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.

AGREEMENT

2019-080602P

Qualified Security Assessor Services

Saint John, NB

AGREEMENT

This Agreement made in duplicate copies this ____ day of _____, 2019.

BETWEEN:

THE CITY OF SAINT JOHN, having its City Hall at 15 Market Square, Saint John, New Brunswick, a body corporate by Royal Charter, confirmed and amended by Acts of the Legislative Assembly of the Province of New Brunswick, hereinafter called the "City"

OF THE FIRST PART

And

[Name of Organization] a [Type of organization], having offices located at [address], in the City of [City] and the Province of [Province], hereinafter referred to as the "Consultant"

OF THE SECOND PART

WHEREAS the City issued Request for Proposal **[2019-080602P]** for **[Qualified Security Assessor Services]** (the "Request for Proposal"); and

AND WHEREAS the Consultant submitted a technical proposal and a financial proposal, both dated **[Date]** in response to the Request for Proposal (collectively, the "Proposal"); and

AND WHEREAS the Request for Proposal and the Proposal are attached hereto as Schedules "A" and "B" respectively and form part hereof;

AND WHEREAS the Financial Proposal forms part of the Proposal, is attached hereto as Schedule "C"; and

AND WHEREAS the Common Council at its meeting held on [Date] resolved that:

"[Resolution]."

NOW THEREFORE THIS AGREEMENT WITNESSETH, that in consideration of the mutual covenants and agreements herein and subject to the terms and conditions set out in the Request for Proposal and the Proposal, the parties for themselves, their successors and permitted assigns respectively, mutually agree as follows:

1. The Consultant shall perform the services and carry out the terms and conditions set out in the Request for Proposal and the Proposal.

2. The City shall pay the Consultant, in return for the services performed, fees as outlined in the financial proposal part of the Proposal, plus HST.

Term

3. The terms of this Agreement is for a period of two (2) years. The City with the consultant's mutual agreement may choose to extend this contract for two (2) additional one (1) year periods.].

Termination

4. The City may immediately terminate this Agreement upon giving notice to the Consultant where:

    a. The Consultant makes an assignment for the benefit of its creditors, is declared bankrupt or commits an act of bankruptcy, becomes insolvent, makes a proposal or otherwise takes advantage of provisions for relief under the *Bankruptcy and Insolvency Act* (Canada)or similar legislation in any jurisdiction, or any other type of insolvency proceedings being commenced by or against the Consultant under the *Bankruptcy and Insolvency Act* (Canada) or similar legislation;

    b. The Consultant breaches any of the terms or conditions of the within Agreement;

    c. In the City's reasonable opinion, the Consultant, prior to or after executing this Agreement, makes a material misrepresentation or omission or provides materially inaccurate information to the City;

    d. The Consultant undergoes a change of control which, in the reasonable opinion of the City, adversely affects the Consultant's ability to satisfy some or all of its obligation under the within Agreement;

    e. The Consultant subcontracts for the provision of part or all of the services without first obtaining the written approval of the City.

The above rights of termination are in addition to all other rights of termination available at law, or events of termination by operation of law.

Performance

5. Both parties agree to do everything necessary to ensure that the terms of this Agreement take effect.

Non-Performance

6. The failure on the part of either party to exercise or enforce any right conferred upon it under this Agreement shall not be deemed to be a waiver of any such right or operate to bar the exercise or enforcement thereof at any time or times thereafter.

Indemnification

7. The Consultant hereby agrees to indemnify and hold harmless the Indemnified Parties from and against any and all liability, loss, costs, damages and expenses (including legal, expert and consultant fees), causes of action, actions, claims, demands, lawsuits or other proceedings, (collectively "Claims"), by whomever made, sustained, brought or prosecuted, for third party bodily injury (including death), personal injury and damage to real or tangible personal property, in any way based upon, occasioned by or attributable to anything done or omitted to be done by the Consultant, its subcontractors or their respective directors, officers, agents, employees or independent contractors in the course of performance of the Consultant's obligations under, or otherwise in connection with, this Agreement. The obligations contained in this paragraph shall survive the termination or expiry of this Agreement.

Remedies

8. Upon default by either party under any terms of this Agreement, and at any time after the default, either party shall have all rights and remedies provided by law and by this Agreement.

