



# 4.2.

## Gestion de l'application système budgétaire automatisé

Le 9 février 2021

**RAPPORT ANNUEL 2020**

Bureau du vérificateur général  
de la Ville de Montréal



# Gestion de l'application système budgétaire automatisé

## Mise en contexte

Le système budgétaire automatisé (SBA) est la principale application budgétaire de la Ville de Montréal (la Ville). Cette application développée à l'interne au début des années 90 contient toutes les données budgétaires de la Ville, autant les dépenses que les revenus. Le budget de fonctionnement 2021 se chiffre à 6,17 G\$.

Le Service des finances (SF) assure les tâches quotidiennes et opérationnelles. De l'autre côté, le Service des technologies de l'information (STI) assume le support de l'application et il a comme responsabilités – entre autres – la programmation et les déploiements des changements, la gestion des demandes d'accès et des incidents et la préparation des copies de sauvegarde.

Cette application, hébergée sur l'ordinateur central IBM, devrait être remplacée à compter de 2024 dans le cadre du projet «Système budgétaire» inscrit au programme décennal d'immobilisations (PDI) 2021-2030. En 2009, une étude sur l'implantation d'un nouveau processus budgétaire a été réalisée qui proposait, entre autres, de remplacer l'application SBA par une solution intégrée au système de comptabilité SIMON et de nouvelles fonctionnalités de suivi des budgets.

## Objectif de l'audit

Le présent audit avait pour objectif de déterminer si les mécanismes de contrôle mis en place pour l'application SBA permettent de s'assurer que celle-ci ne présente aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données.

## Résultats

Nous concluons que pour certains mécanismes de contrôle ci-dessous, il y a une nécessité d'améliorations afin d'éviter la perte de l'intégrité des données et de la disponibilité de l'application, ce qui nuirait de façon importante aux opérations budgétaires de la Ville.

Les rôles et les responsabilités ne sont pas adéquatement documentés. De plus, le propriétaire de l'application SBA n'est pas identifié formellement dans aucune documentation.

Pour la gestion des accès, il n'y a pas de procédure spécifique à l'application SBA, les paramètres de mots de passe ne sont pas conformes aux encadrements de la Ville et il n'y a pas de journalisation ni de surveillance des accès.

La gestion des changements n'est pas encadrée par une procédure formellement documentée, approuvée et diffusée.

Le SF et le STI n'ont pas de plan formel pour assurer la relève des ressources humaines existantes.

La gestion des incidents ne fait pas l'objet d'une procédure formelle.

# Principaux constats

## Rôles et responsabilités

- Les rôles et les responsabilités et le propriétaire de l'application SBA ne sont pas formellement identifiés, documentés et connus par l'ensemble des parties prenantes.

## Gestion des accès

- Il n'y a pas de procédure formelle concernant la gestion des accès à l'application SBA. La configuration des mots de passe n'est pas conforme au nouveau standard de la Ville. Il n'y a pas de journalisation ni de surveillance des accès dans l'application SBA. Par contre, la gestion des profils d'accès, la révision annuelle et la gestion des comptes génériques et à hauts privilèges sont adéquates.

## Gestion des changements

- La gestion des changements ne fait pas l'objet d'une procédure formelle. Les demandes de changements ne sont pas systématiquement documentées. Pour celles qui le sont, elles ne suivent pas les étapes de mise en production d'un changement (p. ex. l'absence d'analyse, l'approbation des changements, les tests et les mises en production).

## Pérennité humaine et technique

- Aucun plan de relève humaine avec un transfert de connaissances n'a été développé. L'application SBA, datant des années 90, fait face à une désuétude technologique.

## Gestion des opérations

- La documentation de gestion des opérations de l'application SBA à la disposition des utilisateurs et des pilotes est adéquate.
- La gestion des incidents ne fait pas l'objet d'une procédure formelle et ceux-ci ne sont pas documentés systématiquement.
- Les copies de sauvegarde sont effectuées de façon régulière et systématique. Cependant, il n'y a pas de procédure de gestion des copies de sauvegarde propre à l'application SBA ni de tests périodiques de restauration sur ces dernières.

