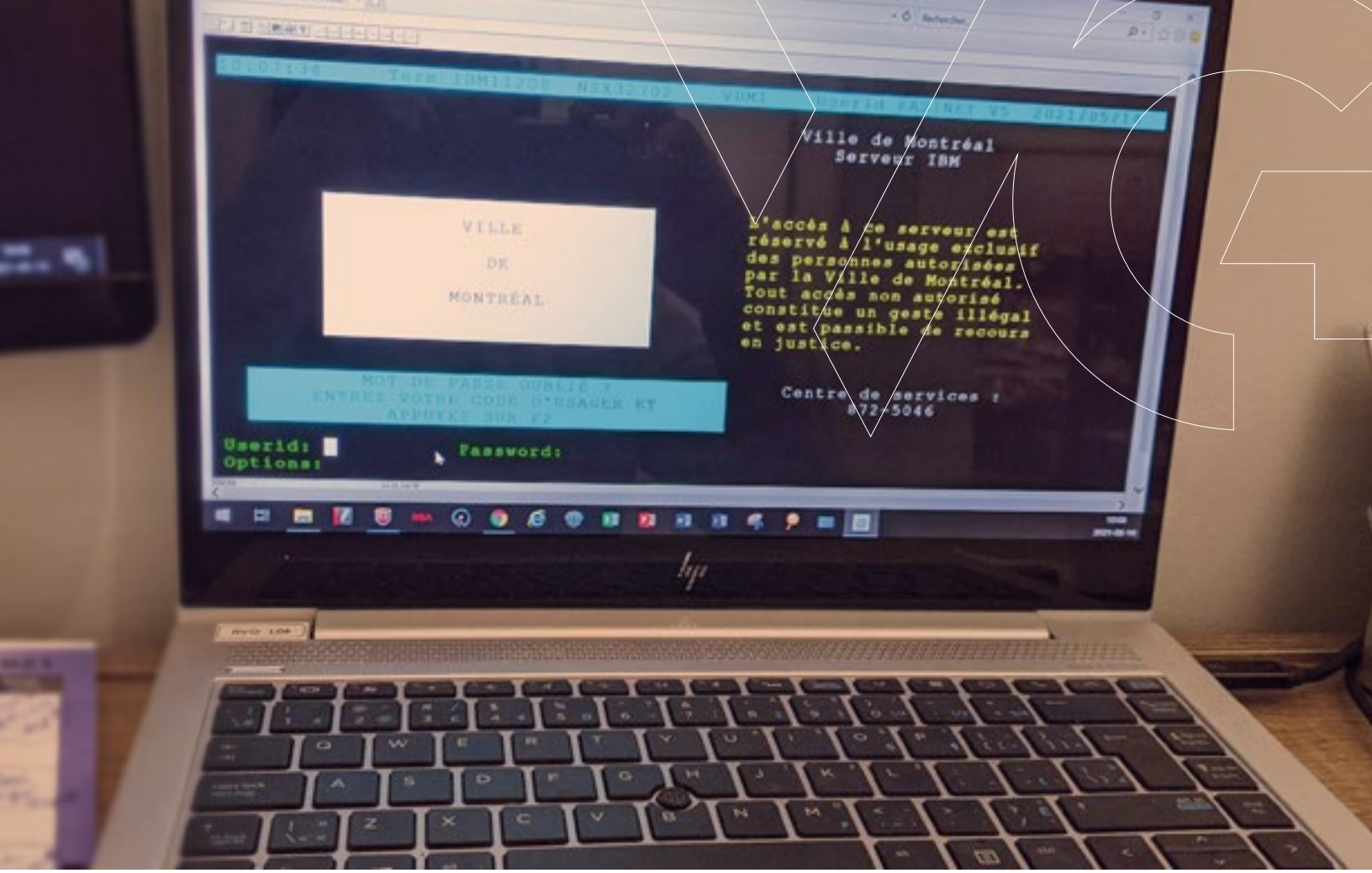

4.2. Management of the Système budgétaire automatisé Application

February 9, 2021

2020 ANNUAL REPORT
Auditor General of the Ville de Montréal

Management of the Système budgétaire automatisé Application

Background

The Système budgétaire automatisé (SBA) is the primary budget application of the Ville de Montréal (the City). This application, which was developed internally in the early 1990s, contains all the City's budget data, both revenues and expenditures. The 2021 operating budget is $6.17B.

