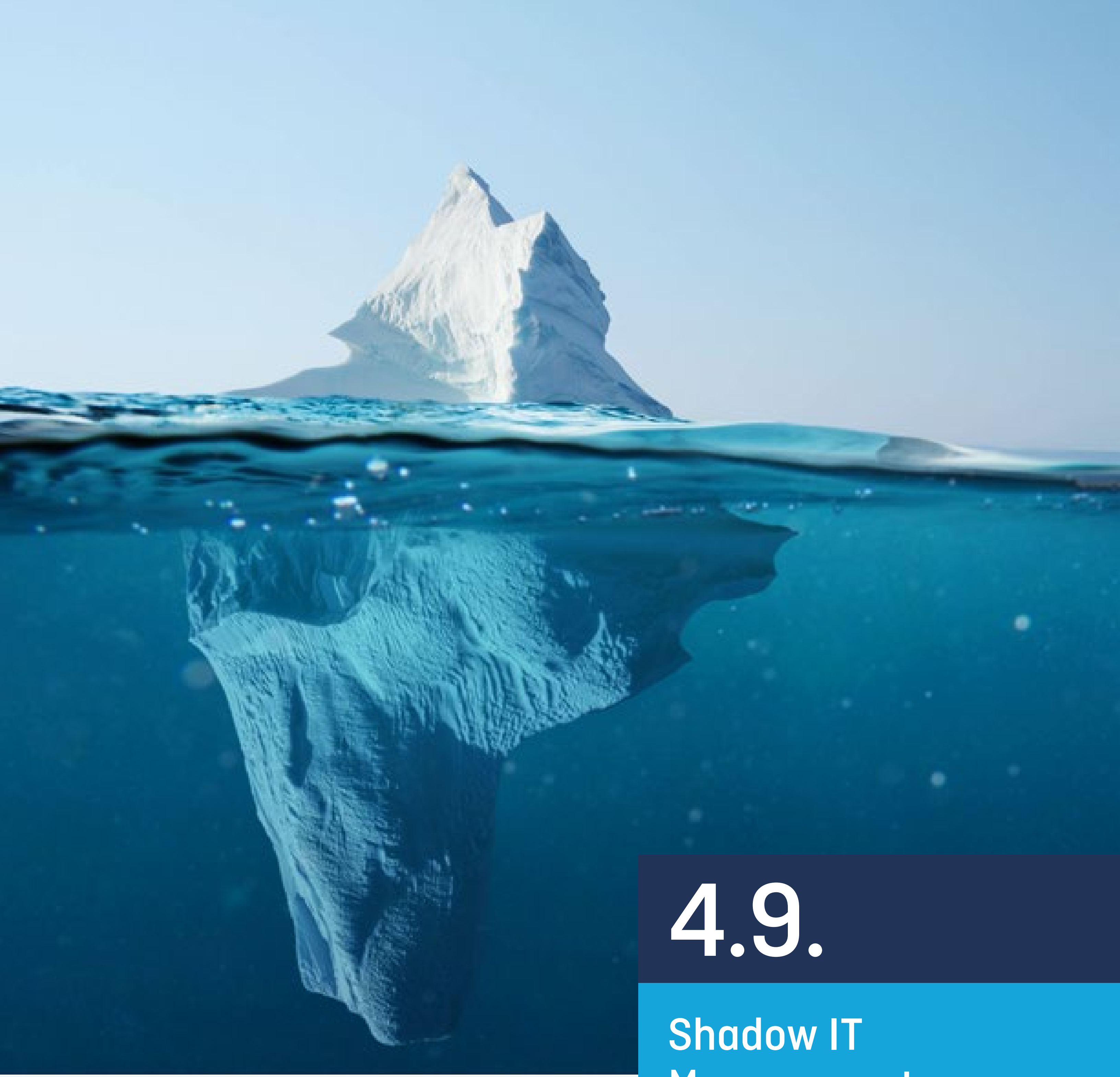

4.9.

Shadow IT Management

April 16, 2020

2019 Annual Report
Auditor General of the Ville de Montréal

OBJECTIVE

Determine whether the control mechanisms established for Shadow IT management within the Ville de Montréal (the City) can help bring the risks of losing data confidentiality, integrity and availability down to an acceptable level.

Shadow IT is defined as the use of tools or applications unknown to the Service des technologies de l'information (STI).

RESULTS

Based on our audit work, we conclude that the City has not established control mechanisms to ensure sound Shadow IT management. Without governance for Shadow IT management or a process for detecting any Shadow IT being produced, the City has only partial knowledge of its use by business units.

These findings, combined with the City's delay in delivering its technology projects, make it increasingly likely that business units will turn to Shadow IT solutions.

Several improvements are required in the areas of governance regulating Shadow IT management, the awareness and training strategy for Shadow IT and the process for detecting it.

