POL00397348

G-097 PCI DSS Compliance HR 130112.doc
IT & Change Weekly Project Highlight Report – submitted to Business_PMO_Reporting mailbox no later than 12 noon every Wednesday
Click the Show/Hide button [¶] on the Standard toolbar to see guidance notes on how to complete this report

Reference Information			
PCI DSS Compliance		PID Reference	
		Project Number	G-097
Change Sponsor	John Scott	Reporting period	w/e 6 January 2012
Project Manager	Wunmi Adeniji	Key Team members	Connie Penn – Programme Manager
Change Objective:	The objective of this project is to get POL full PCI DSS (Payment Card Industry Data Security Standard) Compliance across all card payment channels i.e. Horizon, Paystation, Post & Go, Web, RMG Call Centre and BT Call Centre.		

Project Type	FULL	MEDIUM	XPRESS	NOTED	Delete inapplicable Project Types

Tracking Summary

↔ - No Change ↑ - Change Up (e.g. Amber to Green) ↓ - Change Down (e.g. Green to Amber)

Measurable	*Rating*	*Change*	*Comments (Reason for RAG rating)*
Time	GREEN	↔	On track
Costs (Investment/Budget)	AMBER	↑	There is a likelihood that there would be an increase in project costs as a result of the following CT expected from Fujitsu: • Populating Omniport (audit tool) with BAU repeatable activities • Work required to impact assess the changes between PCI v1.2 and v2.0 and the cost of the actual audit • Work required for any remedial activities to address gaps identified There is also the risk of additional costs from RMG call centres as RM is not willing to become PCI compliant within our timescales so in order to do so, POL may have to pay for the audit.
Benefits	GREEN	↔	On track
Quality	GREEN	↔	On track

Key achievements/decisions/changes made this past week

Meeting Fujitsu, QSA, Don Burgess and CGP went extremely well.

- Key objective - identify impact of compliance with V2 of PCI standard in terms of infrastructure change, change itself, timeframes for remediation and costs.
- As expected, no significant impact on infrastructure from V2 was identified.

- Meeting produced a secondary unexpected deliverable.
    - It became clear Fujitsu are understanding PCI in BAU better,
    - the intensive work, notes made and statements put in OmniPort during the 2-week audit prep in December, means that Fujitsu are now becoming more informed and consequently more focused on how PCI DSS integrates with the POL Fujitsu environment and what needs to be done in BAU to not only deliver PCI compliance, but also a better security posture.
- The CT response for V1.2 vs. v2 will have costs associated, but the work involved has more to do with ensuring the tools used to manage the security of the environment, particularly around patch and vulnerability management are more integrated into event and incident management, rather than an impact from V2 per se.
    - There will be costs associated with doing more risk assessments in BAU, which includes the annual risk assessment.
    - It is also acknowledged that software coding and testing needs to be improved.
    - So costs can be expected for BAU improvements rather than anything significant from V2.
- The key risk and concern from the meeting is that new projects – PODG and Web services could have an impact on PCI at the counters. This is because the introduction of web services will open up the network, which could carry new PCI costs. We have not been involved in evaluating these new services, but we clearly need to look at the risk assessments to ensure PCI was adequately covered.
- Also concerned as to whether Change of Merchant Acquirer has catered fully for PCI, especially in secure coding and testing, including vulnerability and PEN tests.
- Fujitsu are now preparing the response to the CT.
- All the Fujitsu people needed for the audit have been identified and are listed in OmniPort. The dates agreed are being scheduled into Fujitsu's work schedule for February.
- There are some Info Sec items that we need guidance and help with which should be successfully addressed in the Info Sec workshops being scheduled.
- Subject to agreement to response to CT and successful outcome from the Info Sec workshops, we are ready to go with the 2012 PCI DSS audit.

The BT Logica testing on the servers that were upgraded went well last week. Further testing scheduled for this week.

