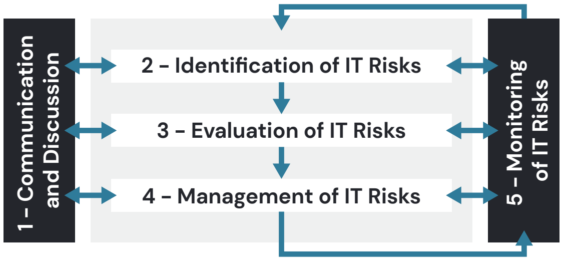
Information Technology Risk Management

Background

Information technology (IT) risk management is an ongoing process that generally involves the business units (the owners of most of the information assets) and the Service des technologies de l'information (STI).

The following diagram illustrates the life cycle of IT risk management:


1 – Communication and Discussion
2 – Identification of IT Risks
3 – Evaluation of IT Risks
4 – Management of IT Risks
5 – Monitoring of IT Risks

An IT risk is an event involving IT that could have a negative impact on the Ville de Montréal (the City), such as the loss or theft of confidential data, the unavailability of important applications, non-compliance with laws and regulations or financial losses following a cyberattack (e.g., ransomware).

Purpose of the Audit

To evaluate the processes, tools and controls put in place by the STI to effectively manage the City's IT risks and thus adequately protect itself against various events that could negatively affect the City's operations and critical services.

Results

The STI set up a team to support the City in its management of technological risks. This team made significant progress in this area. However, we concluded that the City does not effectively manage IT risks.

Indeed, the governance surrounding IT risk management is not sufficiently supported by comprehensive, updated and approved documentation that is distributed to the stakeholders and implemented by them.

The STI does not have the necessary human or technological resources to adequately respond to its IT risk management service offer.

Although the mechanism used to detect technological risks is documented in the *Processus de gestion des risques TI*, it has not been implemented.

This situation increases the likelihood that the quality of IT risk management will be very uneven across business units and stakeholders, and that major IT risks will not be adequately identified, managed or tracked.

Main Findings

IT Risk Governance and Management

- The STI has developed frameworks, including a *Modèle de gouvernance en sécurité de l'information*, a policy, a directive and various processes in relation to IT risk management. Nevertheless, some of these documents are not up to date, while others are being developed or have not yet been approved or distributed.
- IT risk monitoring and accountability reporting as well as the production of IT risk indicators and dashboards provided for in the *Processus de gestion des risques TI* have not been implemented.
- The STI's current quality review process is not documented or systematically carried out by the stakeholders.

Adequacy of Resources

- The STI does not have the necessary human or technological resources to adequately respond to its IT risk management service offer.

Detection of Major Technological Risks

- The mechanism used to detect technological risks is documented in the *Processus de gestion des risques TI*. However, as this process has not been finalized, approved or distributed to the stakeholders, it has yet to be implemented.

Analysis of IT Risks

- The STI has developed a process, tools and templates to facilitate the analysis of IT risks. However, they have not been adequately completed and the overall quality of the information collected varies from one analysis to the next.

Evaluation of IT Risk Management Performance

- Risk management performance is not formally evaluated on a regular basis or reported to the Direction générale of the City. This requirement is nevertheless stipulated in the *Politique de sécurité de l'information*.

In addition to these results, we have made various recommendations to the business units, which are presented in the following pages. These business units were given the opportunity to agree to the recommendations.