Here are the main areas in which improvements are needed:

- No governance is in place for Shadow IT management to define Shadow IT, the roles and responsibilities of the stakeholders involved and security measures for dealing with it.
- The Cybersecurity awareness and training strategy, which is applicable to the City as a whole, does not place enough emphasis on aspects associated with Shadow IT.
- No process for detecting Shadow IT has been implemented.
- To date, there has been no management of Shadow IT solutions, which consists in evaluating them and then, based on the results of this evaluation, either approving or rejecting them.
- Since there is no governance to regulate Shadow IT management, there are no sound practices expected of business units on their use of Shadow IT.
- For four of the nine boroughs that use it, the GoFinance application sold by Saint-Laurent borough is not covered by a service agreement, as required by the *Charter of Ville de Montréal, metropolis of Québec*.

In addition to these results, we have formulated various recommendations for business units.

The details of these recommendations and our conclusion are outlined in our audit report, presented in the following pages.

It should be stressed that business units were given the opportunity to agree to this, and we will submit their comments later.

TABLE OF CONTENTS

LIST OF ACRONYMS

BC	borough council
IT	Information technology
STI	Service des technologies de l'information
TCEP	Three-year capital expenditures program

1. BACKGROUND

Like other large cities, organizations or companies, the Ville de Montréal (the City) is witnessing a growing number of applications, software, devices or services on its computer network, without the explicit authorization of the Service des technologies de l'information (STI).This practice is designated by the commonly used term "*Shadow IT*"[1].

1.1. Definition of Shadow IT

In the City, management of Information technology (IT) is centralized, mainly under the STI. Shadow IT includes the use of any information system component without the knowledge of the STI. As a result, this becomes an element outside of the STI's ownership or control.

One example of Shadow IT is the use of tools or applications whose existence is unknown to the STI. But the STI cannot protect something it does not know about, which is why it is important for it to be aware of all ITs, including all applications, that are being used.

Here are a few common examples of Shadow IT:

- Collaboration tools;
- Task management tools;
- Specialized databases;
- Enterprise resource planning (ERP) tools;
- Financial analysis software;
- File transfer or data exchange solutions;
- IT projects hidden from the view of IT management.

[1] "*Shadow IT*" is a term frequently used to designate information and communication systems produced and implemented within organizations without the approval of information systems management.

In the past, Shadow IT arose from employees' desire to access specific hardware, software and Internet services without having to go through the processes required by the STI. These days, it has expanded further, offering, free of charge, a wide range of online services for which users register without taking into account potential risks to the City's computer systems and data security.

The consumerization of IT, with employees bringing popular mass market technologies into the organization, makes it easy for them to deploy technologies without the STI being aware of it.

The use of Shadow IT is generally symptomatic of users' tendency to believe that IT management does not meet their needs sufficiently and that they therefore cannot do otherwise. Their understanding of the services provided by IT management also has an effect on the practice of Shadow IT.

1.2. Main Advantages of Shadow IT

In the perception of users, one of the main reasons why employees turn to Shadow IT is a desire to work more efficiently. In order to work more quickly and communicate more rapidly, they use applications, services and data sharing and storage functions without going through the IT sector because they consider this to be more efficient and less expensive. In other words, by using technologies they need without permission, employees feel they are increasing their productivity.

It is reasonable to distinguish good Shadow IT from bad Shadow IT and thereby find the right balance that allows employees to use solutions that work for them while at the same time allowing IT management to control their use through appropriate security measures.

1.3. Main Shadow IT Issues

According to a study by Gartner,[2] by 2020, one third of successful attacks encountered by companies will target their Shadow IT resources.

Gartner further stated that:

> *"[...] Business units deal with the reality of the enterprise and will engage with any tool that helps them do the job. Companies should find a way to track shadow IT, and create a culture of acceptance and protection versus detection and punishment."*

In 2016, Microsoft[3] reported that more than 80% of employees in organizations surveyed admitted to having used IT solutions such as SaaS[4] cloud computing[5] applications without their IT management having approved them for business.

The main Shadow IT issues are as follows:

- **Security risk:** The main Shadow IT risk is a security risk. Substantive security measures are taken to protect software and hardware approved by IT sectors, which is not the case with unapproved software and hardware. The City is more at risk for successful cyberattacks targeting its Shadow IT.
- **Leakage, loss, theft or corruption of data:** Some applications, such as data sharing or storage services like Google Docs[6] or DropBox[7] can cause leakage of sensitive, strategic or financial data. This can also create a hidden gateway and result in the loss, theft or corruption of data.
- **Non-compliance:** These applications also pose a risk of non-compliance with laws and regulations such as the *Act respecting access to documents held by public bodies and the protection of personal information*.
- **Bandwidth capacity:**[8] Tools and applications used without the authorization of IT management can affect the bandwidth available due to increased use and prove harmful for other users.

