Agenda

- 2012 PCI Compliance Status Update
  - Budget
  - Staffing
  - Management Recommendations Report
  - Quarterly Vulnerability Testing
  - QSA assessment
  - Technology Innovation Program (TIP)
  - RiskVision
- Staff Awareness Requirement: 2012 Plan
- Control Gap Reporting Process
- 320’s and Point to Point Encryption (P2PE)
- Staffing Changes in Victoria; SLAs
- Governance Committee PCO direction

PCI Governance Committee (PGC)

Minutes (Approved)

April 23, 2012

In Attendance:

Jay Chambers
Don Farley
Kelly Wilson
Constantin Starck

Absent:

Roger Bissoondatt
Gary Kuromi

1. Minutes

n/a - initial meeting of PGC

2. Budget 2013

Consulting s.17 recommended cost items include ArcSight coding, on-line delivery of staff awareness program, as well as advisory services for P2PE and 'control gaps'

Recommended items exceed budget. Also, auxiliary help may be needed to complete the PCI compliance program for the year. Finance will look for alternative budget space elsewhere and report back.

3. Staffing

IS positions will be posted shortly.

Finance PCI lead positions have been held up pending union approval of excluded status. Unresolved challenges include hiring delay due to exclusion process and contingency plan if exclusion is denied. Aux extensions will be required.

4. Updates

- Work on prior year QSA management recommendations is on-going
- Victoria has renewed QSA contract with Control Gap for 2013; fieldwork planned Aug/Sept
- PCI required testing and scanning activities are on-track
- RiskVision: software has been updated; increased manual work due to lack of document library function
- PCI Staff Awareness 2012: on-line delivery recommended for HO (cost $25K); Stores = paper.
- Staff changes in Victoria. New PCI contacts: Tom Caldwell, Derrien Karr.

- PCI related SLAs between Ministry of Finance are still in progress

5. VISA Technology Innovation Program (TIP)

Program can result in cost savings when a QSA assessment is not required. PCI office will research pros and cons and report back.

6. 'control gap' Reporting Process

LDB should consider s.13

so issue is on hold.

7. Ingenico 320 rollout and Alpha Pod PIN pad alarms

Rollout completion is targeted for end of May. As a result of improved physical security from new PIN pad stands and the more secure 320 model, s.13, s.15 a view shared by LDB Corporate Security. The Committee agreed that EMC approval for s.13, s.15 is not required; PCO and IS will discuss and recommend how to proceed.

8. Impact of Point to Point Encryption (P2PE)

Advisory services are recommended to assess the impact on LDB card holder data environment, with a focus on flexibility arising from the Ingenico 320 roll out. Work is on hold pending location of available budget.

9. Allocation of Provincial PCI Costs

There is no SLA between Ministry of Finance and LDB for PCI related services. The annual charge for PCI from Victoria for 2013 has not yet been determined (2012 = $960K).

10. PCI Governance Committee Direction to PCO

Brief discussion. Committee is not considered operational. Preference is for updates and significant issues and decisions.

11. Next Meeting

The next formal meeting of the PCI Governance Committee is scheduled for May 31 2:00pm in the Conference Centre.

Agenda

- Approval of Apr 23 2012 PCI Governance Committee meeting minutes
- 2012 QSA Assessment
- Ingenico 320 PIN pad roll-out progress
- Point to Point Encryption (P2PE)
- Consequences of not achieving P2PE
- Staffing update

PCI Governance Committee (PGC)

Minutes

May 31, 2012

In Attendance:

Jay Chambers
Don Farley
Roger Bissoondatt
Kelly Wilson

Gary Kuromi
Constantin Starck

Absent:

n/a

1. Minutes

The April 23, 2012 minutes were approved.

2. 2012 QSA Assessment

Discussed the PCI v2.0 Report on Compliance (ROC) reporting instructions, which are prescriptive in nature and impose a higher workload on the QSA for a given payment card environment compared to last year.

