FUJ00226332

Document Title:	Horizon Online Data Integrity for Post Office Ltd
Document Reference:	
Release:	N/A
Abstract:	This document describes the measures that are built into Horizon Online to ensure data integrity.
Document Status:	Draft
Author & Dept:	Gareth I Jenkins
External Distribution:	
Security Risk Assessment Confirmed	YES, security risks have been assessed, see section 0.10 for details.

FUJ00226332

0 Document Control

0.1 Table of contents

0.2 Figures and Tables

0.2.1 Table of Figures

0.2.2 Table of Tables

None.

0.3 Document History

FUJ00226332

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1b	02/04/2012	This is a new document	

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
ARC/GEN/REP/0001			HNG-X Glossary	Dimensions
DES/APP/HLD/0020			Branch Database High Level Design	Dimensions
DES/APP/HLD/0123			HNG-X HLD - Settlement Functions	Dimensions
DES/APP/AIS/0018			XML Message Audit between Counter and BAL/OSR	Dimensions

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

0.5 Abbreviations

Abbreviation	Definition
AP-ADC	Automated Payments – Advanced Data Capture. A mechanism that allows Post Office Ltd to produce scripts for specific transaction processing.
APS	Automated bill Payments Service
BAL	Branch Access Layer. The component that handles the interface from the counter and updated BRDB
BRDB	Branch Database
DRS	Data Reconciliation Service. A system used to reconcile transactions carried out with Financial Institutions.
FAD	Financial Accounting District
FI	Financial Institution
HNG-X	Horizon Next Generation – Plan X. Also known as Horizon Online
HR SAP	An SAP system used by Royal Mail Group to remunerate sub-postmasters
LFS	Logistics Feeder System. A System used to interface with Post Office Ltd's Cash and Stock Management services in POL SAP.
jsn	Journal Sequence Number. Unique identifier for an audited message from a specific Branch and Counter Position.
ONCH	OverNight Cash on Hand. The amount of Cash held in a Post Office Branch overnight. This is used to predict future cash requirements for the Branch.
POL SAP	An SAP system that carries out Post Office Ltd's accounting and cash management functions.

FUJ00226332

RAC	Real Application Cluster Or Request, Authorisation, Confirmation. The mechanism used for interfacing to Financial Institutions
TCP / IP	The standard communications protocol used for communications between the Counter and the Data Centre.
TPS	Transaction Processing System

0.6 Glossary

See also document ARC/GEN/REP/0001.

Term	Definition
Back Office	Administrative Functions carried out in a Post Office Ltd Branch such as Remitting In Cash / Stock
Basket	The set of transactions which are processed together. For example all the transactions associated with a single Customer (including those used for Settlement).
Client	An organisation for which Post Office Ltd acts as an Agent, for example DVLA where Post Office Ltd provides Motor Vehicle licences to customers on behalf of DVLA.
FAD Code	Unique identifier for a Post Office Ltd Branch
Settlement	Those transactions that represent the payment by the Customer for goods or Services or to the customer in respect of Out Pay transactions such as Cash Withdrawals.

0.7 Changes Expected

Changes
Review comments etc.

0.8 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.

0.9 Security Risk Assessment

No identified security risks.

FUJ00226332

1 Purpose

This document is a technical description of the measures that are built into Horizon Online (also known as HNG-X) to ensure data integrity and descriptions as to how those measures apply in each case.

Note that this document only covers Horizon Online (HNG-X). It does not cover the original Horizon system, which is specifically excluded from this exercise. There is a separate document covering the original Riposte-based Horizon system.

Section 2 describes the measures taken in the design of the Counter, Branch Access Layer (BAL) and Branch Database (BRDB) to ensure integrity. Section 3 describes the audit system used to preserve the auditable messages sent from the counter to the Data Centre for use in Litigation Support.

The scope of this paper is restricted to showing the Integrity of the Audit trail and that it accurately reflects the transactions entered at the counter.

