



# CITY OF VANCOUVER INTERNAL AUDIT REPORT PCI Compliance Program

## Distribution:

Audit Committee KPMG Patrice Impey – General Manager, Finance, Risk and Supply Chain Management / CFO  
Tim Leung – City Treasurer  
Rajdeep Sidhu – PCI Compliance Officer  
Leo de Sousa – Director, Enterprise Technology  
David Polano – Manager, Cybersecurity

## EXECUTIVE SUMMARY

January 20, 2021

The objective of the audit was to provide reasonable assurance on the effectiveness of the City's PCI Compliance program, and the City's readiness for maintaining compliance given anticipated payment card transaction growth.

With the adoption of the three-lines of defense PCI governance model in 2020, the City has the framework in place to further PCI maturity. The PCI Office has established effective processes for evaluating the City against PCI DSS standards to maintain Level 2 compliance.

However, given continued growth in the City's processing of credit card transactions, further efforts are required to ensure continued compliance to become Level 1 ready. Management has committed to implementing all recommendations.

The more significant findings and recommendations from this audit include:

### **E.1 Formalize the project management for developing a PCI Level 1 readiness roadmap**

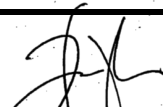
To ensure that the City progresses systematically towards becoming PCI Level 1 ready, a roadmap should be developed and implemented. Formal project management on the implementation of the roadmap should be established as changes to PCI related controls may impact both technology and business processes.


### **E.2 Develop a long-term PCI Office resourcing plan**

Due to challenges in retaining expertise in the PCI Office in a competitive market, an external services firm has provided operational support to the PCI Office since 2017. While the City has benefited from their strong technical skills, a cost-benefits analysis of various resourcing models should be performed to develop a long-term team structure for the PCI Office.

### **E.3 Document risk acceptance of significant PCI risks**

Maintaining PCI compliance is a shared responsibility between all City groups that have a role in PCI related processes. In situations where business unit decisions could introduce excessive risks to the PCI environment and significantly impact PCI maturity or compliance, the PCI Office should report concerns and potential consequences to the PCI Executive Committee and the Risk Management Committee.

