Audit Committee Report

DATE: Monday, January 30, 2023 **WARD(S):** ALL

TITLE: PCI COMPLIANCE AUDIT

FROM:
Kevin Shapiro, Director of Internal Audit

ACTION: FOR INFORMATION

Purpose

To communicate the findings from the PCI Compliance Audit.

Report Highlights

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure organizations that accept, process, store or transmit credit card information maintain a secure environment. The standard was created to increase controls around cardholder data to reduce credit card fraud.
- The City maintains a program that includes development and maintenance of PCI DSS policy. The policy specifies daily administrative and technical operational security procedures that are consistent with the PCI DSS, including roles and responsibilities.
- The audit has identified significant compliance gaps, which if not addressed, could result in the compromise of the City's cardholder data environment. Remediation and improvement are required to ensure risks related to the significant areas of challenge uncovered in the audit are mitigated.
- Management has developed action plans which will mitigate the identified risks and address the recommendations outlined in the report.
- This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*
- Internal Audit will follow up with management and report on the status of management action plans at a future Audit Committee meeting.

Recommendation

1. That the Internal Audit Report on the audit of PCI Compliance be received.

Background

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure organizations that accept, process, store or transmit credit card information maintain a secure environment. The standard was created to increase controls around cardholder data to reduce credit card fraud. Since the City stores and processes payment card information in its daily operations, management needs to ensure that the City is compliant to these standards.

The City maintains a program that includes development and maintenance of PCI DSS policy. The policy specifies daily administrative and technical operational security procedures that are consistent with the PCI DSS, including roles and responsibilities.

In addition to non-compliance to PCI DSS, if credit card information is not secured, there is a greater risk that the information may be compromised.

The objective of the audit is to evaluate the adequacy and effectiveness of the internal controls, processes and procedures in place to mitigate the business risks associated with the management and administration of credit card information and ensure that the City is compliant with PCI DSS.

This audit was co-sourced with Control Gap Inc., who was the successful bidder after a competitive procurement process (RFP22-120).

Control Gap Inc. assisted Internal Audit in:

- Conducting an accurate and thorough assessment of the potential risks and validating the various security controls outlined within the PCI DSS.
- Providing a Gap Analysis of the City's current cardholder data environment and related practices against the current version of the PCI DSS.
- Drafting of applicable Self-Assessment Questionnaires (SAQ) through interviews, Q & A sessions or follow-ups.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

Previous Reports/Authority

Not applicable.

Analysis and Options

In fulfilment of RFP22-120 *Quality Security Assessor for PCI DSS Compliance,* Control Gap Inc., conducted an accurate and thorough assessment of the potential risks and validated the various security controls outlined within the PCI DSS during the period of June 2022 to January 2023.

The results of these activities were captured in a series of reports issued to Internal Audit and Management as outlined below.

- Gap Assessment Report
- Draft SAQs for applicable payment systems

A presentation of the Gap Assessment Report has been provided to the Audit Committee as Attachment 1. Management has developed action plans which will mitigate the identified risks and address the recommendations outlined in the report. The action plans have been provided to the Audit Committee as Attachment 2.

Significant remediations and improvements will be required to ensure risks related to the significant areas of challenge uncovered in the audit are mitigated.

Before the introduction of the PCI DSS, entities processing credit card payments have always been required to follow payment rules of the individual credit card companies (e.g., Visa, Mastercard, AMEX etc.). The City of Vaughan's compliance obligations thus began when the City started accepting credit card payments.

The PCI DSS was first introduced in December 2004, considering each credit card payment brand's rules and working to standardized requirements for merchants and other entities involved in storage, processing, or transmission of cardholder data.

In July 2013, the City undertook an independent assessment with a consultant to validate the City's proposed network architecture for their PCI requirements, which identified several scope reduction and technology recommendations. While some of the technology recommendations were implemented, PCI scope remained a significant issue identified in this audit. Furthermore, the 2013 assessment focused on technical aspects of PCI compliance. Prior to this audit, the City has not conducted a holistic analysis of corporate PCI compliance.

The City of Vaughan did not have dedicated personnel or focused resource efforts managing PCI DSS compliance and ultimately, many compliance requirements were only identified during this audit. The City's practices, for example, leveraging VoIP and email to transmit cardholder data, resulted in complicated compliance footprints for many of the City's systems. These gave rise to payment processes without compliant controls, which require remediation. The audit has identified the following significant compliance gaps, which if not addressed, could result in the compromise of the City's cardholder data environment:

- Diverse groups without central management. As the City has fifteen departments accepting payments by various means, it's extremely challenging for the City to maintain compliance without central management. Departments accepting payments do not have expertise or focus related to payment security, and the City had not previously dedicated staff to managing compliance activities.

- Many non-compliant service providers. Many departments within the City have elected to outsource parts of their payment processing, particularly e-commerce websites. Service providers were not managed in accordance with PCI DSS requirements, which include annual review of service providers to ensure compliance.

- On-premise (in-house) complicated components and VoIP (Voice over Internet Protocol, a technology that allows voice calls using a broadband Internet connection). Currently the City's VoIP systems would have full scope applicability as the City of Vaughan's VoIP infrastructure directly transmits cardholder data in order to enable payments. This poses significant challenges as it results in complicated compliance footprints for many of the City's systems.

- Email. In some isolated instances, a City department leveraged email to receive cardholder data. This is contrary to the City's Cardholder Data Protection Policy 14.A.04. It is cost-prohibitive to secure email and securing email might not be viewed as fiscally responsible. It is more fiscally prudent to not accept payments by email and leverage payment terminals and compliant e-commerce solutions.

Per discussion with management, resource constraints and lack of relevant expertise are cited as the primary causes of the issues identified. A siloed, decentralized approach is followed without clearly defined oversight, responsibilities and accountabilities. The absence of a central governance structure and oversight process increases the risk of non-conformance with the PCI requirements. Non-compliance with PCI DSS could result in financial penalties and reputational damage to the City.

Financial Impact

There are no direct economic impacts associated with this report.

Broader Regional Impacts/Considerations

Not applicable.

Conclusion

Opportunities for remediation and improvement have been highlighted in Control Gap's report. These include:

- Implement central management of PCI. Centrally managed compliance with a governance structure will enable the City to ensure personnel assigned PCI responsibilities are educated and aware of PCI compliance requirements and provides better oversight of payment processes. It can help streamline compliance efforts along with standardization payment processes.

- Reduce scope with standardized PCI processes. Standardization of PCI management with a central management group overseeing all department payment processes would enable the City to ensure compliance across all departments. It will streamline and enable efficient compliance initiatives.

- Leverage compliant service providers to reduce scope. The City is required to manage these service providers and will need to plan for compliance in this area. Once a vendor has demonstrated compliance, year over year effort in managing the third-party service provider should be feasible.

- Implement network segmentation and PCI controls on all systems and networks that remain in scope. With long term strategy in mind, the City should focus first on reducing PCI scope to the smallest scope possible, and then look to implement PCI controls on those systems as required based on the scope of the system.

PCI compliance is an ongoing activity that needs to be well planned based on risk and cost. Management is currently engaged in this process. Management has developed action plans which will mitigate the identified risks and address the recommendations outlined in the report.

Internal Audit will follow up with management and report on the status of management action plans at a future Audit Committee meeting.

For more information, please contact: Kevin Shapiro, Director of Internal Audit, ext. 8293.

Attachments

1. Attachment 1 – Presentation Materials
2. Attachment 2 – Management Action Plans

Prepared by

Hemingway Wu, Audit Project Manager, ext. 8350.

Approved by

Kevin Shapiro, Director of Internal Audit