4.7.

Logical Access Management (SIMON, PAIE, OASIS)

(Service des technologies de l'information, Service des finances and Service des ressources humaines)

January 10, 2020

2019 Annual Report
Auditor General of the Ville de Montréal

OBJECTIVE

Ensure that the logical access to the SIMON, PAIE and OASIS financial applications are correctly managed and limit the risks of unauthorized or inappropriate access in addition to mitigating the risks of fraud or collusion.

RESULTS

The Service des technologies de l'information (STI), the Service des finances and the Service des ressources humaines adequately manage the logical access of the financial applications for which they are responsible.

Indeed, the SIMON, PAIE and OASIS financial applications are protected by the following appropriate control mechanisms:

- Access profiles that are pre-established in accordance with the positions held, where compensatory controls are in place to ensure that the access granted is relevant;
- The parameters set to authenticate and manage the applications are adequate, considering the platforms on which they are hosted;
- The logical access is monitored regularly;
- High-privilege accounts are legitimate and their number is limited. Those of the OASIS and PAIE applications are monitored;
- Existing conflicting rights are restricted and authorized.

Nevertheless, we noted the following aspects which would require improvements:

- With respect to users who perform the incompatible duties of issuing purchase orders and receiving goods and services, although special dispensation requests had been duly approved by their superiors, the business units do not systematically follow up to monitor these operations;
- Even though certain logical access management principles are known and applied, they are not included in the frameworks;
- There is no mechanism enabling the validation of the strength of the passwords chosen;
- Access to the OASIS application for the Bureaux Accès Montréal (BAM) must be reviewed on a more frequent basis;
- High-privilege SIMON accounts are not adequately monitored.

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.

Note that the business units have had the opportunity to formulate their comments, which appear after the audit report recommendations.

TABLE OF CONTENTS

LIST OF ACRONYMS

ACF2	IBM Access Control Facility
BAM	Bureaux Accès Montréal
GITC	General IT Controls
IAM	Identity and Access Management
SPVM	Service de police de la Ville de Montréal
STI	Service des technologies de l'information
TSO	Time Sharing Option (command line interpreter for IBM mainframe systems)

1. BACKGROUND

Access to applications is granted by way of a user ID and password. These elements constitute the access key that will allow their holders to use the applications to perform their respective tasks.

Logical access management consists of granting permissions with respect to a user's authorized actions and data within an application. Best practices dictate that:

- strong passwords must be used;
- a limited number of high-privilege[1] access codes is authorized;
- users' access is re-evaluated regularly;
- users' access is maintained at sufficient and appropriate levels;
- users' access does not allow them to perform incompatible tasks.

At all times, these practices make it possible to limit the risks of unauthorized or inappropriate access and minimize the risks of error, fraud or collusion.

The Ville de Montréal (the City) basically uses three applications to manage its financial information, i.e.:

- SIMON: the City's integrated system that is used mainly for accounting and procurement purposes. It has more than 28,000 users;
- PAIE: the application that manages the payroll of approximately 23,000 employees. The number of users exceeds 280 (approximately $1.9 billion for the 2019 budget);
- OASIS: the system used to manage municipal tax revenue (approximately $4.8 billion in 2019). This application has more than 400 users.

The City's infrastructure hosts all three applications.

As part of the annual audit of the General IT Controls (GITC), work is performed with respect to the logical access management of these financial applications.

[1] Used for the purpose of administering an application. Its user has unlimited rights, including, for example, the right to access any information (read only), to configure parameters and even to modify and delete data.

The SIMON application is an integrated management system that includes general ledger, procurement and payroll modules. It is being used to manage the remuneration of elected officials, judges and retired employees as well as for the Service de police de la Ville de Montréal (SPVM) since January 1, 2019. The platform is an Oracle database.

The PAIE and OASIS applications are hosted on an IBM mainframe computer, and access to them is managed through the IBM Access Control Facility (ACF2). Access to these applications is a two-level process: access to the mainframe computer represents the first level, and access to the application, the second level. SIMON, PAIE and OASIS are therefore hosted in separate IT environments.

