3.6.

Information Technology Risk Management

February 9, 2021

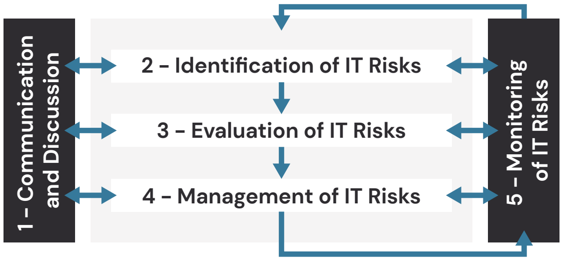
2020 ANNUAL REPORT
Auditor General of the Ville de Montréal

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.

List of Acronyms

GGRTI	Gouvernance et gestion des risques TI
IT	Information technology
STI	Service des technologies de l'information

Table of Contents

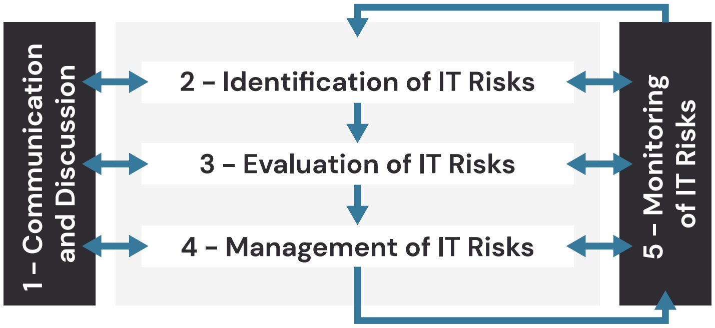
1. Background

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).

It is important for the Ville de Montréal (the City) to effectively manage its IT risks, considering that:

- the City has close to 300 IT applications[1] that operate in a variety of constantly evolving technological environments;
- the development, maintenance and operation of these systems require the contribution of more than 600 employees[2] of the STI;
- the City's IT operating budget will total over $100 million[3] in 2021;
- all users, both employees and citizens, expect these systems to be efficient, secure and available.

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 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).

[1] According to a list of information assets obtained from the Service des technologies de l'information on October 22, 2020.

[2] Source: 2019–2021 Three-Year Capital Expenditure Program.

[3] Budget of the Ville de Montréal – 2021.

In order to protect itself against the advent of such negative effects, the City must regularly and systematically conduct IT risk analysis, especially during events that could potentially trigger such IT risks. For example:

- significant changes made to a critical application;
- the launch of an IT project involving confidential data;
- the addition or significant modification of technological equipment;
- the addition of a major IT supplier;
- a major IT incident that occurred in the City, or in another organization but that could occur in the City;
- the discovery of a significant vulnerability linked to one of the City's critical systems.

Following the analysis of these IT risks, an action plan must be developed and implemented by the business units responsible in order to mitigate the most significant risks. Finally, the progress of these action plans should be regularly monitored and formally reported to the stakeholders.

The following are the main types of IT risks that can be assessed in these analysis:

- the disclosure of confidential information;
- the unavailability of technological material or IT applications;
- non-compliance with the City's laws and regulations;
- the inability to pursue business operations;
- a natural disaster;
- the unavailability or default of a supplier;
- the manipulation of data;
- a loss of performance.

Reporting to the STI, the Gouvernance et gestion des risques TI (GGRTI) Division is made up of five security advisers, and its mission includes notably supporting the City's stakeholders in their IT risk management.

The services offered by the GGRTI Division include the production of the following security deliverables: a security advisory, analysis of security requirements, impact analysis, IT risk analysis and the coordination of computer intrusion (hacking) tests. This includes monitoring the most significant IT risks as well as regular reporting on these IT risks.

2. Purpose and Scope of the Audit

Under the provisions of the *Cities and Towns Act* (CTA), we completed an audit mission on IT risk management. We performed this mission in accordance with the *Canadian Standard on Assurance Engagements* (CSAE) 3001 described in the *CPA Canada Handbook – Assurance*.

The purpose of this audit was 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.

The role of the Auditor General of the Ville de Montréal is to provide a conclusion regarding the objectives of the audit. To do so, we collected a sufficient amount of relevant evidence on which to base our conclusion and to obtain a reasonable level of assurance. Our assessment is based on criteria we have deemed valid for the purpose of this audit. They are presented in Appendix 5.1.