FUJ00226332

2 Horizon Online Data Integrity

2.1 Overview of Normal Operation

Horizon Online is designed to store all data in an online database known as the Branch Database (BRDB). This database is a highly resilient Oracle database implemented using Oracle Real Application Cluster RAC (see also section 2.4). In particular no data concerning Business Transactions is retained at the counter other than in the memory of the Counter Business Application.[1]

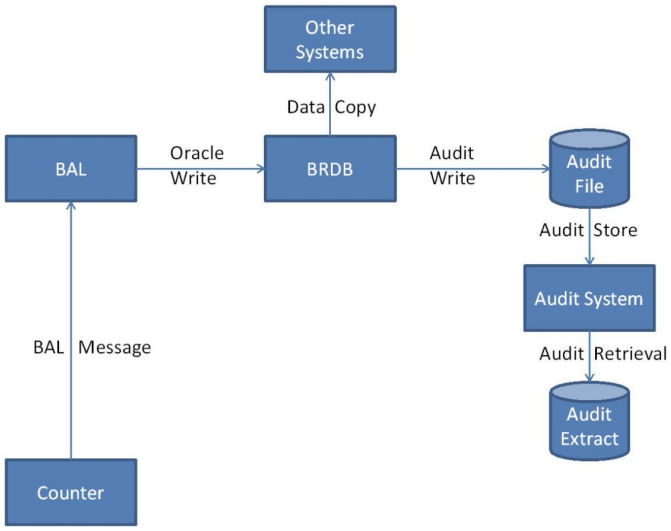

Figure 1 – Primary message flows

Transactions are carried out locally on the Horizon Online counters and a Basket is built up during a Customer Session. Each transaction will result in a Basket Entry consisting of one or more Accounting Lines. At the end of a Customer Session when the Basket has been completed and all Settlement items (or Tender lines) have been processed and added into the Basket as further Accounting Lines, such that the total value of the Basket is zero, the entire Basket is sent to the Data Centre as a BAL Message where the Branch Access Layer (BAL) processes the message and all the Accounting Lines are recorded and committed to the BRDB as part of a single Oracle Commit. This means that either **all** the transactions within a Basket are successfully written or **none** of them are. Once the Accounting Lines have been successfully committed a response is returned to the counter indicating this success and this then allows any receipts to be printed. The Basket is deemed to be fully completed once all relevant receipts have been successfully printed. Note that if there are no receipts to be printed, then the screen is updated to show the top level menu indicating successful completion of the previous Basket.

The Oracle Commit also includes an Audit of the data originally transmitted from the counter to the BRDB. This data is digitally signed at the counter using a key generated as part of the Log On process. It is this audit record that is used to provide the extract of transactions used for Litigation support. Section 3 describes how this audit record is managed after it is committed to BRDB.

[1] In order to support recovery as described in section 2.3.6, the identifier of the last successfully completed Basket is recorded on the Hard disk at the counter. However this is not classed as Business Data.

FUJ00226332

The audit record may also include application events that have been accumulated at the counter since the last auditable message was sent to the Data Centre. All major activities that affect the Branch also have an audit of the data sent from the counter to the Data Centre included in the audit log. Such activities include:

- Log On / Log Off of Users at the counter
- Creation / modification of User Accounts (including change of password)
- Attaching Users to Stock Units
- Balancing a Stock Unit
- Producing the Branch Trading Statement.

Each Audit record includes the following identification:

- Branch identifier (i.e. FAD Code)
- Counter identifier
- Sequence Number (known as a Journal Sequence Number or jsn)
- Counter timestamp

Within any counter (i.e. for a given Branch Id / Counter Id combination), the jsn will always increase by exactly one for each successive audit record. This enables a check to be made that there are no records missing from the audit trail when they are retrieved.

The transactions in a basket are constructed using the principle of double-entry bookkeeping. This means that in addition to the Accounting Lines that relate to the actual business transactions, separate Accounting Lines are also generated for the tender items (such as Cash, Cheques or Credit / Debit Cards), resulting in the total value of all Accounting Lines in a Basket adding up to zero. When the contents of a Basket are written to BRDB a check is made that the net value of all the accounting lines is indeed zero and should it not be, then an alert is raised and the basket is discarded and an error response returned to the counter.

> *Note that this could only happen as a result of a bug in the code and this check is included specifically to check for any such bugs.*

Baskets are also built up during Back Office Sessions and such Back Office baskets are handled in a similar way to Customer Baskets.

2.2 Detail of Normal Processing

The purpose of this section is to expand on the summary in Section 2.1 and identify other documents where more detail of the various steps are covered.