The Service des finances (SF) is responsible for daily and operational tasks. At the other end, the Service des technologies de l'information (STI) provides support for the application and is responsible for, among other things, programming and deploying changes, managing access requests and incidents, and preparing backup copies.

This application, which is hosted on the IBM mainframe computer, will need to be replaced in 2024 as part of the "Système budgétaire" project within the 2021–2030 Ten-year capital works program. In 2009, a study into implementing a new budget process was conducted, which proposed, among other things, to replace the SBA application with a solution integrated into the SIMON accounting system and new budget monitoring functionalities.

Purpose of the Audit

The purpose of this audit was to determine whether the control mechanisms put in place for the SBA application ensure that it does not present any major risk to the confidentiality, integrity and availability of the data.

Results

We concluded that, for certain control mechanisms listed below, improvements are needed to avoid loss of data integrity and availability of the application, which would cause major harm to the City's budget operations.

Roles and responsibilities are inadequately documented. In addition, the owner of the SBA application is not formally identified in any documentation.

Regarding access management, no specific procedure exists for the SBA application, the password parameters do not comply with the City's frameworks, and there is no logging or monitoring of access.

Change management is not framed within a formally documented, approved and distributed procedure.

The SF and the STI have no formal succession plan for existing human resources.

Incident management is not part of a formal procedure.

Main Findings

Roles and Responsibilities

- Roles and responsibilities and ownership of the SBA application are not formally identified, documented and known to all the stakeholders.

Access Management

- No formal procedure exists for managing access to the SBA application. The configuration of the passwords does not comply with the City's new standard. There is no logging or monitoring of access in the SBA application. On the other hand, the management of access profiles, the annual review and the management of generic and highly privileged accounts are adequate.

Change Management

- Change management is not part of a formal procedure. Requests for changes are not systematically documented. Those that are documented do not follow the production steps to implement a change (e.g., lack of analysis, approval of changes, tests and deployment).

Human Resources and Technical Sustainability

- No succession plan for human resources and knowledge transfer has been developed. The SBA application, which dates from the 1990s, is facing technological obsolescence.

Operations Management

- Documentation of the operations management of the SBA application, which is available to users and pilots, is adequate.
- Incident management is not subject to a formal procedure, and incidents are not systematically documented.
- Backup copies are made regularly and systematically. However, there is no procedure specific to the SBA application for the management of backup copies, and no periodic recovery tests are performed on the copies.

In addition to these results, we have made various recommendations to the business units, which are presented in the following pages. These business units were given the opportunity to agree to the recommendations.

List of Acronyms

RACI	Responsible, Accountable, Consulted, Informed
SBA	Système budgétaire automatisé
SF	Service des finances
SIMON	Système intégré Montréal
STI	Service des technologies de l'information
TCWP	Three-Year Capital Works Program

Table of Contents

1. Background

The Système budgétaire automatisé (SBA) is a corporate tool used to prepare the annual budget of the central departments, boroughs and other budget lines (e.g., common expenses, financial expenditures and contribution expenditures). This includes both revenues and expenditures, as well as the number of employee positions. The SBA is the main budget application of the Ville de Montréal (the City).

This application contains all the City's operational budget data. The Ten-year capital works program resides in another application called INVESTI. The 2021 operating budget is $6.17B. The SBA application details revenues and expenditures in several categories (e.g., revenues: property taxes, fines, licences and permits; expenditures: administrative services, public safety, services to citizens) that serve as the basis for the allocation of revenues and expenditures.

The application is open, in modification mode, from June to August for the preparation of the budget. During this period, while budget envelopes are created, users may, for example, change their budget structure or create/remove accounts and salaried employee positions. The application is then reopened in modification mode in September to allow the business units to revise their budgets and make corrections. During the remainder of the year, the SBA application is in read-only mode. At year-end, the budget data is transmitted to the Système intégré Montréal (SIMON) accounting system and the Registre des postes application. The latter is used to manage human resources information on the City's workforce and organizational structure.

The Service des finances (SF) is responsible for daily and operational tasks. The Service des technologies de l'information (STI) supports the application and is responsible for, among other things, programming and deploying changes, managing access requests and incidents, and preparing daily backup copies.