The current assessment plan for the LDB assumes reduced scope for the assessment which should have the effect of reducing compliance effort and cost due to the increased security offered by the Ingenico 320 s.15

3. Ingenico 320 Rollout

The rollout of Ingenico 320 PIN pads has begun and is scheduled to complete by July 31 2012. The 320 PIN pads s.15

4. Point to Point Encryption (P2PE)

LDB currently uses a s.15 to enable the stores to process card transactions s.15 Early work done by the Bell/Privity consultants indicates that s.15

A possible solution to this issue is to consider s.15 Some early statistics were provided. The PCI Office will further investigate and provide recommendations.

[Note: Further work done since the May 31 2012 meeting has led to the conclusion by Bell/Privity that s.15

5. **Staffing**

The PCI lead positions have not yet been posted because we the exclusion status has not yet been determined by the union. Extension of the existing auxiliary position is required.

[Note: On June 12 2012 we received notice from the union that the request for exclusion status has been declined.]

6. **Next Meeting**

The next formal meeting of the PCI Governance Committee is scheduled for July 26 2012 3:00pm in the Conference Centre.

Agenda

- Approval of May 31 2012 PCI Governance Committee minutes
- Event Response Plan (ERP) desk test results from June 29
- 2012 QSA Assessment
- Ingenico 320 PIN pad roll-out progress
- Staffing update
- PCI Staff Awareness

Agenda

- Approval of May 31 2012 PCI Governance Committee minutes
- PCI Staffing
- 2012 QSA Assessment: 320s / P2PE Scope Reduction
- Event Response Plan (ERP) desk test results from June 29
- PCI Staff Awareness

PCI Governance Committee (PGC)

Minutes

Sept 24, 2012

In Attendance:

Elaine Low
Don Farley
Roger Bissoondatt
Donna Mohn
Gary Kuromi
Constantin Starck

Absent:

n/a

1. Minutes

The May 31, 2012 minutes were approved.

2. PCI Staffing

The Committee discussed the risks of losing qualified PCI staff and the suggested possible solution, including variants to the solution. Assuming any HR issues related to the solution could be managed, s.13, s.17

There is an HR meeting scheduled for Oct 2 to explore the feasibility of the possible solution with HR. The Committee would like to wait for the results of this meeting and then have a plan with more details circulated by email to be voted on by the Committee members.

3. 2012 QSA Assessment: Scope Reduction

The Committee agreed that if a control is no longer needed for PCI compliance purposes, the decision as to whether the control should remain in place rests with management, which was clarified to mean management level control owners and stakeholders. Since the majority of the controls are IT oriented, Erin McEwan (Director IT Risk and Security) will be asked to coordinate the revisiting of controls that are no longer needed for PCI.

4. 2012 QSA Assessment Activity

The Committee wanted to know what the current status of the Annual PCI Staff Awareness program. Answer: For the on-line head office staff, approximately 90 out of 500 (18%) have not taken the training as of Aug 22.

For the stores, which required staff to acknowledge the receipt of the Security Awareness booklet, 100% of the stores have responded with the signature lists. The per cent of staff that have not signed is expected to be low, but is not currently known – this statistic can only be calculated after HR has keyed the signature lists into PPIIMS, scheduled for October.

5. ERP Desk test

s.15

6. Next Meeting

The next formal meeting of the PCI Governance Committee is scheduled for Nov 26 2012 11:00am in the Conference Centre.

Agenda

- Approval of Sept 24 2012 PCI Governance Committee minutes
- Barns & Noble incident
- Recent LDB PINpad situations
- 2012 QSA Assessment
- Lotto Express
- PCI Staffing

PCI Governance Committee (PGC)

Minutes

Nov 26, 2012 11:00am

In Attendance:

Elaine Low
Don Farley
Gary Kuromi
Constantin Starck

Absent:

Roger Bissoondatt
Kelly Wilson

1. Minutes

The Sep 24, 2012 minutes were approved.

2. Barns & Noble Breach

The Committee reviewed the circumstances of the Barns & Noble breach that was announced Oct 24 2012. The breach was as a result of PINpad tampering in 63 of 689 stores.