To correctly evaluate the logical access management of each of the financial applications included in our audit, it is important to understand how access creation, modification and withdrawal requests are managed. It is also important to be familiar with the various actions that the assigned profiles can perform within the application in order to be able to detect the access rights that represent the highest risks. Finally, it is important to know which incompatible access profiles lead to the risks of recording transactions that could open a door to fraud or collusion.

2. PURPOSE AND SCOPE OF THE AUDIT

Pursuant to the provisions of the *Cities and Towns Act* (CTA), we carried out a performance audit mission on the logical access management of the SIMON, PAIE and OASIS financial applications. 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 objective of this audit was to ensure that logical access to the SIMON, PAIE and OASIS financial applications is correctly managed and limits the risks of unauthorized or inappropriate access in addition to mitigating the risks of fraud or collusion.

The responsibility of the Auditor General of the Ville de Montréal 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 in 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.

The purpose of our audit dealt solely with logical access management. To limit the scope of our intervention, it was decided that the City's main financial applications would be audited, namely:

- SIMON;
- PAIE;
- OASIS.

In this context, we met with the following three business units for the targeted applications:

1. the Service des technologies de l'information (STI) for the SIMON application;
2. the Service des finances for the OASIS application;
3. the Service des ressources humaines for the PAIE application.

Furthermore, for the purpose of our audit and to avoid duplicating the work, we excluded from our mission the tasks performed to evaluate the general information technology controls pursuant to the audit of the City's financial statements. This work is performed to ensure that the data generated by the financial systems provides information that is free from material misstatements.

We carried out our audit from April 2018 to December 2019, and our tests covered the period from February 2018 to February 2019. As part of our audit, we interviewed staff, reviewed various documents and conducted such tests as we considered appropriate to obtain the necessary evidentiary information. However, we took into account information that was sent to us up until January 2020.

At the end of our work, a draft audit report was presented for discussion to the relevant managers in each of the audited business units. The final report was then sent to the Direction générale as well as to each business unit concerned for the purpose of obtaining action plans and timetables for their implementation.

3. AUDIT RESULTS

3.1. Governance

3.1.A. Background and Findings

The publication of policies and guidelines makes it possible to manage the various facets of a subject and limit the risks of inconsistencies in the actions taken in relation to the elements that make up a process.

To provide a framework for the logical access management process (e.g., granting, modifying, withdrawing and reviewing), the City has issued certain rules. Compliance with these rules ensures that the access granted and the actions that are allowed in these applications is authorized. A periodic review of these access rights ensures that the process is working properly.

We examined the various logical access management rules the City has in place.

We focused on the following policies and guidelines:

- the *Politique de sécurité de l'information* (issued in 2006);
- the *Directive sur la gestion des accès aux ressources informationnelles* (issued in 2006);
- the *Standard sur les clés d'accès aux ressources informationnelles* (issued in 2006).

Also, as part of the Identity and Access Management (IAM) project, we were provided with a draft directive on logical access management. The IAM project allows for the unique identification of users requiring access to the City's informational or physical resources (e.g., space, telephone, equipment). This in turn makes it possible to better manage the impact of events (hirings, promotions, transfers, departures) on the various types of access granted. Security is thus strengthened.

Our first observation reveals that certain password security parameters set out in the *Standard sur les clés d'accès aux ressources informationnelles* are weak or are not complied with. Indeed, beyond an acceptable length for the latter, the standard does not specify any mandatory combination of characters. Also, although the standard specifies that passwords must expire within 30 days, our audit of the systems we examined revealed that a 90-day period is in place.

Furthermore, a review of the rules in place reveals that certain principles are absent, namely:

- Minimum privilege: the assigned access privileges are restricted to the informational resources required to perform the necessary tasks;
- Task segregation privilege: the responsibilities for an activity of a critical or strategic nature are divided among several entities (e.g., people, processes) to prevent a single entity from exercising control over the entire activity;
- Traceability principle: all access and attempted access to information assets supporting critical or strategic business processes are recorded and saved.