With more than 200 users, the SBA application is hosted on the IBM mainframe computer. The application was created around the early 1990s. As a result of this obsolescence, many of the functionalities that could simplify the work of users and managers are missing:

- Automated data entry;
- Changes to access management by group (they are done individually);
- Automated interfaces with other systems (e.g., SIMON);
- Production of comparatives (by year);
- Budget changes (e.g., quarterly report).

Over the years, the City has looked into replacing this application. In fact, a study was carried out by an outside firm in 2009 to evaluate the implementation of a new budget process. The conclusions of this study included, among other things, replacing the SBA application with a solution that would include better budget monitoring (e.g., quarterly) and be integrated with SIMON (the City's accounting system), thereby eliminating the need for data entry and tables of correspondence between the systems. In addition, a project called "budget solution" was launched in 2013. Preparing the call for tenders for this project took two years. Following a restructuring of the STI, it was halted in 2015 before being abandoned due to a lack of human and financial resources. More recently, the project to replace the SBA application resurfaced in the 2021–2030 Ten-year capital works program[1] as part of the "Système budgétaire" project. Work should begin in 2024.

2. Purpose and Scope of the Audit

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

The purpose of this audit was to evaluate the control mechanisms put in place for the SBA application to ensure that it does not present any major risk to the confidentiality, integrity and availability of data.

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

[1] "Système budgétaire" project file 21_4204_068 in the 2021-2030 Ten-year capital works program.

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

Our audit work focused on the period from June 2020 to January 2021. It consisted in conducting interviews with staff, examining various documents, and doing surveys that we deemed appropriate to obtain the necessary supporting information. We also took into account information that was sent to us up to February 2021.

Upon completing our audit, we submitted a draft audit report to the managers of each audited business unit for discussion purposes. The final report was then forwarded to the Direction générale, as well as to the management of each business unit involved in the audit to obtain action plans and timelines for implementing the recommendations concerning it.

3. Audit Results

3.1. Roles and Responsibilities

To define clear accountability regarding roles and responsibilities, these must be properly defined, written down and validated by all the parties concerned. It is common practice for this process to result in the creation of a RACI (Responsible, Accountable, Consulted, Informed) matrix that serves as a reference for each process of the application throughout its life cycle. It can also serve as a basis if the application requires an upgrade or has to migrate towards a new system.

It is also important to define the person responsible for each application, thereby establishing clear accountability for every action that requires a chain of validation. The owner of the application is responsible for its operational management. That person must be involved in every major change and every application migration.

We obtained a draft of the RACI matrix, which is only in its first version. This matrix is therefore incomplete and not formalized (no role has been defined for three of the five phases of budget preparation). It is important to note that the roles and responsibilities are well known to the current, longstanding, main stakeholders. Nevertheless, these roles and responsibilities are not documented. In addition, the owner is not formally identified.

The absence of a matrix of roles and responsibilities could result in shortcomings in the governance of the application, such as:

- Ineffective collaboration between the teams (e.g., users redirected to the wrong teams for access or incident management);
- Application privileges granted without prior validation;
- When the roles and responsibilities of each person are not formally defined and assigned, some tasks run the risk of not being completed, while others could have several persons managing them, which could lead to confusion, omissions and uneven actions taken to manage the SBA application.

3.1.A. Recommendation

We recommend that the Service des finances, jointly with the Service des technologies de l'information:

- **Complete, approve and distribute the matrix of roles and responsibilities for the Système budgétaire automatisé application;**
- **Formalize the owner of the application in the matrix.**

3.2. Access Management

3.2.1. Access Management Policy

Publishing policies and directives provides a framework for certain processes, thereby limiting the risk of inconsistencies in the actions taken and preventing access from being bypassed or privileges abused.

A Politique de gestion des accès usually consists of rules governing the granting, withdrawal, modification and periodic review of access rights.

We concluded that the only guide for requests to access the SBA application consists of an inset box on the City's Intranet. In our opinion, this is not a formal access management procedure.

Granting, modifying and withdrawing access are done based on the following appropriate steps:

- The responsible persons in the business units and boroughs enter access requests directly into the DASI application or "Demande d'accès aux systèmes informatiques";
- These requests are then conveyed to the team in the STI's Centre d'expertise;
- The team creates access codes in the IBM mainframe computer;
- Once the access requests are validated, the SBA application pilot[2] gives access according to the profiles and business units requested.

[2] A pilot is a superuser with in-depth technical knowledge, who acts as an intermediary between the business units and the STI to ensure the application runs smoothly.