As outlined in section 2.1 above, the following is the key behaviour of the handling of a Basket:

1. The Clerk carries out one or more business transactions. Each Business transaction will construct a Basket Entry which is held in the memory of the counter and the value of which is visible on the screen.
2. When all the transactions for a customer have been completed, the clerk selects either the *Fast Cash* or the *Settle* functions on the screen.

> *Note that if the total basket value is zero at this point then either button will result in immediately going to step 3 below.*

FUJ00226332

a. Selecting *Fast Cash* results in the system calculating the amount to required to take the total value of the transactions in the basket to zero and constructs a Basket Entry for the Cash Product for this amount and adds it into the Basket. By definition, the total value of the basket at this point will be zero

b. Selecting Settle results in the system displaying a menu of permissible settlement options. The allowable settlement options are configurable and depend on various Business Rules, however are likely to include the following:

i. Cash

This allows a specific amount of cash to be entered (which may or may not be the full amount). It will take a sign based on attempting to move the Basket total nearer to zero.

A corresponding Basket Entry is created and added to the in memory and On-screen basket display with an updated total.

ii. Cheque

This allows a specific amount for a Cheque to be entered (which may or may not be the full amount). Its sign will always reflect the fact that a cheque is payable to Post Office Ltd (other than for Reversals).

A corresponding Basket Entry is created and added to the in memory and On-screen basket display with an updated total.

iii. Chip and PIN

This allows Chip and PIN transaction to be processed. The amount to be taken is entered, but defaults to the maximum amount allowable by business rules (which may or may not be the full amount). Its sign will always reflect the fact that a payment is being made to Post Office Ltd (other than for Reversals).

The details of the Business Rules are not relevant to the Integrity of the system.

A corresponding Basket Entry is created and added to the in memory and On-screen basket display with an updated total.

iv. Swipe

This allows magnetic swipe payment card to be processed. Note that if the Magnetic stripe indicates that the card is a Chip and PIN card then the transaction will be abandoned at this point. The amount to be taken is entered, but defaults to the maximum amount allowable by business rules (which may or may not be the full amount). Its sign will always reflect the fact that a payment is being made to Post Office Ltd (other than for Reversals).

The details of the Business Rules are not relevant to the Integrity of the system.

A corresponding Basket Entry is created and added to the in memory and On-screen basket display with an updated total.

v. Fast Cheque

This allows Cheque transaction to be processed. However in this case the system calculates the amount required to take the total value of the transactions in the basket to zero and constructs a Basket Entry for the Cheque Product for this amount and adds it into the Basket. By definition, the total value of the basket at this point will be zero

vi. Fast Cash

FUJ00226332

This is the equivalent of the Fast Cash Button described at point a above

c. The User is then able to select any of the available options and add appropriate settlement items into the In memory and On-screen basket as descried. Should the Total value of the Basket not be zero after processing the settlement transaction, the settlement menu is re-displayed allowing further settlement transactions to be selected until the net value of the Basket becomes zero.

3. Once the Basket Total becomes zero, a message is constructed to send the entire basket content to the BAL. The structure of the message sent is defined in [DES/APP/AIS/0018]. A new connection is established to the BAL in order to send this message. The message sent is defined as being an auditable message and so will include a jsn. It may also pick up any outstanding Audit Events and Statistical data that have been accumulated at the counter since the last auditable message was sent from the counter to the BAL. This message will be signed by the counter using a Digital Signature constructed using a key that has been generated as part of the Log On process. This Digital Signature is sent as part of the message to the BAL.
4. When the BAL receives the message it detects that there is an associated jsn. This means that the Audit Filter is invoked which results in the entire data sent from the counter being added to the BRDB table BRDB_RX_MESSAGE_JOURNAL.
5. The BAL then processes the message and updates other tables in BRDB.
6. If all these updates are successful, then the BAL invokes a COMMIT to Oracle on BRDB which will commit all the changes at steps 4 and 5. Should there be any failure, then the BAL will issue an Oracle ROLLBACK which results in none of the changes in steps 4 and 5 being saved and it is then as if the interaction from the counter didn't take place. In either case a suitable response is returned to the counter and the connection tot the counter is closed.
7. When the counter has sent the message to the BAL (at step 3), it waits for a Response. There are 3 possible responses that can occur:

   a. The BAL update was successful (this is the normal case)

   b. There was a failure from the BAL

   c. No response is received within a configurable timeout period (usually 30 seconds)

   The first case is normal. The last 2 cases are considered to be Error Scenarios and are considered further in section 2.3, but are considered to be out of scope of the normal processing.
8. When the response is received, any receipts required are printed and then the In-memory and On-screen baskets are cleared and the screen is updated to the "Home" screen ready for a new Basket to be started.

