Change Audit Server/Workstation Architecture

IAR #003 : Transfer the filtering activity and Correspondence Server build activity from the audit server to the audit workstation.

By relieving the audit server of this workload the potential for parallel builds and filters is limited to the number of audit workstations available and the capability of the operator to multi task.

This would go some way to making the retrieval element of the audit solution truly scaleable subject to the number of Audit Workstations and operators. It follows that improved efficiency at this point in the process must be supported by improvements in the management of DLTs, eg. The introduction of tape silos.

IAR #004 : Move Bootle audit workstation to Feltham.

The workstations in Wigan and Bootle have never been used 'in anger' and better use could be made of one of them if it were transferred to Feltham and placed in the secure room in A0.

Bootle is selected purely on the grounds of convenience and ease of access by the current Audit Manager.

Related NBR Requirements : NBR0459 NBR0315 NBR0448

Related EFT Requirements : EFT7 ISR8

5.4 Enable Retrieval Graphical User Interface

IAR #005 : Improve Resilience of Retrieval GUI.

This was an original CSR+ requirement that was delivered but has not worked successfully for some time.

Related NBR Requirements : NBR0315 NBR0448

Related EFT Requirements : ISR8

5.5 Improve File Selection & Retrieval

IAR #006 : Improve the file selection process to bring about more efficient operation.

IAR #007 : Ensure that current file extraction performance will not degrade with larger data volumes and retention periods.

Part of the Retrieval GUI involves the identification and marking of files for retrieval. This is a time consuming activity that will increase in direct proportion to the volume of data held and requests made for retrievals.

Provide assurance that there will be no degradation in the extraction process as a result of increased data volumes and retention times.

Related NBR Requirements : NBR0315 NBR0448

FUJ00171967

Related EFT Requirements : ISR8

5.6 Confirm Sizing & Technology

IAR #008 : Ensure that the storage technology used is appropriate for the increased volumes and retention period of audit data and the increased retrieval requests anticipated.

Audit data is currently stored on DLT on the grounds of cost and usage as identified in the Audit Data Retrievals Requirements [1]. Network Banking (and subsequently Universal Banking) brings increased data volumes, retention period moving from 18months to 7years and, if PON SI have anything to do with it, potentially a 10 fold increase in data retrieval requests.

Related NBR Requirements : NBR0459 NBR0315 NBR0448 NBR0461

Related EFT Requirements : EFT7 ISR8

FUJ00171967

5.7 Enhance R-Query

IAR #009 : Enhance R-Query to handle Network Banking transactions and improve the useability of the tool.

R-Query is the utility used in the extraction process to interrogate the pseudo Correspondence Server generated on the Audit Server following retrieval from the DLT. The tool provides parameter driven filtering based on the Riposte attribute grammar and export facilities to MS Excel or MS Access.

Network Banking will introduce new attribute grammar to the Horizon system that must be interpretable by both Pathway and PON audit staff.

Related NBR Requirements : NBR0315

Related EFT Requirements : ISR8

5.8 Provide Attribute Grammar Catalogue

IAR #010 : Provide a comprehensive catalogue of the attribute grammar used in the Horizon system.

This requirement has been outstanding for some time. TMS records contain a huge amount of detail whose meaning is defined through the attributes associated with it. Partial catalogues for applications exist in isolation but there is a need to consolidate these into a single Attribute Grammar Catalogue. Without this it is difficult to determine which attributes are the appropriate ones for filtering and almost impossible to decipher a TMS record to determine what the content actually means. This is particularly so for casual users.

This Requirement is important in light of the steady reduction of experienced staff from the project.

Assuming that there will not be any increases in resource to carry out the increased number of audit data retrievals it is imperative that this consolidated document is delivered with Network Banking.

Related NBR Requirements : NBR0315

Related EFT Requirements : ISR8

FUJ00171967

5.9 Capture Network Banking Data

IAR #011 : Capture and store Network Banking audit data that meets contractual, security and audit requirements and in a format that is accessible for subsequent interpretation by ICL Pathway and PON Auditors.

There may be security requirements placed upon the Network Banking data over and above existing audit data such that it may have to be stored in an encrypted form. There is no current requirement for this data to be decrypted on delivery to PON Audit.

Related PON Requirements :	NBR0459	NBR0315	NBR0448
	NBR0461	NBR0057	
Related EFT Requirements :	EFT7	EFT18	EFT24

5.10 Conclusion

The introduction of Network Banking will bring about increases in three key areas :

a. Transaction volumes.

b. Data retention period.

c. Requests for audit data retrievals.

The requirements expressed in this document are intended to mitigate against these increases while at the same time address current system limitations.

By far the most effective improvement would be the introduction of tape silos. There will be a cost associated with this but the alternative is an escalation of the problems we have already experienced. Indeed, the broken audit trail scenario has had to be formally reported to PON IA and we are now technically in breach of contract.

It will not solve all the current problems, for example it will not resolve the issue of the ~500 PON SI requests, but it will go a long way to streamlining both the day to day management of DLTs and the ad hoc data retrieval requests currently received.

6 Issues

There are a number of unresolved issues surrounding these requirements :

a. Neither PON SI nor PON IA have been able to provide substantive figures for data retrievals. A meeting held on 18th June between PON and Pathway identified this as an issue.

b. Who bears the cost of implementing changes to upgrade the audit solution (part of the infrastructure) to handle Network Banking? The changes have to be made to allow Network Banking to operate without degrading the existing service.

FUJ00171967

c. Changes to the audit solution must be made in line with Network Banking timescales. Previous upgrades have been delayed and have only 'worked' due to reduced transaction volumes.

d. The fundamental question of storage medium should be addressed. Is DLT still an appropriate medium for long term data storage with high retrieval requirements? Is it sufficiently robust?

e. The data retrieval process, including DLT loading at the Data Centres, is a manual process and any technological advances will be restricted by the necessary manual interventions unless these are reduced or removed altogether.

FUJ00171967

7 Annex A – Audit Data Archive and Storage Diagram

FUJ00171967

8 Annex B – Audit Data Retrieval and Extraction Diagram

IRRELEVANT