To validate that the access requests follow the steps outlined above, efficacy tests were conducted on a sample of access requests (four selected out of a total of 33 between October 2019 and November 2020). The results of these tests showed that these steps were properly followed.

An appropriate review of access rights is performed annually. Using samples, we examined the access reviews of five administrative units out of a total of 43 for the years 2018 and 2019. The access review requests and associated changes were properly done.

We analyzed the seven administrator accounts and three generic accounts. These were justified and effectively managed.

Without formalized and documented access management, the City could face the following risks:

- Errors due to incorrect interpretation of informal directives;
- Inappropriate access rights granted.

3.2.1.A. Recommendation

We recommend that the Service des finances, in collaboration with the Service des technologies de l'information, create an access management procedure specific to the Système budgétaire automatisé application and ensure that it is distributed to the stakeholders.

3.2.2. Password Management

The access key in an application, i.e., the combination of a user code and a password, must be robust and sufficiently restrictive to limit the risk of unauthorized access. Password authorization settings must be aligned with the City's policy (e.g., minimum length of the password, inclusion of capital letters and special characters, impossibility of reusing earlier passwords).

The SBA application is hosted on the IBM mainframe computer, as is the case with several other applications. Users do not have direct access to the application but must first authenticate themselves to the City's network and then authenticate themselves to the SBA. Password settings are the same for all applications on the IBM mainframe computer.

Very recently, the City distributed new relevant frameworks for access management in:

- The Directive sur la gestion des accès (issued in July 2020);
- The Standard sur la gestion des accès (issued in November 2020).

In comparing password settings in the IBM system with the requirements of the frameworks, we uncovered certain discrepancies.

Unauthorized access could occur when users use passwords that do not comply with the requirements of the new access management frameworks.

3.2.2.A. Recommendation

We recommend that the Service des technologies de l'information comply with the new access management frameworks.

3.2.3. Access Monitoring

An access monitoring process is required to prevent unauthorized access attempts or to detect incidents related to users' access. This monitoring will also allow more efficient analysis in case of access management incidents.

We concluded that there is no logging or monitoring of access in the SBA application.

Without access monitoring, it is impossible to effectively prevent unauthorized access attempts. As well, the absence of an access log makes it difficult to retrace events in case of an incident.

3.2.3.A. Recommendation

We recommend that the Service des technologies de l'information implement a recurring process for logging and monitoring access in the Système budgétaire automatisé application.

3.2.4. Segregation of Duties

To prevent unauthorized access to the SBA application, it is important to segregate profiles and rights granted. To this end, the granting of highly privileged accounts must be regulated and monitored.

We examined the various types of access profiles and concluded that there is no conflict or incompatible task with the pre-established profiles. This confirms that the profiles are satisfactorily managed in the SBA application.

No recommendation is required.

3.3. Change Management

Any change in the production environment must follow a certain number of regulations, processes and validations. Without processes and adapted controls, the integrity and stability of the application are at risk. The use of appropriate tools to follow up, control and monitor changes is paramount.

In a production environment, as opposed to a test environment, it is common to see change errors made by the programming team, since programmers have write access in both environments. When programmers have direct access to production, they can also circumvent official processes.

We obtained a file that summarizes the various steps involved in implementing a change:

- Functional analyses by the pilots and technical and impact analyses by the developers;
- Approval by the pilots and the division head;
- Development by the developers;
- Unit tests by the developers, approval tests by the pilots, and user-expert tests;
- Deployment by the production team at the STI.

Nevertheless, this does not constitute a formally documented and approved procedure that is known to all stakeholders.

To validate that change requests follow the recommended steps up to deployment, efficacy tests were performed on a sample base. For the entire year 2020, we found that only four change requests were entered into the CA Service Desk ticketing tool. Based on our discussions with the stakeholders, other changes were made, but these were not systematically documented.

Nevertheless, we analyzed the four documented change requests and concluded that they did not follow sound change management practices (e.g., lack of analysis, approval of tests and deployment authorizations).

Based on our audit, the sole SBA application programmer does not have access to the production environment, which is proper.

The absence of a formally documented change management procedure increases the risk of unauthorized and undesirable changes being deployed, which could have consequences for the integrity and availability of the SBA application and its data.

3.3.A. Recommendation

We recommend that the Service des finances, in collaboration with the Service des technologies de l'information, establish a formal change management procedure.

