FUJ00172083

cutting through complexity™

HNG-X Data Integrity Phase 0 Report

KPMG Risk Consulting

Report

April 23rd 2012

Version D.004

FUJ00172083

Contents

Disclaimer

This Report is provided solely for the use of Fujitsu in connection with its engagement of KPMG LLP to carry out an independent data Integrity assessment, and for no other purpose. It is based on the information represented and supplied to us by Fujitsu, which has not been independently verified by us.

This Report should not be disclosed to any person or referred to, in whole or in part, other than for Fujitsu internal purposes.

FUJ00172083

Executive Summary

FUJ00172083

Executive summary

Phase 0 – Documentation Readiness Review

Introduction

In accordance with our Letter of engagement signed 26 March 2012, we have completed the Phase 0 work - the documentation readiness review.

Our approach

We have based this report on the information contained in the Fujitsu document "Horizon Online Data Integrity" ref ARC/GEN/REP/1229 dated 25 November 2011together with a sample of additional High and Low Level Design Documents, a site visit to witness a demonstration of the system and subsequent clarification dialogue between KPMG and your system architects.

Our findings

Based on the initial review of documents supplied to us, we believe the documentation to be at a suitable level in terms of scope and detail to enable the processing to be understood and to enable controls to be identified for inclusion in the formal review and assessment Stage.

We have set out in the following section the control points that we have identified against each of the six assertions that you have asked us to consider as part of this review

Scope and exclusions

Excluded from scope are the integrity of the Oracle Real Application Clusters and any issues relating to service reliability and stress testing of all or part of the Horizon Online system. Also excluded from scope are the testing of IT infrastructure controls such as general controls reviews and security assessments. Fujitsu assert that these have been covered in separate reviews and audits, and that we may review and refer to the work of those reviews where necessary for the purpose of our testing and reporting.

Scope and exclusions (cont'd

The deliverable reports from this engagement are not, and will not be treated as, expert witness reports or opinions. As agreed with Fujitsu's legal counsel, third parties should not rely on the deliverable reports as constituting a formal audit or as having reviewed or proved anything not expressly set out in the reports. Fujitsu have drafted commercial terms governing the potential requirement to distribute the reports externally. This will be agreed with KPMG and included in the final deliverable reports as a condition of its release to Fujitsu's third parties.

Budget for testing and reporting

We have considered the resource required to test the controls identified in the following section as underpinning the six assertions supporting the completeness, accuracy and integrity of the audit trail and quote a fee of£131k (in addition to the Phase 0 work already undertaken). This represents a reduction from our earlier fee quote of £205k in total for 20 controls.

Conclusion

We have completed Phase 0 and identified the necessary control points which will require testing to support each of the six assertions.

We hope that you find this satisfactory and look forward to working with you on the next phase of this important project.

GRO

Ervin Jocson, Director KPMG Technology Risk Consulting

FUJ00172083

Control points identified for assertions

FUJ00172083

Assertion 1 – Baskets net to nil

That all of the transactions in a basket (a basket is defined as any number of items for one customer) received from the Post Office branch counter balance to zero against the customer payment.

Nr	Identified control points
1	When the contents of a Basket are written to the 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.
2	The transaction cannot be completed until a successful response has been received from the BAL indicating that the message has been stored.
3	Any failures in committing Auditable activities at the Data Centre will result in an error response being returned to the counter. 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.

Assertion 2 – Basket received is same as that seen by counter

That the basket received at the data centre corresponds to what the counter staff sees on the HNGX screen.

Nr	Identified control points
1	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:
2	1. At Log On, the Counter creates an RSA Public / Private key pair.
3	2. The Public key is sent to the BAL as part of the audited Log On message
4	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
5	4. All subsequent messages are digitally signed by the counter using the private key established at Log On.
6	5. Digitally Signing a message involves taking a SHA-1 Hash of the message and digitally signing the Hash value using RSA.
7	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
8	The first thing BAL does is to record the message

Assertion 3 – Full basket enters audit trail

The full basket goes into the audit trail.

Nr	Identified control points
1	The first thing BAL does is to record the message
2	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.
3	Each night after midnight, the contents of this table for the previous day are copied from the BRDB to a number of serial files.
4	After copying the previous days files 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.
5	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. Should the retry also timeout, then the User is prompted and asked whether they wish to Retry or Cancel the Activity. Such time-outs and any retries will not be visible in the transaction audit, but may be visible in the system Event Log.
6	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.

FUJ00172083

Assertion 4 – All baskets enter audit trail

All baskets get into the audit trail.

Nr	Identified control points
1	Access controls restrictions ensure counter staff cannot access the audit trail to change data other than through the defined process for inputting data via the counter system
2	Access to the counter system which enables the entry of transactions via the BAL is controlled through a secure key exchange mechanism.
3	The jsn is stored within the message body which is securely encrypted using cryptographic keys
4	A check is made that there are no gaps or duplicates in the jsn sequence for any counter.
5	Every auditable request made by the counter will be logged in the message journal before the request is actioned by the BAL, The message journal performs two functions, firstly it provides auditing facility and secondly it provides a duplicate checking facility to prevent counter messages that may have been resent from being reprocessed.

Assertion 5 – No extra baskets enter audit trail

No extra baskets get into the audit trail (i.e. nothing is added that the counter staff has not seen on the HNGX screen).

Nr	Identified control points
1	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 duplicated audit records
2	Every auditable request made by the counter will be logged in the message journal before the request is actioned by the BAL, The message journal performs two functions, firstly it provides auditing facility and secondly it provides a duplicate checking facility to prevent counter messages that may have been resent from being reprocessed.
3	Access to the counter system which enables the entry of transactions via the BAL is controlled through a secure key exchange mechanism.
4	The jsn is stored within the message body which is securely encrypted using cryptographic keys
5	A check is made that there are no gaps or duplicates in the jsn sequence for any counter.

Assertion 6 – Audit trail has integrity

That the integrity of the audit trail has been maintained.

Nr	Identified control points
1	Each message within the audit trail has its message body encrypted using the cryptographic keys used by the counter submitting the basket.
2	The jsn is stored within the message body which is securely encrypted using cryptographic keys
3	Each night after midnight, the contents of the message table for the previous day are copied from the BRDB to a number of serial files.
4	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.
5	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.
6	Whenever data is retrieved for audit enquiries a number of checks are carried out:
7	a) The audit files have not been tampered with (i.e. the Seals on the audit files are correct)
8	b) The individual Baskets (and other records) have their digital signatures checked to ensure that they have not been corrupted.
9	a) 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.
10	There is adequate synchronisation of server and counter clocks throughout the process for time and datestamping purposes

FUJ00172083

Control Testing

FUJ00172083

Phase 2 – Controls testing fee quotation

Our fee quotation to test the controls identified in the preceding section and provide a report on the effectiveness of their design, implementation and operation is as follows.

Tasks	**Number of Days**	**£Total**
Controls testing of 21 discrete controls (as listed in previous section)	68	117
Mobilisation	3	5
Review and Reporting	5	9
Total	**76**	**131**

This quotation is subject to all the terms, conditions and caveats of our Letter of Engagement dated 22 February 2012 and signed by Fujitsu on 26th March 2012 and the above table is to be regarded as an updated and more specific version of the tables on page 5 of that Letter.

Note – based on our review of design documentation and logic of the controls we believe that there will not be a requirement to undertake a separate data analysis stage. Should the identified controls not be operating effectively then we would need to reconsider the need for data analysis.

FUJ00172083