Office of the Chief Information Officer and Financial Services

PCI DSS Assessment - Management Action Plan

Compliance Approach

To facilitate PCI DSS compliance the plan will focus on two major objectives outlined in Control Gap's report. First, to significantly reduce the amount of City's infrastructure that falls under PCI scope and ensure that all payment channels fall under minimally complex compliance requirements. Second, validate a reduced set of controls remaining in scope of direct City responsibility and ensure all service providers are PCI DSS compliant.

With input from the assessment team and Control Gap, Management decided to follow the Control Objectives for Information Technologies (COBIT 2019) framework designed to help businesses develop, organize and implement strategies around information management and governance. COBIT 2019 will support development of a fully functional PCI DSS compliance program and determine appropriate implementation steps as a part of this management action plan. Specifically, COBIT Implementation Guide will be used to ensure all major steps required for a successful implementation of a functioning program are present.

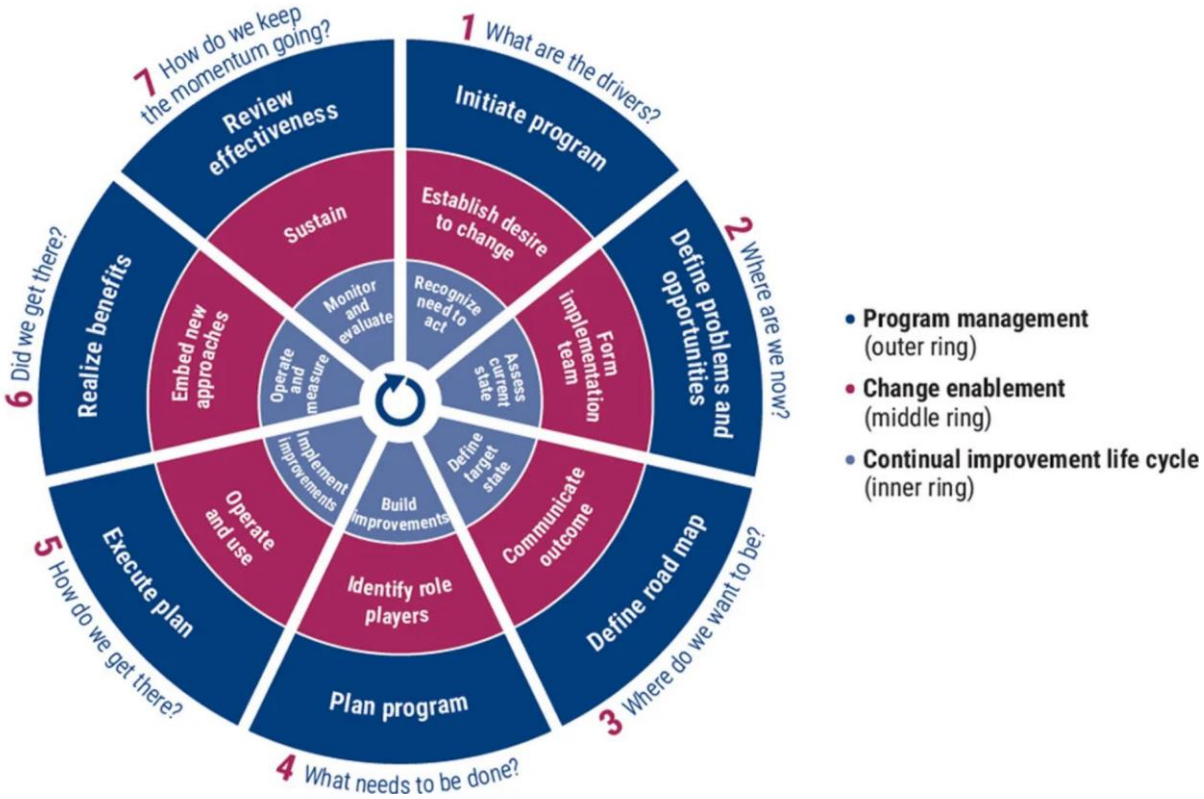

Figure 1 – COBIT Implementation Roadmap Template

Below is the mapping of template steps to artifacts and deliverables created as part of the City's PCI DSS compliance assessment that will inform and enable the creation of holistic PCI DSS compliance program:

Step 1: Commitment to PCI DSS compliance outlined in **Cardholder Data Protection Policy** adopted by the City in 2021

