3.1.

Information Technology Management Used For Remote Work

Service des technologies de l'information

January 19, 2022

2021 ANNUAL REPORT

Auditor General of the Ville de Montréal

3.1. Information Technology Management Used For Remote Work

Information Technology Management Used For Remote Work

Background

Remote work is a way of organizing work that has progressed over the last decades. Technology has made it possible for employees to do some of their regular work from home while still being connected to the office. This is often referred to as "telework" or "remote work."

On March 13, 2020, government guidelines to control the risk of contamination imposed remote work as the employment configuration that replaced all other forms.

Although this practice already exists within the City of Montréal (the City), a shift to remote work on a larger scale was necessary. Up to 4,500 employees work from home in remote work mode simultaneously, accessing the City's network remotely.

Purpose of the Audit

To determine whether the control mechanisms, put in place for managing the information technology (IT) used for remote work within the City, allow to provide the necessary equipment and secure remote access to the City's information technology assets to ensure that employees can continue to perform their work.

Results

We conclude that the City has put in place the control mechanisms to ensure the sound management of the information technology used for remote work.

Indeed, despite the public health emergency caused by the COVID-19 crisis, the City's Service des technologies de l'information (STI) quickly deployed all the necessary efforts in an exceptional context to put in place the technological environment as well as the security mechanisms required to allow all of its employees working remotely to continue their professional activities from home without any interruption of service.

These mechanisms include the STI's guidance on IT used for remote work, the remote work awareness and training strategy, the protection mechanisms surrounding City data access and the operations management surrounding remote workers' corporate equipment.

Main Findings

Remote Work Framework

- Several guidelines on good practices to be adopted by employees working remotely were developed within the organization. They were approved and distributed to all employees through the City's intranet.
- These guidelines provide the information required for employees to safely use IT to work remotely.

Remote Work Training

- Appropriate awareness and training on remote work and its components have been in place since March 2020.

Data Access Protection

- Appropriate authentication mechanisms are used by employees to access data located in the City's network in accordance with sound security practices. The screen lock on City laptops is automatically activated after a centrally defined period of inactivity.
- Appropriate software is installed and updated on all City devices remotely connected to the City's network to protect them from malicious attacks.

Operations Management

- In order to allow employees to work remotely, the STI put in place secure mechanisms to enable employees who do not have a City computer to use their personal computer. Since the beginning of 2021, nearly 2,200 laptops have been distributed to employees allowing them to work remotely. The STI has provided adequate computer support for remote workers.

  The infrastructure in place allows for appropriate redundancy of key components and includes a secure environment for remote work.

Glossary

Centralized Security Information and Event Management System (SIEM): is used to collect, track, and correlate logs and generate dashboards and reports.

Firewall: a device that protects all network traffic and has the ability to identify and block unwanted data traffic.

Intrusion Detection System (IDS): protects organizations from cyberattacks by monitoring network traffic for suspicious activity.

Intrusion Prevention System (IPS): monitors a network to reduce the impact of an attack by stopping malicious requests.

IT: information technology

Malware: contraction of malicious software, refers to software intended to harm the user, which can take the form of, for example, a computer virus.

RDP: Remote Desktop Protocol

Spyware: refers to software that collects personal data in order to send it to a third party.

STI: Service des technologies de l'information

Two-factor or strong authentication: combines something you know (password, confidential code) with something else that can be a biometric element, an object you own or an action you know how to do.

Virtual Private Network (VPN): a method of linking two remote computers through a single private connection, or tunnel, while using a larger network infrastructure, such as the web or a wide area network (WAN). Once activated, a VPN acts as a direct connection to a private network.

Table of Contents

1. Background

Remote work is a way of organizing work that has progressed over the last decades. New technologies have made remote work possible and are even essential to many companies' continued operation.

On March 13, 2020, government guidelines to control the risk of contamination imposed remote work as the employment configuration that replaced all other forms. At the end of March, 39.1% of Canadian workers were working remotely. Although this practice already exists within the City of Montréal (the City), a shift to remote work on a larger scale was required. Up to 4,500 employees simultaneously work from home in remote work mode, accessing the City's network from a distance. These resources come from the various business units.

The generalized rise of remote work multiplies exchanges and access to sensitive company data. Also, personal networks may be less well protected from cyberattacks than private corporate networks.

It is therefore essential to limit the risks as much as possible by putting in place the right tools and establishing secure practices to ensure sound management of the information technology used for remote work.

1.1. Definition of Remote Work

It is increasingly common for people to do at least some of their regular work at home rather than in the office. Technology has made it possible for workers to stay at home while being connected to the office by phone, Internet or email. This is often referred to as "remote work" or "telework."