Overnight, the content of the table BRDB_RX_MESSAGE_JOURNAL is copied to a set of serial files and passed to the Audit system. There is more information on this audit process in section 3 of this document.

2.3 Error Scenarios

2.3.1 Recoverable Transactions

Simplistically it could be assumed that if a Basket fails to commit then the content of that basket can just be discarded.

This is similar to the normal model presented with on-line shopping, in that if your browser fails after trying to commit the basket, you are uncertain as to whether your purchase has been processed or not.

FUJ00226332

You then need to carry out some other activity (e.g. phone the provider or check your Credit Card account the next day) before knowing whether or not to re-attempt the transaction.

However this is not really appropriate in a Post Office environment. For many transactions it can be assumed that the Basket has failed to commit and so the transactions in the basket are discarded and they can be re-attempted at some later date. However in some cases this is not appropriate since the Transaction may have had an impact on some external system. An example of this is a Banking Cash Withdrawal. In this case the Bank has been informed of the Transaction during the processing of the Banking Transaction and has removed the funds from the Customer's account. Therefore it is important that this transaction is completed. Such transactions are considered to be Recoverable Transactions.

If a transaction is to be Recoverable, then information about that transaction is recorded in the BRDB when the transaction is first initiated (and before the transaction is sent to the FI) allowing the transaction to be recovered should there be a failure. Note that this recovery information is not audited.

There are many types of Recoverable Transaction:

- All Banking transactions
- All Credit / Debit Card transactions
- All E-Top up transactions
- All Reversals
- Selected AP-ADC transactions (as defined in the transaction script)

2.3.2 Failures

Any failures in committing Auditable activities at the Data Centre will result in an error response being returned to the counter. Such an error response will be displayed to the User, thus informing them of the situation. The next action then depends upon the Auditable activity:

- If it relates to a basket settlement where the basket that contains 1 or more Recoverable Transactions, then a Forced Log Out is initiated and the normal Recovery process will tidy things up
- If it relates to a basket settlement where the basket doesn't contain any Recoverable Transactions, then the content of the basket is discarded and the User is returned to the Menu to continue working
- If it relates to a non-basket activity, then activity is abandoned and the User is returned to the Menu to continue working

In all cases the User is informed of what is happening.

Such failures will not be visible in the transaction audit, but may be visible in the system Event Log.

2.3.3 Time Outs

Should there be no response from the Data Centre following an attempted commit of an auditable activity within a timeout period (currently set to 30 seconds), an automatic retry is invoked. This sends identical business data to the Data Centre where a check is made to see if the Audit data has already been committed to BRDB.

- If it has been committed, then this means that the original activity was successful, but the response did not reach the counter in time. Therefore no action is taken in terms of updating the BRDB and a Success response is returned to the counter.

FUJ00226332

- If it has not been committed, then the original activity either didn't reach the Data Centre, or it failed to be processed. In either case it is safe to re-process the data and the appropriate response is returned to the counter after the data has been processed which will be handled as if it was from the original request. Note that re-processing the data will include recording an audit of the data if the reprocessing is successful.

Should the retry also timeout, then the User is prompted and asked whether they wish to Retry or Cancel the Activity.

- Selecting Retry results in the Activity being retried once more as described above. If this also times out, then a further automatic retry is attempted and if this is still unsuccessful, then the User is again prompted as to whether to Retry or Cancel. This cycle then continues until either there is success, or the User finally gives up and selects Cancel.
- Selecting Cancel results in a Forced Log Out being invoked.

Such time-outs and any retries will not be visible in the transaction audit, but may be visible in the system Event Log.

2.3.4 Forced Log Out

Continual failures to Update the Database at the Data Centre mean that it is not clear at the counter whether or not the database accurately reflects the situation in the Branch. Therefore the safest thing is to force a Log Off at the counter and ensure that when communications are re-established, that the Recovery process is invoked to reconcile the counter view with that on BRDB.

