Vérificateur général
de la Ville de Montréal

Report of the Auditor General of the Ville de Montréal
to the City Council and to the Urban Agglomeration Council

For the Year Ended December 31, 2015

4.5

Information and Communications Technology Recovery Management

Table of Contents

List of Acronyms

BIA	business impact analysis
DEEU	Direction de l'épuration des eaux usées
DEP	Direction de l'eau potable
HAZOP	hazard and operability study
HP	Hewlett Packard Canada
ICT	information and communications technology
RAO	Répartition assistée par ordinateur
SIM	Service de sécurité incendie de Montréal
SIMON	Système intégré Montréal
SPVM	Service de Police de la Ville de Montréal
STI	Service des technologies de l'information

4.5. Information and Communications Technology Recovery Management

1. Background

Organizations such as the Ville de Montréal (the City) are more vulnerable than ever, because natural, technological and social incidents occurring at the local or regional level now have major impacts on their normal operations. The City provides services to approximately 1.8 million people. Some of these services are provided by essential business units such as:

- **The Service des technologies de l'information (STI)**: It is mandated to maintain and support the modernization of the City's key technological services;

- **The Service de l'eau:**
  - **Direction de l'épuration des eaux usées (DEEU):** It is mandated to manage sewage discharge and treatment at the wastewater treatment plant;
  - **Direction de l'eau potable (DEP):** Its mandate includes the production and distribution of drinking water to the population, organizations and industries of the Montreal agglomeration;

- **The Service de sécurité incendie de Montréal (SIM):** Its mandate is to make the City safer by protecting lives, property and the environment;

- **The Service de Police de la Ville de Montréal (SPVM):** Its mission is to protect the lives and property of citizens, to maintain the peace and ensure public safety, to prevent and fight crime and to enforce existing laws and regulations.

These essential business units have activities considered critical because they depend heavily on information and communications technology (ICT). It is crucially important that the City be prepared for any emergency situation that might cause a shutdown or major disruption of these activities.

ICT recovery management, an essential part of the process of business continuity management[1] that ensures continuity in the City's critical activities in the event of a disaster,

[1] Refer to section 4.9 of the 2014 Annual Report, "Business Continuity Management."

is a process of planning to ensure that ICT system and infrastructure operations essential to the City's critical activities are resumed.

ICT recovery management must be based on a program that includes the following components:

- **ICT disaster recovery program management frameworks and structure:**
  The structure of the ICT disaster recovery program is based on a governance system (e.g., assignment of responsibilities, management and accountability mechanisms) that ensures ICT recovery can be managed effectively. It defines management frameworks necessary for the establishment of effective strategies, an ICT recovery culture and relevant, measurable and achievable objectives;

- **Major incident management structure:**
  Business units responsible for ICT infrastructures and systems must establish a major incident management structure that handles ICT recovery responses from strategic and operational standpoints and ensures coordination and communication among stakeholders and interested parties;

- **Risk and impact analysis and ICT recovery strategies:**
  - Risk analysis establishes the components of ICT systems and infrastructures that are most at risk of causing a major power failure or a technological disaster. It is also used to identify and implement mitigation measures to reduce both the probability of their occurrence and their impacts;
  - A business impact analysis (BIA) is in itself a step in the business continuity management process and is mentioned here only because of its importance as a cornerstone in the ICT recovery process. Business impact analyses assess the impacts of a disaster and determine a department's critical activities and its tolerance to disruptions or data loss. They also identify the ICT systems and resources essential for maintaining these activities;
  - ICT recovery strategies correspond to the measures adopted to meet the ICT needs identified by the business unit as part of its impact analysis. In particular, they help ensure that the maximum acceptable period of disruption is not exceeded and they ensure the availability of ICT systems, resources, data and equipment required to meet these needs in the event of a disaster;

- **ICT recovery plans and procedures:**
  ICT recovery documentation helps the City react appropriately to a crisis by providing all instructions needed to resume the operation of critical ICT systems and infrastructures;

- **ICT recovery training:**
  All stakeholders involved in ICT recovery following a disaster have received appropriate training, in particular by participating in the establishment of recovery processes and by taking part in exercise drills to validate ICT recovery procedures;

- **ICT recovery exercise programs:**
  The only way to adequately validate ICT recovery measures and procedures is to carry out test exercises regularly. These exercises are prepared on the basis of objectives to be achieved and are subject to a post-mortem to objectively assess the achievement of the objectives and the corrective measures taken to address the deficiencies observed;

- **Updating ICT recovery documentation:**
  To ensure effectiveness and continuity, ICT recovery documentation is always updated in accordance with a formal process.

2. Purpose and Scope of the Audit

The purpose of our audit was to determine whether the City takes the necessary steps to address risks that a major disaster might affect its information and telecommunications systems and thereby ensure adequate ICT recovery.

This audit is the logical continuation of our previous business continuity management audit, conducted in 2014.[2]

For the present audit, we relied on the following international standards:
- ISO 27001 – Information security management systems;
- ISO 22301 – Business continuity management systems;
- ISO 31000 – Risk management.

Our audit was conducted with the participation of specialists recognized in the field of ICT recovery management.

As a follow-up to the results of our risk analysis, our audit focused on the following business units, which we considered critical:
- STI;
- Service de l'eau – DEEU;
- Service de l'eau – DEP;

[2] Refer to section 4.9 of the 2014 Annual Report: "Business Continuity Management."

- SIM;
- SPVM.

Our audit evaluated the following sections:

- Section 1 – ICT disaster recovery program management frameworks and structure;
- Section 2 – Major incident management structure;
- Section 3 – Risk and impact analysis and ICT recovery strategies;
- Section 4 – ICT recovery plans and procedures;
- Section 5 – ICT recovery training;
- Section 6 – ICT recovery exercise programs;
- Section 7 – Updating ICT recovery documentation.

Our audit did not cover business continuity management or emergency preparedness, which were the subjects of separate reports, in 2014 and 2007 respectively. Moreover, it should be stressed that a separate audit report on the urban agglomeration's voice radiocommunications system (SÉRAM) will be produced later and will include its own ICT recovery management.

It should be noted that this report is in no way an audit of the 9-1-1 Emergency Centre's compliance with provincial regulations governing 9-1-1 emergency centres.

The period covered by our audit was September 2015 to January 2016, and the results of our audit are based on the state of affairs prevailing on January 31, 2016. Consequently, changes or improvements that may have been made since then are not reflected in this report.

3. Main Findings

The main findings resulting from this audit are as follows:

- **ICT disaster recovery program management frameworks and structure**
  There is no management framework for ICT recovery that sets out relevant, measurable and achievable objectives. Roles and operational responsibilities are not clearly defined. Staff are generally assigned to ICT recovery activities on an ad hoc basis. In most departments, ICT recovery is not part of the culture, with the exceptions of the SIM's computer-assisted dispatch system (Répartition assistée par ordinateur [RAO]), and the SPVM's 9-1-1 Emergency Centre;

- **Major incident management structure**
  Adequate structures are in place for the RAO and the 9-1-1 Emergency Centre. In the cases of the STI and the Service de l'eau, a major incident management structure is in place but does not include certain aspects of ICT recovery;

- **Risk and impact analysis and ICT recovery strategies**
  Since there is no formal process for conducting a risk and impact analysis, it is not possible for business units to identify critical systems and infrastructures properly or to justify acceptable recovery times or levels of data loss. These data are essential for developing and implementing effective ICT recovery strategies that meet their needs;

- **ICT recovery plans and procedures**
  For the RAO and the 9-1-1 Emergency Centre, adequate plans and procedures are in place. For the Service de l'eau (DEEU), plans and procedures are being developed. Existing ICT recovery plans and procedures at other business units are inadequate;

- **ICT recovery training**
  For the RAO and the 9-1-1 Emergency Centre, the service providers that manage these systems are responsible for training. For the other systems managed by the City, those responsible for implementing ICT recovery plans are not well informed or not properly trained on their roles and responsibilities or existing measures;

- **ICT recovery exercise programs**
  There is no ICT recovery exercise program that can be used to validate recovery strategies, plans and procedures. The 9-1-1 Emergency Centre carries out adequate recurring exercises. Exercises are also carried out for the RAO, but one important scenario was omitted;

- **Updating ICT recovery documentation**
  There is no formal process for updating ICT recovery documentation. However, coordination committees exist to ensure documentation is up to date for the RAO and the 9-1-1 Emergency Centre.

4. Audit Results

4.1. Information and Communications Technology Disaster Recovery Program Management Frameworks and Structure

An information and communications technology (ICT) disaster recovery program is effective if it has the minimum required components for establishing adequate strategies, a culture of ICT recovery and relevant, measurable and achievable objectives.

These minimum components are as follows:

- Management frameworks and organizational structure of the program;
- Resource allocation and operating budgets;
- A common approach and program tools and coordination.

Management Frameworks and Organizational Structure

Management frameworks are documents that determine the scope, requirements, roles and responsibilities of business units under an ICT disaster recovery program. These documents generally take the form of administrative policies and directives. Rather than establishing the composition or implementation of the program, they set the objectives that must be achieved.