  
Tony Hui, CPA, CA, CRMA  
Chief of Internal Audit

  
Jenny Lau, CIA, CISA  
Senior Internal Audit

## A. BACKGROUND

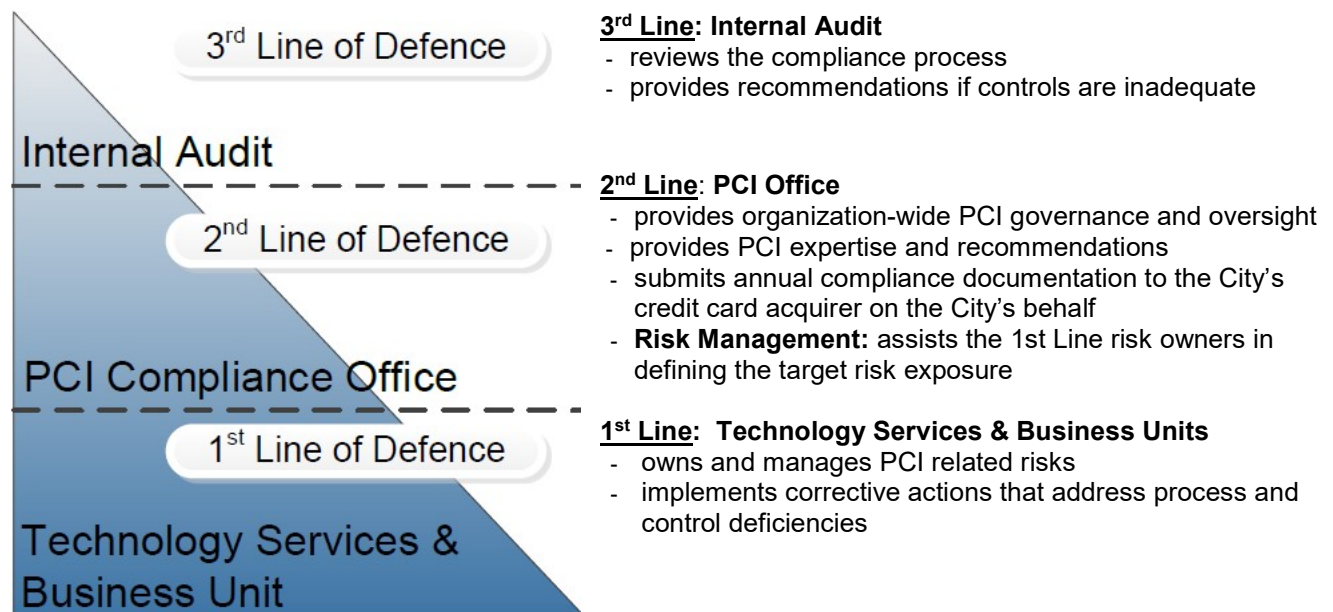
### PCI DSS

Payment Card Industry's Data Security Standard (PCI DSS) is a mandatory compliance requirement for all organizations that process, store, transmit or access cardholder information for the major payment card brands. The standards provide a set of controls for securing cardholder data to prevent data breaches and fraud.

Organizations that fail to comply may be subjected to fines, penalties of higher percentages, or the loss in ability to accept credit card payments.

### Three-lines of defense for PCI compliance

In 2020, the City adopted a three-lines of defense model for implementing PCI compliance:



Source: City PCI Governance Charter (March 2020)

### City-wide responsibilities for PCI compliance

While formal governance is in place, business units across the City that handle credit card information or processes are responsible for implementing and executing procedural and security controls. A breach in one business unit impacts the City's compliance as a whole.





## PCI Office responsibilities

To provide organizational-wide governance and oversight for PCI, the PCI Office:

- Triages and addresses day-to-day operational enquiries on PCI DSS from departments.
- Evaluates PCI compliance of potential new vendors with Supply Chain Management.
- Evaluates IT changes and their potential PCI impacts with the Change Advisory Board.
- Works with Technology Services and business units to address new security requirements from the City's credit card acquirer or payment brands.
- Performs annual PCI assessments of Technology Services and business units.
- Informs Technology Services and business units about control issues identified from the PCI annual assessment to be addressed and remediated.
- Submits annual compliance documentation to the City's credit card acquirer.

## PCI compliance levels

There are four PCI compliance levels based on annual credit card transaction volume:

	<b>PCI Level</b>	<b># of Card Transactions Annually</b>	<b>Compliance</b>
<b>anticipated status in ~2-4 years</b> 	Level 1	6+ million	External audit by QSA
<b>current status</b> 	Level 2	1 to 6 million	Self-reported
	Level 3	20,000 to 1 million	Self-reported
	Level 4	fewer than 20,000	Self-reported

## City's Level 2 compliance

The City has maintained PCI compliance as a Level 2 merchant. As a Level 2 merchant, the PCI Office self-reports using the Self-Assessment Questionnaires (SAQ) on behalf of the City to the City's credit card acquirer, Moneris.

## City progressing towards Level 1

It is estimated that the City will become a Level 1 merchant within the 2 to 4 year timeframe. This projection is based on the City's current merchant standing and continued digitalization of services offering credit card payment options.

Compliance to Level 1 requirements involve more rigorous conformity to PCI DSS controls. Level 1 compliance is independently evaluated by an external PCI Qualified Security Assessor (QSA).

## **B. SCOPE**

The objective of the audit was to provide reasonable assurance on the effectiveness of the City's PCI Compliance program, and the City's readiness for maintaining compliance given anticipated payment card transaction growth. Our work included interviews with members of the PCI Office, Technology Services, business unit teams, and procedures that included:

- Review of policy documents such as the PCI Governance Charter, PCI Office Assessment Reports, and Site PCI Scorecard Reports.
- Observed meetings conducted relating to the PCI annual assessment, PCI working group and procurement processes.
- Review of procurement related documents for evaluation of PCI technical requirements.

The audit was not designed to detect fraud. Accordingly, there should be no such reliance.

## C. CONCLUSION

With the adoption of the three-lines of defense PCI governance model in 2020, the City has the framework in place to further PCI maturity. The PCI Office has established effective processes for evaluating the City against PCI DSS standards to maintain Level 2 compliance. However, given continued growth in the City's processing of credit card transactions, further efforts are required to ensure continued compliance to become Level 1 ready.

Findings and recommendations were discussed with Management and their responses were incorporated in this report. Management has committed to implementing all recommendations. We thank the PCI Office and Technology Services teams for their assistance with the audit.