If there is a basket currently being processed, then a special Disconnected Session Receipt will be produced showing which transactions have been discarded and which are to be recovered making it clear what money needs to be exchanged with the Customer.

2.3.5 Terminal Failure

Clearly a counter terminal can fail at any time. However the situation is not very different from that where a failure to contact the Data Centre has occurred as described above. Therefore the behaviour of the User needs to be as follows:

1. Work out the value of any Recoverable Transactions (there ought to be printed receipts associated with all of these)
2. From this work out what is owed to, or due from the customer
3. Consider whether any Credit / Debit Card payments may have been successful
4. From this work out any cash due to / from the customer.
5. Write out any necessary receipts by hand
6. Keep a record of exactly what happened to be used at Recovery time.

Clearly in this case the system is unable to assist the User in guiding them as to what to do.

2.3.6 Recovery

Recovery after a failure must always take place on the same counter position. Note that if the terminal has failed and needs to be replaced by an engineer, then recovery cannot be carried out until the replacement terminal is working correctly.

At every Log On a check is made in the Central Database to see if any Recovery is required. The following checks are carried out:

FUJ00226332

1. Is there any outstanding Recovery Data associated with this terminal?

   If so return the outstanding Recovery Data to the counter so that the transactions can be recovered using Rollforward Recovery

2. Did the last session carried out on this terminal have a tidy Log Off?

   If not, return details of the last Basket (if any) that was successfully written from the last Log On session to the counter so that further recovery checks can be made

Otherwise all is well and No Recovery is required (i.e. the normal case).

During the Log On process, if the counter receives an indication that recovery may be required (i.e. one of the two cases described above), then the following occurs before the Log On is completed:

1. If Rollforward Recovery is requested, then for each Transaction with associated Recovery Data, then the appropriate Recovery script is executed, which will result in a Rollforward Recovery Basket being produced which is then settled to the Branch Database as normal and this will generate a recovery Receipt. This will normally match any Disconnected Session receipt (or other information recorded at the time of failure).
2. If there was no Basket Details of a Last successful Basket returned, then No Recovery is required
3. If further checks are requested, then the following checks are made at the counter:
   a. What was the identifier of the last successful Basket sent from the counter?

      The identifier of the last successful Basket is written to the Counter Hard Disk at the completion of the basket (i.e. after all Receipts have been successfully printed).

      Therefore, provided that the Terminal has not been replaced, then this is available to be checked for automatically.

      Where the terminal has been physically replaced, a dialogue is invoked to get the user to confirm the identity of the last Successful session which may involve displaying the last basket known to the Data Centre.

   b. If this matches the identifier of the Last Successful Basket that was returned from the Data Centre, then No Recovery is required and all is well.

   c. If they don't match (i.e. the Basket returned from the Data Centre was the one that the counter was trying to save at the time of failure), then the Forced Log Off process will have assumed that the Basket failed. Therefore the Recovery process needs to generate a Basket that reverses any non-recoverable transactions in that basket (since the forced Log Off would have discarded them). This is known as Rollback Recovery. This will also produce a Receipt. However it will not match the Disconnected Session Receipt exactly.

2.4 Database Characteristics

The database uses Oracle version 10gR2. It uses an Oracle Real Application Cluster (RAC), which runs the database over multiple nodes (servers). In practice there are normally 4 such database nodes

Partitioned tables store branch specific data. This provides high performance and scalability. Applications need to know in which partitions data is stored and which nodes manage these partitions. They use a convention based on Branch codes.

The design of the Branch Database supports non-stop trading during core hours.

FUJ00226332

- Oracle RAC is resilient. If one node fails, the remaining nodes carry on running and the database remains available for use. The database can meet its performance targets if one node fails.
- The standby database allows very fast recovery if there is a data corruption that takes the live database offline. The maintenance of the standby database is automatic.

A disaster recovery site remotely mirrors the data. The mirroring of data is synchronous. This guarantees that no data is lost if there is a catastrophic site failure.

Data associated with a Basket is stored in 3 separate areas of the Branch database:

1. A copy of the actual Basket data as transmitted from the counter together with the associated digital signature is held in a table known as the message journal.