Step 2: Assessment of existing state conducted by Control Gap in **2022 Strategic Gap Analysis Report**

Step 3: Recommendation documented in **2022 Strategic Gap Analysis Report (Section 5)**

Step 4: Roadmap, including timelines defined in **PCI DSS Compliance Management Action Plan**

Step 5: Execution of the **PCI DSS Compliance Management Action Plan** to be managed through a formal Project Management Methodology

Step 6: Achievement of objectives will be gauged through monitoring of Key Performance Indicators defined in **PCI DSS Program Operations Manual**

Step 7: Compliance will be sustained though governance structure defined in **PCI DSS Program Operations Manual**

PCI DSS Program Components and Resourcing (Area of Challenge 4.1.1)

The PCI assessment has demonstrated an urgent need for the City to introduce a central management approach to standardize and reduce the number of unique vendors as well as a formal PCI DSS compliance program (the "Program") with dedicated resources.

The Program will be fully defined in **PCI DSS Program Operations Manual** and will serve as a central point of reference for all stakeholders and will simplify any future Program modifications. It will address PCI DSS requirements, enable better PCI DSS scope control, and provide ongoing visibility into the status of the City's PCI compliance through formal key performance measures. The following essential Program components were identified by the assessment team.

As per the gap assessment report: *"The PCI SSC has published several guidance documents to assist organizations with managing PCI. In particular, the Information Supplement "Best Practices for Maintaining PCI DSS Compliance" helps with guidance around sustainability. Each of these documents reference central compliance teams responsible for managing PCI DSS compliance within the organization's environment. This will enable the organization to have staff well versed in the complex requirements and it will enable the organization to dedicate efforts towards this activity as business units or departments accepting payments have focus outside of PCI."*

To maintain a healthy compliance program, it is essential to allocate a dedicated resource with experience and certification in PCI DSS field to oversee all components of this Program. An Additional Resource Request (ARR) will be put forward as a part of the management action plan to request appropriate funding required for a PCI DSS compliance lead full-time equivalent (FTE), included in the 2023 budget.

Establish Process for Acquiring AOCs and Responsibilities Matrices from Vendors (Area of Challenge 4.1.2)

The gap assessment stressed the need to leverage PCI compliant vendors. PCI Attestation of Compliance (AOC) and Responsibilities Matrix are an essential part of demonstrating compliance. Multiple vendors, currently used at the City failed to provide the required documentation and in turn, demonstrate compliance.

The PCI Attestation of Compliance (AOC) is a document signed by a Qualified Security Assessor (QSA) that validates an organization's PCI DSS compliance status. The Attestation of Compliance (AOC) is valid for one year at which point it must be renewed. Vendors without a valid attestation of compliance who accept payments on behalf of the City, may be putting residents at a greater risk of a cardholder data compromise.

Responsibilities matrix is a vendor provided document and a mandatory PCI requirement designed to make clear the responsibilities of each party as it relates to the maintenance and operation of the payment infrastructure. A responsibilities matrix is to be collected every year.

To ensure compliance the City will prohibit purchase of software products and services for payment processing purposes from vendors without a valid AOC and responsibilities matrix readily available. The limitation will be put in place via policy and enforced through PCI DSS governance structure. The City will also obtain AOCs and matrices from all existing vendors and take appropriate action (which will be decided as part of the management action plan deliverables) against existing service providers who will be unable to provide an AOC. An ongoing AOC validation process will be put in place and any lapses in compliance will be addressed through the new governance structure.

Phone-Based Payment Channels (Area of Challenge 4.1.3)

Phone-based, Card-not-Present (CNP) payments introduce a different compliance challenge. The City must consider that phone-based transactions using City's VOIP and soft-phone phone systems will put a significant portion of corporate infrastructure in a scope of PCI. As outlined in the Gap assessment: *"VoIP systems directly transmitting cardholder data would not be eligible for reduced applicability and all controls from SAQ D would need to be validated. This would in essence list out all 12 high-level requirements and the vast majority of the sub requirements for each of those as well. This is considered an extremely burdensome and complex environment. We would not recommend leveraging these types of complex environments or components without very careful and thought-out planning"*

To address this challenge the team will develop a decision document to holistically analyze details of existing phone-based payment channels and provide a recommendation that will enable scope reduction and channel compliance while taking into account cost, complexity and client experience. The document will then be presented to the newly created governance committee for decision. Implementation timing, cost and impact to compliance will vary based on option selected.