The Auditor General of the Ville de Montréal applies *Canadian Standard on Quality Control* (CSQC) 1 from the *CPA Canada Handbook – Certification* and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. In addition, it complies with the independence and other ethical requirements of the *Code of ethics of chartered professional accountants*, which are founded on fundamental principles of integrity, professional competence and due diligence, confidentiality and professional conduct.

Our audit focused on the period from July to December 2020. Our work consisted of conducting interviews with employees, reviewing various documents and conducting surveys that we deemed appropriate to gather relevant supporting information. We also took into account information that was sent to us up to February 2021.

Upon completing our audit, we submitted a draft audit report to the managers of each audited business unit as well as to each of the business units concerned to obtain action plans and timelines for implementing them.

3. Audit Results

3.1. Information Technology Risk Governance and Management

3.1.1. Strategy, Policy and Management Framework

The stakeholders involved in sound IT risk management must have at their disposal the necessary strategic frameworks to understand the City's IT risk management orientations and thus exercise the roles and responsibilities expected of them.

No single document exists that directly presents the City's IT risk management strategy. Indeed, we noted that this strategy is partially presented in the following four documents:

- the *Modèle de gouvernance en sécurité de l'information*;
- the *Politique de sécurité de l'information*;
- the *Directive sur la gestion des risques TI*;
- the *Processus de gestion des risques TI*.

Modèle de gouvernance en sécurité de l'information

This document sets out the responsibilities assigned to the business units (1st line of defence), the chief information security officer and the STI (2nd line of defence) and the comptroller general (3rd line of defence) with respect to information security and IT risk management.

Considering that this model assigns important responsibilities to several of the City's business units, it is important that it be formally communicated by the Direction générale to all stakeholders so that they adhere to it and prioritize the implementation of this model.

We found that such communication has not been formally carried out. This leads to the risk of low stakeholder buy-in and incomplete assumption of responsibility for the activities required to adequately manage IT risks within the City.

Politique de sécurité de l'information

This policy (IT security policy) sets out a number of frameworks for IT risk management at the City, including the following:

- the person responsible for an information asset must manage the risks of that asset;
- the *Comité de sécurité de l'information* must regularly assess risk management performance and report on it to the Direction générale.

However, this policy was last updated in 2006. It is imperative that the content of this policy be quickly reviewed to ensure that it responds to current reality, particularly with respect to aspects involving IT risk management.

Directive sur la gestion des risques des technologies de l'information

This directive (IT risk management) was presented to the *Comité de sécurité de l'information* in January 2020. Its main objective is to dictate a common vision and direction for IT risk management within the City. It is our opinion that it adequately covers the main elements expected in this field.

Indeed, it presents the following guiding principles:

- Associating IT risk management with the achievement of the City's strategic or business objectives;
- Aligning IT risk management with the City's integrated risk management;
- Balancing the costs and benefits of IT risk management;
- Promoting adequate communication on IT risks;
- Establishing an organizational framework oriented towards effective IT risk management;
- Integrating the *Processus de gestion des risques TI* into the City's daily operations.

However, this directive has not been approved by the Direction générale, nor has it been distributed to stakeholders or implemented. As a result, this leads to the risk of a non-uniform approach to IT risk management.

Processus de gestion des risques des technologies de l'information

The documentation surrounding the *Processus de gestion des risques TI* has not been finalized. As such, it has not been approved or distributed to the stakeholders.

This situation leads to the risk of a non-uniform approach to IT risk management, as well as a failure to respect the stakeholders' roles and responsibilities when carrying out activities related to IT risk management.

Alignment with Integrated Risk Management

IT risk management is a subset of the City's integrated risk management. Sound practices call for IT risk management to be linked to the frameworks developed and distributed by the sector responsible for integrated risk management in order to ensure consistent and efficient actions.

Since the City's project to implement integrated risk management is currently under way, it is possible that guiding principles for IT risk management (e.g., risk appetite and tolerance, impact and probability thresholds, risk level metrics) may differ from those later defined by integrated risk management.

In the event of such discrepancies, it will not be possible to adequately compare IT risk assessments with the City's other risks (i.e., a high-level IT risk may be presented as less significant than an "average" level integrated risk). As a result, the City would not be able to adequately prioritize its IT risk management actions.