The organizational structure of the program, made up of committees and stakeholders, is responsible for supervising, coordinating and implementing initiatives in a structured, aligned and effective way. This structure also ensures that the measures adopted meet ICT recovery objectives.

Resource Allocation and Operating Budgets

Setting up an ICT disaster recovery program cannot be a one-time exercise; it cannot be done on a project-by-project basis that is not be integrated into ongoing operations. It must be based on a recurring allocation of financial, material and human resources.

A Common Approach, Tools, and Municipal Coordination of the Program

To ensure the development and implementation of a coherent, effective ICT disaster recovery program, the City must have a step-by-step procedure (or approach) in place to properly frame the efforts of each business unit and ensure that ICT recovery objectives are achieved. To facilitate development and implementation, tools will also be needed, such as:

- training on the desired approach;
- manuals or templates for each development phase;
- models or procedures to follow for performing exercises;
- tools for sharing and exchanging ideas (e.g., collaboration websites).

4.1.A. Findings – Service des technologies de l'information

During our audit, we noted the following:

- No formal management framework for ICT recovery has been developed by the Service des technologies de l'information (STI) and no procedure for using standardized tools is in place;
- There is no accountability reporting by the STI on ICT recovery to the Direction générale;
- The STI did not have an organizational structure, budget or resources allocated specifically to ICT recovery.

We consider the risk level to be **high** (see Table 1), because the STI faces the following potential risks:

- Without a management framework for ICT recovery, there is no centralized coordination, common approach, monitoring of activities or definition of recovery objectives. Business units do not have access to internal expertise;
- With no accountability reporting to the Direction générale, the City would not be able to determine its actual disaster preparedness;
- Without an organizational structure for ICT recovery or recurring financial and human resources, any process would lack cohesiveness and relevance to business units' ongoing operations. The ICT recovery objectives would probably not be achieved, putting their critical operations at risk in the event of a disaster;
- In the event of a technological disaster, there is no guarantee that the City's critical activities, which depend heavily on ICT systems and infrastructures, would be maintained.

Table 1 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	PROBABLE	Possible	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	Critical	**HIGH**	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of the impact levels and probability of occurrence levels is given in the appendix.

4.1.B. Recommendation

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

- **Develop corporate frameworks for information and communications technology recovery along the same lines as those for the City's business continuity, and ensure that, at the very least, they provide for:**
  - **a definition of the objectives;**
  - **a detailed risk and impact analysis of disruptions;**
  - **recovery strategies for reducing these impacts;**
  - **recovery plans that describe in detail the activities that will ensure critical operations of information and communications technology systems and infrastructures are resumed within the required timeframes;**
  - **a regular review and exercise drill schedule;**
- **Develop a management structure to implement the information and communications technology recovery program, including:**
  - **assigning responsibility for information and communications technology recovery;**
  - **establishing specific objectives for each of its management teams and business units whose information technologies are managed by the Service des technologies de l'information;**
  - **establishing a coordinated process ensuring strategic directions for and communication, monitoring and accountability of the achievement of objectives;**
  - **documenting the roles and responsibilities of all program stakeholders;**
  - **appointing an information and communications technology recovery coordinator and implementing a process for coordinating the efforts of the various information and communications technology recovery stakeholders (business units, service providers);**
- **provide specific recurring budgets for information and communications technology recovery;**
- **make municipal tools (cook books) available to business units, such as:**
  - **the operational structure of the information and communications technology recovery program;**
  - **training sessions on the desired process;**
  - **manuals or templates for each development phase;**
  - **tools for sharing and exchanging ideas (such as collaboration websites).**

Business unit's response:

[TRANSLATION] Corporate frameworks for information technology recovery will be created to provide guidelines, models and tools for defining all the elements needed to ensure IT recovery for each business activity.

The STI will assist departments in establishing their specific objectives, particularly in terms of maximum acceptable data loss (MADL) and the maximum acceptable period of disruption (MAPD).

These frameworks will fall within the scope of an information technology services continuity program that is still in the development phase. ***(Planned completion: April 2017)***

A person has been designated to handle ICT recovery issues and an information technology services continuity program is currently being developed.

This program, which will be aligned with business relations management, will help ensure that the recommendations of this report are implemented along the lines of the City's needs. It will cover accountability, training and documentation related to recovery plans.

The program management information will specify the objectives, management and organizational structure, relations with the proposed logistical support mission, communications strategies, roles and responsibilities.

The appointment of an ICT recovery coordinator will be based on an analysis of the roles and responsibilities needed to ensure continuity of activities.

The critical activities of the four following departments will be covered first: the Service de l'eau, the Service de Police de la Ville de Montréal (SPVM), the Service des incendies and the STI. The other departments' needs will be addressed in the second phase of the information technology services continuity program. ***(Planned completion: April 2017)***

An initiative will be started to document the budget and resources needed for the information technology services continuity program. Recurring costs will be specified when the tests and simulations required by the recovery plan are defined. ***(Planned completion: December 2016)***

Deployment of a collaborative information-sharing tool that includes manuals, templates and all information that the City uses to ensure ICT continuity and recovery. ***(Planned completion: March 2017)***

4.1.C. Findings – Service de l'eau

During our audit, we noted the following:

- At the Direction de l'eau potable (DEP), plant process control system ICTs are managed by its own staff. However, at the Direction de l'épuration des eaux usées (DEEU), staff supplied by the STI's Solutions gestion de l'eau division manage ICT;
- All of the so-called "administrative" ICT systems used by the Service de l'eau and the telecommunications links outside the plants are managed by the STI;

- The DEP and the DEEU did not have a management framework, organizational structure or budgets for ICT recovery;
- Responsibility for ICT recovery is not assigned to a member of the Service de l'eau management team and is not monitored systematically. Unofficial responsibility is given to the automation engineer with the most experience and knowledge of a system. The Service de l'eau is accountable for its own general disaster preparedness, and no specific accountability process exists for ICT recovery;
- ICT recovery is geared to the robustness of processes' automated control systems;
- The DEP and the DEEU each carried out an analysis to produce business continuity plans and ICT recovery plans for their in-plant activities. While there is no question that this work is useful, these two management teams used different methodologies that led to different results.

We consider the risk level to be **moderate** (see Table 2), because the Service de l'eau (DEP and DEEU) faces the following potential risks:

- Without a management framework and an organizational structure for ICT recovery or recurring financial and human resources, any process would lack cohesiveness and relevance to the ongoing operations of the Service de l'eau. The ICT recovery objectives would probably not be achieved, putting the DEEU's and the DEP's operations at risk in the event of a disaster;
- With no formal responsibility or centralized coordination within the Service de l'eau, a common approach cannot be shared, there is no monitoring of activities and the department's actual disaster preparedness is not known;
- Service recovery initiatives are not subjected to a systematic, standardized approach. This might result in inadequate procedures that fail to meet ICT recovery objectives. The efforts would be incomplete, inconsistent, uneven, erratic in their effectiveness and inconsistently applied;
- Plant process control systems might become less efficient.

Table 2 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.1.D. Recommendation

Subject to Recommendation 4.1.B., addressed to the Service des technologies de l'information, we recommend that the Service de l'eau (Direction de l'épuration des eaux usées and Direction de l'eau potable):

- **Develop its management frameworks along the lines of those of the City's (Service des technologies de l'information), and ensure that, at the very least, they provide for:**
  - **a definition of the department's information and communications technology recovery objectives;**
  - **a detailed risk and impact analysis of disruptions;**
  - **an information and communications technology recovery strategy for reducing these impacts;**
  - **information and communications technology recovery plans;**
  - **a regular review and exercise drill schedule;**
- **Develop its management structure to implement the information and communications technology recovery program by:**
  - **making a member of its management team responsible for information and communications technology recovery;**
  - **establishing specific objectives for each management team;**
  - **developing a coordinated communications, monitoring and accountability process on the achievement of objectives;**
  - **documenting the roles and responsibilities of all stakeholders in the Service de l'eau;**
  - **establishing a process for monitoring activities;**
- **Provide for recurring financial and human resources for information technology recovery.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] The DEEU already has an IT recovery plan, currently being finalized, that was last updated in March 2015. This recovery plan contains the various headings listed here. ***(Planned completion: summer 2016 – awarding of contract)***

André Thang Phan-Cao has been appointed.

Objectives are currently being established. ***(Planned completion: April 2016)***

Development of the process is currently being finalized. ***(Planned completion: May 2016)***

The documentation process is ongoing.