*En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées dans les pages suivantes. Ces unités d'affaires ont eu l'opportunité de donner leur accord relativement aux recommandations.*

# Liste des sigles



<b>PDI</b>	programme décennal d'immobilisations
<b>PTI</b>	programme triennal d'immobilisations
<b>RACI</b>	Réalisateur, Approbateur, Consulté et Informé
<b>SBA</b>	système budgétaire automatisé
<b>SF</b>	Service des finances
<b>SIMON</b>	Système intégré Montréal
<b>STI</b>	Service des technologies de l'information



# Table des matières

<b>1. Contexte</b>	<b>501</b>
<b>2. Objectif de l'audit et portée des travaux</b>	<b>502</b>
<b>3. Résultats de l'audit</b>	<b>503</b>
3.1. Rôles et responsabilités	503
3.2. Gestion des accès	504
3.2.1. Politique de gestion des accès	504
3.2.2. Gestion de mots de passe	506
3.2.3. Surveillance des accès	506
3.2.4. Ségrégation des tâches	507
3.3. Gestion des changements	507
3.4. Pérennité humaine et technique	508

3.5. Gestion des opérations	509
3.5.1. Documentations	509
3.5.2. Gestion des incidents et des problèmes	509
3.5.3. Gestion des sauvegardes	510
<b>4. Conclusion</b>	<b>512</b>
<b>5. Annexe</b>	<b>514</b>
5.1. Objectif et critères d'évaluation	514





# 1. Contexte

Le système budgétaire automatisé (SBA) est un outil corporatif utilisé pour confectionner le budget annuel des services centraux, des arrondissements et des autres postes budgétaires (p. ex. les dépenses communes, les dépenses financières et les dépenses de contributions). Cela inclut autant les dépenses et les revenus de même que le nombre de postes en termes d'employés. SBA est la principale application budgétaire de la Ville de Montréal (Ville).

Cette application contient toutes les données budgétaires de fonctionnement de la Ville. Le programme décennal d'immobilisations (PDI), quant à lui, réside dans une autre application nommée INVESTI. Le budget de fonctionnement 2021 se chiffre à 6,17 G\$. L'application SBA détaille les revenus et les dépenses en plusieurs catégories (p. ex. pour les revenus: les taxes foncières, les contraventions, les licences et les permis; pour les dépenses: les services administratifs, la sécurité publique, les services aux citoyens) qui servent de base pour la répartition des revenus et des dépenses.

L'application est ouverte, en mode modification, pendant la confection du budget de juin à août. En effet, dans cette période, les utilisateurs viennent entre autres, lors de la création des enveloppes budgétaires, modifier leur structure budgétaire, créer/supprimer des comptes et des postes de salariés. Par la suite, l'application est rouverte en modification en septembre lorsque les unités d'affaires révisent leur budget et apporte des corrections. Le reste de l'année, l'application SBA est en mode lecture seulement. En fin d'année, les données budgétaires sont transmises vers le système comptable Système intégré Montréal (SIMON) et l'application Registre des postes. Ce dernier permet la gestion d'informations en ressources humaines sur la main-d'œuvre et sur la structure organisationnelle de la Ville.

Le Service des finances (SF) s'assure des tâches quotidiennes et opérationnelles. Le Service des technologies de l'information (STI) assume le support de l'application et a comme responsabilités, entre autres, la programmation et les déploiements des changements, la gestion des demandes d'accès et des incidents et la préparation des copies journalières de sauvegarde.

Dénombrant plus de 200 utilisateurs, l'application SBA est hébergée sur l'ordinateur central IBM. Elle a été créée vers le début des années 90. En conséquence de cette désuétude, beaucoup de fonctionnalités qui pourraient faciliter le travail des utilisateurs et des gestionnaires sont manquantes :

- L'entrée de donnée automatisée;
- La modification au niveau de la gestion des accès s'effectue à la pièce et non par groupe;
- Les interfaces automatisées avec les autres systèmes (p. ex. SIMON);
- La production de comparatifs (par année);
- L'évolution budgétaire (p. ex. un bilan trimestriel).

Au cours des années, la Ville s'est penchée sur le remplacement de cette application. En effet, une étude avait été réalisée par une firme externe en 2009 pour évaluer l'implantation d'un nouveau processus budgétaire. Les conclusions de cette étude comprenaient, entre autres, le remplacement de l'application SBA pour une solution qui inclurait un meilleur suivi budgétaire (p. ex. par trimestre) qui devra être intégré à SIMON (le système comptabilité de la Ville) éliminant de la saisie de données et les tables de correspondances entre les systèmes. En plus, un projet nommé « solution budgétaire » avait été démarré en 2013. Ce projet s'est étalé sur une période de 2 ans pour la phase de préparation de l'appel d'offres. Après une restructuration du STI, il a été arrêté en 2015 avant d'être abandonné à cause d'un manque de ressources humaines et financières. Plus récemment, le projet de remplacement de l'application SBA a refait surface dans le PDI 2021-2030<sup>1</sup> dans le cadre du projet « Système budgétaire ». Les travaux devraient débuter en 2024.