3.1.1.A. Recommendation

We recommend that the Direction générale:

- ensure consistency and alignment of integrated risk management with information technology risk management, particularly with respect to risk appetite and tolerance, impact and probability thresholds and risk-level metrics;
- approve the *Directive sur la gestion des risques des technologies de l'information*;
- ensure that the directive is distributed to the business units and implemented by them;
- formally communicate its approval of and commitment to the information security governance model to the business units so that they subscribe to it and prioritize its implementation.

3.1.1.B. Recommendation

We recommend that the Service des technologies de l'information:

- upgrade and distribute the *Politique de sécurité de l'information*;
- finalize the documentation surrounding the *Processus de gestion des risques des technologies de l'information* and ensure it is distributed and that the business units subscribe to it.

3.1.2. Sharing of Roles and Responsibilities

The sharing of the stakeholders' roles and responsibilities with respect to the City's IT risk management is essentially presented in the following four documents:

- the *Modèle de gouvernance en sécurité de l'information*;
- the *Politique de sécurité de l'information*;
- the *Directive sur la gestion des risques TI*;
- the *Processus de gestion des risques TI*.

Modèle de gouvernance en sécurité de l'information

This governance model was presented to and adopted by the *Comité de sécurité de l'information* and the Direction générale. It sets out the responsibilities of business units, the chief information security officer, the STI and the comptroller general with respect to information security and IT risk management.

Politique de sécurité de l'information

This policy specifies certain responsibilities assigned to the business units as well as to the *Comité de sécurité de l'information* with respect to IT risk management.

Directive sur la gestion des risques des technologies de l'information

This directive assigns responsibilities for IT risk management to a number of stakeholders, including:

- the *Comité de gestion de la Direction générale*;
- the *Comité de sécurité de l'information*;
- the comptroller general;
- the chief information security officer;
- the business units.

Processus de gestion des risques des technologies de l'information

This process assigns certain responsibilities to the comptroller general, the STI and the business units.

We note that not all roles and responsibilities have been formalized. Indeed, although several roles and responsibilities are adequately defined within these four documents, not all of them have been completed, approved or distributed to the stakeholders (see section 3.1.1.).

As a result, some tasks may not be completed and others may have more than one person responsible for them. Such a situation can have a major impact on the governance and quality of IT risk management.

3.1.2.A. Recommendation

We recommend that the Service des technologies de l'information:

- complete the documentation of the roles and responsibilities of the stakeholders involved in the *Processus de gestion des risques des technologies de l'information* following approval of the related directive;
- ensure that these roles and responsibilities are distributed and understood.

3.1.3. Procedures, Guides and Tools

Various IT risk management procedures, guides and tools have been developed by the STI to enable stakeholders to complete quality IT risk analysis. In particular:

- a *Processus de gestion des risques TI*;
- a template to define the parameters of risk analysis (including risk, impact and probability levels, types of risks to be assessed, risk tolerance thresholds);
- templates related to risk analysis requests, acceptances, drafting of risk assessment reports, another template if a risk is waived.

Processus de gestion des risques des technologies de l'information

As mentioned in section 3.1.1. of this report, this process has not been finalized, approved or distributed to the stakeholders.

This process provides that the STI is to regularly monitor IT risks. Based on the IT risk register, the STI must ensure that the City's IT risks are under control and that the actions taken to control them are coordinated and consistent. To this effect, the STI must implement indicators in order to monitor the four states of risk it has defined, namely:

- non-critical;
- under evaluation;
- being processed; or
- accepted by the City as critical.

These indicators must be used to improve – qualitatively or quantitatively – the City's IT risk management system. They must also feed various IT risk dashboards.

The resulting indicators and dashboards should be regularly presented to the stakeholders and at each meeting of the *Comité de sécurité de l'information*.

Following our work, we noted that the production of indicators and dashboards and the monitoring and reporting on IT risks are not formally and regularly carried out.

As a result, there is a possibility that significant IT risks may not receive the required attention from the stakeholders and that the City may be exposed, without its knowledge, to significant events such as critical system failures or cyberattacks that threaten the integrity and confidentiality of data held by the City.

Use of Templates in Risk Analysis

The STI has developed templates to facilitate the IT risk analysis.

We noted that these templates are relatively complete. However, they have not been finalized and therefore have not been formally approved or distributed to the stakeholders. As a result, the quality of IT risk analysis may be uneven and the results may fail to reveal certain significant IT risks.

