POL00396887

Weekly Highlight Report

PCI Compliance - HNG-X & BP Sales		**Programme number**	
Essential Information			
Sponsor	David Smith	**Reporting period**	25/07/08 - 01/08/08
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. • In addition there is a cost to eliminating Track 2 from the daily submission file to appease Visa. Business case passed for £25,000. This work will not impact HNG-X timeframes • Costs for eliminating Track 2 from the audit log to make it PCI compliant will be higher; we are currently trying to find a solution. Then we will measure cost. • Cost of File Integrity Monitoring has finally been agreed at £175,000.00, £37.000.00 over original estimate.
QUALITY	**GREEN**	Project documentation produced so far meets the requirements of the auditor
Measurable for BP Sales	**Rating**	Comments
TIME	**Red**	• The BT Buynet {PSP} integration for the RMG Portal now reporting directly into the IT

POL00396887

		• Roadmap. • Progress - The PM has finally been appointed. Meeting scheduled 27/08. .
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	Doug Warwick attempting to set up meeting with BOI compliance. Keith Woollard supporting the initiative. Reported red as so far they have not received a satisfactory response/engagement with BoI. However there was a major breach on an Irish e-commerce site reported in Irish papers 08/08/08. This may prompt more focus on the subject.

Progress Summary

What went well this week:

1. POL asked by the BRC to write up how they secure their PEDs at Point of Sale. The POL process to be published as a "Best Practice"
2. Meeting with Matt Hibbard, [Andrew Carter's replacement] in Chesterfield went extremely well. He is keen to forge ahead with the Streamline relationship.
3. Meeting with Alan Green training in Rugby. He is in the last stages of completing the training package for security and keen to start the training package for Operations.

What did not go so well this week:

- Deborah Howarth did not turn up for the meeting in Chesterfield to conclude the review of their mapping of PCI into the ISO standards, due to personal reasons
- Despite having failed to deliver on a number of documents end of July, Fujitsu proposed next meetings for beginning of September, completely passing over August. Pulled back dates to 22nd August.
- PCI project team meeting. There is just so much to do and everybody has so little time. Do not feel we are making progress.
- No progress with the QSA, so the contract negotiations are still stalled.

Key Activities planned for next week:

- Meeting in London with M. Burley to review PCI project. He is concerned with lack of progress on project.
- Conference call with legal and security re making the historical audit logs PCI compliant while maintaining their integrity for prosecution purposes.

POL00396887

- Updating the Audit documentation. This is now the main focus of the project and the detail over the 12 requirements will take a great deal of time and effort.
- Updating the status of ~Fujitsu's deliverables. Many documents and information for the audit were due for delivery 230/07/08 and have not been delivered, so they need to move into red and start to be chased for new delivery dates. Update the delivery milestones.

Issues and Risks

- There is now an issue with Fujitsu's failure to deliver promised documents and information. Need to work on a strategy to pull this back. Some action already planned
  1. Direct communication with Fujitsu and meeting set for 22/08/08. Earliest available date due to holidays in Fujitsu.
  2. Despite Fujitsu's failure to make a PCI update meeting in July, the "Fujitsu meeting record" document has been updates to reflect the current status of project on 10/08/08
  3. Separate meeting scheduled with J. Sweeting also for 22/08/08. This meeting is between Dave King and J. Sweeting and John Halfacre. I have given D. King a complete list of items OS. So Dave King has a complete written record of the status of each item and our expectations from Fujitsu on each individual item, particularly in relation to J. Sweeting's deliverables and have requested a detailed update in writing on actions and dates agreed at the meeting
  4. Torstein Godeseth has also been given a list of the deliverables that have been delayed and he is also aware from the PCI team meeting and the records of the PCI team meeting of the items that have been delayed. He will raise the subject directly with J. Sweeting's manager.

