Bond Dickinson

QUESTIONS ON DELOITTE'S "BRAMBLE" DRAFT REPORT DATED 7 OCTOBER 2016

	Section of Report	**BD Question**	**Deloitte Response**
1	1.2.1 (page 3) and Appendix 6 (page 41)	Do some or all of the "*No Relevant Exceptions Noted*" comments in section 1.2.1 need to be amended in light of the findings in Appendix 6?	
2	1.2.1 (page 4)	In relation to the Fujitsu quote regarding access to both HNG-X environments: • what are the auditing controls in place? • what does "*technical controls around not being able to change audit items*" mean?	
3	1.2.1 (page 4)	In the bullet point regarding analytics procedures, is it 18 or 20 branches?	
4	1.2.2 (page 5) Similar in 4.3.3, finding 4 (page 24)	Regarding the comment: *'The control wording is not accurate. A small number of users are granted extended privileges which enable them to update / delete records. However the control is operating in line with management's expectations. Access to the privileged role is restricted to users explicitly authorised for this access. User actions are audit logged, and not proactively reviewed.'* • what does "*in line with management's expectations*" mean? • what does not "*proactively reviewed*" mean and would you expect this access to be proactively reviewed?	
5	1.2.3 (page 7)	Regarding the comment: *'Review of the audit settings for the Audit Server noted that the audit policy change which relates to change of user rights was set to log success events only, with failure not enabled.'* • would you expect this to log failures?	

		• do we know whether this has always been the case?	
6	2.1 (page 11) and 5.1 (page 32)	Should references to suspense accounts be deleted?	
7	3.2.1 (pages 12 and 13)	Can references to “previous “Bramble” work” be deleted (may give rise to waiver of privilege issues)?	
8	4.2.1 (page 14)	Does “*the level of comfort that can be gained over such controls provides a view on the inherent risk of such errors*” mean that the more robust the controls are, the lower the risk of errors?	
9	4.2.1 ii) a. ii) (page 15)	“*The Audit Store extraction routines check for this at the point of extraction*” – what would happen if the extraction routines found an invalid signature?	
10	4.2.1 iii) (page 15)	Are these two tranches of data analytics work the work summarised in Appendix 6?	
11	4.2.3, finding 3 (page 18)	• Can we state how far back the case data goes? • Is it 18 or 20 branches (same as point 3 above)?	
12	4.2.3, finding 6e (page 19)	• What is an EDAPC transaction? • What does “*no rollbacks or roll-forwards*” mean? • Do we know how many products this relates to?	
13	4.3.1 b (page 22)	Is it possible to set out the “*various layers of the Horizon infrastructure [where] there exist accounts with privileged access rights…*”? If a transaction was inserted “*directly onto the backend*”, would that be visible to the Subpostmaster and would it cause a discrepancy in the branch accounts?	
14	4.3.1 b vii) (page 22)	Have these data analytics procedures been done?	
15	4.3.2 (page 23)	This summary table relates to Scope Area 1 not Scope Area 2 – please provide for Scope Area 2.	

16	4.3.3, finding 5 (2A)	What does "*Users to not have the ability to bypass this role restriction by running SUDO command*" mean? What restriction is being referred to?	
17	4.4 D ii) (page 28)	Which POL staff duties are segregated?	
18	4.4 D iii) (page 28)	Can we give examples of the checks carried out by POL staff?	
19	4.4.3 (page 31)	This needs to be in landscape – please provide a complete version of the table.	
20	Appendix 3, Ref B (page 36)	What does "*written to standard output*" mean?	
21	Appendix 3, Ref C (page 36)	What does "*There also needs to be a level of obfuscation to ensure that the audit mechanism is robust*" mean?	
22	Appendix 6 (page 41)	Please delete reference to QC's Advice	
23	Appendix 6a, Analytic 1	This seems to be a significant number of gaps. Is that the case? What are such gaps indicative of?	
24	Appendix 6a, Analytic 2	What are such gaps indicative of?	
25	Appendix 6a, Analytic 5	This seems to be a significant number of transactions with a quantity not equal to zero. Is that the case? What is this indicative of?	
26	Appendix 6a, Analytic 6	What inherent system controls mean that this should not be possible?	
27	Appendix 6a, Analytic 7	As these 17 users are global users, does this mean that they did not enter these transactions remotely.	