The needs related to the establishment of an activity monitoring process will be submitted to the DEEU. ***(Planned completion: September 2016)***

The needs will be submitted to the DEEU. ***(Planned completion: May 2016)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] The DEP has embarked on a process of auditing cyber resilience with Public Safety Canada. ***(Planned completion: March 2016 – Audit complete)***

The results of this audit will be delivered to the DEP and will serve as input for next steps. ***(Planned completion: April 2016 – Audit results)***

The DEP plans to award two professional services contracts for the purpose of developing:

1. *an ICT risk analysis covering operational systems, telecommunications and office space. This risk analysis is based on standard NIST SP 800-82;* ***(Planned completion: fall 2016 – Execution from 2017 to 2019. Implementation)***

2. *an ICT resilience plan covering operational systems, telecommunications and office space. The resilience plan will be based on standards ISO 27002 and ISO 27005. This plan will address the issues raised.* ***(Planned completion: fall 2016 – Drafting of technical specifications from 2017 to 2019 – Execution)***

The DEP will develop management frameworks based on the resilience plan recommendations. ***(Planned completion: 2017)***

Responsibility for recovery issues is entrusted to the manager of the automation section.

An action plan that includes milestones, target dates and responsibilities will be developed. ***(Planned completion: from May 2016 and ongoing until 2019)***

A chart of TI recovery roles and responsibilities will be developed. ***(Planned completion: June 2016)***

Monitoring will take place regularly, every three months, and a biannual assessment will be presented to the BVG. ***(Planned completion: June 2016)***

Enter sufficient funds in both the operating budget and the three-year capital expenditures program to cover needs related to the implementation of the resilience plan. ***(Planned completion: May 2016)***

4.1.E. Findings – Service de sécurité incendie de Montréal

During our audit, we noted the following:

- The Service de sécurité incendie de Montréal (SIM) is responsible for its general disaster preparedness but not for managing the ICT infrastructures it uses, since these are managed by the STI. It therefore does not need a specific ICT recovery organizational structure, resources or budgets;
- In the case of the Répartition assistée par ordinateur (RAO), the STI delegates management to Hewlett Packard Canada (HP), which has submitted information and documents showing that the RAO and its infrastructures are covered by an ICT recovery plan that meets the SIM's needs;
- Resources are assigned to monitoring work affecting ICT infrastructures that are managed by the STI and HP.

Since we consider the risk level to be **low** (see Table 3), no recommendation is necessary.

Table 3 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.1.F. Findings – Service de Police de la Ville de Montréal

During our audit, we noted the following:

- 9-1-1 Emergency Centre systems are managed by external providers;
- The SPVM is responsible only for a few ICT infrastructures and systems used specifically for certain police activities, including the 9-1-1 Emergency Centre;
  The STI is responsible for the other ICT infrastructures and systems (the SPVM's centralized IBM environment, "administrative" networks and systems);
- ICT recovery is not assigned to a department manager and is not systematically monitored;
- The SPVM has no management frameworks, organizational structure, budget or resources allocated specifically to ICT recovery. As we noted during our business continuity management audit, the reason for this cited by the SPVM is that the systems that it manages do not require immediate recovery measures;
- The operations of the 9-1-1 Emergency Centre and of its ICT systems and infrastructures are governed by a province-wide framework for certification of 9-1-1 emergency centres. This framework calls for several structural and operational components that meet this component of the audit.

Since we consider the risk level to be **low** (see Table 4) for the activities of the 9-1-1 Emergency Centre, no recommendation is necessary.

Table 4 – Residual Risk Level – 9-1-1 Emergency Centre

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

For ICTs other than the 9-1-1 Emergency Centre, we consider the risk level to be **moderate** (see Table 5), because the SPVM faces the following potential risks:

- Without a management framework and organizational structure for ICT recovery or recurring financial and human resources, any process would lack cohesiveness and relevance to the SPVM's ongoing operations. The ICT recovery objectives would probably not be achieved, putting its operations at risk;

- With no formal responsibility or centralized coordination within the SPVM, a common approach cannot be shared, activities are not monitored, and actual disaster preparedness is not known;
- The department's recovery initiatives are not subjected to a systematic, standardized approach. This might result in inadequate processes that fail to meet ICT recovery objectives. The efforts would be incomplete, inconsistent, uneven, erratic in their effectiveness and inconsistently applied;
- In the event of a disaster, some SPVM activities would operate in backup mode.

Table 5 – Residual Risk Level — Other SPVM Activities

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.1.G. Recommendation

Subject to Recommendation 4.1.D., addressed to the Service des technologies de l'information, we recommend that the Service de Police de la Ville de Montréal:

- **Develop its management frameworks along the same lines as the City's (Service des technologies de l'information) and ensure that, at the very least, they provide for:**
  - **a definition of the department's information and communications technology recovery objectives;**
  - **a detailed risk and impact analysis of disruptions;**
  - **an information and communications technology recovery strategy for reducing these impacts;**
  - **information and communications technology recovery plans;**
  - **a regular review and exercise drill schedule;**
- **Develop its management structure to implement the information and communications technology recovery program by:**
  - **making a member of its management team responsible for information and communications technology recovery;**
  - **establishing specific objectives for each of its management teams;**
  - **developing a coordinated communications, monitoring and accountability process for the achievement of objectives;**
  - **documenting the roles and responsibilities of all stakeholders in the Service de Police de la Ville de Montréal;**
  - **establishing a process for monitoring activities;**
- **Provide specific recurring budgets for information and communications technology recovery.**

Business unit's response:

[TRANSLATION] A management framework for ICT recovery will be developed for systems supported by the SPVM exclusively (other than its 9-1-1 Emergency Centre). This management framework will be based on those of the City and will include the definition of recovery objectives, the requirement for each system to undertake a detailed analysis of the risks and impacts of disruptions, documentation of an ICT recovery strategy for reducing impacts, the requirement for an ICT recovery plan that is revised at a predetermined frequency and regular recovery exercises. ***(Planned completion: July 2016)***

A management structure for the implementation of the ICT recovery program will be documented. This structure will involve making a member of the SPVM management team responsible for ICT recovery, establishing specific objectives for each management team, developing a coordinated communications, monitoring and

accountability process for the achievement of objectives, documenting the roles and responsibilities of all SPVM stakeholders and establishing an activity monitoring process. ***(Planned completion: October 2016)***

After management frameworks are developed for recovery and for a management structure, a recurring budget adapted to needs will be requested to support ICT recovery processes. ***(Planned completion: November 2016)***

4.2. Major Incident Management Structure

When a technological disaster occurs, the City must react quickly and effectively to minimize the impacts of the disaster and resume operations quickly.

In order for a major incident management structure to be effective, members must have a clear understanding of their roles and responsibilities, their areas of concern, the tools to be used and the communications protocols that must be applied.

4.2.A. Findings – Service des technologies de l'information

During our audit, we noted that the STI did not have a comprehensive incident management structure for ICT recovery:

- An incident management process exists (power failures), but it is not associated with ICT recovery teams or plans;
- The STI's mobilization process provides for a way to contact resources if an incident occurs, but resources needed for ICT recovery are not identified;
- Roles and responsibilities for ICT recovery are not defined in either of the above two processes.

It should be mentioned that ICT recovery can be integrated into the incident management process and the mobilization plan.

We consider the risk level to be **high** (see Table 6), because the STI faces the following potential risks:

- Without a comprehensive major incident management structure, actions taken by the STI during a disaster would be improvised and might significantly increase ICT recovery time;
- Since the distribution of roles and responsibilities for ICT recovery is not clearly defined, the STI could not react promptly or ensure a coherent response to an emergency;
- ICT services might sustain a prolonged interruption, with significant consequences for the City's critical activities.

Table 6 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	PROBABLE	Possible	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	Critical	HIGH	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.2.B. Recommendation

We recommend that the Service des technologies de l'information adjust its major incident management structure so that it includes processes that ensure, at the time of a technological disaster:

- **mobilization of information and communications technology recovery resources;**
- **coordination of activities and responses;**
- **rapid, effective communication among the various stakeholders and interested parties.**

Business unit's response:

[TRANSLATION] A continuous improvement initiative will be established from May until December 2016 to review the major incident management process.

The new document on roles and responsibilities at the time of major incidents will be updated to reflect processes associated with major incidents and ICT recovery. It will be integrated into the information technology services continuity program.

The update will address the description of priorities and the correlations among high-priority incidents, major incidents and crisis management (with potential or confirmed recovery need).

Major incident (and crisis) management process activities will be reviewed to ensure responsibility is assigned and efforts coordinated at the time of a declared major incident or technological disaster. The communications strategy and the crisis shutdown procedure will be updated, and roles and responsibilities will be adjusted. ***(Planned completion: December 2016)***

4.2.C. Findings – Service de l'eau

During our audit of the Service de l'eau, we noted the following:

- Concerning the DEEU:
  - There is a documented on-call system and an informal escalation process. The first and second response levels are provided by automation engineers at the management level, and the third level is provided by manufacturers of the equipment and systems involved. However, the resources needed for ICT recovery are not determined;
  - There is no process for managing or coordinating activities, and roles and responsibilities are not clearly established in the event of a disaster. The plant's everyday operational structure would be used, but it does not include all the elements needed to manage a disaster;
  - The DEEU is currently developing and documenting specific operational procedures for ICT recovery;

- Concerning the DEP:
  - There is a list of people to call and of support priorities for system disruptions that identifies the levels and groups of stakeholders needed for support, but the resources required for ICT recovery are not established;
  - These support levels are integrated into the plants' operational structure and would apply at the time of a disaster;
  - The response structure does not include all the elements needed to manage a disaster affecting ICTs.

