

PCI Assessment

Audit Committee – January 30, 2023



Today's Presentation

- Audit Objective
- Scope and Methodology
- Audit Conclusion
- Issues, Observations & Recommendations
- Management Action Plans
- Next Steps
- Questions

Audit Objective

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 cardholders' data and assess the compliance with PCI DSS.

Audit Scope & Methodology

This audit was co-sourced with Control Gap Inc. (RFP22-120). The engagement involved:

- 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 (SAQs) through interviews, Q & A sessions or follow-ups.

Audit Conclusion

- Significant remediations and improvements will be required to ensure risks related to the significant areas of challenge uncovered in the audit are mitigated.
- The audit has identified significant compliance gaps, which if not addressed could result in the compromise of the cardholder data environment.

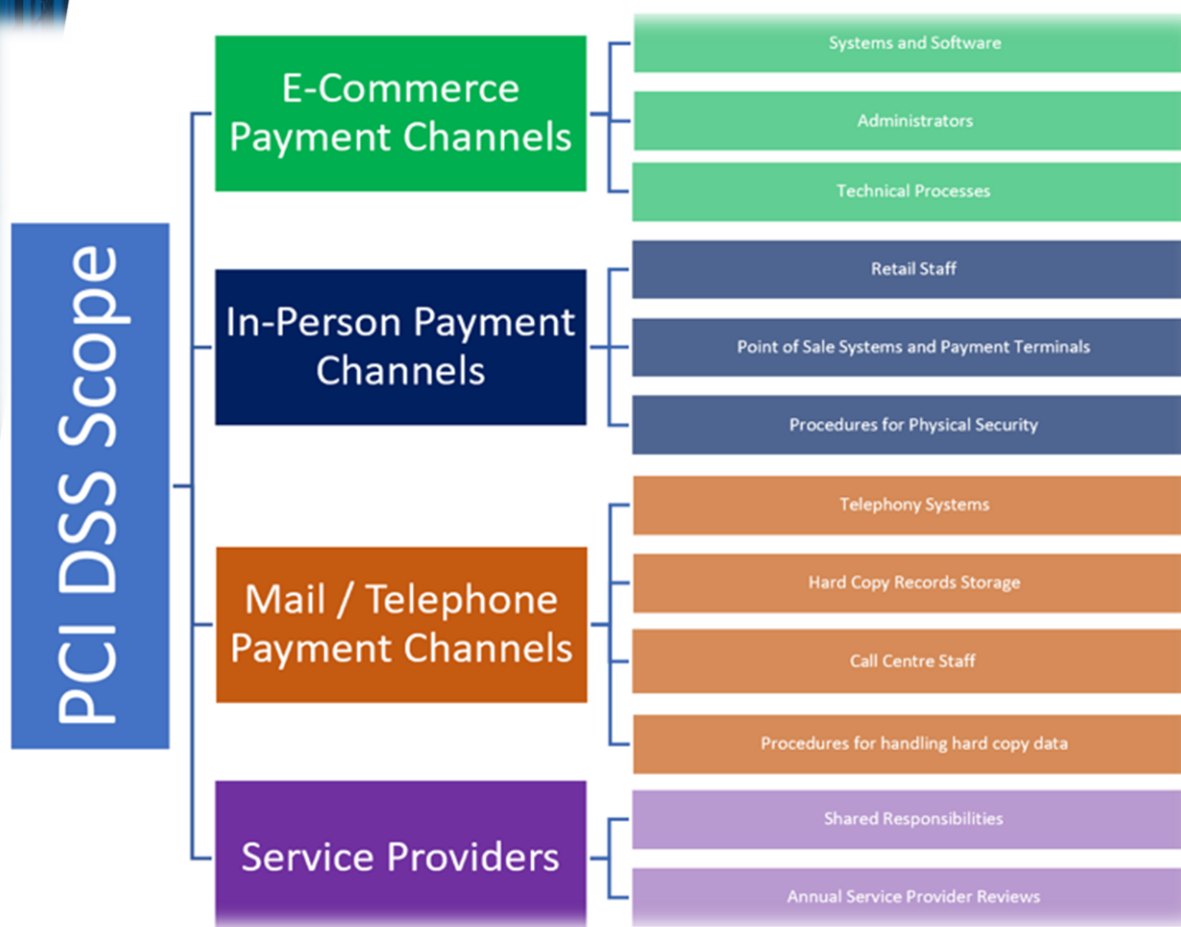
Issues, Observations, & Recommendations

Background information – PCI DSS – The Essentials:

- Payment Card Industry Data Security Standard = PCI DSS
- Required by the Payment Brands and enforced via acquiring banks.
- Aims to protect cardholder data (CHD) at-rest and in-transit.
- Applies to all people, processes, and technology that store, process, or transmit CHD.
- ***Non-compliance has consequences.***



Issues, Observations, & Recommendations



Background information – PCI DSS – Scope:

- PCI scope plays a major role with respect to effort to achieve and maintain compliance.
- Security impacting systems are also in scope.
- Storing card data has more security requirements than other means of processing.










