www.pwc.com/ca

Statement of Work

Access and Privacy of Information Internal Audit Project

Submitted on July 31, 2018
for SPC on Finance on August 7, 2018

July 31, 2018

City of Saskatoon SPC on Finance
222 Third Avenue North
Saskatoon, Saskatchewan S7K 0J5

Statement of Work – Internal Audit Plan – Access and Privacy of Information Internal Audit Project

Recommendation:

- **That the enclosed Statement of Work for the Access and Privacy of Information Internal Audit Project be approved and that SPC on Finance allocate $38,160 and 240 hours for this project as outlined in the approved 2018 Internal Audit Plan.**

Please find enclosed the Statement of Work for the above referenced project. Note that the total proposed scope of the project is 240 hours. Detailed planning and preparation for the project have been ongoing since April 2018 and detailed fieldwork efforts on the project will continue upon approval of the Statement of Work by SPC on Finance.

Yours truly,

PricewaterhouseCoopers LLP

Jesse Radu, CPA, CA
Partner

1. Background

The Saskatchewan Information and Privacy Commissioner is an independent office of the Saskatchewan Legislative Assembly. It oversees three Saskatchewan statutes, which establish the access to information and privacy rights of citizens: *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and *The Health Information Protection Act* (HIPA).

The City of Saskatoon is a local authority under the LA FOIP and, as such, is responsible for following the requirements of the Act relating to access to information in the custody or control of the City and the protection of individual privacy.

The Access and Privacy Officer role was established within the Records, Information and Legislative Services function of the City Clerk's Office in 2017. This role is responsible for handling the Access and Privacy Management Program for the City. Prior to this time, work in the Access and Privacy area was handled by the Deputy City Clerk/Manager, Records, Information and Legislative Services Manager who reports to the City Clerk, the designated "head" under LA FOIP. No further staffing exists, other than minimal administrative support, for the Access and Privacy Management Program.

The City's Access and Privacy Management Program (the "Program") is in the early stages of maturity with a newly developed framework, supported by the design of policy and procedure in certain key areas, such as Privacy and Confidentiality, and Video Surveillance, as well as Privacy Breach Protocols. The Program also includes a Privacy Impact Assessment process to mitigate privacy risks in the design of City programs. An ongoing Program priority is the development of additional policies and tools, as well as education and training, to improve awareness and accountability for addressing the City's responsibility in access to information and protection of privacy.

2. Scope of Work and Approach

The City's Strategic Risk Register includes Risk A&FS-9, which states "*The City may not be adequately protecting information created by or entrusted to it".* City Council has identified this risk as a "medium" priority.

The scope of this internal audit project will provide for an identification of root causes that may affect the risk mitigation activities performed under the Program. Risk A&FS-9 outlines examples of potential root causes such as: lack of understanding of what information is confidential/personal, absence of policies that govern collection, use, creation and storage of information, inadequate information security measures, intentional/ unintentional breach of information security measures or release of information.

The scope of this internal audit project will also include improvement opportunities to align the information management lifecycle with applicable privacy regulatory requirements and good practices for in-scope assessment areas. An implementation plan will be provided for Administration's consideration.

In-scope assessment areas include:

- Policy and Program Framework - including Access, Privacy Impact Assessment (PIA) and Privacy by Design (PbD)
- Breach management
- Training and Awareness
- Third-party management

Out-of-scope areas include:

- Records management
- Cybersecurity assessment
- Access to information requests
- Assessment against operational effectiveness of controls in place

We acknowledge the City is currently implementing a new ERP system to decrease risk of manual activity errors and control risks, and increase data driven reporting capabilities and automated process efficiencies. We will work with stakeholders to ensure alignment of identified improvement opportunities with Program business requirements already defined as part of the ERP project.

Our approach to assess the current state of the Program, and to provide the City with recommendations for improvement, is outlined in detail in the section that follows.

Access and Privacy of Information Program: Current State Risk Assessment and Implementation Plan

Objectives - Gain an understanding of the City's current approach to protecting information created by or entrusted to it against applicable privacy legislation (e.g. LA FOIP). Identify opportunities for improvement and develop a plan to help the City implement the identified recommendations for overall program improvement.

Approach -

1. **Current State Risk Assessment**

   Key Activities:

   - Gather and review relevant Program documentation related to in-scope areas identified above (e.g., Program organizational structure, policies, procedures)
   - Identify relevant stakeholders and conduct interviews to assess design and awareness of controls related to the information management lifecycle of personal information stored in hard-copy and electronic format (e.g., Privacy, Third-Party Management, Information Security stakeholders)
   - Identify applicable privacy legal, regulatory and policy requirements (e.g., Canadian Standards Association Code's ten privacy principles)
   - Perform a risk assessment by analysing the current state of the in-scope areas against applicable privacy legal, regulatory and policy requirements, as well as good practice in control design

2. **Implementation Plan**

   Key Activities:

   - Prioritize identified privacy risks according to an agreed upon risk ranking scheme
   - Develop recommendations for improvement
   - Develop a remediation roadmap to mitigate identified privacy risks, including considerations related to the organizational structure of the Access and Privacy function

Deliverables – A written findings report including control design and awareness observations and gaps against applicable regulatory requirements. A written recommendations report including observations and gaps against good practice, as well as improvement opportunities to create awareness throughout the organization and mature the function to a desired future state that is both realistic and achievable.

3. Stakeholders

The key stakeholders of the internal audit project from the City are the City Clerk's Office, Information Technology Division, and the Director of Corporate Risk. As this project affects the organization as a whole, the Administrative Leadership Team is also a key stakeholder.

4. Budget

Our fees are based on actual hours incurred at the agreed upon hourly billing rates. We estimate our fees for the completion of our services under this Statement of Work will be $38,160, plus out of pocket expenses and applicable taxes, which will be charged on an actual basis. We estimate out of pocket expenses to be $4,000.