## D. RISK ANALYSIS

The potential risks considered if PCI compliance processes were not effective included:

- Financial loss due to inability to process credit card payments
- Fines and penalties
- Reputational harm from loss of trust to the integrity of City systems
- Regulatory penalties from breach of personal or financial information

## E. AUDIT ISSUES, RECOMMENDATIONS AND MANAGEMENT RESPONSES

### E.1 Formalize the project management for developing a PCI Level 1 readiness roadmap

#### City progressing towards Level 1 requirements

The City is currently a Level 2 merchant that self-reports compliance. It is estimated that the City will become a Level 1 merchant in approximately 2 to 4 years based on the City's current merchant standing and continued digitalization of services offering credit card payment options.

Compliance to Level 1 requirements involve more rigorous conformity to PCI DSS controls. Level 1 compliance is independently evaluated by an external PCI Qualified Security Assessor (QSA), and not self-assessed as with Level 2 compliance.

#### 2020 internal maturity assessment of Level 1 readiness

Based on the PCI Office's internal maturity assessment of Level 1 readiness, improvements were made in the past year:

- The level of compliance for controls increased for "Compliant" controls.
- The estimated risk perceived of breach was decreased for "Critical / High / Medium" risks.

However, notable improvements still exist in the security environment, and the City is not ready to undergo a formal Level 1 readiness assessment. There are controls deemed "Partially" or "Marginally" compliant against Level 1 requirements that require additional attention. Also, the severity of estimated risk of breach should be further reduced before reaching Level 1 compliance.

#### Develop a Level 1 readiness roadmap

To ensure that the City progresses systematically towards Level 1, a roadmap should be developed and implemented. Formal project management on the development and implementation of the roadmap should be employed as anticipated changes to PCI related controls impact both technology and business processes. In addition, the progress on the Level 1 readiness roadmap should be included in the quarterly updates to the PCI Executive Committee.

**Recommendation:**

**E.1.1 The PCI Compliance Officer should formalize the development and implementation of the PCI Level 1 readiness roadmap as a project with the FRS Project Management Office. Within the project, the DARCI matrix tool should be used to document accountability for delivery on various parts of the roadmap. In addition, progress on the project should be made to the PCI Executive Committee on a quarterly basis. This should be completed by August 31, 2021.**

**Management Response:**

Please check one:

Agree with the findings

Disagree with the findings

Please check one:

Agree with the recommendations

Disagree with the recommendations

**Management Action Plan:**

*Starting Q1 of 2021 PCI Office has engaged the PMO Office to secure a Project Management resource to build out a comprehensive Level 1 Readiness Plan which includes the Engagement Model and DARCI.*

*Starting early 2019 PCI Office has started to define high-level work packets to include in the Level 1 Readiness Project. These work packets will be incorporated into project requirements.*

*During the 2019 Audit Assessment PCI Office has documented a detailed maturity index against current PCI DSS Requirements. This maturity index has been updated to reflect updates in 2020 and can be incorporated into the gap analysis for the Level 1 Readiness Project.*

**E.2 Develop a long-term PCI Office resourcing plan**

Use of external services firm since 2017

To quickly ramp up PCI capabilities in late 2017, PCI technical experts were engaged from an external firm to support PCI annual assessment and reporting processes. Due to challenges in retaining expertise in a competitive market and delays with finalizing a PCI governance model between the PCI Office and Technology Services, the external team has continued to provide support to the PCI Office since 2017.

Currently, the PCI Office is comprised of the PCI Compliance Officer supported by the external team. The team provides operational support such as addressing enquiries from departments on PCI DSS, evaluating PCI compliance of potential new vendors, and performing annual assessments of PCI controls.

The costs of the external team has been partially off-set by the vacancies on the team. The table below outline the costs by the external services firm to the PCI Office:

PCI Office Support – External Contractor Costs			
2017	2018	2019	2020
\$166K	\$301K	\$304K	\$381K

*Note: Increase in 2018 was due to ramp-up of the PCI Office. Contractor rates were static until 2020. Increase in 2020 was related to changes to assessment results reporting and contractor rates aligning to market.*

### Develop a long-term resourcing model

While the City has benefited from the strong technical skills of external PCI experts, management has started to review the long-term resourcing model for the PCI Office. The review should include a cost-benefits analysis to compare various options from City staff operating the PCI Office, to the current model of external consultants. If external consultants are involved, proper knowledge transfer to City staff should be performed to ensure business continuity.