There is no official definition of remote work in Québec. Studies on this topic define it based on two main components[1]:

- The existence of a remote workplace outside the conventional workplace;
- Remote work being performed using information and communication technology (ICT)[2].

Organizations therefore need to develop an internal policy or guideline to define remote work.

[1] Remote work – Chaire BMO – Université de Montréal.

[2] Smartphones, tablets, laptops and desktop computers.

1.2. Description of the Information Technology Used for Remote Work

The IT used to work remotely includes the City's remote computers, which are configured with remote access solutions. In addition, telecommunications equipment is in place to ensure the sound management of data transfers between remote computers and the City's computer network.

The City uses Remote Desktop Protocol (RDP) technology for personal computers and Virtual Private Network (VPN) technology for the City's computers as a method of authentication to access corporate data and applications.

1.3. Main Benefits Associated with Working Remotely

The main benefits of remote work for any organization, other than the square footage savings and productivity gains, are listed as follows:

- Accelerated ability to maintain or recover operations in the event of a disaster (power failure or ice storm);
- Pandemic preparedness (reducing the risk of contagion, managing collective stress levels);
- Accommodation of people with disabilities or reduced mobility (on a temporary or permanent basis);
- Increased recruitment assets and retention.

1.4. Main Challenges Associated with Working Remotely

The main challenges associated with working remotely for an organization are as follows:

- Increased online fraud (e.g., exploiting unsecured network connections to monitor traffic as well as sending fake password reset reminders);
- Data theft;
- Connection overload;
- Poor management of logical access, including unreinforced password security;
- Inappropriate use of equipment by third parties in private homes;
- Unlicensed tools, software and applications;
- Non-progressive or non-existent deployment of updates;
- Overworked IT help desk teams and employees receiving less support from those teams.

2. Purpose and Scope of the Audit

Pursuant to the provisions of the *Cities and Towns Act*, we conducted a performance audit of the Information Technology Management Used for Remote Work. We carried out this mission in accordance with the *Canadian Standard on Assurance Engagements* (CSAE) 3001 of the *CPA Canada Handbook–Assurance*.

The purpose of this audit was to determine whether the controls in place for managing the information technology that the City uses for remote work are sufficient to provide the necessary equipment and secure remote access to the City's IT assets to ensure that employees can continue to perform their work.

The role of the Auditor General of the Ville de Montréal is to provide a conclusion regarding the purpose of the audit. To that end, we gathered sufficient and appropriate relevant evidence on which to base our conclusion and obtain a reasonable level of assurance. Our assessment is based on criteria we deemed valid for the purposes of this audit. These criteria are presented in Appendix 5.1.

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

The purpose of our audit dealt solely on the information technology management used for remote work to provide the necessary equipment and secure remote access to the City's IT assets to ensure that employees can continue to perform their work.

In order to perform our audit work, we audited the STI, which is responsible for managing the IT used to work remotely.

We excluded the Service de Police de la Ville de Montréal (SPVM) from the scope of our audit, as its IT management criteria differ greatly from the City's. In fact, the SPVM must respect specific security rules in order to protect access to the Centre de renseignements policiers du Québec. This is a database that police officers use on a daily basis.

Our audit work covered the period from February 2021 to October 2021. Our work consisted in conducting interviews with employees, reviewing various documents and conducting surveys that we deemed appropriate to gather the necessary evidence. We also took into account information that was sent to us up to January 19, 2022.

At the end of our work, a draft audit report was presented for discussion to the relevant managers in the audited business unit. The final report was then forwarded to the management of the business unit concerned as well as to the City's Direction générale.

3. Audit Results

3.1. Remote Work Framework

Establishing guidelines on the technology used for remote work consists in developing a normative framework on the use of dedicated computer equipment, a VPN and a data-filtering firewall as well as limiting the addition of applications, protecting networks and ensuring devices are configured in a secure manner according to the *Politique de sécurité de l'information*.

In addition, this framework must be approved by the appropriate authorities, kept up to date and distributed to all of the City's employees working remotely to prevent unsafe practices on their part that could result in significant security breaches.

