POL00396909

Weekly Highlight Report

PCI Compliance - HNG-X & BP Sales		**Programme number**	
Essential Information			
Sponsor	David Smith	**Reporting period**	08/10/08 – 15/10/08
Owner	David X Gray		
Programme Manager	Connie G. Penn MIMC	**Key Team members**	
Change Objective:	**Card Scheme Compliance for Card Acceptance**		

Tracking Summary		
Measurable for HNGX	***Rating***	***Comments (Reason for RAG rating)***
Time	**Red**	This section is red because we are unable to meet the deadline for PCI compliance – December 2008.
Cost	**Amber**	Costs generally are managed by the HNGX programme. Costs for eliminating Track 2 from the audit log to make it PCI compliant is still an unknown quantity. We have identified three potential suppliers. They need engagement with Fujitsu via the design authority to identify the size of the job. Then we will measure cost. The design authority has now decided not to engage with the outside companies – subject due for discussion 02/10/08.
QUALITY	**GREEN**	Project documentation produced between April and July so far meets the requirements of the auditor. The documents delivered late by Fujitsu in September have not yet been supplied to the auditor for evaluation. They are not yet signed off, but it is the quality of the documents that is important at this point. Nothing is sent to the auditor until signed off by POL
Measurable for BP Sales	**Rating**	
TIME	**Red**	• The BT Buynet {PSP} integration for the RMG Portal now reporting directly into the IT Roadmap. • Progress – IT Roadmap programme now overseeing this project. TMC now scheduled for live Feb/March 09 – a result.
COST	**GREEN**	• Cost for the compliance for the RMG portal resides with RMG. • There is no cost to POL for compliance where the POL Third Party has its own direct relationship with an acquirer.
Quality	**RED**	Keith Woollard now engaged with his risk counterparts in BoI. Reporting red because it is important we now progress with engagement from a brand perspective.
Progress Summary		
What went well this period:		

POL00396909

1. The meeting with Streamline to resolve the issue of their perceived need for multiple MID's for the portal shopping basket, delivered. It turned out to be a total non event except for the result "yes you can have a single mid for the Portal shopping basket". This means the portal development can proceed quickly now. A major result.

What did not go so well this period:

1. After a delay of 3 months we finally received the Incident Response document from Fujitsu, [20/09/09,] that feeds into the Incident Response Plan we delivered to Fujitsu in May.
   - There was huge resistance from Fujitsu to incorporate the PCI incident Response into the existing Incident response process. I assumed that was for commercial reasons. Upon reading the original document I now suspect that Peter Sewell, in particular, knew that the original document was "not fit for purpose" and was perhaps trying to keep the original document out of my sight. To indicate the original document is "Not fit for purpose" is a kindness.
   - PCI is a slightly different scenario to e.g. a scenario whereby a cash depot is broken into and all the cash is stolen. But both would fit into a Major Incident Category and the same process would be followed in terms of logging, recording, escalating, categorising and managing the incident, and then different operational steps will be followed in dealing with the actual incident.
   - A PCI incident has been added to the Incident Response, but is sits almost as a separate disjointed scenario, rather than part of the overall process. Same applies to general security incidents and I feel a lot is still missing. I have submitted a list of changes, through the response process, but existing diary commitments prevented these comments from being returned in the timeframe originally required.
   - Overall I am disappointed in the document so far, I would have expected more, bearing in mind the document was 3 months late in delivery. I firmly believe that Howard Pritchard could not have read this document prior to release.
2. Still no absolute confirmation as to the date that Fujitsu will do the BSI audit for ISO 27001/2. However, it is now clear that Howard Pritchard is not on top of the job, so this has now become an issue and the problem as to when and how the BSI audit will be done is a problem that needs to be resolved elsewhere. The next PCI board meeting needs to decide if this should be put on the risk register.
3. Still have not resolved the issues on the statement of work from the auditor. The auditor will now be given a PO to allow the workshops to proceed and if the subject is not resolved by the end of this week, there is a proposal to refer the matter to the PCI council, who are currently heavily engaged in reviewing QA for the PCI auditors.

Key Activities planned for next period:

- Second PCI workshop on the control objectives, scheduled for Thursday.
- Review of PCI DSS V 1.2

Issues and Risks

Issue around the failure of Fujitsu to submit to an external audit [BSI] for ISO27001 is an issue for the project and a risk to the PCI project. This needs discussion at next weeks Project Board meeting before the subject is written up.