These principles, which are however found within the IAM project of the directive that was presented to us, are currently applied in an informal manner.

The lack of rules, policies and procedures could lead to inconsistencies in the handling and management of logical access (e.g., granting unauthorized or unjustified access).

In our opinion, as part of the IAM project, the *Standard sur les clés d'accès aux ressources informationnelles* should be revised such as to establish future parameters with respect to password strength and the frequency of password changes.

We also believe that it is appropriate to pursue the adoption of a logical access management directive that would contain the principles set out above.

We are aware, however, that the obsolescence of certain technological platforms hinders:

- the standardization and implementation of more rigorous parameters;
- the updating of the rules regarding password parameters.

RECOMMENDATION

3.1.B. We recommend that the Service des technologies de l'information, as part of the Identity and Access Management project:

- **update its rules relating to the logical access management and more specifically the *Standard sur les clés d'accès aux ressources informationnelles* in order to establish future parameters with respect to password strength and the frequency of password changes;**
- **continue its efforts to adopt a directive on logical access management so that the principles of minimum privilege, task segregation and traceability are clearly established.**

BUSINESS UNIT'S RESPONSE

3.1.B. Service des technologies de l'information

[TRANSLATION] The logical access management standard is currently being developed and will include criteria consistent with industry best practices covering password length, complexity and validity period.

The implementation of these good practices is under way as part of the security program. This initiative is in the implementation phase and is to be rolled out in 2020.

The Directive sur la gestion des accès logiques was submitted to the Comité de sécurité de l'information and is now under review by committee members. Afterwards, it will be submitted to the director general for approval. ***(Planned completion: December 2020)***

3.2. Granting Access

3.2.A. Background and Findings

The access granted to an application must be appropriate to the tasks to be performed by the user. In addition, users must not hold access rights that are superfluous to their needs.

To ensure that access is granted on an as-needed basis and that the principle of minimum privilege is respected when access to the applications subject to our audit is granted, we sought to answer the following questions:

- Is the access granted appropriate for the user's tasks?
- Does the user have more rights in the application than necessary?

Given the complexity of the types of access granted to certain applications, the use of pre-established profiles based on the tasks to be performed by model users makes it possible to better manage access and minimize the risks of granting these users rights that are superfluous to their needs.

Our audit revealed that, for the SIMON, PAIE and OASIS applications, the granted access is appropriate and takes into account the user's tasks. Furthermore, in the case of the PAIE and OASIS applications, pre-established profiles are used to grant this access. For the SIMON application, a script generates a daily report to identify the users who have transferred to new positions. Following this report, a manual review of the access rights held must be carried out and, if necessary, the required corrections made. Our tests confirmed that these reviews were effective.

No recommendation is necessary.

3.3. Password Authentication and Management

3.3.A. Background and Findings

An application's access key, i.e., the combination of a user ID and a password, must be robust and restrictive enough to limit the risks of unauthorized access.

We reviewed the parameters of the passwords that were set for each of the three applications we audited. Our work revealed that the parameters set are adequate given the technological limitations of the platforms that host the applications. Indeed, due to the obsolescence of the OASIS and PAIE applications, changing the parameters would require considerable effort, given that the applications could be replaced in the near future.

It should be noted, however, that there is no mechanism for identifying the strength of the chosen passwords used by all of the application's users beyond the criteria set by the parameters. These mechanisms make it possible to qualify passwords according to best practices, so the user would immediately obtain a comment on the security of the password (e.g., insufficient, good, excellent) and the password could then be reviewed for robustness.

Although it is not efficient to develop such mechanisms on older platforms, it would be relevant to consider setting up mechanisms for identifying the strength of user passwords for future sensitive applications, particularly in the context of the IAM project.

Unauthorized access could result if users chose passwords that were not strong enough. However, malicious users do not have direct access to the application and must first sign in to the network.