[2] Gartner, "Gartner's Top 10 Security Predictions 2016," June 15, 2016 https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

[3] Microsoft, "Microsoft Cloud App Security is generally available," April 6, 2016 https://www.microsoft.com/security/blog/2016/04/06/microsoft-cloud-app-security-is-generally-available/

[4] Software as a Service is a software distribution model in which a third-party supplier hosts applications and makes them available for its clients through the Internet.

[5] Cloud computing is a method of processing a client's data, to be used via the Internet in the form of services provided by a service provider.

[6] Internet-based word processing software and Google Office Suite.

[7] Online file sharing and storage service.

[8] Amount of information that can be sent simultaneously through a transmission line.

- **Hidden costs:** If it is not IT management that carries out the tool development, configuration and testing, users will do this during their work hours and will not be performing the tasks for which they are remunerated during this time.
- **Reputation:** The City's reputation can be greatly damaged by successful attacks targeting components not managed by IT management, and this can be accompanied by a loss of credibility and the trust of its citizens.

These risks are not always known to users, even if instances of cyberattacks and data theft are more and more present in the media.

2. PURPOSE AND SCOPE OF THE AUDIT

Pursuant to the provisions of the *Cities and Towns Act*, we conducted a performance audit mission on Shadow IT management. We carried out this mission in accordance with the Canadian Standard on Assurance Engagements (CSAE 3001) of the CPA Canada Handbook – Assurance, as well as with the other Canadian assurance standards that apply to the public sector, as issued by the Auditing and Assurance Standards Board, with the support of CPA Canada.

The purpose of this audit was to determine whether the control mechanisms established for Shadow IT management within the City can help bring the risks of losing data confidentiality, integrity and availability down to an acceptable level.

The responsibility of the Auditor General of the Ville de Montréal (the City) consists of providing a conclusion on the audit's objective. For that purpose, we gathered sufficient and appropriate evidence to support our conclusion and gain reasonable assurance. Our evaluation is based on the criteria that we deemed valid under the circumstances. These criteria are presented in Appendix. 5.

The Auditor General of the Ville de Montréal applies the *Canadian Standard on Quality Control* (CSQC) 1 of the CPA Canada Handbook – Assurance. Consequently, he maintains an extensive quality control system that includes documented policies and procedures with respect to compliance with the rules of ethics, professional standards and applicable legal and regulatory requirements. He also complies with the rules on independence as well as with the other rules of ethics of the *Code of ethics of chartered professional accountants*, which are based on the fundamental principles of integrity, professional competence and diligence, confidentiality and professional conduct.

Our audit focused solely on Shadow IT applications or software tools, more specifically, those purchased or available free of charge from cloud computing. In brief, these are applications not managed by and not known to the STI that are used to meet specific needs.

We excluded from the scope of our audit hardware[9] that can meet the definition of Shadow IT and boroughs not managed by the STI because their IT purchases do not constitute Shadow IT.

To conduct our audit, we selected the following business units:

- Saint-Laurent borough;
- Le Plateau-Mont Royal borough;
- Mercier–Hochelaga-Maisonneuve borough;
- Côte-des-Neiges–Notre-Dame-de-Grâce borough;
- Ville-Marie borough;
- LaSalle borough;
- Le Sud-Ouest borough;
- Villeray–Saint Michel–Parc-Extension borough;
- the Service de l'environnement;
- the Service des ressources humaines;
- the Service de l'infrastructure du réseau routier;
- the STI.

Our audit work focused on the period from July 17, 2019, to January 16, 2020. It consisted in conducting interviews with staff, examining various documents and conducting surveys that we deemed appropriate to obtain the necessary evidentiary information. We also took into account information that was sent to us up to April 2020.

Upon completing our audit work, we submitted a draft audit report to managers of each audited business unit for discussion purposes. The final report was then forwarded to the Direction générale and to the management of each business unit involved in order to obtain action plans and timelines for implementing the recommendations concerning them. A copy of the final report was also submitted to the deputy director-general of the Service aux citoyens, to the deputy director-general of Mobilité et attractivité, to the deputy director-general of Qualité de vie, to the director of the Service de la concertation des arrondissements and to borough directors not directly targeted by our audit, so that they could implement recommendations when the situation justifies it.

[9] The hardware could be a printer or a server, for example.

3. AUDIT RESULTS

3.1. Governance

3.1.A. Background and Findings

Governance for Shadow IT management should be formally established to limit the use of applications not approved and not managed by the STI. This governance consists in defining a management framework for Shadow IT management (i.e., in the form of directives and standards) accessible to all the City's employees through its Intranet. The purpose of this management framework is to define what is meant by Shadow IT and the roles and responsibilities involved, and to put together a list of factors aimed at preventing high-risk behaviours, leaks or theft of information.