We consider the risk level to be **moderate** (see Table 7), because the Service de l'eau (DEEU and DEP) faces the following potential risks:

- Without a comprehensive major incident management structure, actions taken by the Service de l'eau might increase the ICT recovery time in the event of a disaster;
- Since the distribution of roles and responsibilities for ICT recovery were not clearly defined, the department could not react promptly or ensure a coherent response to an emergency;
- Plant process control systems might become less efficient.

Table 7 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	Moderate	MODERATE	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.2.D. Recommendation

We recommend that the Service de l'eau adjust its operational management structure so that it includes processes that ensure, at the time of a technological disaster:

- **mobilization of resources;**
- **coordination of activities and responses;**
- **rapid, effective communication among the various stakeholders and interested parties.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] Coordination with ICT remains to be included. ***(Planned completion: December 2016)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] Review of incident response processes for control systems. ***(Planned completion: December 2016)***

Insert an ICT section in the DEP emergency measures plan. ***(Planned completion: December 2017)***

4.2.E. Findings – Service de sécurité incendie de Montréal

During our audit of the SIM, we noted that the service provider, HP, which is responsible for the management of RAO systems and infrastructures, has an adequate major incident management process in place.

Since we consider the risk level to be **low** (see Table 8), no recommendation is necessary.

Table 8 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.2.F. Findings – Service de Police de la Ville de Montréal

During our audit, we noted the following:

- With the exception of the 9-1-1 Emergency Centre, the SPVM is not responsible for ICT infrastructures and systems requiring immediate recovery;

- For the 9-1-1 Emergency Centre:
  - Management of critical ICT infrastructures and systems is entrusted to external providers;
  - The responsibilities of managers on duty at the SPVM are properly understood and the implementation of the ICT recovery strategy and its technological requirements is documented;
  - Coordination with service providers during major incidents is part of the operational procedures of the 9-1-1 Emergency Centre;
  - The department is not responsible for everyday management of ICT infrastructures and systems that are critical to 9-1-1 Emergency Centre operations.

Since we consider the risk level to be **low** (see Table 9), no recommendation is necessary.

Table 9 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.3. Risk and Impact Analysis and Information and Communications Technology Recovery Strategies

Business impact analysis (BIA) is an essential component of an effective ICT recovery process.

Risk analyses establish the components of ICT systems and infrastructures that are most at risk for causing a major power failure or technological disaster. They are also useful for identifying and implementing prevention or mitigation measures in order to reduce probabilities of occurrence and impacts.

Business units must notify their ICT service providers of their minimum service requirements, which must be clearly defined and based on their operational and ICT recovery needs. These requirements are based on the BIA procedure that establishes the maximum tolerances for ICT service disruption and data loss.

These are the requirements used for identifying critical ICT services and their tolerance to disruptions and data loss and for then developing ICT recovery strategies, service agreements and communications and alert protocols in the event of a disaster. ICT recovery will thus meet the actual needs identified and justified by business units.

4.3.A. Findings – Service des technologies de l'information

During our audit, we noted the following:

- As noted during our business continuity management audit,[3] the City did not have a process for conducting a risk and BIA. Furthermore, the business units did not follow a formal municipal procedure to inform the STI of their clearly defined minimum service requirements based on their ICT recovery and operational needs;
- There is no formal process for conducting a risk and impact analysis at the STI. As a result, the STI has not determined its own priorities or its equipment and applications needs to ensure adequate ICT recovery;
- Risk and impact analyses were conducted only for the integrated management system (Système intégré Montréal [SIMON]), but only a draft version dating from 2008 exists;
- The STI provided us with a list of critical applications. However, we were unable to obtain comprehensive documentation justifying the conclusions of the process. This list was amended as a result of the questions we asked during our audit;
- With the exceptions of the centralized IBM environment and SIMON, the STI has not established ICT recovery strategies for its critical infrastructures and systems;

- Concerning the City's centralized IBM environment:
  - The recovery strategies for the centralized environment are based only on the STI's perceptions of needs or undocumented discussions with business units;
  - The recovery strategy documents and diagrams were incomplete and inadequate;
  - Service restoration of its systems is covered by an agreement with an external provider at a specialized recovery site;
  - A formal process for making backup copies is in place, but copies are checked completely only at the time of the annual recovery exercise.

We consider the risk level to be **critical** (see Table 10), because the STI faces the following potential risks:

- With no clear requirements specified by business units through a formal process, the STI cannot ensure that the ICT recovery strategies established meet its needs;
- Without a risk and impact analysis of its own operations, the STI cannot ensure that the ICT recovery strategies in place meet its needs;
- Performing only a single yearly validation of all backup copies in the centralized IBM environment increases the risk of having corrupted data.

[3] Refer to section 4.9 of the 2014 Annual Report, "Business Continuity Management."

Table 10 – Risk Level

Impact[a]	Probability of occurrence[a]				
	HIGHLY PROBABLE	Probable	Possible	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	CRITICAL	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.3.B. Recommendation

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

- **Ask business units to provide clearly defined minimum service requirements based on their operational and information and communications technology recovery needs;**
- **Establish a process for conducting risk and impact analyses;**
- **Evaluate, establish and document recovery strategies that meet the needs expressed by business units and the Service des technologies de l'information for all information and communications technology platforms other than the centralized IBM environment;**
- **Review the recovery strategy diagrams and documents for the centralized environment, in particular, by specifying the recovery sequences for the applications concerned;**
- **Carry out more than one validation per year of all backup copies in the centralized IBM environment.**

Business unit's response:

[TRANSLATION] Assist the City's business units in documenting the operational needs of each of the business processes in question in order to determine their IT service continuity needs.

Evaluate, establish and document recovery strategies that meet the needs expressed by business units and the STI. ***(Planned completion: April 2017)***

Review and integrate recovery documentation for the centralized environment. ***(Planned completion: February 2017)***

Develop a plan to test the operability of recovery on the centralized environment. ***(Planned completion: March 2017)***

4.3.C. Findings – Service de l'eau

During our audit, we noted the following:

- There is no common ICT recovery approach within the Service de l'eau;
- Redundancy mechanisms are integrated into the technological architecture of the drinking water and water treatment plants process control systems and infrastructures. These are elements of ICT recovery strategies, and they reduce the risk of a disaster;

- Concerning the DEEU:
  - A BIA procedure performed for the plant identified the critical business operations and their tolerances to interruptions and data loss;
  - Some technological risks have been identified, which are single points of failure for which an action plan is being developed;
  - The ICT recovery strategies and measures in place are based on the redundancy and distribution of infrastructures in different locations, all at the plant site. Most of these measures are illustrated using diagrams and an initial draft version of the ICT recovery plan consolidates the strategies that were established, some of which must be finalized;
  - Concerning data backup, process control data are replicated on separate servers, and data on all other servers are backed up once a month;

- Concerning the DEP:
  - It used the hazard and operability study (HAZOP) at the Lachine plant, a pilot project that is still under way, and decided on some components of a BIA. The process:
    - Ø has not identified tolerances to disruptions or data loss for critical functions and their applications;
    - Ø was used as the basis for an initial working document on what the DEP expected from the services provided by its main ICT service provider, the STI;
  - Once the pilot project is completed, the DEP plans to repeat the procedure for all of its plants.

We consider the risk level to be **moderate** (see Table 11), because the Service de l'eau faces the following potential risks:

- Without a common approach to ICT recovery, the efforts required to coordinate results, pool data and tools or share all the information with the other management teams will be a limiting factor;

- Without a thorough risk and impact analysis process, it is possible that certain critical functions and certain single points of failure would not be detected and as a result would not be covered by adequate, documented ICT recovery strategies;
- At the time of a disaster, the Service de l'eau might not be able to identify all its critical functions within the established timelines.

Table 11 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	MODERATE	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.3.D. Recommendation

We recommend that the Service de l'eau establish a risk and impact analysis process for the entire department.

For the Direction de l'épuration des eaux usées in particular, we recommend that it:

- **Implement corrective measures to mitigate the single points of failure identified;**
- **Continue to develop, document and illustrate using diagrams information and communications technology recovery strategies;**

Specifically for the Direction de l'eau potable, we recommend that it:

- **Complete the Lachine plant pilot project and apply it to all its plants;**
- **Develop, document and illustrate using diagrams information and communications technology recovery strategies.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] The risk analysis process is already defined in the existing recovery plan.

In the process of being completed. ***(Planned completion: December 2016)***

90% are already completed, the remaining 10% are under way. ***(Planned completion: December 2016)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] Will be covered by the professional services contracts mentioned in 4.1.D.