In order to evaluate the extent to which these templates are adequately used by the stakeholders during IT risk analysis, we selected a sample of six IT projects out of the 50 that had been overseen by a security adviser from the GGRTI Division. We then analyzed the documents produced as a result of this oversight and met with the security advisers who coordinated these activities and participated in the production of the required deliverables.

Overall, we noted the following for our sample of six projects:

- three projects included IT risk analysis;
- one project had minor impacts and therefore did not require an IT risk analysis;
- two projects were the subject of impact analysis, but the risk analysis had not yet been carried out.

The three IT risk analysis evaluated were carried out using the template provided for this purpose, and the result was approved by the stakeholders. However, we noted that these analysis were often incomplete (i.e., no details of the controls in place, no risk treatment, no action plan or timeline to complete an action plan).

In addition, certain other templates are rarely used (e.g., the risk analysis request template, the risk acceptance template).

As a result, the fact that IT risk analysis are not fully documented and that certain templates are not used leads to the risk that the quality of IT risk analysis will vary from one analysis to the next. In turn, this could lead to the materialization of significant risks that were incorrectly assessed and not addressed. This calls for the implementation of systematic quality reviews of these IT risk analysis.

Quality Review

We noted that quality reviews are sometimes performed by STI resources following the production of various deliverables related to IT risk management.

However, this activity is not supported by formal documentation, it is not carried out systematically and it does not cover all STI activities and deliverables (i.e., the extent to which all expected templates have been adequately completed, approved and distributed).

It is therefore possible that the quality review may not detect non-compliance with certain items expected from the *Processus de gestion des risques TI* (e.g., the use of expected templates, obtaining required approvals, the production of requested deliverables, compliance with different stages in the process). This situation could result in an incomplete IT risk analysis or an analysis that does not meet expectations of stakeholders.

3.1.3.A. Recommendation

We recommend that the Service des technologies de l'information:

- implement recurring monitoring of information technology risks and report them to the stakeholders;
- define and implement information technology risk indicators and dashboards and present them regularly to the stakeholders;
- approve and distribute the information technology risk analysis templates developed;
- document and implement a systematic quality review process for information technology risk analysis that covers all deliverables and expected activities.

3.2. Adequacy of Resources

While responsibility for managing IT risks rests with the City's business units, the STI is responsible for a number of activities related to IT risk management, including:

- developing and distributing IT risk management frameworks;
- supporting business units in managing their IT risks;
- producing various deliverables for business units related to IT risk management (e.g., the security advisory, the analysis of security requirements, impact analysis, IT risk analysis, vulnerability assessments, security tests);
- maintaining and updating the IT risk register;
- monitoring significant IT risks and reporting on them to the stakeholders.

In this respect, we note that the five security advisers assigned to these activities only allow the STI to carry out part of these activities. Indeed, as noted during our audit, here are the important points:

- frameworks are neither completed, approved nor distributed to the stakeholders;
- only a portion of IT projects are subject to IT risk analysis;
- few IT risk analysis are carried out in a context other than that of an IT project;
- the IT risk register is updated sporadically rather than systematically;
- there is no systematic monitoring and reporting of IT risks.

In addition, other IT risk management activities included in the STI's service offering are currently not carried out, such as the systematic development and distribution of performance and IT risk indicators, the development of an IT risk awareness program, and third-party IT risk management.

Thus, we note that the STI does not have sufficient human resources to adequately carry out all of these important activities. Such a situation increases the likelihood that significant risks will not be managed adequately, possibly resulting in a loss of availability of critical systems, theft of confidential data or the occurrence of major cyberattacks.

Furthermore, the main tools used by the STI to support business units in managing their IT risks are limited to office software and a dashboard generator. Such tools do not foster optimal integrated IT risk management and require IT risks to be manually collected, updated, monitored and reported.

Yet there are integrated technological tools on the market that facilitate:

- the compilation of IT risk management activities;
- the systematic monitoring of these IT risks;
- effective reporting of IT risks to the stakeholders.

As a result, several manual entries have to be made, which increases the risk of errors, omissions and efficiency losses.

3.2.A. Recommendation

We recommend that the Direction générale ensure that the Service des technologies de l'information obtain the human and technological resources required to adequately respond to its current offer of information technology risk management services.

3.3. Detection of Major Technological Risks

In order for the City to be adequately protected against the advent of significant events, such as the failure of an obsolete system leading to the unavailability of critical applications or the loss of data following a cyberattack, the City must implement an effective mechanism to allow for the timely detection of significant IT risks.