We noted that there is no management framework for Shadow IT management. The definition of this term within the STI itself varies from one resource to another. The constitution of the City, which is subdivided into boroughs, each managed by a separate borough council (BC), increases the complexity of the application of shared governance. In this context, governance is a major issue within the City.

We noted that Shadow IT management is not covered by any management framework. The STI alone is not responsible for developing a management framework for Shadow IT management, because it actually does not manage all the business units' computer systems. Governance must originate from the City's Direction Générale, which has the appropriate authority to secure the commitment of all City's business units and employees and ensure that they implement and comply with it.

Table 1 shows the profile of IT management in boroughs.

Table 1 – **Profile of IT Management in Boroughs**

BOROUGHS	IT MANAGEMENT
Ahuntsic-Cartierville	STI
Côte-des-Neiges–Notre-Dame-de-Grâce	STI
Le Plateau-Mont-Royal	STI
Le Sud-Ouest	STI
Mercier–Hochelaga-Maisonneuve	STI
Rivière-des-Prairies–Pointe-aux-Trembles	STI
Rosemont–La Petite-Patrie	STI
Ville-Marie	STI
Villeray–Saint-Michel–Parc-Extension	STI
Lachine	In the process of being transferred to the STI
LaSalle	In the process of being transferred to the STI
Pierrefonds-Roxboro	In the process of being transferred to the STI
Verdun	In the process of being transferred to the STI
Anjou	Borough
L'Île-Bizard–Sainte-Geneviève	Borough
Montréal-Nord	Borough
Outremont	Borough
Saint-Laurent	Borough
Saint-Léonard	Borough

The lack of a management framework providing formal guidelines for Shadow IT within the City makes it impossible for the STI to promote sound practices regarding its use. This situation could lead to the use of applications that are not known to, not managed by and not approved by the City's STI, as has been found to be the case in some of the business units audited.

Roles and responsibilities that are not defined, not disclosed, and not known to stakeholders in the management of Shadow IT could lead to a disparity in the right to use it, an increase in its presence, breaches of and non-compliances with its management framework. This in turn could lead to undetected security breaches, theft or loss of strategic, confidential data (e.g., personal information).

RECOMMENDATION

3.1.B. We recommend that the Direction générale define governance for Shadow IT management, disseminate the associated management frameworks and keep them up to date.

RESPONSE

3.1.B. *The audit report was issued to the business unit concerned between February 25 and April 15, 2020. The business unit agrees with the recommendation. The Bureau du vérificateur général has asked the business unit to establish an action plan for implementing this recommendation by August 7, 2020.*

3.2. Awareness and Training

3.2.A. Background and Findings

An awareness and training strategy for Shadow IT increases awareness, provides training and instills behaviours that are in line with the City's guidelines in this area. The strategy helps make employees aware of potential risks related to the use of Shadow IT, such as theft, disclosure or loss of strategic or confidential information (e.g., personal information), the spread of security breaches and damage to the City's reputation. It is therefore aimed at mitigating these risks to an acceptable level for the City.

We noted that the City has a Cybersecurity awareness and training strategy, which can be consulted to gain a better understanding of Cybersecurity, recognize threats and prevent them through good habits. The STI portal of the City's Intranet has several training capsules for this purpose.

This strategy is part of a project aimed at *"Increasing employees' awareness of cybersecurity and training them: Improving users' awareness of their responsibility to comply with security frameworks and protect information assets."* However, the scope of this strategy does not include aspects associated with Shadow IT.

The Cybersecurity awareness and training strategy's lack of emphasis on the use of Shadow IT and the responsibilities that are incumbent on all employees could result in malfunctions in critical applications and breakdowns in the City's computer network arising from successful cyberattacks targeting their Shadow IT resources, and it could cause strategic, confidential data (e.g., personal information) to lose its confidentiality.

RECOMMENDATION

3.2.B. We recommend that the Service des technologies de l'information add aspects associated with Shadow IT to its Cybersecurity awareness and training strategy applicable to the City as a whole.

RESPONSE

3.2.B. *The audit report was issued to the business unit concerned between February 25 and April 15, 2020. The business unit agrees with the recommendation. The Bureau du vérificateur général has asked the business unit to establish an action plan for implementing this recommendation by August 7, 2020.*

3.3. Shadow IT Detection

3.3.A. Background and Findings

Shadow IT detection consists in using manual or automated procedures for discovering the presence of Shadow IT. It is aimed at providing an accurate picture of the extent of Shadow IT use and providing assurance to the City that its computing environment consists of applications and software approved by the STI. These should be subject to significant security measures, which is generally not the case for Shadow IT applications and software.