New risk raised on PCI project, because there is a risk of an RMG info Sec audit. PCI Project has suggested turning the risk into a positive, through Info Sec and PCI working together to address the requirements of both audits as a single audit, i.e. do both audits at the same time, pooling resources in POL as well as in Fujitsu and thus saving cost and resource. PCI DSS is just Info Sec good practice. PCI is just more prescriptive in how it wants the security posture to be evidenced

Key achievements/decisions/changes planned for next week

- Engage with Info Sec to see if we can pool resources to do RMG Info Sec and PCI audit at same time and consequently pool resources to agree enhancements that are needed in the security environment to improve the security posture in BAU.
- Schedule meetings with POL Info Sec to seek guidance on some BAU info Sec items that need to be addressed for PCI audit.
- Review all the work done during the PCI audit prep in December
- Address stakeholders concerns on shortfall in output from audit prep during December and re-issue output.
- Agree with Info Sec how the work that needs to be done in POL is scheduled and completed.
- Agree with Info Sec how OmniPort will be managed and used
- Search out the risk assessments on PODGE and Web Services and work with Info Sec to ensure their introduction does not impact PCI
- Review the Fujitsu response to the CT when received.
- Continue to support BT Logica testing.

Recognition

Who	***Project responsibility***	***What did they do that deserves recognition?***	***What can we learn from their actions?***
Don Burgess	Data and Process Architect	Nominated By: Connie G. Penn Fujitsu wanted to review the changes between v1.2 of PCI DSS and V2, with the PCI auditor. Info	

		Sec were unable to provide support for the meeting due to holiday commitments and pre-scheduled meetings. I did not feel qualified to represent POL on architecture matters and to contribute to the discussions on Blade frame Technology and felt POL should be more fully represented at the discussion between the auditor and the Fujitsu architects. Aware of my concerns, Don cut into his holiday and agreed to spend the day in Bracknell at the meeting so that POL is more appropriately represented from an architect and system perspective.	

New/major risks

Because (of)...there is a risk that...which will result in....	Because Royal Mail call centre is not PCI compliant as it records calls, does not operate a clean desk environment, card data is verbalised to the agent and entered into the agent desktop which also has email and web access. This may result in the current POL certificate of compliance being withdrawn i.e. not given a certificate this year until such time as all channels are compliant which could have a significant impact on the business relationship with Environment Agency and in a wider context an impact on POL's ambition to process more and more Governments payments. Not having a certificate of Compliance for 2012, would be a significant backward step for Post Office.
Proximity	31/3/12
Response/mitigation	1. POL investigated a potential solution and recommended that RMG use Semaphone to eliminate card data from call recordings and to facilitate a PCI compliant journey for the call centre. - Due date: 31/12/11 2. POL has asked CAP Gemini to identify a solution, cost and timeframe to make the new payment journey PCI compliant
Status	**Risk Score** – 25 **Update** 28/11/11 - RMG commissioned Deloitte to identify the touch points and the impact for PCI compliance, which was received 23/11/11. Awaiting update from RMG. Cap Gemini have been asked to deliver a plan by December 2011 for a solution to be implemented by 1st Quarter 2012. October 2010 solution was rejected by RMG as RMG wanted to use Deloitte to define compliance remediation. August 2011 CGP engaged with Steve S Bedoes to initiate negotiations with CAP to deliver compliance for call centre. Oct 2011, on the back of the success of the Logica Semafone integration, CGP encouraged BT to embrace the use of Semafone in the BT Cloud eliminating RMG from the equation and the cost of maintaining compliance around the Semafone solution. BT receptive. CAP have indicated that they have a solution with data cash, awaiting details of the solution 30/12/11 - CP spoke to Andrea Ghigo (RM Project Manager) who confirmed that an IVR solution that was PCI compliant was been installed in RMG environment only and not Post Office. Requested details of solution, Andrea indicated she was unable to share as it was RMG confidential. CP indicated that as we are still part of RMG we should be able to have site of the documentation of solution used. To date, documentation not received. Email chaser for documentation sent 30/12/11. 3/1/12 - Documentation received from Andrea Ghigo