The City has a number of frameworks in place that address, one way or another, best practices for remote workers. These frameworks are as follows:

- The STI's guideline *Utilisation des appareils et des technologies mis à la disposition des employés de la Ville de Montréal*, dated June 15, 2018, provides a framework for the use of computing devices and technology services to prevent illegal, wrongful, abusive or unreasonable use by certain users. This guideline clarifies the rules for using the Internet, the City's email, cell phones and remote access services;
- The consent form referenced in Section 9.5 – *Utilisation d'appareils qui n'appartiennent pas à la Ville* of the above guideline states the following: *[TRANSLATION] "Applicable users must sign a consent form ahead of time for the use of a personal device in a business setting and comply with the security requirements set out in that form."* This form, updated in the context of the pandemic, includes useful links to the remote work guideline and cybersecurity capsules;
- The guideline *Directive sur le télétravail des employés de la Ville de Montréal* of the Service des ressources humaines came into force on March 13, 2020 in emergency mode. It aims to provide a framework for the practice of remote work. It specifies the nature of the privileges granted, the eligibility conditions, the roles and responsibilities as well as the rules and measures to be observed. It also refers to complementary frameworks, including the above-mentioned guideline;
- The *Guide de sécurité de l'information pour l'employé en télétravail* was developed in March 2021 by the STI's Direction Sécurité de l'information. This guide can be found in the *Zone TI, Cybersécurité*. It details, for example, good practices, secure workstation configurations (including laptops) and secure configurations of connection networks (i.e., home wired and wireless networks);
- The *Encadrement administratif sur le modèle hybride d'organisation du travail*, dated June 28, 2021, of the Service des ressources humaines, makes references to the frameworks cited above. In the section on rules

for the use of computer equipment, it includes the guideline on using the City's technology and, in the section on security and data protection, the information security guide for employees working remotely.

These frameworks were approved and distributed to all employees through the City's intranet.

We believe that the frameworks in place prior to the pandemic and those developed subsequently provided the information required for employees to safely use IT for remote work.

No recommendation is necessary.

3.2. Remote Work Training

Remote work training typically consists of training on detecting email scams and phishing attempts, using strong passwords and secure wireless networks, monitoring devices and communicating when security issues arise. Such training can be done through different media such as conferences, training capsules or recognized websites.

To increase awareness and maintain employee reflexes on these key topics, the key is repeating the messages.

We found that through hyperlinks on the City's intranet, remote workers could learn about the various remote access solutions put in place by the City, important updated new items and information related to remote work, and email scam awareness with a link that redirects the user to a video released by the City on YouTube in February 2019. The video is titled *Cybersécurité : l'accès à distance en toute sécurité*[3] and explains *Comment sécuriser vos informations et vos outils avec le téléaccès de la Ville pour ceux qui travaillent à distance*. In addition, the form *Consentement pour l'autorisation d'utilisation d'un ordinateur personnel en télétravail* to be completed by employees redirects them to useful links, including the cybersecurity capsules available on the City's training portal.

We also noted that, during the month of October 2021[4], two conferences were held on remote work cybersecurity and cybersecurity trends. The STI should facilitate additional conferences throughout the awareness campaign based on the identified needs of their target audiences.

In addition, the security capsules developed by the STI's Direction Sécurité de l'information are monitored to ensure that all connected employees view and complete them within a reasonable time frame. If necessary, a manager is notified by the STI that an employee should promptly retake a given training.

We have been informed that as part of the project *Sensibilisation et formation des employés*, the training capsules on various cybersecurity topics are being revised.

[3] https://www.youtube.com/l'accès à distance en toute sécurité

[4] October is *Cybersecurity Awareness Month*. This international campaign aims to educate the public about the importance of cybersecurity.

In fact, according to this project, the gradual release of these capsules should take place throughout the current awareness campaign until fall 2022. All "connected" employees, approximately 12,000, will be required to complete the capsules.

We estimate that appropriate awareness and training on remote work and its components have been in place since March 2020.

No recommendation is necessary.

3.3. Data Access Protection

Protecting remote access involves several technical approaches, including the use of two-factor or strong authentication[5], through a secure VPN[6] and a firewall[7] that filters incoming and outgoing data. City computers that provide remote access should have a screen lock automatically activated after a period of inactivity and have up-to-date anti-malware software[8].

3.3.1. Authentication Mechanisms

Strong authentication mechanisms are in place to enable remote computers to access City data. Indeed, during our audit, we observed the use of two types of authentication mechanisms: the VPN used on the City's workstations and the RDP used on personal computers. An employee working remotely could connect using the VPN or the RDP.

3.3.1.1. Virtual Private Network – Used on City of Montréal Workstations

Remote VPN client access was implemented during the large-scale deployment of the remote working mode with a robust two-factor authentication. We considered, among other things, the configuration of the key components of the VPN environment, the two factors used during session length authentication and the user documentation made available to remote workers.

We believe that the above-mentioned items are in line with what is normally expected.