We noted that the City does not have a process for detecting Shadow IT. In fact, no detection tool has been implemented on the City's computer network. Only one proof of concept of a Shadow IT detection product is under way, with no intent to purchase, and it has been so for more than a year. We obtained a preliminary report from the information security team on the situation regarding Shadow IT use. This report was intended as a reference source for identifying the Shadow IT solutions detected. We found, for example, cloud storage services and online document conversion services. However, its insufficient level of detail did not provide us with information on the type of data transferred or on the users of these solutions. As a result, the STI has only partial knowledge of its use by business units.

The fact that no process is in place for detecting Shadow IT could cause it to spread, leading to security breaches without the STI knowing it, and this in turn could result in the theft or loss of strategic or confidential data (e.g., personal information).

RECOMMENDATION

3.3.B. We recommend that the Service des technologies de l'information introduce a process for detecting Shadow IT.

RESPONSE

3.3.B. *The audit report was issued to the business unit concerned between February 25 and April 15, 2020. The business unit agrees with the recommendation. The Bureau du vérificateur général has asked the business unit to establish an action plan for implementing this recommendation by August 7, 2020.*

3.4. Shadow IT Management

3.4.A. Background and Findings

Sound Shadow IT management consists in evaluating whether it represents the best solution, based on the risks involved, and thereby determining whether its use is appropriate or not. Following this evaluation, a decision should be made either to approve or reject this Shadow IT solution, and the corresponding subsequent measures should be taken.

We found that to date there has been no Shadow IT management, let alone a process for detecting it.

In addition, the STI has not defined a list of the permitted applications to help guide users in choosing solutions.

The absence of Shadow IT management by the STI could lead to an overabundance of Shadow IT solutions that it has not authorized. This could cause security breaches ranging up to the theft or loss of strategic or confidential data (e.g., personal information).

RECOMMENDATION

3.4.B. We recommend that the Service des technologies de l'information establish a process for managing Shadow IT, subject to recommendations 3.1.B and 3.3.B.

RESPONSE

3.4.B. *The audit report was issued to the business unit concerned between February 25 and April 15, 2020. The business unit agrees with the recommendation. The Bureau du vérificateur général has asked the business unit to establish an action plan for implementing this recommendation by August 7, 2020.*

3.5. Use of Shadow IT by Business Units

3.5.A. Background and Findings

The use of Shadow IT within organizations arises from needs and requests for specific computer services for business units processes not delivered by the IT sector.[10] This reality requires the implementation of sound management practices regarding the use of Shadow IT by business units to prevent the emergence of risks associated with it.

Without management frameworks within the City, sound practices recommend to business units to keep an inventory of the Shadow IT used, to confirm that no equivalent product is supplied by the STI, to conduct a risk analysis before choosing a Shadow IT solution and, finally, to define action plans for mitigating the risks identified.

The establishment of these sound practices can help mitigate risks such as a loss of uniformity in the City's computer equipment and of control of strategic, confidential data.

To get an idea of the extent of their use of Shadow IT, we selected six business units:

- Le Plateau-Mont-Royal borough;
- Mercier–Hochelaga-Maisonneuve borough;
- Côte-des-Neiges–Notre-Dame-de-Grâce borough;
- The Service de l'environnement;
- The Service des ressources humaines;
- The Service de l'infrastructure du réseau routier.

During our interviews with these business units, they mentioned that they do not obtain all the services they request and expect from the STI, which does not necessarily understand their needs or their realities. For example, the use by some of them of the GoFinance application (developed and sold by Saint-Laurent borough) arises from specific needs not covered (e.g., viewing data using a Web interface, probing for financial information and monitoring expenditures). They have been awaiting the Qlik Sense application, which is supposed to fulfil these needs, for more than two years.

[10] Reference: Atos, "Shadow IT: a 20% increase expected in 2015" London, March 30, 2015 https://atos.net/fr/2015/communiques-de-presse/communiques-generaux_2015_03_30/pr-2015_03_30_01

Similarly, as part of another of our audit missions on the STI's Management of the Bureau de projets:

- We noted that 99 projects are provided for in the Three-year capital expenditures program (TCEP) 2020-2022, with a budget varying from $83 million to $89 million for each of these three years.
- Of the 41 IT projects entered in the TCEP for 2019-2021 and 2020-2022 for which a budget was required, we found that the schedules of about 50% of them were postponed by two or more years.
- The same statistic applies to the 28 IT projects entered in the TCEP that were prioritized for 2020 by the STI. In fact, 13 of these 28 prioritized projects were postponed by two or more years in the last TCEP.

These postponements in the delivery of IT projects could increase the likelihood that business units will turn to Shadow IT solutions originating from cloud computing or other applications that are not under the control of the STI.