Payment Processing Using Corporate PCs (Area of Challenge 4.1.3)

Currently a number of payment flows include manually entering payment card information on behalf of a resident using a corporate PC, which puts the entire internal IT infrastructure in scope of PCI and significantly increases compliance complexity.

To address this challenge the team will develop a decision document to holistically analyze details of existing payment channels involving corporate PCs and provide a recommendation that will enable scope reduction and channel compliance while taking into account cost, complexity and client experience. This document will then be presented to the newly created governance committee for decision. Implementation timing, cost and impact to compliance will vary based on option selected.

Payment Processing Using Office 365 (Area of Challenge 4.1.4)

During the assessment the team discovered an instance of use of the City's Office 365 environment as a payment channel. Using services such as Exchange Online (Corporate Email), SharePoint or Teams to store or transmit cardholder information, puts a significant compliance burden on the City and makes for a less secure process for residents.

The discovered instance was addressed via direct communication between the specific department and Financial Services. To prevent future occurrences, e-mailing and storing payment card information in Office 365 will be restricted via written policy. Additionally, a Data Loss Prevention (DLP) policy will be put in place to prevent payment card information storage in the Office 365 cloud as well as to block e-mail capabilities. Alerts will be setup to inform dedicated resources who will address violations and recommend any necessary adjustments to the payment channels.

Action Plan Timelines

ID	Action Item	Estimated Timeline	Additional Validators
1	Secure ARR approval, create job description and release posting for a PCI DSS Compliance Lead role	Q1 2023	
2	Implement a DLP (Data Loss Prevention) policy to prevent Cardholder information from residing in Office 365 or e-mailed with Exchange Online	Q1 2023	
3	Define PCI DSS Program components including governance structure, KPIs, awareness, workplan, risk management, etc. and create an operations manual	Q1 2023	
4	Re-architect Libraries payment processing channel to bring it into SAQ A compliance by fully outsourcing all components of the payment website and acquiring appropriate AOC and responsibilities matrix	Q1 2023	Procurement Service, Legal Services, Vaughan Public Libraries
5	Determine and document appropriate action for non-compliance with AOC and Responsibilities Matrix requirements	Q2 2023	Procurement Service, Legal Services
6	Modify annual web-based training to include physical terminal inspection component	Q1 2023	
7	Complete first-pass for appropriate SAQs targeting reduced scope requirements	Q2 2023	
8	Update internal PCI DSS questionnaire to include SAQ requirements to be addressed by the departments involved in payment processing	Q1 2023	
9	Draft Terms of Reference for both governance levels “Enterprise Governance of IT” and “PCI DSS Compliance Team”	Q1 2023	
10	Establish PCI DSS Program governance meetings at executive and operational levels	Q2 2023	SLT-E, Procurement Services, HR, Legal Services
11	Update RFP and Contract Templates to mandate PCI DSS compliance for all service providers engaged in payment processing on City’s behalf	Q2 2023	Procurement Service, Legal Services
12	Define and integrate PCI compliance validation (AOC and roles and responsibilities matrix) into the procurement process and templates.	Q2 2023	Procurement Service, Legal Services
13	Define process for obtaining AOC and Responsibilities matrices from existing service providers and finalize obtaining all outstanding documents including pursuing non-compliant service providers	Q2 2023	Procurement Services, Legal Services
14	Initiate projects to discontinue services provided by non-compliant service providers	Q3 2023	
15	Update Cardholder Data Protection policy to address the following: -Prevent procurement of services from vendors unable to provide appropriate AOC and responsibilities matrix	Q3 2023	SLT-E, Procurement Services, HR, Legal Services

	-Assign annual awareness verification responsibility -Assign responsibility to notify training administrator of new hires -Mandate formal solution owner for each payment processing application on OCIO and Business side -Mandate physical inspections of PIN pads		
16	Finalize decision documents to de-scope phone-based and PC-based payment channels scope	Q3 2023	SLT-E, Recreation Services, Access Vaughan, Financial Services, Fire and Rescue Services, Environmental Services, By-law & Compliance
17	Update the PCI DSS compliance program details in the operations manual to address PCI 4.0 requirements	Q4 2023	
18	Conduct PCI DSS SAQ compliance re-assessment to confirm compliance status	Q1 2024	

Note: Additional Validators are internal City of Vaughan business units required to validate the proposed changes as it might have an impact on their service levels and/or business processes.