No recommendation is necessary.

3.3.1.2. Remote Desktop Protocol – Used on Personal Computers

To expedite the implementation of remote work, and depending on laptop delivery deadlines, RDP authentication was enabled on personal computers for employees authorized to log on to their office workstations and access City data. However, the City could revoke this privilege at any time.

[5] The two-factor, or strong, authentication method combines something you know (password, confidential code) with something else that can be a biometric element, an object you own or an action you know how to do.

[6] A VPN is a method of linking two remote computers through a single private connection, or tunnel, while using a larger network infrastructure, such as the web or a wide area network (WAN). Once activated, a VPN acts as a direct connection to a private network.

[7] A firewall is a device that protects all network traffic and has the ability to identify and block unwanted data traffic.

[8] Malware or malicious software refers to software intended to harm the user which can take the form of, for example, a Trojan horse or computer virus.

We examined the configuration of the RDP environment, the password change process, the login process, the multi-factor authentication process, the duration of RDP sessions, the functionalities for copying or saving data, as well as the end-user and technical documentation for this option.

We believe that the above-mentioned items are adequate and provide a secure multiple authentication environment.

No recommendation is necessary.

3.3.2. Screen Lock

We were informed that City laptops used by workers are configured with an automatic screen lock after a period of Windows session inactivity that varies according to the nature of the information asset (critical or not).

We found that the Windows session on these laptops locks in accordance with the logical access management standard as of November 2, 2020. We believe that this is adequate.

No recommendation is necessary.

3.3.3. Anti-malware Software

We were informed that all City workstations and laptops are equipped with anti-malware software. This tool is used to filter emails and web pages consulted by employees.

We found that the configuration of this anti-malware environment is consistent with sound practices, including hourly updates of the server components hosting this software and security agents (i.e., virus signatures, spyware[9], etc.), intelligent scanning of anti-malware and anti-spyware signatures, automatic website reputation assessment[10] and predictive machine learning[11]. In addition, detection of suspicious malicious connections and monitoring of malware behaviour are enabled on the server.

We were also informed that the hardening of security agents installed on all workstations, including laptops, is under way and that an increase in the security level of its firewall component is planned based on best practices, vendor recommendations and the City's business and operational needs. This is in line with one of the initiatives of the Acquisition of Security Technology Infrastructure project currently under way.

We consider that this solution with its different layers is adequate.

No recommendation is necessary.

[9] Spyware refers to software that collects personal data in order to send it to a third party.

[10] The website reputation feature assesses the security risk associated with a requested URL.

[11] This learning is an advanced technology that detects new and unknown security risks in suspicious processes or files with low prevalence.

3.4. Operations Management

Sound operations management aims to supply corporate equipment with communications tools for remote workers. This includes providing IT support to employees to respond to security incidents related to remote access and monitoring the data links between the computers that employees are using and the City's network.

Redundancy of the different types of authentication servers with data replication is essential to maintain service availability and load balancing of remote access requests. Network segmentation[12] between office workstations and remote computers should be implemented to prevent suspicious communications from infiltrating the City's computer network.

3.4.1. Supply of Laptops

In the current pandemic context, the STI has been gradually rolling out measures to expand remote work. Initially, the STI did not have enough laptops available for all remote workers. As a result, employees without City laptops who required access to the City's computer network were allowed to use their personal computers to perform their work. This use of personal computers follows a rigorous process of requesting authorization from the employee's manager. The City could revoke the privilege of using a personal device to access its technological environment at any time.

We noted that since the beginning of 2021, a distribution of corporate laptops is under way, with nearly 2,200 laptops already distributed to employees working remotely.

No recommendation is necessary.

3.4.2. Technical Support

The STI's teams helped the Centre de services TI to expedite the implementation of remote work in March 2020. Employees were asked to provide telephone support to help remote workers connect to the City's computer network remotely. This continued during the first weeks of the emergency caused by the pandemic. Once the situation had stabilized, the Centre de services TI resumed management of the calls.

The Centre de services TI has 20 dedicated support agents for the City, of which five have been hired since March 2020 to meet needs. For support requests regarding technological tools in the context of remote work, users can signal an incident using the self-service IT system or call them.

We found that the support process for remote workers includes sending emails with online user documents on VPN and RDP connection methods with links and videos to guide users. In addition, calls are redirected to IT technicians specialized in these areas to resolve complex situations.

[12] Network segmentation refers to dividing a network into several sub-networks.

We analyzed the list of incidents that occurred from March 20, 2020, to September 14, 2021, and found that there were no incidents related to remote access.