The HAZOP pilot project in Lachine involving a functional analysis of control processes and systems is currently being finalized. ***(Planned completion: September 2016)***

The procedure will be repeated for each of the other five plants and pumping stations. ***(Planned completion: December 2018)***

Will be covered by the professional services contracts mentioned in 4.1.D.

4.3.E. Findings – Service de sécurité incendie de Montréal

During our audit, we noted the following:

- The SIM has not conducted a recent risk and impact analysis for the purpose of establishing business continuity plans or guiding the development of ICT recovery plans;
- For the RAO, a needs analysis identified tolerances to disruptions and data loss as part of the work of preparing specifications for this critical system;
- An adequate recovery strategy for the RAO is described in several operational records provided by Hewlett Packard Canada (HP) and the SIM;
- According to an architectural analysis of RAO systems, the link for transferring data to vehicles was identified as involving a risk of partial failure, since this link was not redundant. The function of this link is to transfer specific response data to field teams and deliver vehicle geolocation data to the RAO;
- As part of a major project for maintaining uninterruptible power supply (UPS) systems at the main site, an impact analysis specifically targeting this work was conducted. Some deficiencies were identified and steps were taken to mitigate or correct them.

We consider the risk level to be **high** (see Table 12), because the SIM faces the following potential risks:

- Without thorough, detailed impact analyses, it would not be possible to detect certain critical functions, with the exception of the RAO, and they would therefore not be covered by adequate, documented ICT recovery strategies. It would not be possible to identify these functions when a disaster occurs;
- Without the link for transferring data from the RAO to vehicles:
  - Certain information critical to firefighter response would not be transmitted, which might jeopardize their health and safety;

- Vehicles' geolocation data would not be transmitted to the RAO, which would reduce the effectiveness of the distribution process and might increase response time.

Table 12 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	Critical	High	HIGH	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.3.F. Recommendation

We recommend that the Service de sécurité incendie de Montréal:

- **Complete a business impact analysis procedure;**
- **Take steps to mitigate the point of failure for the transfer of data to vehicles.**

Business unit's response:

[TRANSLATION] The SIM will request a comprehensive, detailed impact analysis of the critical functions supporting response management systems in order to eliminate all obsoleteness and associated risks to ensure redundancy and system continuity. ***(Planned completion: end of 2016)***

This year the SIM will replace the obsolete "Data Radio" system with a much more robust, more reliable "LTE" system to ensure data transfer to vehicles. ***(Planned completion: end of 2017)***

4.3.G. Findings – Service de Police de la Ville de Montréal

During our audit, we noted the following:

- The SPVM is responsible only for a few ICT infrastructures and systems used specifically for certain police activities. However:
  - These systems do not require immediate recovery measures and no ICT recovery measures exist;
  - The SPVM benefits from the services of other police forces to compensate for a prolonged technology failure;

- Systems operating in server environments are managed by the STI and are replicated at the recovery site;
- The SPVM has conducted risk analyses for the main sites and the recovery site of the 9-1-1 Emergency Centre. However, these analyses do not cover ICT risks;
- No impact analysis has been conducted to determine the criticality of other applications used by the department or their tolerances to interruptions and data loss;
- Even though the SVPM's centralized IBM environment does not require immediate recovery, its backup copies have never been subjected to a validation test involving a complete reloading of the operating environment (operating system, applications and data).

We consider the risk level to be **high** (see Table 13), because the SPVM faces the following potential risks:

- Without a thorough, detailed impact analysis, some systems needing to be recovered might not be identified and would as a result not be covered by adequate, documented ICT recovery strategies;
- Concerning the SVPM's centralized environment, since backup copies are not tested, there is no guarantee that this environment can be made operational again. With this environment, the SPVM runs the risks of prolonged application failures and data loss.

Table 13 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	Critical	High	**HIGH**	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.3.H. Recommendation

We recommend that the Service de Police de la Ville de Montréal:

- **Complete an impact analysis in the event of systems failure;**
- **Evaluate, establish and document information and communications technology recovery strategies for systems under its responsibility that require recovery;**
- **Inform the appropriate information and communications technology service providers of the results of these analyses;**
- **Evaluate and monitor the information and communications technology recovery strategies developed and established by its service providers;**
- **Ask the Service des technologies de l'information to establish a strategy for testing backup copies that involves completely reloading and restarting the Service de Police de la Ville de Montréal's systems that operate on the IBM environment.**

Business unit's response:

[TRANSLATION] A systems failure impact analysis will be documented. ***(Planned completion: February 2017)***

ICT recovery strategies for systems that are under the SPVM's responsibility and require recovery will be evaluated, documented and established. ***(Planned completion: February 2017)***

The results will be communicated to the appropriate ICT service providers. ***(Planned completion: May 2017)***

The recovery strategies established by these service providers will then be evaluated and monitored. ***(Planned completion: May 2017)***

The STI's acting Public Safety Director has been asked to establish a strategy for testing backup copies. ***(Planned completion: July 2017)***

4.4. Information and Communications Technology Recovery Plans and Procedures

When a disaster strikes, the City must respond quickly in order to minimize its impacts and quickly resume operations. It is important that organizations destabilized by an incident be able to perform critical activities in an orderly fashion so that they can resume operations as quickly as possible.

As a way of facilitating decision-making under pressure, the ICT recovery plan must account for all the activities and procedures established in the organization to maintain or quickly resume ICT operations, systems and infrastructures.

Management tools that give clear details on “who does what, when, how and where” for specific situations help reduce uncertainty time due to any incident, as well as ensuring ICT recovery teams develop optimum response reflexes.

4.4.A. Findings – Service des technologies de l’information

During our audit of the STI, we noted the following:

- Even though the City’s centralized IBM environment is covered by an ICT recovery strategy, no procedure describes its implementation and the transfer of activities to the recovery site. The existing documentation does not provide an adequate guarantee that the STI will be able to switch its activities to the recovery site effectively;
- The only system covered by an ICT recovery plan containing the required elements is SIMON. However, since this is only a draft version dating from September 2015, the vast majority of ICT systems managed by the STI are not covered by an ICT recovery plan.

We consider the risk level to be **critical** (see Table 14), because the STI faces the following potential risks:

Without ICT recovery plans and procedures:

- The measures to be implemented for ICT recovery would be improvised; responses would not be coordinated and might interfere with each other;
- Critical systems would not be available for business units, which might not recover their critical operations within the required timelines;
- Essential public services that depend on ICTs might not be maintained, which could have serious consequences for public welfare.

Table 14 – Risk Level

Impact[a]	Probability of occurrence[a]				
	HIGHLY PROBABLE	Probable	Possible	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	CRITICAL	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.4.B. Recommendation

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

- **Develop recovery plans for all critical information and communications technology systems and infrastructures, including, the following components:**
  - **alert processes and processes for activating plans;**
  - **processes for activating or accessing recovery sites;**
  - **a definition of the roles and responsibilities of each stakeholder or each recovery team;**
  - **a definition of information and communications technology recovery activities;**
  - **identification of critical resources (staff, equipment) needed to relocate essential operations;**
  - **a list of employees from the department and third parties who must participate in ICT recovery, including ways to contact them;**
  - **the development of operational procedures for information and communications technology recovery;**
- **Finalize the recovery plan for the SIMON application.**

Business unit's response:

[TRANSLATION] Recovery plans will be developed in accordance with the City's business needs. The documentation of these plans will cover:

- *alert processes and processes for activating plans;*
- *processes for accessing recovery sites;*
- *definitions of stakeholders' roles and responsibilities;*
- *definitions of recovery activities, in order to recover or relocate essential operations;*
- *contact information for employees' and service providers that are to participate in the recovery;*
- *information technology recovery procedures.* ***(Planned completion: April 2017)***

Finalize the recovery plan for the SIMON application and integrate it into the information technology service continuity program. ***(Planned completion: December 2016)***

4.4.C. Findings – Service de l'eau

During our audit, we noted the following:

- Following its BIA, the DEEU is currently preparing a draft version of the ICT recovery plan for its plant process control systems and developing several operational and recovery procedures;
- There is no ICT recovery plan for the DEP's drinking water production plants, but the diagrams illustrating redundant elements in their process control infrastructures are kept up to date;
- Neither of the two management teams has developed a management tool to coordinate activities pertaining to ICT recovery or monitoring responses in the event of a disaster.

We consider the risk level to be **moderate** (see Table 15), because the Service de l'eau faces the following potential risks:

- Without an ICT recovery plan, responses would not be coordinated, and they might interfere with each other or with redundant elements in process control systems;
- The plant process control systems might become less efficient.