Since the City does not have a detection process, there is no inventory that would have enabled us to determine which Shadow IT applications were used by business units. Furthermore, at meetings held at the start of our audit, the six business units selected had brought to our attention the fact that they did not know whether their employees were using Shadow IT solutions, because this concept was unknown to them due to the lack of a municipal management framework for it. As a result, none of the business units interviewed had created a Shadow IT inventory.

After explaining to them what Shadow IT is all about, we obtained their lists of Shadow IT applications that were produced manually, and based on their good faith. From an analysis of these lists, we noted the presence of applications originating from cloud computing, as well as the use of applications that were purchased or developed internally and installed locally on the City's computer systems to meet specific needs.

Table 2 shows the Shadow IT profile according to information obtained from each business unit interviewed.

Table 2 – Shadow IT Profile According to the Information Obtained from Each Business Unit Interviewed

BUSINESS UNITS (BOROUGHS AND DEPARTMENTS)	SHADOW IT APPLICATION	INTERNET APPLICATION	AT-RISK APPLICATION[11]
Le Plateau-Mont-Royal	1	1	1
Côte-des-Neiges–Notre-Dame-de-Grâce	1	1	1
Mercier–Hochelaga-Maisonneuve	5	0	0
Service de l’environnement	0	N/A	N/A
Service des ressources humaines	38	10	1
Service des infrastructures du réseau routier	37	2	2
TOTALS	**82**	**14**	**5**

[11] Internet applications that may contain strategic or confidential data.

Table 3 shows the four Internet applications that may contain strategic or confidential data, the associated risks and the boroughs using them.

Table 3 – Internet Applications That May Contain Strategic or Confidential Data, the Associated Risks and Boroughs Using Them

INTERNET APPLICATIONS THAT MAY CONTAIN STRATEGIC OR CONFIDENTIAL DATA	TYPE OF RISK	BOROUGHS USING THEM
Asana **Project monitoring tool.** Example of data: working documents, information on the major deliverables of a project, breakdown of projects, tasks to be executed.	• Security risk; • Leakage, theft or corruption of data on deliverables and on the breakdown of a project; • Reputation.	• Côte-des-Neiges–Notre-Dame-de-Grâce; • Service des ressources humaines.
DropBox **Document filing tool.** Example of data: documents of consultants and contractors, videos, photos, plans.	• Security risk; • Leakage, theft or corruption of data on the working documents of consultants; • Reputation.	• Service des infrastructures du réseau routier.
Monday **Project resource planning tool.** Example of data: project progress, statements of work completed and expenditures made serving as a basis for payments to be made to the contractor.	• Security risk; • Leakage, theft or corruption of data on statements of work completed and expenditures made; • Reputation.	• Service des infrastructures du réseau routier.
Trello **Project management tool used to simplify collaboration.** Example of data: task management charts, geolocation data (mainly addresses), attached documents, photos, videos.	• Security risk; • Leakage, theft or corruption of data on attached documents; • Reputation.	• Le Plateau-Mont-Royal.

As a result of the lack of a management framework and a specific awareness and training strategy for Shadow IT, business units do not have the knowledge or skills needed to implement the sound management practices expected of them.

Improper use of Shadow IT by business units could result in risks, such as loss of uniformity in the City's computer equipment and security breaches with an impact on the confidentiality and integrity of strategic, confidential data.

RECOMMENDATION

3.5.B. **We recommend that Le Plateau-Mont-Royal, Côte-des-Neiges–Notre-Dame-de-Grâce, Mercier–Hochelaga-Maisonneuve boroughs, the Service des ressources humaines and the Service des infrastructures du réseau routier, pending the implementation of recommendations 3.1.B and 3.2.B:**

- **keep their Shadow IT inventory up to date;**
- **confirm that no equivalent product is supplied by the Service des technologies de l'information;**
- **conduct a risk analysis before deciding on a Shadow IT solution;**
- **establish action plans to mitigate the risks identified.**

RESPONSE

3.5.B. *The audit report was issued to the business units concerned between February 25 and April 15, 2020. The business units agree with all the recommendations concerning them. The Bureau du vérificateur général has asked them to establish action plans for implementing these recommendations by August 7, 2020.*

RECOMMENDATION

3.5.C. We recommend that the Service des technologies de l'information, pending the implementation of recommendations 3.1.B and 3.2.B, support business units and increase their awareness for the purpose of:

- **keeping their Shadow IT inventory up to date;**
- **confirming that no equivalent product is supplied by the Service des technologies de l'information;**
- **conducting a risk analysis before deciding on a Shadow IT solution;**
- **establishing action plans to mitigate the risks identified.**