We believe that the Centre de services TI has the resource capacity and tools needed to provide IT remote access support to remote workers.

No recommendation is necessary.

3.4.3. Monitoring the Virtual Private Network Link

We found that administrator access to the VPN gateway console remains open during office hours. This console continuously monitors the performance of the hard drives and resources used by this gateway. The administrator thus conducts spot checks.

The Centralized Security Information and Event Management System (SIEM)[13] was implemented and training was provided to the administrator of the telecommunications network. In addition, monitoring through the SIEM is being configured with the integration of security logs for automated alerts and security data analysis.

Currently, alerts are logged and sent to the log management application (Graylog), and no alerts are sent to the administrators. The SIEM will address this issue.

It is our opinion that the implementation and configuration of the SIEM currently under way will allow for continuous monitoring through the collection, storage and real-time analysis of events on the data link between the computer used by the employee and the City's network (i.e., the VPN link for remote access).

We already issued a recommendation in this regard during a previous audit. No new recommendation is necessary.

3.4.4. Equipment Redundancy

We obtained documentation on remote work solutions. One document provides high-level details on the remote access solutions – RDP and VPN – with infrastructure diagrams. Another document presents a more detailed diagram of the RDP environment. From the documentation and resources we consulted, we found that there is indeed redundancy at the equipment level.

We consider that the different types of authentication servers with data replication between them are in place and that there exists an adequate level of redundancy between all key components.

No recommendation is necessary.

[13] A SIEM is used to collect, track and correlate logs as well as to generate dashboards and reports.

4. Conclusion

We conclude that the City of Montréal (the City) has the control mechanisms in place to ensure the sound management of the information technology (IT) used for remote work.

Indeed, despite the public health emergency caused by the COVID-19 crisis, the City's Service des technologies de l'information (STI) very quickly deployed all the necessary efforts to put in place the technological environment as well as the security mechanisms required to allow all of its remote workers to continue their professional activities from home without any interruption of service.

These mechanisms include the STI's guidance on IT used to work remotely, the remote work awareness and training strategy, the protection mechanisms surrounding City data access and the operations management surrounding remote workers' corporate equipment.

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

Evaluation Criterion – Remote Work Framework

Several guidelines on sound practices to be adopted by remote workers were developed within the organization. They were approved and distributed to all employees through the City's intranet.

These frameworks provide the information required for employees to safely use IT for remote work.

Evaluation Criterion – Remote Work Training

Appropriate awareness and training on remote work and its components have been implemented since March 2020 and expected to continue through fall 2022.

The STI follows up on the cybersecurity training capsules to ensure that all employees who are "connected" to the City's network successfully complete these capsules within a reasonable time frame.

Evaluation Criterion – Data Access Protection

Strong authentication mechanisms are used by employees to access data located on the City's network in accordance with sound security practices. The screen lock of corporate laptops is automatically activated after a centrally defined period of inactivity.

Appropriate anti-malware software is installed and updated on all corporate devices remotely connected to the City's computer network. Among other things, this software filters emails and web pages visited by employees and scans files according to the configured analysis parameters.

Evaluation Criterion – Operations Management

In order to allow employees to work remotely, the STI put in place secure mechanisms to enable employees who do not have a City computer to use their personal computer. Since the beginning of 2021, nearly 2,200 laptops have been distributed to employees to allow them to work remotely.

The Centre de services TI has the resource capacity and tools needed to provide adequate IT support to remote workers.

There is appropriate redundancy of key components of the Virtual Private Network and Remote Desktop Protocol authentication solution environments.

5. Appendix

5.1. Objective and Evaluation Criteria

Objective

To determine whether the control mechanisms, put in place for managing the information technology (IT) used for remote work within the City of Montréal (the City), allow to provide the necessary equipment and secure remote access to the City's IT assets to ensure that employees can continue to perform their work.

Evaluation Criteria

Our work focused on the following evaluation criteria:

Criterion 1: Governance
A normative framework for information technology used for remote work was developed by the Service des technologies de l'information (STI), approved and distributed to City employees.

Criterion 2: Remote Work Training
Ongoing training is provided to employees to raise awareness of security issues related to remote work and to remind them of good practices. The STI monitors this training.

Criterion 3: Data Access Protection
Robust authentication mechanisms are in place to access data. Remote computers are equipped with appropriate security mechanisms (e.g., anti-malware software).

Criterion 4: Operations Management
The STI provides laptops with remote communication tools to remote workers in a timely manner. The STI also provides oversight of remote work operations to ensure that they remain available to employees (e.g., IT support).