SAINT JOHN

COUNCIL REPORT

M&C No.	2019-184
Report Date	July 24, 2019
Meeting Date	July 29, 2019
Service Area	Corporate Services

His Worship Mayor Don Darling and Members of Common Council

SUBJECT: ***Qualified Security Assessor (QSA) Consulting Services Contract***

OPEN OR CLOSED SESSION

This matter is to be discussed in open session of Common Council.

AUTHORIZATION

Primary Author	Commissioner/Dept. Head	City Manager
Sarah Ranson	***Stephanie Rackley-Roach*** ***Kevin Fudge***	***John Collin***

RECOMMENDATION

The City Manager recommends that:

1) Mayor and Council enter into an agreement with Grant Thornton for Qualified Security Assessor (QSA) consulting services for a term of two years with possible extension of two additional years (for a total of four years).

2) The Mayor and Common Clerk be authorized to execute the necessary contract documents.

EXECUTIVE SUMMARY

The Information Technology and Finance service areas require Qualified Security Assessor (QSA) consulting services to assist in achieving Payment Card Industry Data Security Standard (PCI DSS) compliance. The City is contractually required to meet this standard as a merchant that accepts credit cards for payment. Additional benefits of PCI DSS compliance are reduced risk of a data breach and avoidance of the potentially significant cost of non-compliance.

PREVIOUS RESOLUTION

N/A

REPORT

The Payment Card Industry (PCI) Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection and continuity of operations. The Payment Card Industry Data Security Standard (PCI DSS) forms part of the operating regulations that are the rules under which merchants are allowed to operate merchant accounts. Security threats are non-stop and evolve every day, which is why PCI DSS compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

Given the City accepts credit and debit card payments, the City is contractually obligated to be PCI DSS compliant as a condition of the agreement with Chase Paymentech. The City is working on becoming PCI DSS compliant to ensure the protection of personal data and the City's interests in the delivery of efficient public service.

City staff has taken the initial steps towards compliance. This work included network scans and implementing a PCI DSS compliant third party service provider for online parking ticket payments. Although outsourcing online payment processing simplifies security requirements and can reduce the City's risk exposure, using a third party payment processor does not provide automatic compliance or exclude the City from PCI DSS compliance.

In order to meet PCI DSS compliance, the Finance and Information Technology service teams have completed a procurement process for a Qualified Security Assessor (QSA) to advise and guide the City as we work toward achieving and maintaining a compliant status. This requires understanding and implementing twelve requirements for PCI DSS compliance noted below. Failure to achieve even one of the requirements results in failure to be compliant.

PCI DSS Requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

The PCI DSS compliance project will include a review of our current processes, assessment of our security standards, completion of a gap analysis, and implementation of the necessary controls or remediation. The project team will

also determine how to integrate PCI DSS compliance into organizational work planning and budgeting processes. The implementation project ends when our **Attestation of Compliance (AOC)** is accepted by our acquirer, Chase Paymentech, the company that processes our credit and debit card payments with the banks. At this point, PCI DSS compliance becomes part of our business operations. Maintaining PCI DSS compliance is an ongoing process of assessment, remediation and reporting.

The benefit of using a QSA is to have subject-matter expertise for understanding the twelve requirements, completing on-site security assessments required by PCI DSS, and for guidance when implementing compensating controls. Compensating controls may be considered if the City cannot meet a PCI DSS requirement explicitly as stated due to legitimate technical or documented business constraints. In summary, leaning on a QSA's expertise will ultimately lead to a successful AOC submission.

STRATEGIC ALIGNMENT

As outlined in Council Priorities, the City supports valued customer service delivery. PCI DSS compliance contributes to this priority by ensuring citizen's personal and cardholder data is handled properly. There is also a fiscal benefit as the City reduces the risk of data breaches.

SERVICE AND FINANCIAL OUTCOMES

The agreement is for two years, with the possibility of extending for two additional one year periods. The contract is valued at $41,200.00 each year, although there is no guarantee of volume of work. Funds for this work is allocated in the Information Technology and Finance service area operating budgets. The business risks and ultimate costs of non-compliance, such as fines and legal fees, could exceed the cost of implementing PCI DSS standards.

INPUT FROM OTHER SERVICE AREAS AND STAKEHOLDERS

Materials Management facilitated the Request for Proposal (RFP) process to solicit proposals for Qualified Security Assessor Services. As such, the RFP closed on June 6, 2019 with the following proponents responding by submitting proposals:

- Grant Thornton LLP — Halifax, NS
- Digital Boundary Group — London, ON
- Bell Aliant — Saint John, NB
- MNP LLP — Mississauga, ON
- Online Business Systems — Winnipeg, MB

A review committee, consisting of staff from Materials Management, Finance and our IT Department reviewed the submissions for completeness and

compliance with the RFP requirements and selection criteria consisting of the following:

1. Quality and Completeness
2. Demonstrated Understanding of the Project and Deliverables
3. Proposed Approach
4. Specific Experience, Qualifications and Expertise of Key Personnel
5. Cost

Also in accordance with the City's standard procedures, the committee members evaluated and ranked each proposal based on the proposals' technical merits. Following this, the financial proposals were opened and evaluated and corresponding scores were added to the technical scores.

Grant Thornton LLP's proposal was ranked the highest based on an overall rating of the evaluation criteria as well as offering the lowest cost.

The above processes are in accordance with the City's Procurement Policy and Materials Management support the recommendations being put forth.

ATTACHMENTS

The agreement template is attached as information. Pending approval and formal resolution from Council, the Materials Management service will send the agreement package to Grant Thornton and the Common Clerk for signatures.