3.4. Human and Technical Continuity

In the case of an application developed internally that dates from the early 1990s and uses old technology, it is especially important to:

- Conduct updates to ensure adequate technological advances (given that the SBA is an in-house application, updates are done through change requests. See Section 3.3 of the report);
- Develop a succession plan for adequate and sufficient human resources to ensure the continuity of operations.

According to the STI and the SF, the availability of specialized human resources on the job market is a major issue, yet no formal succession plan has been put in place for existing resources and to ensure knowledge transfer. We found no designated replacements for the one programmer/developer in the STI and the three pilots in the SF. The latter are eligible for retirement within the next four to six years.

In the 2021–2030 Ten-year capital works program,[3] plans are to replace the SBA application as part of the "Système budgétaire" project starting in 2024.

The City is facing a lack of specialized human resources and a major technological liability:

- Lack of a human resources succession plan, including ensuring knowledge transfer;
- Lack of availability of competent resources (e.g., mastery of old technology and accounting knowledge) on the job market.

Human and technical continuity problems could cause a loss of knowledge and mastery of the application. It would then be difficult to keep the SBA application operational until its replacement and would make proper budget management difficult for the City.

3.4.A. Recommendation

We recommend that the Service des finances and the Service des technologies de l'information put in place a human resources succession plan, including knowledge transfer.

[3] "Système budgétaire" project file 21_4204_068 in the 2021-2030 Ten-year capital works program.

3.5. Operations Management

3.5.1. Documentation

Clear documentation that is regularly updated is important to ensure the operational efficacy and maintainability of the application.

We noted that the procedures and guides available to users and pilots are adequate. We found, among other things, descriptions of the tasks and activities to be performed by the pilots, as well as the various SBA application procedures for preparing the budget (e.g., fiscal year change, budget approval, data transfers).

No recommendation is required.

3.5.2. Management of Incidents and Problems

Each detected incident must be properly documented in a ticketing application that makes it easy to identify the specific incident by documenting the origin of the problem, its impact and its resolution.

An incident follow-up process requiring an action plan must be put in place to ensure that mitigation measures have been implemented.

Apart from a training document and a process diagram outlining the various steps for the use and creation of incident tickets in the CA Service Desk tool, there is no complete, documented, approved and distributed procedure for the management of incidents specific to the SBA application.

Some users create a ticket in the CA Service Desk tool managed by the STI. However, most users call the pilot of the application directly at the SF to report an incident. Between January 2019 and September 2020, we noted only four incidents documented in the tool, which confirms that incidents are not systematically documented in the CA Service Desk tool. During our audit, we were able to validate the existence of the following relevant information for the four incidents:

- Date the ticket was created;
- Priority;
- Impact;
- Description;
- Status of the incident;
- Resolution.

In the absence of a formal procedure, the different incident management steps cannot be defined or standardized, with the result that incidents are not systematically documented. The SF faces the following risks:

- Incidents may not be resolved in a timely manner;
- The absence of an incident history may make it impossible to prevent recurring events, which could result in needless costs and wasted time.

3.5.2.A. Recommendation

We recommend that the Service des finances, in collaboration with the Service des technologies de l'information:

- **Create an incident management procedure for the Système budgétaire automatisé;**
- **Systematically document incidents.**

3.5.3. Management of Backup Copies

In the event of an incident, the backup copy process ensures that the data lost can be restored in its entirety. This process must be documented and subjected to recovery tests on a regular basis to ensure that it is working smoothly.

We should mention from the outset that there is no formal procedure for the management of backup copies of the SBA application. According to the information we collected, backup copies are made at the following two levels:

- Database: backup of all databases in the IBM mainframe computer (including the SBA application) according to the following schedule:
  - weekly for all IBM application discs;
  - weekly and daily for databases and all logs;
  - weekly and incrementally for sequential files[4];
- Application: daily backup of all SBA application data.

[4] These are saved copies processed one after the other.

Apart from recovery on demand, the STI does not conduct regular recovery tests of the SBA application.

There are also global tests performed once a year on all IBM databases (including the SBA application), but these are done in the context of a computer contingency plan aimed primarily at restoring the services of the platform and its data, but not specifically for a set of data, such as the SBA application.

The absence of a formal procedure to manage backup copies of the SBA application and conduct regular recovery tests of SBA application data could have an impact on the ability to recover the system in a timely manner. This could result in the loss of data and time.