This IT risk detection mechanism is presented in the document titled "*Processus de gestion des risques TI*." It consists of assigning to the business units, IT project teams and the IT operations team responsibility for determining, in light of the City's priorities, the operations that require an IT risk analysis.

When one of these stakeholders decides that it is relevant to conduct an IT risk analysis, it will contact the STI's GGRTI Division for support.

In addition, in order to guide these stakeholders, the process presents 12 events that can lead to the completion of IT risk analysis, namely:

- the integration of a new IT product or service;
- the development of an IT system;
- the evolving needs of citizens;
- new business requirements;
- changes in the operational environment;
- work restructuring;
- changing strategic and/or organizational orientations;

- the detection of emerging threats;
- the identification of new vulnerabilities;
- the development and/or maintenance of the IT infrastructure;
- the use of a new IT tool/functionality;
- an update to a patch.

For this approach to identifying IT risks to work effectively, we believe that these stakeholders must:

- have received the required documentation related to this process;
- be fully aware of their roles and responsibilities with respect to IT risk management;
- have demonstrated their formal acceptance of these responsibilities;
- have been trained to effectively identify their IT risks and adequately apply the *Processus de gestion des risques TI*;
- communicate regularly with a dedicated STI IT risk management resource to inform them of any developments regarding IT risks (i.e., new risks, the development of action plans to mitigate significant risks, a change in the importance of a risk).

We noted that these five prerequisites are not in place. Indeed, as mentioned in section 3.1.1, the documentation surrounding the *Processus de gestion des risques TI* has not been finalized. As such, it has not been approved, distributed or applied by the stakeholders concerned. As a result, activities related to awareness-raising, buy-in, training and regular communication with stakeholders have also not been completed.

Consequently, in the absence of an effective detection process, significant IT risks would not receive the required attention, which could lead to critical situations such as the unavailability of systems, cyberattacks possibly resulting in the theft of confidential data, or the loss of integrity of important data.

3.3.A. Recommendation

Subject to recommendation 3.1.1.A. for the part concerning the *Processus de gestion des risques des technologies de l'information*, we recommend that the Service des technologies de l'information:

- set up a training and awareness-raising program for the stakeholders concerned, particularly with regard to identifying information technology risks;
- provide for an effective mechanism to ensure that regular communication is maintained between the Service des technologies de l'information and the stakeholders concerned in order to monitor how their information technology risks are evolving.

3.4. Analysis of Technological Risks

The mechanism used to analyze technological risks is documented in the *Processus de gestion des risques TI*. The STI has developed various templates to facilitate the analysis of IT risks by the stakeholders.

However, as indicated in section 3.1.1, the Processus de gestion des risques TI has not been finalized, approved or distributed. This leads to the risk of a non-uniform approach to IT risk analysis.

Furthermore, section 3.1.3. mentions that these templates have not been approved or formally distributed. This leads to the risk that the quality of IT risk analysis may vary from one analysis to the next, which could lead to significant risks being incorrectly assessed and not addressed.

In order to validate the quality of the IT risk analysis process, effectiveness testing was carried out on a sample of IT risk analysis (see section 3.1.3.). The results of these tests show that the quality of these analysis is uneven, which calls for the implementation of a regular quality review of all stages of the *Processus de gestion des risques TI*.

No further recommendations are required, as our findings are already addressed in recommendations 3.1.1.A., and 3.1.3.A.

3.5. Performance Evaluation of Information Technology Risk Management

Pursuant to the *Politique de sécurité de l'information*, IT risk management performance must be regularly evaluated by the *Comité de sécurité de l'information* and the results of this evaluation must be reported to the Direction générale.

Such a performance evaluation ensures that IT risk management meets the City's expectations and evolves regularly to adapt to frequent technological changes.

We noted that the *Comité de sécurité de l'information* does not formally undertake this activity on a regular basis. Consequently, it is not possible to ensure that IT risks are managed in accordance with the City's strategic orientations.

3.5.A. Recommendation

Subject to the implementation of the other recommendations presented in this report, we recommend that the Service des technologies de l'information formally evaluate the performance of information technology risk management on a regular basis and present the results of this evaluation to the Direction générale.

4. Conclusion

The Service des technologies de l'information (STI) set up a team responsible for supporting the Ville de Montréal (the City) in managing its technological risks. This team made significant progress in this area. However, we have reached the conclusion that the City does not effectively manage the information technology (IT) risks to which it is exposed.