RESPONSE

3.5.C. *The audit report was issued to the business unit concerned between February 25 and April 15, 2020. The business unit agrees with the recommendation. The Bureau du vérificateur général has asked the business unit to establish an action plan for implementing this recommendation by August 7, 2020.*

3.6. Service Agreement for the Sale of Applications by a Borough

3.6.A. Background and Findings

The *Charter of Ville de Montréal, metropolis of Québec* (hereinafter the City's charter) requires that a service agreement be developed for the sale of applications by a borough to another borough. Section 85.1 stipulates that:

> *"A borough council may, on the conditions it determines, provide to the council of another borough any service related to one of its jurisdictions. The resolution offering such a provision of service becomes effective on the adoption of a resolution accepting the offer."*

So, the conclusion of a service agreement between two boroughs requires that a resolution be passed by each BC. The adoption of these resolutions is proof of the conclusion of the service agreement between the two boroughs.

A borough that has developed an application internally for its own needs can use it by virtue of section 144 of the City's charter, which is worded as follows:

> *"The borough council is responsible for the management of the borough budget adopted by the city council [...]."*

We noted that Saint-Laurent borough sold the GoFinance application it developed to nine of the City's boroughs. According to information obtained from boroughs, this application was meeting real needs not served by the STI. In fact, the GoFinance application can be used to view data in the SIMON accounting system through an interface accessible from a Web browser. It helps probe for financial information on the operating budget, invoices and purchase orders issued to suppliers and the TCEP project expenditures for the last five years.

Saint-Laurent borough sells the GoFinance application for $50,000 and charges annual fees of $10,000 for support.

Table 4 lists the ten boroughs that use the GoFinance application.

Table 4 – **List of the Ten Boroughs That Use the GoFinance Application**

BOROUGHS	UNDER STI MANAGEMENT
Côte-des-Neiges–Notre-Dame-de-Grâce	Yes
Le Plateau-Mont-Royal	Yes
Le Sud-Ouest	Yes
Mercier–Hochelaga-Maisonneuve	Yes
Ville-Marie	Yes
Villeray–Saint-Michel–Parc-Extension	Yes
LaSalle	In Progress
Pierrefonds-Roxboro	In Progress
Saint-Laurent	No
Saint-Léonard	No

We consider GoFinance to be a Shadow IT application, because eight of the boroughs under the control of the STI use it without having informed the department about it beforehand.

With respect to the proposed service partnership agreement and the BC resolutions required to establish a service agreement, Table 5 presents our findings for the nine boroughs that purchased the GoFinance application.

Table 5 – **Boroughs That Purchased the GoFinance Application**

BOROUGHS	PROPOSED SERVICE PARTNERSHIP AGREEMENT (SAINT-LAURENT BOROUGH)	BOROUGH COUNCIL RESOLUTION TO SELL (SAINT-LAURENT BOROUGH)	BOROUGH COUNCIL RESOLUTION TO PURCHASE
Côte-des-Neiges–Notre-Dame-de-Grâce	Yes	Yes	Yes
LaSalle	Yes	Yes	Yes
Le Plateau-Mont-Royal	No	No	No
Le Sud-Ouest	No	No	No
Mercier–Hochelaga-Maisonneuve	No	No	No
Ville-Marie	Yes	Yes	Yes
Villeray–Saint-Michel–Parc-Extension	No	No	No
Pierrefonds-Roxboro	Yes	Yes	Yes
Saint-Léonard	Yes	Yes	Yes
TOTALS	**5**	**5**	**5**

So, although nine boroughs purchased the GoFinance application, only five of them, Côte-des-Neiges–Notre-Dame-de-Grâce, LaSalle, Ville-Marie, Pierrefonds-Roxboro and Saint-Léonard, have the proposed service partnership agreement with Saint-Laurent borough and have adopted the BC resolutions of the stakeholders involved in accordance with the City's charter.

The fact that there is no duly completed proposal for a service partnership agreement and that no BC resolutions were passed by boroughs is in violation of the City's charter. Furthermore, the fact that there is no accountability reporting on this situation would prevent elected officials, management and the City's business units from being aware of its existence.

RECOMMENDATION

3.6.B. We recommend that Saint-Laurent borough, as part of the sale of its GoFinance application:

- **define a proposed service partnership agreement and submit it to purchasing boroughs;**
- **present a resolution to its borough council to have it adopted.**

RESPONSE

3.6.B. *The audit report was issued to the business unit concerned between February 25 and April 15, 2020. The business unit agrees with the recommendation. The Bureau du vérificateur général has asked the business unit to establish an action plan for implementing this recommendation by August 7, 2020.*

RECOMMENDATION

3.6.C. We recommend that the boroughs of Le Plateau-Mont-Royal, Le Sud-Ouest, Mercier–Hochelaga-Maisonneuve and Villeray–Saint-Michel–Parc-Extension, as part of the purchase of the GoFinance application:

- **make sure they obtain the proposed service partnership agreement with Saint-Laurent borough;**
- **present a resolution to its borough council to have it adopted.**

RESPONSE

3.6.C. *The audit report was issued to the business units concerned between February 25 and April 15, 2020. The business units agree with all the recommendations concerning them. The Bureau du vérificateur général has asked them to establish action plans for implementing these recommendations by August 7, 2020.*

4. CONCLUSION

Based on our audit work, we conclude that the Ville de Montréal (the City) has not established control mechanisms to ensure sound Shadow IT management. Without governance for Shadow IT management or a process for detecting any Shadow IT being produced, the City has only partial knowledge of its use by business units.