Issues, Observations, & Recommendations

Background information – PCI DSS – Assessments:

- All assessments begin with scope confirmation or review.
- Level 1 assessments, Reports on Compliance (ROCs) require use of a QSA (Qualified Security Assessor).
- Level 2 and other lower-level assessments are Self-Assessment Questionnaires = SAQs
- Different SAQs exist for different payment processing options.
- Different challenges exist for each SAQ, and this relates directly to the concept of Compliance “Footprints”.

Issues, Observations, & Recommendations

Compliance “Footprints”

SAQ Type	# of Requirements	Relative Effort	Commentary
A e-commerce / MOTO	24		<i>This is often considered the most straightforward path to compliance.</i>
A-EP e-commerce / MOTO	191		<i>CAUTION: The increased effort for validating additional requirements could result in exponential increases in effort. Additional systems may be drawn into scope and many requirements and controls require costly activities on a yearly basis, thus causing exponential increases in efforts.</i>
B Face-to-face / MOTO	41		<i>This SAQ applies to payment terminals not currently in use by the City of Vaughan but is included for completeness.</i>
B-IP Face-to-face / MOTO	86		<i>This SAQ applies to payment terminals not currently in use by the City of Vaughan but is included for completeness. Although this SAQ has slightly more requirements, the complexity and challenge of these requirements is low overall.</i>
C Face-to-face / MOTO	160		<i>CAUTION: The increased effort for validating additional requirements could result in exponential increases in effort. Additional systems may be drawn into scope and many requirements and controls require costly activities on a yearly basis, thus causing exponential increases in efforts.</i>
C-VT Face-to-face / MOTO	83		<i>CAUTION: The increased effort for validating additional requirements could result in exponential increases in effort. Additional systems may be drawn into scope and many requirements and controls require costly activities on a yearly basis, thus causing exponential increases in efforts.</i>
P2PE Face-to-face / MOTO	33		<i>P2PE solutions provide drastic scope reductions however they require that the solution is validated and listed on the PCI SSC website.</i>
D-Merchant	329		<i>SAQ-D would apply if an organization directly handled cardholder data, stored cardholder data, or for any other reason is not eligible to complete a different SAQ.</i>
D-Service Provider	356		<i>Service providers have additional PCI requirements applicable only to them, as they are larger targets for attackers. This is because a service provider compromise may result in compromising many merchant environments.</i>

Issues, Observations, & Recommendations

Current State Issues:

- A lack of central management with many diverse sub-groups has caused challenges with compliance.
- Complex payment processing environments exist but should be avoided, if possible.



Issues, Observations, & Recommendations

Areas of Significant Challenge:

- Diverse groups without central management.
- Many service providers who must still validate compliance.
- On-premise complicated components and VoIP.
- Leveraging email to receive cardholder data. This payment channel has already been remediated.

Issues, Observations, & Recommendations

Recommendations:

- Build-up a PCI Team with a governance structure and individuals who are trained such as PCIPs or Internal Security Assessors (ISAs).
- Standardize processes for credit card payments.
- Leverage only PCI compliant service providers.
- Implement processes to ensure controls are put in place and maintained.