Indeed, based on our audit, the governance surrounding IT risk management is not sufficiently supported by comprehensive, up to date and approved documentation that is distributed to the stakeholders and implemented by them. Without such documentation, those stakeholders involved in IT risk management do not have all the information they need to effectively and consistently manage the IT risks in their respective sectors of activity.

Furthermore, the mechanism used to detect IT 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. As a result, it is possible that events involving significant IT risks will not be evaluated and that this may result in service breakdowns, system failures or the loss of confidential data.

In order to be able to offer its IT risk management services, the STI should ensure that it has the necessary human and technological resources. We note that these resources are currently insufficient. As a result, certain activities provided pursuant to its service offering are not carried out or only partially carried out, which exposes the City to additional risks.

This lack of formal supervision and of human and technological resources increases the likelihood that:

- the quality of IT risk management will be very uneven from one business unit to the next and from one stakeholder to the next;
- significant IT risks will not be adequately identified, managed and tracked.

More specifically, here are the details according to the following evaluation criteria:

1. Evaluation Criterion – Information Technology Governance and Risk 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. However, some of these documents must be updated, while others are being developed or have not yet been approved or distributed. As a result, many of the orientations and strategies contained in these frameworks are not currently being implemented by the stakeholders concerned. In addition, the roles and responsibilities of the stakeholders involved in IT risk management are not all adequately documented within the frameworks.

Procedures, guides and tools, including various templates to facilitate IT risk management, have been developed by the STI. These documents are generally complete and up to date. However, they have not all been approved and distributed to the stakeholders. IT risk monitoring and accountability reporting activities 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. Also, the STI's current quality review process has not been documented or systematically implemented by the stakeholders.

2. Evaluation Criterion – Adequacy of Resources

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

3. Evaluation Criterion – Detection of Major Technological Risks

A *Processus de gestion des risques TI* is currently being developed. As such, it has not been approved or distributed to the stakeholders. In particular, the process sets out an approach aimed at detecting and addressing significant technological risks. This process requires the active participation of the City's business units. However, several prerequisites will need to be implemented to ensure that it is operational and effective.

4. Evaluation Criterion – Analysis of Technological Risks

The STI has developed a process as well as 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.

5. Evaluation Criterion – Periodic Performance Evaluation of Information Technology Risk Management and Accountability to the Stakeholders

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

5. Appendix

5.1. Objective and Evaluation Criteria

Objective

To evaluate the processes, tools and controls put in place by the Service des technologies de l'information to effectively manage the information technology (IT) risks to which the Ville de Montréal (the City) is exposed and thus adequately protect itself against various events that could negatively affect the City's operations and critical services.

Evaluation Criteria

We based our audit on the following evaluation criteria divided into five parts:

1. Information Technology Governance and Risk Management

1.1. There exists a strategy, policies and a specific management framework related to the City's IT risk management. These documents are complete, up to date, formally approved and distributed to the stakeholders, who implement them.

1.2. The roles and responsibilities of the stakeholders involved in managing the City's IT risks are documented, complete, up to date, formally distributed to the stakeholders and implemented by them.

1.3. Procedures, guides and tools (including a risk taxonomy and its risk tolerance level) have been developed to facilitate IT risk management. These tools are complete, up to date, formally distributed to the stakeholders and implemented by them.

2. Adequacy of Resources

Sufficient and adequate resources are in place to implement IT risk management that meets sound industry practices.

3. Detection of Major Technological Risks

A process is in place to effectively detect and address major technological risks. This process includes, in particular, systematic monitoring of the following:

- emerging risks;
- security incidents;
- risks related to new IT projects;
- major technological changes.

4. Analysis of Technological Risks

The IT risk analysis process includes:

- data collection;
- formal involvement of the stakeholders;
- the determination and justification of the business impact and probability;
- a description of the controls;
- the determination of the residual risk;
- the evaluation of the residual risk relative to risk tolerance;
- processing the risk (i.e., acceptance, refusal, mitigation, transfer);
- where appropriate, a plan to adequately mitigate this risk;
- a formal presentation of the analysis results to the stakeholders and their approval.

5. Periodic Performance Evaluation of Information Technology Risk Management and Accountability to the Stakeholders

Risk management performance is evaluated on a regular basis or reported to the Direction générale of the City.