RECOMMENDATION

3.3.B. We recommend that the Service des technologies de l'information develop and implement mechanisms to identify the strength of passwords for appropriate future applications.

BUSINESS UNIT'S RESPONSE

3.3.B. Service des technologies de l'information

[TRANSLATION] A detailed architecture document on the mechanisms to be put in place to validate password strength is being drafted and is part of the work that will be implemented in 2020.

(Planned completion: December 2020)

3.4. Access Monitoring and Review

3.4.A. Background and Findings

A process for assigning access is in place for each of the applications covered by our audit. However, there may be several events in the holder's career (e.g., promotion, transfer, departure). It is therefore essential to implement an efficient recurrent review mechanism of existing access in order to remove any access that is no longer legitimate.

To this effect, we examined the access review processes in place for the applications covered by our audit.

SIMON Application

Access within this application is allocated by module (e.g., GL, Purchasing, Inventory), by responsibility (e.g., to make a query or a transaction) and by level of intervention (e.g., global, administrative unit, amount).

It should be noted at the outset that all employees have a default access to the SIMON application for bidding purposes (the online job application service) as well as to view their electronic payroll slip (the online employee service).

There is no formal regular validation with managers. However, a script is launched daily to deactivate access following the transfer of a user recorded in the register of positions. This register compiles all employee transfers during their career with the City.

In addition, this script generates a report to be reviewed by the people in charge of the *Centre d'expertise SIMON* to ensure that appropriate action is taken. Other analysis scripts are also produced to detect changes in the need to access the SIMON application.

In addition, routines performed by system administrators (sysadmin[2]) on a daily, weekly or monthly basis, as the case may be, make it possible to identify anomalies in the rights granted to users and quickly correct them. Finally, any right assigned to perform a specific action in a module (e.g., responsibility) that is not used for a period of six months is automatically deactivated.

We validated various reports between September 11, 2018, and January 21, 2019, and corrective action had been taken.

No recommendation is necessary.

PAIE Application

Access to the PAIE application is a two-level process. Access to the IBM mainframe computer represents the first level and access to the PAIE application, the second level. Access to this application is validated annually to ensure that the assigned rights are still appropriate or relevant. Access is also validated every two months in the case of departures. This exercise makes it possible to clean up the list of the application's users because, if the user does not connect to the IBM mainframe computer (ACF2) within a period of three months, their IBM access code will initially be suspended and subsequently destroyed after 13 months of inactivity. The code used to access the PAIE application will remain active and present in the list of the application's users even if this access is suspended after a period of six months. The review of the access makes it possible to eliminate access codes that are no longer needed.

We examined the November 2018 reports and our audit enabled us to conclude that the described procedures are carried out.

No recommendation is necessary.

OASIS Application

As is the case for the PAIE application, access to the OASIS application is a two-level process. Access to the IBM system is automatically suspended and ultimately destroyed if the user does not log on within the aforementioned prescribed periods.

Given the destruction parameter, the user will no longer have access to the OASIS application even though the user remains active in the application. While it is important to regularly review access permissions, an effort should be made in these circumstances to remove unwarranted access permissions from the application's database.

[2] An administrator access allows access to all of an application's functions and data. It can also be used for maintenance purposes.

Based on our audit of the OASIS application, which covered the period from February 2018 to January 2019, we concluded that monthly follow-up is carried out with the application users' managers. However, with respect to the Bureaux Accès Montréal (BAM), this exercise is only carried out twice a year. A review of the access codes that have not been used for more than one year is also carried out by the person responsible for the security of the OASIS application.

We reviewed reports from September 2018 to January 2019 on access that had been unused for more than a year, and the unused access permissions were removed.

However, we are of the opinion that the review of access to the BAM would benefit from a more frequent schedule since the majority of people who work in these offices have access to tax collection data.

Illegitimate access may remain active in the absence of regular monitoring and review of authorized access.

RECOMMENDATION

3.4.B. We recommend that the Service des finances conduct more frequent reviews of access to the OASIS application granted to people working in the Bureaux Accès Montréal.