POL00396887

Deliverable	Responsible	POL Owner	Dependencies/notes	Planned Date	Forecast/ Actual Date	R/A/G ☺😐☹ ✓
Incident Response Plan – POL **Draft**	Alan Simpson	AS		30/05/08	22/05/08	✓
Incident Response Plan – FS **Draft**	Pete Sewell	AS	Peter Sewell in FS, working on it. Progress update 28/07	30/05/08	30/07/08	☹
Network diagrams **Draft**	J. Sweeting	DMK		30/03/08	26/04/08	✓
Permeation Maps/ Clear View Cardholder Environment, incl. all touch points and FIM locations **Draft**	J. Sweeting	DMK		30/06/08	26/04/08	✓
POL [CISP] Policies **Draft**	S. Lowther	CGP	On schedule. Reviewed on 21/07 within POL Information Security and PCI. Further review scheduled 17/08	30/07/08	30/08/08	😐
FS [RMGA] Policies nd **Draft**	H. Prichard	CGP		01/05/08	30/06/08	😐
Review RMG Policies			Awaiting next steps from PWC review	30/07/08	30/08/08	☹
FS Security Architecture Document **Draft**	J. Sweeting	CGP	V1.4 of Security Architecture received and initial review done. Detail being incorporated into PCI audit document. Second review done & submitted, Response promised end of Aug	30/06/08	30/08/08	😐
Key Management Documentation **Draft**	Pete Sewell	CGP	J. Sweeting says not being done, as he has not received a formal request to do it. This is not PCI specific. It is part of the architecture and operational process of Horizon and HNGX. HP has asked P. Sewell of FS to get involved. HP will revert with new delivery date.	01/05/08	30/08/08	😐
FS to Start internal audit for ISO 27001 prep for BSI Audit	H. Pritchard	CGP	Started internal audits 01/04/08. Due to conclude 30/08/08. BSI audit has been delayed, as internal audit delayed due to illness. But reviews now underway again. Networks, HR and Access being reviewed currently.	07/07/08	15/10/08	😐

POL00396887

BSI start Audit in FS	H. Pritchard	CGP		30/10/08	30/10/08	☺
BSI to issue ISO 27001 Certificate	H. Pritchard	CGP		27/10/08	27/10/08	☺
Operating Procedure around PCI Sign- Off	C G Penn	CGP		29/08/08	29/08/08	☺
Sign off the full Cryptographic key management process	T Godeseth	TG		30/10/08	30/10/08	☺
POL Change Control Documents	A. Banacheck	SL		30/09/08	30/09/08	☺
FS Change Control Documents	H. Prichard	CGP	Output from FS ISO 27001 certification	30/09/08	01/10/08	☺
Removal of Track 2 from RBS Submission File	T Godeseth	CGP	Scheduled for Aug 08,	30/08/08	30/08/08	☺
Removal of Track 2 from Audit Log	C. G. Penn	CGP	Cant occur until Belfast in live operation & pilot HNG-X	30/04/09	30/04/08	☺
CCN 1202 Development Starts	HNGX	TG	External dependency for PCI	04/08/08	04/08/08	☺
CCN 1202 Completion	HNGX	TG	External dependency for PCI	06/03/09	06/03/09	☺
Data Centre testing commence	HNGX	TG	External dependency for PCI	19/01/09	19/01/09	☺
Data Centre testing complete	HNGX	TG	External dependency for PCI	06/03/09	06/03/09	☺
HNGX Pilot (model Office)	HNGX	TG	External dependency for PCI	30/03/09	30/03/09	☺
HNGX Pilot (live Offices)	HNGX	TG	External dependency for PCI	30/03/09	30/03/09	☺
Network Diagrams Sign-off	D King	DMK	Completion cannot happen until Belfast completes testing	30/01/09	30/01/09	☺
Permeation Map Signed Off	J Sweeting	DMK	Completion cannot happen until Belfast completes testing	30/01/09	30/01/09	☺
Key Management Signed Off	C G Penn	CGP		30/01/09	30/01/09	☺
Bladeframe: IRM sign-off the controls Fujitsu propose to put in place separating live and test [Data Segregation on Bladeframe]	QSA	CGP		30/11/08	30/11/08	☺
PCI Security Incident Planning Sign-Off	S Lowther			09/10/08	09/10/08	☺
Security Architecture Sign-Off	J Sweeting			30/11/07	01/07/08	☺
Agree audit plan with FS and QSA	C G Penn			27/06/08	27/06/08	
Agree Audit date with Streamline	C G Penn			30/10/08	30/10/08	☺

POL00396887

Give formal notice of audit to Fujitsu	C G Penn		Data Centre testing commence	30/10/08	30/10/08	☺
Agree remediation on Portal and plan for implementation	T Simms		PM not yet appointed.	14/03/08	14/07/08	😐
Get sign-off of all SAQ for RMG Portal	Central Audit		New PSP and New UI on Portal	29/10/08	29/10/08	☺
Agree remediation on EDG11 and get plan for implementation	C G Penn			14/08/08	14/08/08	☺
Get sign-off of future approach and procedures for dealing with 3rd parties	Central Audit			29/10/08	29/10/08	☺
Agree remediation for relevant 3rd parties and plan for implementation	Central Audit			29/10/08	29/10/08	☺
Central Audit sign off PCI Compliance for Portal	Central Audit	CGP		29/10/08	29/10/08	☺
Start Audit for HNGX			HNGX Pilot (live Offices)	13/04/09	13/04/09	☺
RoC from Auditor for POL infrastructure			HNGX Pilot (live Offices) and completion of PCI Audit	01/11/09	01/11/09	☺