Because (of)...there is a risk that...which will result in....	Because Cap Gemini's contract requires them to deliver a PCI compliant web platform and RMG have refused to allow the environment to be audited there is a risk that, while the transaction journey itself may be compliant, Cap Gemini will not be able to provide PCI with acceptable evidence of compliance as they do not have PCI Certification. Like above, this risk may result in the current POL certificate of compliance being withdrawn i.e. not given a certificate this year until such time as all channels are compliant which could have a significant impact on the business relationship with Environment Agency and in a wider context an impact on POL's ambition to process more and more Governments payments. Not having a certificate of Compliance for 2012, would be a significant backward step for Post Office.
Proximity	14/2/12
Response/mitigation	In the face of RMG's refusal to allow an audit, CGP is negotiating with the PCI council a method whereby a miniature audit will be conducted to identify that Cap Gemini has hosted the payment pages correctly and as a consequence, the shopping cart is out of scope of PCI. IRM have agreed to define the test criteria and CGP meeting with UK Cards and UK Acquirers on 16/11/11 to get UK Cards to instigate a formal request to PCI council championing the approach.
Status	**Risk Score** – 20 **Update** 16/11/11 - The approach is being accepted. Next step finalise the test criteria with PCI council through the QA process. This activity will take 3-4 months but auditor is engaged in the process. Have discussed approach with Paul Lewis in CAP who in turn have discussed with Kevin King in CAP. CAP pleased with the approach because it significantly reduces the cost to them to evidence PCI compliance. 30/12/11 - The PCI council offered a date but CP unable to accept due to commitment on Horizon online. Alternative date requested

Because (of)...there is a risk that...which will result in....	There is a risk to failing PCI audit 2 on Horizon because the regular repeatable activities and other BAU InfoSec activities that demonstrate maintenance of the security posture attained for audit 1 is not being managed. This would result in the current compliance on Horizon being withdrawn and could threaten our relationship with clients such as the Environment Agency who is keen for us to be PCI complaint.
Proximity	14/2/12
Response/mitigation	1/ PCI Project has helped Fujitsu record the audit requirements for PCI and ISO27001 in a GRC framework. Maintenance of the framework would help demonstrate continuous compliance as required by PCI. 2/ Engage with SD to help them understand recording of the data in the monthly ISMF report in a format suitable for review by an auditor as part of a service catalogue.
Status	**Risk Score** – 20 **Update** July 2011 - arranged RGB to view GRC tools. IRM's OmniPort and Fujitsu's acuity STREAM. PCI Project followed up with recommendation paper. Awaiting feedback from RJB. 17/10/11 - discussions with Neil Leckie-Thompson & Don Burgess re: framework, both understand usefulness of same. Discussions with IRM to identify cost and options to migrate to OMNIPORT at this late stage. 15/11/11 - Purchase of the framework agreed in principle. PO to be raised. 22/11/11 - PO issued to purchase Omniport 25/11/11 - Migration of data to Omniport commenced 30/11/11 - CR raised to request Fujitsu to re-issue the evidence of BAU in line with the PCI BAU spreadsheet for the whole of 2011. To be reviewed 16/12/11 30/12/11 - Awaiting response from Fujitsu

New/major issues

Issue description	None.
Impact	

Action to resolve	
Expected closure date	
Status	

Milestone Tracker

☺ - On track. - Delivery problem. ☹ - Major delivery problem. ✓ - Complete

Milestones in light turquoise shaded cells are mandatory

Milestone	Unique ID	Owner	Baselined Date	Planned Date	Actual Date	R/A/G ☺😐☹✓
Gating & Other Mandatory Milestones						
Project Initiation Document assured by Gating Forum	<<text here>>	<< text here>>	<<text here>>	<<text here>>	<<text here>>	<< icon here>>
POLIC approval given	G097	<< text here>>			July 2011	✓
Approval to go-live *(except Noted Projects)*						
Go-live		Connie Penn		31 Mar 12		☺
Approval to close		Project Manager		30 June 12		☺
Project Handover		Project Manager		31 July 12		☺
Finish		Project Manager		31 July 12		☺
Post Implementation Review completed		Project Manager		November 12		☺
Project Specific Milestones						