BUSINESS UNIT'S RESPONSE

3.4.B. Service des finances

[TRANSLATION] The audit carried out on the OASIS application covered the period from February 2018 to January 2019.

The procedure was reviewed following receipt of the audit recommendations. Two important changes were made to the process in relation to the accesses Bureaux Accès Montréal:

1. *The boroughs' accesses are now validated every quarter;*
2. *The Système de point de vente was implemented in all of the Bureaux Accès Montréal. With this Système de point de vente, the only changes they can make are changes of address. The offices do not have access to any data other than in view mode. Consequently, the risk of access raised by the audit has been eliminated.*

We consider that the recommendation has been resolved.

(Planned completion: Immediate)

3.5. High-Privilege Accounts

3.5.A. Background and Findings

Usually, users should only have the access at the level requried to perform their tasks. However, the applications include so-called high-privilege access codes, which allow specific tasks to be performed and which cannot be devolved other than by regular access rights to the application. This is therefore a highly sensitive type of access that has a great impact on the data.

This type of access should be granted on a limited basis and closely monitored.

Each of the applications we audited has its own high-privilege access codes.

SIMON Application

Our audit pointed out that three users have system administrator rights (sysadmin) in the applications that are linked to their user ID. Furthermore, these same users have access to the sysadmin[3] generic account–a practice that is acceptable.

We also identified the rights to grant high-privilege access to the application. Our audit revealed that these rights are granted only to the system administrators as well as the people working at the *Centre d'expertise SIMON*, which is appropriate.

We found that transactions made using the sysadmin generic account are not adequately logged[4], as the log is entered manually. As part of the annual work on the GITC, the auditors also issued the "SIMON application high-privilege generic account" recommendation in 2015 to this effect, but the situation still remains to be addressed.

Based on our work, we conclude that privileged access to this application is adequately granted but not monitored.

Apart from the recommendation made in 2015, no further recommendation is necessary.

PAIE Application

This application's high-privilege access corresponds to the access granting and payroll processing profiles. However, the importance of a user's access is multiplied if the user also has modification rights in the *Registre des postes* application (e.g., changing pay rates following promotions, or statutory increases) or in the Time Sharing Option application (command line interpreter for IBM

[3] A generic account is an account that is not assigned to a specific user. It is usually used in emergency situations only by a restricted group of administrators.

[4] According to the Office québécois de la langue française, logging makes it possible to keep track of certain events for future audits.

mainframe systems (TSO)) on the mainframe that provides direct access to data. Granting access to these last two applications is not the responsibility of the payroll department.

The review of high-privilege accounts revealed the following highlights:

- Three users can grant access in the PAIE application. The other users of this application have profiles that essentially allow them to generate the payroll, which is normal given their work;
- Two users have high-privilege access to the three aforementioned applications (PAIE, *Registre des postes* and TSO). These people are the payroll coordinators. However, not all payroll coordinators have the ability to grant access to the PAIE application, which is satisfactory;
- In addition, we found that 12 individuals have high-privilege access to two of these applications (*Registre des postes* and TSO). Several of these individuals are administrative payroll and benefits control officers who require such access, including the ability to modify pay rates when required.

Administrative payroll reconciliation controls (e.g., code-to-code) and exception reports are reviewed to control how these codes are used.

Based on our work, we conclude that the privileged access to this application is adequately granted and monitored.

No recommendation is necessary.

OASIS Application

We inventoried two types of high-privilege accounts providing access to the following:

- the application security;
- the application's parameters.

Our audit revealed that only those people designated as members of the security personnel have security rights. Indeed, one person has all of the rights in the application and two other persons can intervene for security reasons and to grant access, which is an acceptable practice. All security actions are logged and reviewed on a daily basis.

We also examined the users who had access to the application's parameters. They are nine in total and work for the STI as programmer analysts or consulting analysts.

Based on our work, we conclude that the privileged access to this application is adequately granted and monitored.

No recommendation is necessary.