These findings, combined with the City's delay in delivering its Information technology (IT) projects, make it increasingly likely that business units will choose solutions other than those offered by the Service des technologies de l'information (STI), in other words, Shadow IT solutions.

In fact, we find significant improvements need to be made in the areas of a management framework for Shadow IT management, an awareness and training strategy for dealing with Shadow IT and a process for detecting it.

More specifically, here is a breakdown according to the following evaluation criteria:

Evaluation Criterion – Governance

The City does not have a management framework for the main strategic guidelines for managing Shadow IT.

The STI is therefore unable to promote sound practices concerning the use of Shadow IT, to ensure that business units have a uniform understanding of it or to develop and implement requirements needed for the establishment of minimum controls.

Roles and responsibilities related to this process have not been formally defined.

Evaluation Criterion – Awareness and Training

The City has a Cybersecurity awareness and training strategy. However, because of the limited scope of this strategy, not enough emphasis is placed on aspects associated with Shadow IT.

Evaluation Criterion – Detection of Shadow IT

The City does not have a process for detecting Shadow IT. No Shadow IT detection product has been officially implemented on the City's computer network. Only one proof of concept of a detection product is under way, with no intent to purchase. At this point, the STI has no detailed report on the use of Shadow IT in the City.

Evaluation Criterion – Shadow IT Management

No Shadow IT management has been established to evaluate the risks associated with Shadow IT solutions being produced in the City and, based on the results of this evaluation, to approve or reject these solutions.

Evaluation Criterion – Use of Shadow IT by Business Units

While five of the six business units in our sample use Shadow IT applications, there are no sound practices expected of business units in their use of Shadow IT in place. As a result, there is no governance for Shadow IT management and no awareness and training strategy for dealing with this issue.

Evaluation Criterion – Service Agreement for the Sale of an Application by a Borough

GoFinance, which is a Shadow IT application developed by Saint-Laurent borough, was sold to nine of the City's boroughs. Only five of them comply with the requirements of the City's charter.

5. APPENDIX

5.1. Objective and Evaluation Criteria

Objective

Determine whether the control mechanisms established for Shadow IT management within the City can help bring the risks of losing data confidentiality, integrity and availability down to an acceptable level.

Evaluation Criteria

Criterion 1: Governance

The City has an existing management framework for Shadow IT to define the safety requirements, the inclination to adopt it and the acceptable use for Shadow IT.

The roles and responsibilities of the stakeholders involved in managing Shadow IT are defined, disclosed and known to them.

Criterion 2: Awareness and Training

Citywide awareness of Shadow IT for all municipal employees is incorporated in the training and awareness strategy.

Shadow IT training is given to targeted specialized staff.

Criterion 3: Shadow IT Detection

Processes are in place within the City to discover the use of Shadow IT quickly. These processes involve:

- reviewing unauthorized applications and software identified by discovery tools;
- monitoring network traffic to detect and review unapproved IT solutions;
- recording calls made to the technical assistance department and related incidents to detect and analyze systems that are not in the IT inventory.

Criterion 4: Shadow IT Management

Shadow IT solutions are evaluated on the basis of risks to determine whether their use is appropriate for the City.

Shadow IT solutions are approved or rejected by a competent authority.

Shadow IT solutions are classified based on the results of a risk assessment, and existing solutions are examined periodically as part of the risk assessment process.

Following the assessment, action is taken either to accept the Shadow IT solution and mitigate the associated risk or to reject it.

These actions consist in:

- listing detailed information on Shadow IT solutions in the IT inventory;
- defining the minimum controls required according to the classification of each Shadow IT solution;
- blocking Shadow IT solutions that were rejected and replacing them in a timely manner with endorsed applications.

Criterion 5: Use of Shadow IT by Business Units

- Business units keep their Shadow IT inventory up to date.
- Business units make sure that no equivalent product is supplied by the STI.
- Business units conduct a risk analysis before choosing a Shadow IT solution and define action plans to mitigate the risks identified.

Criterion 6: Service Agreement for the Sale of Applications by a Borough

Service agreements exist for each application sold by a borough.