3. Recent PINpad Situations at LDB

The Committee was presented with a summary of 7 recent PINpad situations in LDB stores where the common thread was that stores were not following s.15 procedures.

Since s.15 are the first line of defence against PINpad-tampering based breaches, the committee was asked if LDB should consider reporting and consequences for non-compliance.

The committee agreed. An efficient process to do s.15 and reporting would need to be developed.

Elaine Low had to leave the meeting at 11:30am

4. TD Reporting on Recent PINpad Situations at LDB

In order be able to rule out the possibility of s.15 the PCI Office is working with TD on a process for reporting s.15 back to LDB.

5. 2012 QSA Assessment

The 2012 QSA Assessment of LDB is complete with a Report on Compliance dated November 23 2012. The second compliance year can be challenging for a variety of reasons, but LDB has avoided problems by:

- keeping skilled / knowledgeable PCI staff in place
- design, planning and implementation of a sustainment program
- achieving scope reduction to address PCI DSS v2.0

6. Lotto Express

Control Gap has reviewed the proposed LDB infrastructure for Lotto Express from a PCI compliance point of view. Conclusion: s.15

7. PCI Staffing

A Case Conference to appeal the denial of exclusion status for the PCI Lead positions is scheduled for Dec 3 [Note: the date has subsequently been moved to Jan 3]. If denial is upheld and the positions become included,

s.13, s.17

An alternative staffing solution, the option of s.13 is still being explored. Current status of this idea is that a briefing note and business case are being prepared.

8. Next Meeting

The next formal meeting of the PCI Governance Committee is scheduled for January 31, 2013 2:00pm in the Conference Centre.

Agenda

- Approval of Nov 26 2012 PCI Governance Committee minutes
- PCI Staffing
- ArcSight
- Scope reduction control review
- TIP
- Meeting frequency

PCI Governance Committee (PGC)

Minutes

January 31, 2013 1:30pm

In Attendance:

Roger Bissoondatt
Don Farley
Gary Kuromi
Constantin Starck

Absent:

Elaine Low
Kelly Wilson

1. Minutes

The Nov 26, 2012 minutes were approved.

2. PCI Staffing

The Case Conference to appeal the denial of exclusion status for the PCI Lead positions was held Jan 9. The appeal was denied. The next level of appeal is the Joint Exclusion Committee, which has been scheduled for April 22.

s.13, s.17

The Committee discussed alternative staffing solutions as brought forward in the previous meeting. Noted that s.13

The PCI staffing problem remains unresolved.

3. ArcSight

The Committee discussed the future of ArcSight logging and monitoring application as delivered by SSBC. s.15 Currently, LDB's share of the annual ArcSight cost is $400k. Key outstanding questions include the future annual ArcSight fees to LDB, for the LDB share of any remaining variable or fixed (unamortized) costs.

LDB is exploring s.15

4. Controls Review

As a result of the s.15 the PCI team is performing a s.15 evaluation with a view to make recommendations on s.15 from a PCI point of view.

5. TIP (Technology Innovation Program)

The TIP is a VISA program that potentially allows merchants to self-maintain PCI compliance, thus avoiding the cost of an annual QSA assessment. MasterCard has a parallel program. This is a new program and details are not fully known at this time, for example the availability of the MasterCard TIP-equivalent program in Canada. Victoria has applied for TIP.

TIP approved merchants will need qualified staff to perform field audits, so while the QSA assessment may be saved, there are staffing and training implications of moving to TIP.

6. PCI Governance Meeting Frequency

The provincial PCI Executive Steering Committee has agreed to lower meeting frequency to annual with ad-hoc meetings as required. Since the LDB PCI program is operating well in the sustainment phase, our meeting frequency could also be reduced from the current schedule of every two months.

The Committee agreed to a regular annual meeting with ad-hoc meetings to be called as required. The annual meeting should coincide with the self-assessment or QSA assessment.

7. Next Meeting

In accordance with item 6 above, the next formal meeting of the PCI Governance Committee is scheduled for Thursday Nov 28, 2013 2:00pm in the Conference Centre.

.