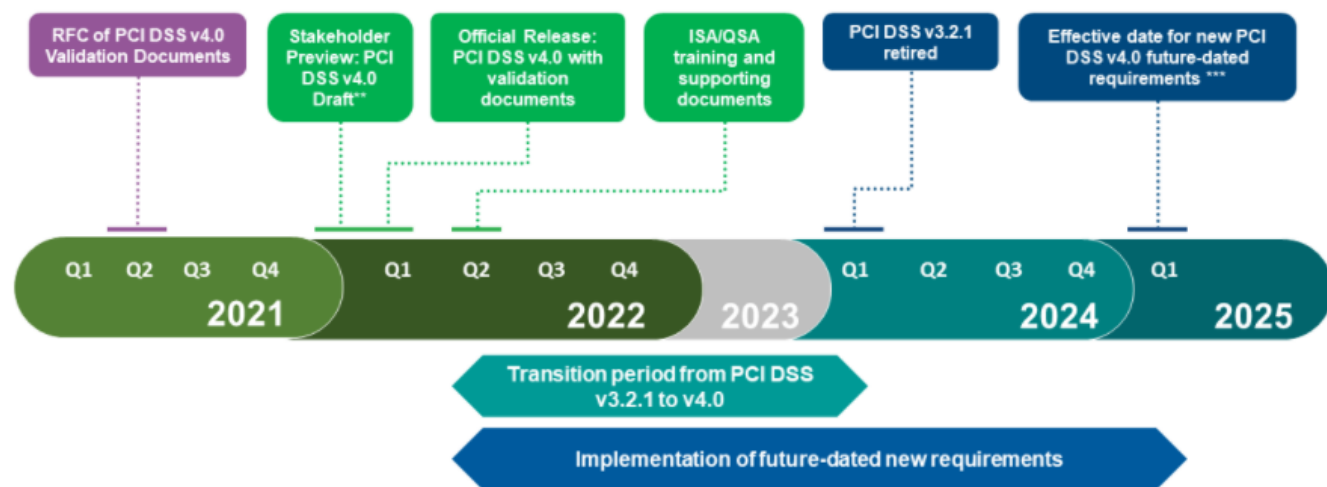
Issues, Observations, & Recommendations

High-level Summary of existing PCI Responsibilities:

- Annual training requirements.
- Payment terminal inspections.
- Incident response and reporting.
- Service Provider Management.
- Annual Assessments and Reporting.
- Additional technical requirements depend on the technical environment. For example, e-commerce data security or technical processes involving CHD may have many additional requirements.

Issues, Observations, & Recommendations

PCI DSS v4.0 Transition Timeline*



* All dates based on current projections and subject to change

** Preview available to Participating Organizations, QSAs, and ASVs

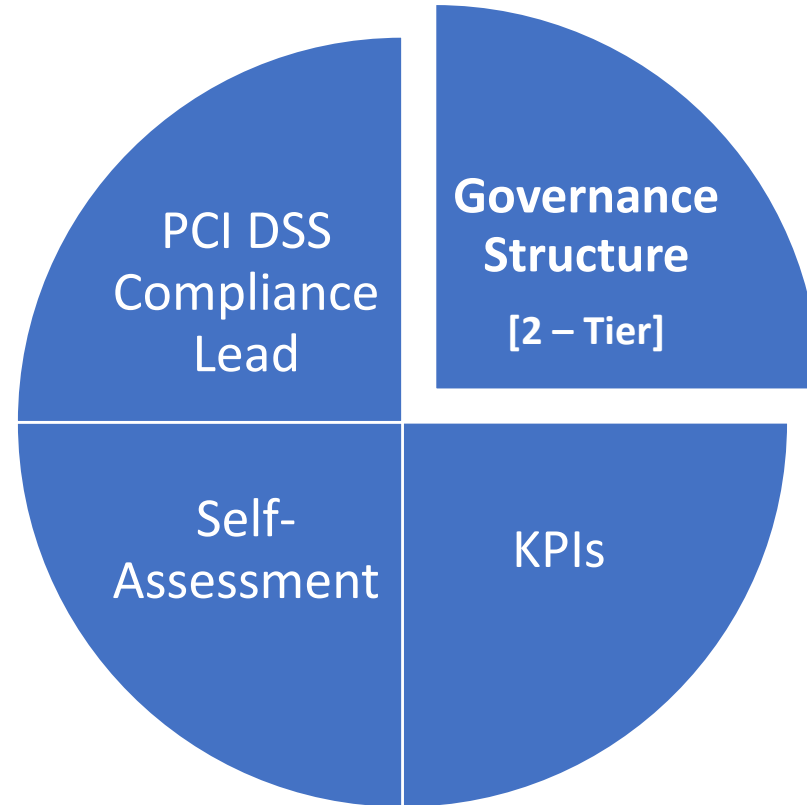
*** Effective date for future-dated requirements to be determined upon confirmation of all new requirements

New Requirements Coming Soon!

<https://blog.pcisecuritystandards.org/updated-pci-dss-v4.0-timeline>

Management Action Plans

Establish and Resource PCI DSS Program



Management Action Plans

Update Existing PCI DSS Components



Management Action Plans

Establish Process for Acquiring Attestation of Compliance (AOCs) and Responsibilities Matrices from Vendors including:

- Updates to procurement processes
- Compliance enforcement for existing service providers
- Elimination of non-compliant service providers

Management Action Plans

Revise Existing Payment Channels



Management Action Plans

Reduce Scope and Compliance Complexity of Phone-Based and PC-Based Payment Channels:

- Analyze existing business processes
- Identify options and provide recommendations
- Implement selected options

Management Action Plans (Key Milestones)

2023 Q1

- Hire Program Lead
- Establish Governance
- Conduct Initial SAQ Validation

2023 Q3

- Select Descoping Options and Commence Descoping
- Update Policy
- Initiate Project(s) to Replace Non-compliant Vendors

2024 Q1

- Conduct SAQ Validation (v3.2.1)

2023 Q2

- Update Contract Templates
- Conclude Vendor Validation

2023 Q4

- Update Compliance Program for version 4.0

Next Steps

- Action plans have been developed
- Implementation is underway or completed
- Internal Audit will follow up and report on the status of these action plans



Questions?





Thank You