#### **Recommendation:**

**E.2.1 The City Treasurer should perform a cost-benefits analysis of various resourcing models and develop a plan and team structure to support the PCI Office. The plan should consider relevant compensation schemes given the competitive environment for IT security expertise. The model should be presented to the General Manager, Finance, Risk and Supply Chain Management for approval. This should be completed by December 31, 2021.**

#### **Management Response:**

Please check one:

Agree with the findings

Disagree with the findings

Please check one:

Agree with the recommendations

Disagree with the recommendations

#### **Management Action Plan:**

*PCI Office has found it challenging to hire based on the current job classifications and requirements. PCI Office continues to engage industry experts (consultants) to fill resourcing gaps as needed.*

*In 2019, the PCI Office identified to the GM FRS the challenge with the current classifications and the position descriptions.*

*PCI Office will update Job Descriptions to ensure all position requirements are identified. The classification and compensation will then be reviewed with Human Resources Compensation.*

*These results are expected in late 2021. The PCI Office will also review resourcing options for both internal and consulting resources.*

### **E.3 Document risk acceptance of significant PCI risks**

Maintaining PCI compliance is a shared responsibility between all City groups that have a role in PCI related processes. Decisions made by individual business units could impact PCI maturity and compliance for the City as a whole.

The PCI Office provides recommendations to business units to ensure PCI requirements are met when changes are introduced to the PCI environment. Changes could be introduced from the adoption of new vendor software or changes to existing technology or processes. Business units include the PCI Office's recommendations as input for making decisions.

However, in situations where business unit decisions introduce excessive risks to the PCI environment and significantly impact PCI maturity or compliance, the PCI Office should document and report concerns to the PCI Executive Committee and the Risk Management Committee.

**Recommendation:**

**E.3.1 The PCI Compliance Officer should ensure that significant risks introduced to the PCI environment due to system or process changes are documented and reported to the PCI Executive Committee or the Risk Management Committee. This should be completed by June 30, 2021.**

**Management Response:**

Please check one:

Agree with the findings

Disagree with the findings

Please check one:

Agree with the recommendations

Disagree with the recommendations

**Management Action Plan:**

*PCI Office has been presenting risks at various forums to various stakeholders such as the Operations Directors, Project Steering Committees, directly to the Business Units and the CRO.*

*PCI Office has documented in Q2 2021 a formal PCI Risk Template. PCIO will further refine the process of documenting, presenting and disseminating risks to the PCI Executive Committee or the Risk Management Committee as appropriate.*

**E.4 Develop a technical incident response playbook for PCI**

Cybersecurity Incident Response Plan recently updated

In 2020, Technology Services updated the Cybersecurity Incident Response Plan and completed a tabletop exercise of the plan. Going forward, there are plans to further develop cybersecurity incident response through development of incident specific playbooks and further exercises to test the plans.

Incident response playbook for cybersecurity incidents involving PCI

In the event of a PCI related security incident, a PCI specific playbook should be available given the compliance requirements. Information that maybe specific to PCI incidents include:

- technology response procedures to be performed;
- timelines and procedures required by the City's credit card acquirer or payment brands on incident reporting or notification;
- specific language or wording to be used in communications;
- involvement of other teams such as the Privacy Office or Legal Services; and
- activation of processes and procedures that enable acceptance of alternative channels or forms of payment.

**Recommendation:**

**E.4.1 The Director Enterprise Technology, working with the PCI Office, should develop a PCI technical incident response playbook in the event of a cybersecurity incident involving PCI. This should be completed by September 30, 2021.**

**Management Response:**

Please check one:

Agree with the findings

Disagree with the findings

Please check one:

Agree with the recommendations

Disagree with the recommendations

**Management Action Plan:**

*The Director Enterprise Technology will lead the work, in collaboration with the PCI Office and Risk Management, to create a PCI specific playbook that will be part of the City's overall Cybersecurity Incident Response plan by Sept 2021.*

**F. OTHER OBSERVATIONS**

**F.1 Service Level Agreement between the City and VPL for IT services**

The City and the Vancouver Public Library (VPL) each manage their own IT services teams and IT infrastructure. However, there are aspects of the City's network that VPL relies on. While there have been discussions between the City and VPL's technology services teams, a formal shared services agreement between the City and VPL for IT services is not in place.

As Internal Audit is schedule to perform an audit of VPL's cybersecurity in 2021, observations relating to an IT service level agreement between the City and VPL will be detailed in that report.