3.6. Incompatible Tasks

3.6.A. Background and Findings

Good access practices dictate that no single user should be able to control an organization's process from beginning to end (e.g., recording and paying invoices).

Indeed, segregating incompatible tasks makes it easier to detect errors and prevents fraud since carrying out the tasks requires collusion between two or more people, which complicates matters.

Given the nature of each of the applications covered by our audit, we identified specific incompatible tasks and also analyzed who had access rights to them.

SIMON Application

For this application, we started off by examining the responsibilities granted in each of the boroughs on the basis that task segregation is sometimes more difficult to achieve given the limited number of people holding a given position.

Next, we examined access to a combination of responsibilities that, if held by the same user, constitute risky profiles.

The following combinations of responsibilities were examined:

- entering and carrying forward entries in the City's logs;
- entering invoices and receipts;
- entering invoices and paying and releasing invoices;
- issuing purchase orders and entering receipts.

Our audit revealed that some users have multiple access with incompatible tasks. When access is granted, despite the fact that the principle of task segregation is not respected, a special dispensation request must be produced and approved. Those responsible for granting access to the SIMON application follow up on requests that have an end date (temporary access).

With respect to the special dispensation requests that we observed, our audit revealed that access was assigned under exceptional circumstances, because teams are restricted or for emergency situations. In these cases, subsequent compensatory controls are carried out (e.g., reporting on transactions carried out using the access).

However, we found that there is an exception for the 149 users who handle the following two incompatible responsibilities, issuing purchase orders (*SIMON – Atelier Acheteur PO*) and entering receipts (*SIMON – Achat en ligne ICX*). Indeed, these incompatible tasks allow users to both create purchase orders and receive goods and services. Although special dispensations were requested and justified by their managers, the managers do not systematically follow up on the transactions carried out by the holders of the two profiles. Yet it is stipulated in an administrative directive on task segregation that managers are required to do exactly that.

We were also informed that, as part of a new business model, the Service de l'approvisionnement intends to centralize the issuance of all purchase orders within its unit. This action will, among other things, ensure compliance with the directive on task segregation.

The absence of mechanisms to monitor users who perform these incompatible tasks increases the risk of unauthorized transactions.

RECOMMENDATION

3.6.B. We recommend that the Service de l'approvisionnement, as part of the new procurement business model, implement a subsequent control in order to monitor the operations of users with the following incompatible responsibilities:

- ***SIMON – Atelier Acheteur PO*****;**
- ***SIMON – Achat en ligne ICX*****.**

BUSINESS UNIT'S RESPONSE

3.6.B. Service de l'approvisionnement

[TRANSLATION] Prior to finalizing the implementation of the Service de l'approvisionnement's new business model, the following actions will be undertaken:

- *Issue a communication to the business units reminding them of the framework and the obligation to carry out subsequent controls by means of the control report designed for this purpose;*
- *Before March 31, 2020, return the list of special dispensations to the departments concerned for reassessment and clarification of the duration of the special dispensation;*
- *Periodically (quarterly) reassess the special dispensations and extract non-compliant transactions.* ***(Planned completion: in the current year, with follow-up on December 31, 2020)***

PAIE Application

This application does not present profiles with incompatible tasks because operations are segregated such as to have conflicting actions performed by another section or by an application of the human resources department. As mentioned in section 3.5 “High-Privilege Accounts”, the accumulation of access through various applications can result in the multiple rights held by a user being incompatible.

However, based on our audit, we determined that only two users have a combination of high-privilege access. This access is justified given the users' tasks.

We believe that conflicting rights are satisfactorily managed for this application.

No recommendation is necessary.

OASIS Application

For this taxation application, there is also a high level of segmentation of operations between various operational sections. Indeed, the operations are functionally divided between taxation, collection and receipts. Typical access profiles are created from a set of groups of screens and rights within them that allow users to perform their tasks.

Each type of operation has screens that are specific to its needs. For example, access for taxation confers rights that grant access to certificates of appraisement. Similarly, the screens related to the accounting of receipts should not be included in the access available to those working in taxation.