   Use of the data in the message journal is described further in section 3.

2. Individual accounting lines are extracted from the basket and each accounting line is written to two separate tables:

   a) Detailed transaction information for passing to Post Office Ltd Back end systems

      This data is retained for sufficient time to ensure it has been successfully passed to Post Office Ltd's back end systems (in practice it is held for about 4 days)

   b) Summary transaction information to support reporting and Branch accounts

      This data is retained to allow it to be used for any reporting and accounting period within the branch (in practice it is held for about 60 days)

Each night the reporting data is summarised within the branch database to provide daily totals for transactions based on product, mode, stock unit and accounting period. This summarised data is used (together with transactions for the current day) when balancing a stock unit, thus minimising the amount of data that needs to be considered.

Although the data used for generating the counter reports and passing to Post Office Ltd's back end systems is taken from the tables described in point 2 above, any data provided by Fujitsu in order to support litigation is based on the Audit taken at point 1 above. Since the processing for producing any report is based on the same source of data (ie the audited data sent from the counter) it is asserted that any report could be regenerated based solely on the audited data. As described in section 2.1, the audited data consists not only of the Basket information, but also any other significant events and in particular the Opening Figures (ie cash and stock levels) calculated at the start of a new period based on the balancing of an accounting period.

> *It should be noted that such data is **not** presented as evidence as part of the normal litigation support service. Similarly we do **not** have tools that extract data such as Opening Figures into a readable form or to be able to re-generate reports based on the audit trail. However such data **is** available in the audit trail, and if required, such tools could technically be developed to resolve any dispute in that area. (Though there are clearly commercial considerations in terms of the cost and effort involved in doing so.)*

FUJ00226332

3 Audit System

As outlined in section 2.1 and described in section 2.4, any auditable message from the counter is stored, together with its Digital Signature and other key attributes in an "Audit table" (known as the Message Journal) in BRDB.

To ensure that the message is not tampered with after being sent from the counter, each message has an associated Digital Signature. The mechanism for creating this Digital Signature is as follows:

1. At Log On, the Counter creates an RSA Public / Private key pair.
2. The Public key is sent to the BAL as part of the audited Log On message
3. The Log On message is concatenated with the Digital Signature and the BAL's signing certificate for its Public Key and signed by a BAL Private key (held in the data Centre Key Store) and added to the audit trail with a BAL generated jsn
4. All subsequent messages are digitally signed by the counter using the private key established at Log On.
5. Digitally Signing a message involves taking a SHA-1 Hash of the message and digitally signing the Hash value using RSA.
6. The Digital signature is stored alongside the message in the Journal table and is extracted with it into the Audit file as described below

Each night after midnight, the contents of this table for the previous day are copied from the BRDB to a number of serial files.

> *A number of files are generated due to the volume of data processed each day. All data from a given Branch will be concentrated into a small number of these files for ease of retrieval.*

At this point a check is made that indeed there are no missing or duplicate jsns for any counter and should any be found an alert is raised.

> *Note that this could only happen as a result of a bug in the code or by somebody tampering with the data in BRDB and this check is included specifically to check for any such bugs / tampering.*

These files are then copied to the Audit system where they are sealed with digital seals. They are held there for a period of 7 years during which time they may be retrieved and filtered to produce the relevant audit data for a particular Branch.

The Digital Seal is calculated using an MD5 hash of the entire content of the file being sealed. This value is stored in a separate "Seals Database" held on the Audit Server.

Whenever data is retrieved for audit enquiries a number of checks are carried out:

a) The audit files have not been tampered with (i.e. the Seals on the audit files are correct)
b) The individual Baskets (and other records) have their digital signatures checked to ensure that they have not been corrupted.

> *This involves finding the Public Key which has been saved with the Log On message and also checking the integrity of the Log On message using the Public Key Certificate of the BAL's signing key which is stored as part of the Log On audit message.*

c) A check is made that no records are missing or duplicated. I.e. a check is made that there are no gaps or duplicates in the jsn sequence for any counter.

It should be noted that this same Audit system was used to hold similar data from the old Horizon system. However on the old Horizon system the audit point was the message journal on the Riposte Correspondence Servers and thus the technology used for producing the audit of data is completely different between the old Horizon system and Horizon Online.