

Audit Trail Break – Pathway Position

- Problem was initially identified as an incomplete TMS audit trail for the period 8th to 14th August 2000. This was caused by coincidental DLT failure at both datacentres. Pathway could therefore not meet Requirement 699 and 829 in respect of these dates – specifically RFI 8 could not be met in full.
- Subsequent investigation by Pathway identified that Correspondence Server backup tapes that may have covered the period were still available. It was known to be possible to reconstitute the TMS audit trail from these backup tapes.
- Recovery action was instigated in August culminating in full scan of the backup tapes during November. Scanning activity confirmed that whilst were not able to recover all of the data in the period, 66% was recoverable.
- In respect of RFI 8 (the request that highlighted the existence of the break) the unrecoverable period is from 19:27 on Sunday 6 August until 16:09 on Monday 7 August. This compares to the original reported break of 8 August to 14 August inclusive (late hoarding caused late reporting of the problem).
- The normal expiry for all of this audit data is 14 February 2002.
- There are two options:
- Rebuild the audit trail from the 66% available data on the Correspondence Server backup tapes and provide data for RFI 8 within the constraints outlined in the previous bullet. Hold the backup tapes up to normal expiry pending any further RFIs for that period which will be dealt with on a per-RFI basis.
- Rebuild in its entirety the audit data and place into the audit archive. The current estimate for this work is 18 days effort spread over an elapsed period of 36 working days.

Our recommendation is for Option 1 for the following reasons:

- Completion of the 66% recovery is unlikely to be achieved before normal expiry of the data;
- Skills required to undertake the recovery work are those required to deal with normal RFI work;
- Based on an analysis of RFI metrics we believe that POL Security and Investigations are dealing with matters more current than August 2000 and are therefore unlikely to require more data from this particular period.

Audit Trail Break - August 2000

Day / Date	Cluster 1							Cluster 2							Cluster 3							Cluster 4									
	S	T	U	V	W	X	Y	S	T	U	V	W	X	Y	Z	S	T	U	V	W	X	Y	S	T	U	V	W	X	Y	Z	
Saturday 5 th	O K							O K								O K								O K							
Sunday 6 th	F	r	o	m	2 3	:	2 8	F	r	o	m	1 9	:	3 5		F	r	o	m	1 9	:	2 6		F	r	o	m	1 9	:	2 7	
Monday 7 th																								T	o			1 6	:	0 9	
Tuesday 8 th																								O K							
Wednesday 9 th																								O K							
Thursday 10 th	T	o			0 8	:	5 5	T	o			0 8	:	5 9		T	o			0 9	:	0 0		O K							
Friday 11 th	O K							O K								O K								O K							
Saturday 12 th	F	r	o	m	1 5	:	1 8	F	r	o	m	1 4	:	1 9		F	r	o	m	1 4	:	2 1		F	r	o	m	1 5	:	4 7	
Sunday 13 th																															
Monday 14 th	T	o			1 5	:	1 2	T	o			1 5	:	2 9		T	o			1 5	:	2 9		T	o			1 5	:	0 0	
Tuesday 15 th	O K							O K								O K								O K							

Key:

- Green Data exists in current Audit Trail at EITHER Bootle OR Wigan
- Yellow Data missing in Audit archive but readable/reconstitutable from backup tapes
- Red No hope of recovering data due to damaged OR unreadable backup tapes