

Potential Audit Issue – Horizon

The following is not necessarily intended to be the vehicle via which we communicate the issue to management in R&RMG. But is intended to be a first draft via which we clarify our thoughts as to what needs to be said. It is also only at this stage, targeted at the initial goal of defining the problem for R&RMG management and is **certainly not** intended for wider consumption eg with Post Office in its current state.

1 Summary

An email dialogue on Peak PC0152376 started a line of enquiry in the audit space. It appears that in certain situations the Horizon counter application may find itself locked out from writing to the Riposte Message Store. The PEAK 152376 describes one such occurrence. Information from the Riposte Message Store is a key element in the information built up in the Horizon Audit system and on request supplied to Post Office to support evidence in court cases. If the counter were to mis-handle a financial transaction, whilst simultaneously failing to write to the Riposte Message Store, this could have potentially serious implications on the integrity of the audit information supplied to Post Office.

The other factor is the POL investigation into Branch 141832 “Craigpark” which is related to Peak 152376 (or perhaps a similar peak). A consequence of this is that POL are aware that we have had an issue on this branch and also another benign occurrence of the event at a different time. They are now asking questions about the extent of the issue. It was this thread that cause things to be escalated (the Peak had been considered inconsequential and it had been agreed not to fix it in RMF).

At this stage we do not have tangible evidence that this is the case, but there are sufficient concerns given the seriousness of the eventual use, that warrant further detailed investigation.

At the time of writing – this investigation continues as a matter of the highest priority.

The following problem description is taken from the Kepner Tregoe Systematic Approach to Problem Solving and in the first instance consists of getting an accurate description of the IS & IS-NOT of the problem against What / Where / When & Extent. (or the deviation of the behaviour against those 4 criteria)

Any paper to management would also need to cover other headings such as background, when this started, what we are doing, recommendations etc.

2 Problem Description

2.1 Introduction

Whilst reading the following, it is worth being aware that there are 5 potential sources of information related to counter activity:

The Riposte Message Store (information from which is fed through to the Horizon Audit System)

The Counter’s NT event log (some information from which after 3 filters is fed to Horizon Audit)

The Counter’s Audit (or diagnostic) log

Note that this last is diagnostic information and not “audit” within the meaning of the Horizon Audit System.

The PS ~~of~~ standard log

Tuneable trace information

2.2 What is the problem?

In certain instances during the processing of application transactions, the running of multiple processes on a Horizon counter causes lock-outs such that information is not written to the Riposte Message Store.

These lock-outs are accompanied by the creation of “red events” which after filtering and some truncation are transmitted through to the Horizon audit system. Note that lock outs can also occur on reads.

2.2.1 What is it not?

Normal application transactions where lock-outs are not involved. May need to refine that a bit. Gerald’s investigation shows that the Lock outs can occur on normal application transactions. However in that case, the Clerk will be aware that data has not been written and will need to try again or abandon what they are doing. The Audit issue is concerned with cases where the lock out is silent as far as the clerk is concerned.

2.3 Where is the problem seen?

On about 8000 Horizon counters, both Slaves and Gateways (spread over 4,900 branches)
(from information gleaned so far from the Counter's NT event logs as relayed through to the audit system)

2.3.1 Where is it not seen?

On the balance of 32,000 counters (ie some 24,000) counters (I think the figures are probably 35,000 and so 27,000 clean.

2.4 When is the problem seen?

From the "red events generated" it appears to be seen throughout the day and year.

We have particular peaks as shown on some graphs produced by Dave Johns.

The Peak in question related to a spike that we can see at around 19:00 hours daily when EOD is run, but Dave's further analysis reveals that we get the red dots throughout the day and throughout the year.

*****Details of the spikes to go in here**

2.4.1 When is it not seen?

To be supplied

2.5 What is the extent of the problem?

ie how big / many are the deviations observed, and in how many instances

*****Details of the incidence of the problem and relating this to the total volume of transactions etc.**

2.5.1 Where are they not observed?