Table 15 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	**MODERATE**	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.4.D. Recommendation

We recommend that the Service de l'eau develop information and communications technology recovery plans for all its systems and critical operations, including:

- **Alerting and mobilization processes;**
- **A definition of criteria for activating the recovery plans;**
- **Processes for activating or accessing recovery sites;**
- **A definition of the roles and responsibilities of each stakeholder or each recovery team;**
- **A definition of the information and communications technology recovery activities and recommendations;**
- **Identification of critical resources (staff, equipment) needed to relocate essential operations;**
- **A list of employees from the department and third parties who must participate in recovery activities, including ways to contact them;**
- **The development of operational procedures in the event of a disaster.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] Generally, the ICT recovery plan and the emergency measures plan meet all these recommendations. The plan will be included in the DEEU emergency plan. ***(Planned completion: September 2016)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] Will be covered by the professional services contracts mentioned in 4.1.D. ***(Planned completion: September 2018 [first three elements])***

The DEP also wishes to propose an ICT recovery centre infrastructure project. Essentially, the project would include a data recovery centre and an operations recovery centre:

1. *Needs and feasibility study;* ***(Planned completion: March 2017)***
2. *Plans and specifications;* ***(Planned completion: December 2017)***
3. *Execution.* ***(Planned completion: March 2019)***

4.4.E. Findings – Service de sécurité incendie de Montréal

During our audit, we noted the following:

- The SIM is not responsible for the critical ICT infrastructures or systems on which it depends;
- The RAO is managed by HP, which provided several documents that meet ICT recovery requirements.

Since we consider the risk level to be **low** (see Table 16), no recommendation is necessary.

Table 16 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.4.F. Findings – Service de Police de la Ville de Montréal

During our audit, we noted the following:

- Concerning the 9-1-1 Emergency Centre:
  - The call-dispatch systems and call-handling systems are completely redundant, greatly reducing the risk of a total disruption;
  - The process for activating recovery measures is integrated in the staff's operational procedures;
  - These systems are managed by external service providers. No information on ICT recovery plans was provided by the SPVM. However, recovery infrastructures and systems were used a few times without any major problems;
- There is no ICT recovery plan for systems operated by the SPVM for certain police activities because they do not require immediate recovery measures. However, operations that use these systems could obtain the assistance of other police forces, which would reduce the impact of a major power failure on operations.

Since we consider the risk level to be **low** (see Table 17), no recommendation is necessary.

Table 17 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.5. Information Technology Recovery Training

An ICT recovery procedure cannot succeed without an education component. All employees should receive training on the response process, steps to take and procedures to follow in order to maximize the effectiveness of responses if a disaster occurs. Training promotes a common understanding of the objectives and decision-making processes and ensures uniformity in the response methods used by the organization when an emergency situation arises.

4.5.A. Findings – Service des technologies de l'information

Since there is no ICT disaster recovery program, the STI has not developed a training and awareness program for its staff.

We consider the risk level to be **high** (see Table 18), because the STI faces the following potential risks:

- Without a training and awareness program, staff members who need to respond during disruptions in operations would not be prepared to take action. Their responses would be improvised and largely ineffective. The department would probably not be able to identify critical ICT infrastructures and systems that affect both its clients' and its own critical functions. Essential public services might not be maintained.

Table 18 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	Critical	High	HIGH	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.5.B. Recommendation

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

- **Integrate a training program dedicated to information and communications technology recovery into existing training programs. This program must include:**
  - **identification of the target audience;**
  - **training objectives;**
  - **type of training or awareness activity;**
  - **frequency of activities;**
- **Establish a process for evaluating the results of the training program.**

Business unit's response:

[TRANSLATION] Documentation on training, including the definition of training programs adapted for target audiences, a training schedule and a continuous training plan will be available through the information technology services continuity program.

Training will be aligned with the STI's skills development plan so that outcomes can be measured and training programs adapted as needed. ***(Planned completion: April 2017)***

4.5.C. Findings – Service de l'eau

In the absence of an ICT disaster recovery program, the Service de l'eau has not developed a training and awareness program for its staff.

It should be mentioned that in the interest of knowledge transfer, a planning process is under way for the replacement of staff eligible for retirement at the DEEU. At the DEP, training programs have been set up for in-plant staff, but none is adapted specifically for ICT staff.

We consider the risk level to be **moderate** (see Table 19), because the Service de l'eau faces the following potential risks:

- Without an awareness and training program, staff members who need to respond during service disruptions would not be prepared to take action. Their responses would be improvised and ineffective;
- Plant process control systems might become less efficient.

Table 19 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.5.D. Recommendation

We recommend that the Service de l'eau:

- **Set up an information and communications technology recovery training program. This program must include the following:**
  - **identification of the target audience;**
  - **training objectives;**
  - **type of training or awareness activity;**
  - **frequency of activities;**
- **Establish a process for evaluating the results of the training program.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] A training program dedicated to ICT recovery remains to be developed. The budget is also to be provided. ***(Planned completion: December 2017)***

A process for evaluating results remains to be developed. This budget is also to be provided. ***(Planned completion: December 2017)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] The training program will follow the definition of the ICT resilience plan. ***(Planned completion: fall of 2018)***

The evaluation process will be integrated into the training plan. Evaluation will follow training. ***(Planned completion: fall of 2018)***

4.5.E. Findings – Service de sécurité incendie de Montréal

Since the SIM is not responsible for the infrastructures and systems on which it depends for its critical functions, it is not required to establish an ICT recovery training and awareness program for its staff.

Since we consider the risk level to be **low** (see Table 20), no recommendation is necessary.

Table 20 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
NEGLIGIBLE	Low	Low	Low	**LOW**	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.5.F. Findings – Service de Police de la Ville de Montréal

For 9-1-1 Emergency Centre systems, employees are provided with training that covers the use of technologies at both the main site and the recovery site. These features are included in the 9-1-1 Emergency Centre operational procedures.

Since the other systems falling under the responsibility of the SPVM do not require immediate recovery measures, it is not required to establish an ICT recovery training and awareness program for its staff.

Since we consider the risk level to be **low** (see Table 21), no recommendation is necessary.

Table 21 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
NEGLIGIBLE	Low	Low	Low	**LOW**	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.6. Information and Communications Technology Recovery Exercise Program

An organization's effectiveness in reacting to an emergency situation or crisis will depend largely on the exercise programs that it establishes.

A program involves planning ICT recovery exercises over a period of several years. The planning process takes into account the training program, changes in recovery objectives and the general preparedness of the organization.

ICT recovery exercises give participants the opportunity to put theoretical learning into practice, become familiar with their roles and responsibilities and test the different systems and procedures. Getting procedures under way, making decisions quickly and communicating effectively become automatic reflexes. The response as a whole therefore becomes more efficient.

Exercises also play a key role in determining concrete improvements to make to correct existing deficiencies.

4.6.A. Findings – Service des technologies de l'information

Since the STI does not have an ICT disaster recovery program, it has not developed an exercise program. However:

- The only ICT recovery exercises concern the City's centralized IBM environment, for which annual exercises are conducted to reinstall the infrastructure at the external provider's recovery site;

- We think these exercises are too limited for us to be able to confirm that the STI will be able to transfer its centralized environment and its applications from its main site to the recovery site within the prescribed timelines. In fact:
  - Over the past three years, objectives have basically remained unchanged, with no changes made to their level of complexity following previous exercises;
  - Some documents provide only a broad indication of the objectives of the exercises and an observation of the situation that amounts to a note on whether the objectives have been achieved or not;
  - Users of business units are not involved in the tests;
  - Interdependence with other systems is not tested;
- There are no ICT recovery exercises for other technological platforms.

We consider the risk level to be **critical** (see Table 22), because the STI faces the following potential risks:

- If drill exercises for ICT recovery plans are not performed regularly as part of a structured program, the recovery process cannot be validated effectively;
- Without a structured, recurring procedure for carrying out exercises, strengths, weaknesses, deficiencies and possible solutions would not be identified or documented. This might affect people's perception of actual disaster preparedness;
- The ICT systems and infrastructures on which the City's critical activities depend might not be recovered in a timely manner, which would lead to a loss of public services.

Table 22 – Risk Level

Impact[a]	Probability of occurrence[a]				
	HIGHLY PROBABLE	Probable	Possible	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	**CRITICAL**	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.6.B. Recommendation

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

- **Develop an exercise program for members of information and communications technology recovery response teams. This program must include:**
  - **the types of exercises required;**
  - **an exercise drill schedule;**
  - **a list of stakeholders required based on the type of exercise and the environment targeted;**
  - **the process for carrying out the exercises;**
- **Perform, on a regular basis, at least once a year, information and communications technology recovery exercises on all environments that support critical functions, including application and communication tests. Each exercise requires:**
  - **a planning document that includes:**
    - Ø **the disaster scenario;**
    - Ø **the scope of the exercise;**
    - Ø **the objectives of the exercise, in order of increasing complexity;**
    - Ø **the stakeholders involved;**
    - Ø **a communications plan;**
  - **an exercise assessment report;**
- **Develop an action plan to correct any deficiencies observed.**

Business unit's response:

[TRANSLATION] Tests will be developed for each recovery plan. They will describe objectives, participants and responsibilities, testing and simulation scenarios and a schedule. ***(Planned completion: April 2017)***

These recommendations will be integrated into the information technology service continuity program for recovery tests affecting several systems or more all-encompassing simulations.