3.5.3.A. Recommendation

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

- Document the procedure for managing backup copies of the Système budgétaire automatisé application;
- Conduct regular recovery tests of backup copies of the Système budgétaire automatisé application.

4. Conclusion

The Système budgétaire automatisé (SBA) is the primary budget application of the Ville de Montréal (the City). This application, developed internally in the early 1990s, contains all the City's budget data (both revenues and expenditures). The 2021 operating budget is $6.17B.

While there is a plan to begin to replace this outdated application in 2024, our recommendations will enable the City to offset the risks associated with the shortcomings we found until that time.

Based on our audit, we concluded that some control mechanisms need to be improved to mitigate the risks related to the confidentiality, integrity and availability of data in the SBA application:

- Roles and responsibilities are not adequately documented. In addition, the owner of the SBA application is not formally identified. Consequently, some tasks risk not being performed and others could have several persons managing them, which could lead to confusion, omissions and uneven actions taken to manage the application.
- Regarding access management, there is no formal procedure specific to the SBA application, password settings do not comply with the City's frameworks, and there is no logging or monitoring of access. The absence of these elements could increase the risk of changes being made to data by unauthorized persons.
- The lack of a formally documented change management procedure increases the risk of unauthorized and undesirable changes being made, which could have an impact on the integrity and availability of data and of the SBA application.
- In the absence of a formal succession plan for existing human resources and knowledge transfer, the SBA team may be unable to ensure sound management of the application, which could have an impact on the quality of services provided to users.

More specific details below are provided in terms of the evaluation criteria:

Evaluation Criterion – 1. Roles and Responsibilities

Roles and responsibilities and the owner of the SBA application are not formally identified using documentation such as a RACI (Responsible, Accountable, Consulted, Informed) matrix.

Evaluation Criterion – 2. Access Management

There is no formal procedure for managing access to the SBA application. The configuration of passwords does not comply with the City's new standard. Access is not logged or monitored in the SBA application.

However, access profiles are managed satisfactorily for this application. As well, the annual review and management of generic and highly privileged accounts are adequate.

Evaluation Criterion – 3. Change Management

There is no formal change management procedure. Requests for changes are not systematically documented. Where they are, they fail to follow the steps outlined below for implementing a change:

- Functional analyses by pilots and technical and impact analyses by developers;
- Approval by pilots and the division head;
- Development by the developer;
- Unit tests by developers, acceptance testing by pilots, and user-expert tests;
- Deployment by the production team at the STI.

Evaluation Criterion – 4. Human and Technical Continuity

Despite the fact that the availability of specialized human resources on the job market is a major issue for stakeholders, no succession plan for human resources and knowledge transfer has been developed. The SBA application, which dates from the 1990s, is facing technological obsolescence.

Evaluation Criterion – 5. Operations Management

The documentation regarding the operations management of the SBA application available to users and pilots is adequate.

Incident management is not subject to a formal procedure, and incidents are not systematically documented.

Backup copies of the SBA application are made regularly and systematically. However, no formal procedure exists for the management of backup copies specific to the SBA application, and periodic recovery tests are not performed on these backup copies.

5. Appendix

5.1. Objective and Evaluation Criteria

Objective

To determine whether the control mechanisms in place for the Système budgétaire automatisé (SBA) application ensure that it does not present any major risk to the confidentiality, integrity and availability of data.

Evaluation Criteria

1. Roles and Responsibilities

Roles and responsibilities are defined, approved and communicated, and provide clear accountability. The owner is formally identified.

2. Access Management

A procedure to create, modify, delete and revise access rights to the SBA application is properly documented. The application uses robust enough authentication settings to maintain a secure environment. The profiles and rights granted allow for adequate segregation of tasks to prevent unauthorized access and changes to data. Monitoring activities are in place to detect incidents in a timely manner.

3. Change Management

Production changes are properly documented, traced, tested and validated by the appropriate authorities. The access of programmers to the production environment is restricted and controlled.

4. Human and Technical Continuity

Updates are periodically conducted to ensure adequate technological development, qualified staff and sufficient succession throughout the life cycle of the application.

5. Operations Management

The application has documentation that minimizes operational risks. Each production incident is part of a unique ticket that retraces the origin, type and resolution of the problem. An action plan is associated with major problems and incidents. A backup plan is properly documented and followed. In addition, recovery tests on backup copies are performed on a regular basis.