9. No delay or omission by either party in exercising any right or remedy shall operate as a waiver of them or of any other right or remedy, and no single or partial exercise of a right or remedy shall preclude any other or further exercise of them or the exercise of any other right or remedy. Furthermore, either party may remedy any default by the other party in any reasonable manner without waiving the default remedied and without waiving any other prior or subsequent default by the defaulting party. All rights and remedies of each party granted or recognized in this Agreement are cumulative and may be exercised at any time and from time to time independently or in combination.

Mediation

10. All disputes arising out or in connection with this Agreement, or in respect of any legal relationship associated with or derived from this Agreement, shall be mediated pursuant to the National Mediation Rules of the ADR Institute of Canada, Inc. Despite this Agreement to mediate, a party may apply to a court of competent jurisdiction or other competent authority for interim measures of protection at any time. The place of mediation shall be the City of Saint John and Province of New Brunswick.

Force Majeure

11. It is agreed between the parties that neither party shall be held responsible for damages caused by delay or failure to perform his undertakings under the terms of the Agreement when the delay or failure is due to fires, strikes, floods, acts of God, lawful acts of public authorities, or delays or defaults caused by common carriers, which cannot be reasonably foreseen or provided against.

No Assignment

12. This Agreement is not assignable. Any attempt to assign any of the rights, duties or obligations of this Agreement is void.

Time

13. This Agreement shall not be enforced, or bind any of the parties, until executed by all the parties named in it.

Notices

14. Any notice under this Agreement shall be sufficiently given by personal delivery or by registered letter, postage prepaid, mailed in a Canadian post office and prepaid courier, addressed, in the case of notice to the City of Saint John, to the Common Clerk, 15 Market Square, P. O. Box 1971, Saint John, New Brunswick, E2L 4L1 and in the case of notice to the Consultant to [Address], or to any other address as may be designated in writing by the parties, and the date of receipt of any notice by mailing shall be deemed conclusively to be 5 days after the mailing.

Amendments

15. No change or modification of this Agreement shall be valid unless it is in writing and signed by each party.

Acknowledgment of Terms and of Entirety

16. It is agreed that this written instrument embodies the entire agreement of the parties with regard to the matters dealt within it, and that no understandings or agreements, verbal or otherwise, exist between the parties except as expressly set out in this instrument.

Further Documents

17. The parties agree that each of them shall, upon reasonable request of the other, do or cause to be done all further lawful acts, deeds and assurances whatever for the better performance of the terms and conditions of this Agreement.

Validity and Interpretation

18. Descriptive headings are inserted solely for convenience of reference, do not form part of this Agreement, and are not to be used as an aid in the interpretation of this Agreement.

19. It is intended that all provisions of this Agreement shall be fully binding and effective between the parties, but in the event that any particular provision or provisions or part of one is found to be void, voidable or unenforceable for any reason whatsoever, then the particular provision or provisions or part of the provision shall be deemed severed from the remainder of this Agreement and all other provisions shall remain in full force.

Governing Law

20. This Agreement shall be governed by and construed in accordance with the laws of the Province of New Brunswick.

Successors, Assigns

21. This Agreement shall enure to the benefit of and be binding on the respective successors and permitted assigns of each of the parties.

Independent Legal Advice

22. The parties each acknowledge having obtained their own independent legal advice with respect to the terms of this Agreement prior to its execution.

Acknowledgment of Receipt of Copy

23. Each party acknowledges receipt of a true copy of this Agreement.

Defined Terms

24. When used in this Agreement, the following word or expression has the following meaning:

"**Indemnified Parties**" means the City, its officers, directors, employees, agents or independent contractors.

IN WITNESS WHEREOF the parties have affixed their respective corporate seals, attested by the hands of their respective officers duly authorized in that behalf on the day aforementioned.

SIGNED, SEALED & DELIVERED	)	**THE CITY OF SAINT JOHN**
In the presence of:	)	per
	)	
	)	_____
	)	Mayor
	)	
	)	_____
	)	Assistant Common Clerk
	)	
	)	Common Council Resolution:
	)	
	)	_____
	)	
	)	**[Organization]**
	)	Per:
	)	
	)	_____
	)	[Title]