All aspects will be covered in the exercise drills for each specific recovery plan. ***(Planned completion: June 2017)***

4.6.C. Findings – Service de l'eau

In the absence of an ICT disaster recovery program, the Service de l'eau has not developed a recovery exercise program. However:

- The design of the process control systems integrates several levels of redundancy and continuous verification loops in the communication lines of their data and operations;
- Any incident is reported to operators and documented in operational reports;

- A few incident reports exist; the incidents covered by these reports are considered exercises by plant management teams. The formats of these reports vary according to the people writing them and the management team and does not provide for any formal process for following up on corrective measures taken;
- The maintenance activities for some equipment are also used to validate the operation of redundant equipment.

We consider the risk level to be **moderate** (see Table 23), because the Service de l'eau faces the following potential risks:

- If drill exercises for ICT recovery plans are not performed regularly or properly, the recovery plans or the strategies they document cannot be validated effectively;
- Stakeholders who do not have the opportunity to perform simulation exercises or other types of exercises would probably not be able to develop the necessary reflexes to respond effectively to destabilizing events;
- The plant process control systems might become less efficient.

Table 23 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.6.D. Recommendation

We recommend that the Service de l'eau:

- **Develop an exercise program for members of information and communications technology recovery response teams. This program must include:**
  - **the types of exercises required;**
  - **an exercise drill schedule;**
  - **a list of stakeholders required based on the type of exercise and the environment targeted;**
  - **the process for carrying out the exercises;**
- **Perform, on a regular basis, at least once a year, information and communications technology recovery exercises on all environments that support critical functions, including application and communication tests. Each exercise requires:**
  - **a planning document that includes:**
    - Ø **the disaster scenario;**
    - Ø **the scope of the exercise;**
    - Ø **the objectives of the exercise, in order of increasing complexity;**
    - Ø **the stakeholders involved;**
    - Ø **a communications plan;**
  - **an exercise assessment report;**
- **Develop an action plan to correct any deficiencies observed.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] An exercise program remains to be developed. The budget is to be provided. ***(Planned completion: 2017)***

Regular recovery exercises have yet to be established. Exercises have already been performed with no disruption of service. ***(Planned completion: 2017)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] These features will be covered by the professional services contracts mentioned in 4.1.D. to follow up on actions outlined in 4.2.D. emergency measures plan. ***(Planned completion: fall of 2019)***

An infrastructure project for an ICT testing and process monitoring environment will be proposed: ***(Planned completion: 2018)***

1. *Needs and feasibility study;* ***(Planned completion: March 2017)***
2. *Plans and specifications;* ***(Planned completion: October 2017)***
3. *Execution.* ***(Planned completion: October 2018)***

4.6.E. Findings – Service de sécurité incendie de Montréal

The SIM is not responsible for the infrastructures and systems on which it depends for its critical functions.

Concerning the RAO, however, we noted the following:

- Under the terms of its contract, the service provider is responsible for performing exercises, which consist of a series of checks performed when applications are updated or workstations are switched to the recovery site;
- No recovery exercise was performed to simulate a disaster involving a total loss of the main site's infrastructures and systems;
- The recovery site is used frequently, but RAO's production and recovery systems and infrastructures are always linked with each other.

We consider the risk level to be **high** (see Table 24), because the SIM faces the following potential risks:

- If drill exercises for the RAO recovery plan are not performed based on a scenario of a total loss of ICTs at the main site, it cannot be validated effectively;
- The availability of the RAO might be compromised.

Table 24 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	Critical	High	HIGH	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.6.F. Recommendation

We recommend that the Service de sécurité incendie de Montréal require that the service provider of the computer-assisted dispatch system (RAO) include a scenario of the total loss of infrastructures and systems at the main site in its exercise plan.

Business unit's response:

[TRANSLATION] The SIM will require the HP service provider to include in its exercise plan the scenario of a total loss of infrastructures and systems at the main site supporting the RAO system. ***(Planned completion: fall of 2016)***

In April–May 2016 we plan to carry out an exercise simulating a total failure of power for communications system infrastructures and the RAO for the purpose of replacing the new power generation system (UPS) at its headquarters. ***(Planned completion: May 2016)***

4.6.G. Findings – Service de Police de la Ville de Montréal

During our audit, we noted the following:

- Concerning the 9-1-1 Emergency Centre:
  - Regular systems recovery exercises are performed. A register of the use of the 9-1-1 recovery centre is kept;
  - Formal exercises consisting of toggling between the primary and secondary servers and between sites are performed on the dispatching system;
- Concerning ICT infrastructures and systems used specifically for certain police activities for which the SPVM is responsible, when backup copies exist, they are not restored in their entirety to validate their integrity.

Since we consider the risk level to be **low** for the 9-1-1 Emergency Centre (see Table 25), no recommendation is necessary.

Table 25 – Risk Level – 9-1-1 Emergency Centre

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
NEGLIGEABLE	Low	Low	Low	**LOW**	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

We consider the risk level to be **moderate** for the other ICT systems used specifically for SPVM activities (see Table 26), because although these systems do not require immediate

ICT recovery, since their backup copies are not fully checked, it is possible that some data might be lost forever for the SPVM.

Table 26 – Risk Level – Other SPVM Activities

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.6.H. Recommendation

We recommend that the Service de Police de la Ville de Montréal implement a process for testing backup copies of its information and communications technology systems used specifically for certain police activities.

Business unit's response:

[TRANSLATION] We will implement a process for testing backup copies of the systems used specifically for certain police activities. ***(Planned completion: February 2017)***

4.7. Updating Information and Communications Technology Recovery Documentation

Like all organizations, the City goes through changes over time, with evolving business processes, staff turnover and operations being redefined. The result of these changes is that some aspects of ICT recovery plans cease to be consistent with the reality of the organization.

Updating the components of the ICT disaster recovery program ensures that it is reliable and accurate. Timeframes are determined on the basis of the type of information to be kept up to date. This updating can also be done following an exercise.

4.7.A. Findings – Service des technologies de l'information

During our audit, we noted the following:

- Since there is no ICT disaster recovery program, no process for updating the documentation has been developed;
- Several documents obtained during our audit had not been updated recently.

We consider the risk level to be **critical for the STI** (see Table 27) because, with no process in place for updating ICT recovery documentation, the program would quickly become obsolete, significantly reducing the department's ability to maintain its essential operations in the event of a disaster.

Table 27 – Risk Level

Impact[a]	Probability of occurrence[a]				
	HIGHLY PROBABLE	Probable	Possible	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
MAJOR	CRITICAL	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.7.B. Recommendation

We recommend that the Service des technologies de l'information establish a process for updating information and communications technology recovery documentation, including, the following activities:

- **Determining elements that need to be updated;**
- **Developing a regular review schedule;**
- **Informing various stakeholders of changes;**
- **Making changes to plans to take into account new learning acquired during exercises or when plans must be used during disruptions in operations;**
- **Aligning processes with those of incident and change management.**

Business unit's response:

[TRANSLATION] A process for updating plans and the different features of the information technology service continuity program will be developed.

A procedure for monitoring required changes, including activities involving a review of various related processes, will be established. ***(Planned completion: April 2017)***

4.7.C. Findings – Service de l'eau

During our audit, we noted that no process is in place for updating ICT recovery documentation. However, because of the industrial nature of the Service de l'eau's activities, operational, technological or application changes are infrequent. It is nevertheless necessary to ensure their stability and reliability.

We consider the risk level to be **moderate** (see Table 28), because, since the Service de l'eau has no process for updating ICT recovery documentation, the program would become obsolete and would reduce the department's ability to maintain its essential operations in the event of a disaster.

Table 28 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.7.D. Recommendation

We recommend that the Service de l'eau establish a process for updating information and communications technology recovery documentation that includes the following activities:

- **Determining the components that need to be updated;**
- **Developing a regular review schedule;**
- **Informing the different stakeholders of changes;**
- **Making changes to plans to take into account new learning acquired during exercises or when plans must be used during interruptions in operations;**
- **Aligning processes with those of incident and change management.**

Business unit's response:

DIRECTION DE L'ÉPURATION DES EAUX USÉES

[TRANSLATION] A recovery plan update is planned.
It will follow the introduction of exercises. ***(Planned completion: 2018)***
Incidents are entered in the Elogger application. ***(Completed)***

DIRECTION DE L'EAU POTABLE

[TRANSLATION] This process will be implemented following submission of the ICT resilience plan deliverables and annual revision of ICT recovery documentation. ***(Planned completion: 2019)***

A process for auditing the implementation of the ICT resilience plan will be established. ***(Planned completion: 2020)***

4.7.E. Findings – Service de sécurité incendie de Montréal

During our audit, we noted the following:

- The process for updating the RAO recovery documentation is the responsibility of the service provider;
- The documentation obtained from the service provider was up to date;
- Regular meetings are held with the service provider to hold discussions and ensure the continuity of the RAO.

Since we consider the risk level to be **low** (see Table 29), no recommendation is necessary.