For each of the taxation, collection and receipt operations, we validated that there is no access profile that gives the possibility of intervening in the other groups' specific screens. In addition, we verified that no user had accumulated profiles that would have allowed this incompatible access.

We therefore conclude that conflicting rights are satisfactorily managed for this application.

No recommendation is necessary.

4. CONCLUSION

Based on our audit, we conclude that the Service des technologies de l'information (STI), the Service des ressources humaines and the Service des finances respectively manage the logical access to the SIMON, PAIE and OASIS applications adequately.

The control mechanisms in place make it possible to limit both the impacts of unauthorized or inappropriate access and the risks of fraud or collusion.

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

Evaluation Criterion – Governance

The Ville de Montréal (the City) has directives that cover the main spheres of logical access management. The STI is responsible for enacting these directives. However, some of these directives need to be updated, as some parameters have changed since they were initially drafted and are no longer representative of the current situation. Indeed, certain principles of logical access management (i.e., the minimum privilege, task segregation and traceability principles) are applied without, however, being present within the directives.

Evaluation Criterion – Granting Access

The access granted to the SIMON, PAIE and OASIS applications is appropriate in light of users' tasks. Profiles have been pre-established according to the positions held for the PAIE and OASIS applications. As for the SIMON application, a script launched daily removes access from users who have changed jobs.

Evaluation Criterion – Password Authentication and Management

The password parameters set for authentication and password management purposes are adequate in the case of the SIMON, PAIE and OASIS applications. However, there is no mechanism enabling the strength of the chosen passwords to be validated.

Evaluation Criterion – Access Monitoring and Review

Access monitoring and review are adequate for the SIMON, PAIE and OASIS applications. In the case of the PAIE and OASIS applications, there is formal periodic validation with managers. In addition, any access not used for six months is first suspended and then deleted from the main IBM platform. It should be noted, however, that the review of the access granted to the Bureaux Accès Montréal (BAM) staff could be carried out more frequently in the case of the OASIS application.

For the SIMON application, despite the absence of formal periodic validations with managers, scripts launched daily, weekly and monthly make it possible to detect abnormal access and implement appropriate corrective action. In addition, access to any function that is not used within six months is automatically disabled.

Evaluation Criterion – High-Privilege Accounts

In the case of the SIMON, PAIE and OASIS applications, the number of high-privilege accounts is limited and they are closely monitored, with the exception of the SIMON application, which is monitored manually and therefore inadequately.

Evaluation Criterion – Incompatible Tasks

Conflicting rights are handled satisfactorily for the PAIE and OASIS applications. In fact, the use of pre-established access profiles as well as how work is organized from an operational standpoint ensure that potentially conflicting situations are not found within the same application or under the responsibility of the same section of their respective departments.

Conflicting rights are managed satisfactorily for the SIMON application, except for users who are responsible for both creating purchase orders and receiving goods and services. In this case, although exemption requests were duly approved, the business unit managers do not systematically follow up to ensure that users with dual access are not making unauthorized transactions.

5. APPENDIX

5.1. Objective and Evaluation Criteria

Objective

Ensure that logical access to the SIMON, PAIE and OASIS financial applications is correctly managed and limits the risks of unauthorized or inappropriate access in addition to mitigating the risks of fraud or collusion.

Evaluation Criteria

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

1. **Governance**
   The City documents, communicates and assigns responsibilities for its application access management policies and procedures.
2. **Granting Access**
   The administrative units grant access to applications and keep the access active only if it complies with the requirements.
3. **Password Authentication and Management**
   The City's password parameters are robust.
4. **Access Monitoring and Review**
   The administrative units carry out regular reviews of the access granted, making it possible to withdraw access from users that is no longer required or justified.
5. **High-Privilege Accounts**
   The administrative units limit privileged access to only those users who need it.
6. **Incompatible Tasks**
   The administrative units ensure that users do not hold access rights that would allow them to significantly control a transactional process.