AUDIT AND OPERATIONAL REVIEW COMMITTEE JUNE 2, 2010

PAYMENT CARD INDUSTRY (PCI)
DATA SECURITY STANDARDS COMPLIANCE

Recommendation

The Commissioner of Finance/City Treasurer, in consultation with the City Manager, Chief Information Officer (CIO), and the Director of Financial Services recommends:

That this report be received.

Contribution to Sustainability

Not applicable.

Economic Impact

To assist the City with the Payment Card Industry (PCI) compliance program, the services of an external consulting organization was acquired, in consultation with Purchasing. The associated consulting services costs are estimated to be $75,000. Sufficient funding is available in the 2009/2010 approved budget for this initiative.

Communications Plan

Quarterly updates are provided to the Program Sponsors and Owners by the Program Manager. Each project within the program has team meetings either monthly or weekly.

Purpose

The purpose of this report is to provide the Audit and Operational Review Committee with information pertaining to the Payment Card Industry mandatory data security standards compliance requirements and provide an update on the City's program to reach compliancy.

Background - Analysis and Options

PCI Data Security Standards were established by the PCI Security Standards Council which is made up of major payment card brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The standards cover operational, as well as technical aspects of credit card payment processing.

Compliance with the PCI set of standards is mandatory for businesses/organizations that process credit card information. The City processes credit card information with VISA, MasterCard and American Express. The City's credit card processing bank, TD CanadaTrust, is engaged with the City and is monitoring the City's progress towards compliance on behalf of the PCI Security Standards Council.

In Q3 2008, the Commissioner of Finance & Corporate Services at the time initiated the PCI data security standards compliance program. A high level assessment of the City's processes, computer applications and technology infrastructure was conducted and a report was developed outlining recommendations to move towards PCI data security standards compliance. The PCI data security standards program is being managed by the Information & Technology Management (ITM) department's Project Management Office (PMO) and is focused on identifying:

- Where credit card data is stored or handled
- What is being done to secure the storage, transmission and handling of credit card data via policies and infrastructure/application set up
- Who is involved and should be involved in the various PCI related processes
- How will security of credit card data be maintained and monitored
- Proving that policies and procedures are applied and enforced, and that infrastructure/ applications are secure.

A roadmap consisting of the following projects has been developed to address the above items, these projects include:

1. PCI Business Compliance;
2. Class 7.0 Upgrade;
3. PCI ITM Implementation;
4. Maintenance Plan; and
5. Validation & Certification.

1. PCI Business Compliance Project

The first project initiated was the PCI Business Compliancy Project in Q1 2009. The objective of this project is to develop and train staff on PCI data security standards related policies and procedures. The project team is comprised of representatives from Clerks, Corporate Communications, Enforcement Services, Financial Services, Human Resources, ITM, Legal, Public Works, Purchasing, Recreation & Culture departments, as well as, Vaughan Business Enterprise Centre (VBEC) and Vaughan Public Library. To-date the team has documented current and new credit card processes and created PCI related policies. Any high risk credit card processing issues were addressed immediately. The PCI related policies are currently in the revision stage and should be completed by Q2 2010 and then presented to Council for approval as necessary. Remaining activities include the documentation of new procedures and staff training. Included in the new procedures is an Incident Response Plan (IRP). The IRP will be invoked upon the report of a credit card breach. This project is slated for completion Q3 2010.

2. Class 7.0 Upgrade Project

The Class solution is used by City residents and City staff to register for Recreation & Culture programs and book facilities. This system was identified as requiring changes to accommodate PCI data security standards. The Class 7.0 Upgrade Project was dependant upon the availability of the upgraded solution from the vendor. Therefore, the Class 7.0 Upgrade Project was initiated in Q4 2009. The project team consists of representatives from Financial Services, ITM and Recreation & Culture. This project's objective was to upgrade the Class Solution to version 7.0, as well as, comply with the new HST tax. The upgraded Class solution has been live since May 5, 2010. This project will be completed upon final HST changes July 1st, 2010.

3. PCI ITM Implementation Project

The PCI ITM Implementation Project was initiated in Q4 2009. This project's objective is to ensure City technology infrastructure is PCI data security standards compliant. The project team consists of various resources within the ITM department. Some of the activities required for this project are dependent on the Class 7.0 Upgrade Project, therefore, the project planning for this initiative has commenced and planning should be completed by Q2 2010. A project completion date is currently estimated to be Q4 2010.

4. Maintenance Plan Project

The Maintenance Plan Project has not been initiated to-date. This project is dependant on the completion of the PCI Business Compliancy, Class 7.0 Upgrade and PCI ITM Implementation Projects. Since PCI data security standards compliance requires adherence to the latest PCI data security standards version and regular audits of City procedures and technology, a maintenance plan will be required. This plan will establish governance, assign PCI related roles and scheduled activities to ensure on-going PCI data security standards compliance within the City. This project has been slated for completion Q4 2010.

5. Validation & Certification Project

The Validation & Certification Project has not been initiated. This project is dependant on the completion of the Maintenance Plan Project. This project will include the completion of a Self Assessment Questionnaire. This questionnaire is a validation tool for merchants to review various business practices. As well, qualified assessors must be engaged to perform certified vulnerability scans on our computer systems. Upon successful completion of the questionnaire and scans the City will be deemed PCI data security standards compliant. This project has been slated for completion Q1 2011.

PCI Data Security Standards compliancy is crucial to the City's continuous service to our Residents and Businesses. It is important to note that this initiative is considered a program as compliancy is only valid until the next PCI data security standards version change or vulnerability scan. Therefore, adherence and commitment to the maintenance plan must be enforced.

Relationship to Vaughan Vision 2020

This report is consistent with the priorities previously set by Council and the necessary resources have been allocated and approved.

Specifically, the recommendations of this report support the following Vaughan Vision 2020 initiatives:

Service Excellence

- Pursue Excellence in Service Delivery

Management Excellence

- Enhance Productivity, Cost Effectiveness & Innovation
- Maintain Assets & Infrastructure

Regional Implications

None

Conclusion

The City is being diligent in becoming PCI data security standards compliant by initiating and maintaining PCI compliance program. PCI data security standards compliance is crucial to maintaining "good standing" with our credit card processing bank and to continue the delivery of services to our residents and businesses.

Attachments

None

Report prepared by:

Lucy Pasianotto, Project Manager,
Business Solutions Services, ITM – Ext. 8068

Respectfully submitted,

____
Barbara Cribbett, CMA
Commissioner of Finance/City Treasurer