Table 29 – Risk Level

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.7.F. Findings – Service de Police de la Ville de Montréal

During our audit, we noted the following:

- The process for updating ICT recovery documentation for the 9-1-1 Emergency Centre is the responsibility of service providers. However, the SPVM does not ensure that documents are updated;
- For ICT systems used specifically for certain police activities, which do not require immediate recovery measures, no process is in place for updating recovery documentation, because the documentation does not exist. However, at the very least there should be documentation pertaining to backup copies, especially regarding backup tests.

Even though we consider the risk level to be **low** (see Table 30) for the 9-1-1 Emergency Centre, if the SPVM does not ensure that ICT recovery documentation is up to date, there is a risk that it might not reflect current reality, and ICT recovery might become less effective.

Table 30 – Risk Level – 9-1-1 Emergency Centre

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	Possible	UNLIKELY	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
Moderate	High	High	Moderate	Moderate	Moderate
MINOR	Moderate	Moderate	Moderate	**LOW**	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.7.G. Recommendation

We recommend that the Service de Police de la Ville de Montréal check with its service providers to ensure that information and communications technology recovery documentation is up to date.

Business unit's response:

[TRANSLATION] We will ask our service providers to ensure that ICT recovery documentation is up to date and that a regular updating process is in place. ***(Planned completion: May 2017)***

We consider the risk level to be **moderate** (see Table 31) for the other ICT systems used specifically for certain SPVM activities, because without updating the documentation on the process of testing backup copies of ICT systems used specifically for certain SPVM activities, these tests might become less effective and data might be lost.

Table 31 – Risk Level – Other SPVM Activities

Impact[a]	Probability of occurrence[a]				
	Highly probable	Probable	POSSIBLE	Unlikely	Improbable
Catastrophic	Critical	Critical	Critical	High	High
Major	Critical	High	High	High	Moderate
MODERATE	High	High	MODERATE	Moderate	Moderate
Minor	Moderate	Moderate	Moderate	Low	Low
Negligible	Low	Low	Low	Low	Low

[a] A description of impact levels and probability of occurrence levels is given in the appendix.

4.7.H. Recommendation

Subject to the recommendation in section 4.6.H, we recommend that the Service de Police de la Ville de Montréal establish a process for updating documentation, particularly with regard to tests conducted on backup copies of the information and communications technology systems used specifically for certain police activities.

Business unit's response:

[TRANSLATION] A process for updating documentation will be established, particularly in the area of testing backup copies for our ICT systems, including those used specifically for certain police activities. ***(Planned completion: May 2017)***

5. Conclusion

Overall, we may conclude that the City does not have an information and communications technology disaster recovery program (ICT) that would enable it to deal with the risks of major disasters affecting its information and telecommunications systems. There is no doubt that the City would resort to improvising its responses. As a result, it is likely that many ICT systems and infrastructures on which the City's critical activities depend would not be recovered in a timely manner.

Nevertheless, the computer-assisted dispatch system (Répartition assistée par ordinateur [RAO]) of the Service de sécurité incendie de Montréal (SIM) and the 9-1-1 Emergency Centre systems of the Service de Police de la Ville de Montréal (SPVM) have adequate ICT recovery measures in place.

The City has mandated the Service des technologies de l'information (STI) to maintain and support the modernization of the City's key technological services. The disaster recovery program is an essential part of sound ICT management.

Based on the results of our audit, we think that the STI is not fulfilling its role in ICT recovery. The STI has not:

- established a structured, common approach to ICT recovery management;
- made ICT recovery part of its major incident management process;
- conducted risk and impact analyses for all its activities;
- adequately documented ICT recovery strategies and plans;
- systematically performed ICT recovery exercises, except for the centralized IBM environment. In this case, the exercises performed are too limited to validate recovery processes effectively.

It should be noted that no formal process is in place for business units to transmit their minimum ICT recovery requirements to their service providers (internal or external).

Within the Service de l'eau, the Direction de l'eau potable (DEP) and the Direction de l'épuration des eaux usées (DEEU) have each undertaken an analysis process to produce business continuity plans and ICT recovery plans for their in-plant activities. While there is no question that this work is useful, these two management teams used different but complementary methodologies. They have no recovery plans or regular recovery exercise programs in place. However, because of the industrial nature of their operations, redundancy mechanisms are integrated into the technological architecture of the process control systems for drinking water and waste water treatment plants. These elements are part of ICT recovery strategies and reduce the risks of a disaster.

Table 32 shows the overall results of our audit based on the risks identified.

Table 32 – Overall Results for Each Risk Area

Risk area	Inherent risk[a]	Residual risk[b]				
		STI	Service de l'eau	SIM	SPVM	
					9-1-1	Other
Organizational structure of the information and communications technology disaster recovery program System recovery objectives are not relevant, measurable or achievable. Operational responsibilities and roles are not defined. Resources are lacking and staff assignment is temporary. No ICT recovery culture.	HIGH	HIGH	MODERATE	LOW	LOW	MODERATE
Major incident management structure No coordination or decision-making elements are in place at the time of an incident, emergency or disaster. This leads to a loss of efficiency, a risk of interference and poor communication among stakeholders.	CRITICAL	HIGH	MODERATE	LOW	LOW	LOW
Risk and impact analysis and information and communications technology recovery strategies Without a comprehensive, detailed risk impact analysis, several critical ICT systems are not identified and cannot be properly recovered. Essential public services are not maintained.	CRITICAL	CRITICAL	MODERATE	HIGH	HIGH	HIGH
Information and communications technology recovery plans and procedures The plans and procedures required to implement ICT recovery strategies are non-existent, with the result that the ICT systems required by business units' critical activities are not available, and essential public services are not maintained.	CRITICAL	CRITICAL	MODERATE	LOW	LOW	LOW
Information and communications technology recovery training Those responsible for implementing ICT recovery plans are poorly informed or receive no training on their roles and responsibilities. As a result, they will not be able to maintain critical systems in the event of a disaster.	HIGH	HIGH	MODERATE	LOW	LOW	LOW
Information and communications technology recovery exercise programs If drill exercises for ICT recovery plans are not performed regularly or adequately, the plans cannot be validated effectively. This loss of efficiency during the management of an emergency can jeopardize essential public services.	CRITICAL	CRITICAL	MODERATE	HIGH	LOW	MODERATE
Updating information and communications technology recovery documentation ICT recovery documentation and information are obsolete because they have not been updated. If a disaster occurs, critical systems will not be recovered in a timely manner. Essential public services will no longer be available.	CRITICAL	CRITICAL	MODERATE	LOW	LOW	MODERATE

[a] Gross risk without taking monitoring mechanisms into account.
[b] Exposure to risk following an evaluation of the monitoring mechanisms in place.

ICT recovery management is a key component of responsible ICT management. In this regard, the STI should implement the following constituent parts of an ICT disaster recovery program:

- specific management frameworks that will establish objectives, scope, requirements and roles and responsibilities. These management frameworks should apply to all business units that manage ICT infrastructures and systems;
- an accountability mechanism that is based on an understanding of the program objectives, goals and expectations;
- centralized, standardized tools and access to internal expertise.

Business units that manage ICTs should implement the measures required to achieve the ICT disaster recovery program objectives, specifically in the following areas:

- program structure;
- organization of major incident management;
- risk and impact analysis and ICT recovery strategies;
- ICT recovery plans and procedures;
- training, exercises and documentation updates.

Business units should inform the STI and, if applicable, any other service provider involved, of their ICT recovery needs.

We believe that if the City introduces an ICT disaster recovery program that is aligned with the business continuity program, it would have the necessary measures in place to deal with the risk of a major disaster affecting its information and telecommunications systems. This would reduce impacts on public services.

6. Appendices

6.1. Description of Risk Levels

Impact	Probability of occurrence				
	Highly probable	Probable	Possible	Unlikely	Improbable
Catastrophic	CRITICAL	CRITICAL	CRITICAL	HIGH	HIGH
Major	CRITICAL	HIGH	HIGH	HIGH	MODERATE
Moderate	HIGH	HIGH	MODERATE	MODERATE	MODERATE
Minor	MODERATE	MODERATE	MODERATE	LOW	LOW
Negligible	LOW	LOW	LOW	LOW	LOW

6.2. Description of Impact Levels

Impact Levels	Description
Catastrophic	Disastrous operational, financial and legal consequences, as well as disastrous consequences for the City's reputation following a disaster, resulting in, for example, a shutdown of a critical ICT system, with direct impacts on public health and safety.
Major	Major operational, financial and legal consequences and damage to the City's reputation.
Moderate	Impacts on the City's operations leading to moderate financial and legal consequences and damage to the City's reputation.
Minor	Minor impacts on the City's operations and business units. Loss of public confidence in the City unlikely.
Negligible	Very minor, or non-existent impacts on the City's operations. No public impact.

6.3. Description of Levels of Probability of Occurrence

Probability of occurrence	Description
Highly probable	Will occur in most circumstances.
Probable	Will probably occur in most circumstances.
Possible	Should occur at some point.
Unlikely	Should not occur.
Improbable	May occur only in exceptional circumstances.