## 2. Objectif de l'audit et portée des travaux

En vertu des dispositions de la *Loi sur les cités et villes*, nous avons réalisé une mission d'audit de performance portant sur la gestion de l'application SBA. Nous avons réalisé cette mission conformément à la Norme canadienne de missions de certification (NMC) 3001 du Manuel de CPA Canada – Certification.

Le présent audit avait pour objectif de faire l'évaluation des mécanismes de contrôle mis en place pour l'application SBA, permettant de s'assurer que celui-ci ne présente aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données.

La responsabilité du vérificateur général de la Ville consiste à fournir une conclusion sur l'objectif de l'audit. Pour ce faire, nous avons recueilli les éléments probants suffisants et appropriés pour fonder notre conclusion et pour obtenir un niveau d'assurance raisonnable. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances. Ces derniers sont exposés en Annexe.

<sup>1</sup> Fiche du projet 21\_4204\_068 « Système budgétaire » au PDI 2021-2030.

Le vérificateur général de la Ville applique la *Norme canadienne de contrôle qualité* (NCCQ 1) du Manuel de CPA Canada – Certification et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. De plus, il se conforme aux règles sur l'indépendance et aux autres règles de déontologie du *Code de déontologie des comptables professionnels agréés*, lesquelles reposent sur les principes fondamentaux d'intégrité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Notre audit a été réalisé de juin 2020 à janvier 2021. Il a consisté à effectuer des entrevues auprès du personnel, à examiner divers documents et à réaliser les sondages que nous avons jugés appropriés en vue d'obtenir l'information probante nécessaire. Nous avons toutefois tenu compte d'informations qui nous ont été transmises jusqu'en février 2021.

À la fin de nos travaux, un projet de rapport d'audit a été présenté, aux fins de discussions, aux gestionnaires concernés au sein de chacune des unités d'affaires auditées. Par la suite, le rapport final a été transmis à la Direction générale, ainsi qu'à chacune des unités d'affaires concernées, pour l'obtention de plans d'action et d'échéanciers pour leur mise en œuvre.

## 3. Résultats de l'audit

### 3.1. Rôles et responsabilités

Afin de définir une imputabilité claire en matière des rôles et des responsabilités, ces derniers doivent être correctement définis, écrits et validés par toutes les parties concernées. Il est commun que ce processus donne naissance à une matrice RACI (Réalisateur, Approbateur, Consulté et Informé), servant de référence pour chaque processus de l'application tout au long de son cycle de vie. Elle peut servir de base si l'application est appelée à évoluer ou migrer vers un nouveau système.

De plus, pour chaque application, il est important de pouvoir définir qui sera la personne responsable de celle-ci, permettant une imputabilité claire pour chaque action nécessitant une chaîne de validation. Le propriétaire de l'application est le responsable de la gestion opérationnelle de celle-ci. Il doit être impliqué pour chaque changement majeur et pour chaque migration applicative.

Nous avons obtenu une ébauche de matrice RACI qui n'en est qu'à la toute première version. Celle-ci est donc incomplète et non formalisée (pour trois des cinq phases de préparation du budget, aucun rôle n'a été défini). Précisons que les rôles et les responsabilités sont bien connus des principaux intervenants en poste depuis longtemps. Cependant, ces rôles et responsabilités ne sont pas documentés. De plus, le propriétaire n'est pas formellement identifié.

L'absence d'une matrice des rôles et des responsabilités pourrait causer des dysfonctionnements dans la gouvernance applicative comme :

- la collaboration inefficace entre les équipes (p. ex. les utilisateurs redirigés vers les mauvaises équipes pour la gestion des accès ou d'un incident);
- l'octroi de privilèges applicatifs sans validation au préalable;
- lorsque les rôles et les responsabilités de chacun ne sont pas formellement définis et attribués, certaines tâches risquent de ne pas être réalisées et d'autres pourraient avoir plusieurs responsables ce qui pourrait engendrer de la confusion, des omissions et des actions inégales quant à la gestion de l'application SBA.

### 3.1.A. Recommandation

Nous recommandons au Service des finances conjointement avec le Service des technologies de l'information de :

- compléter, approuver et diffuser la matrice des rôles et des responsabilités pour l'application système budgétaire automatisé;
- officialiser le propriétaire de l'application dans la matrice.

## 3.2. Gestion des accès

### 3.2.1. Politique de gestion des accès

La publication de politiques et de directives permet d'encadrer certains processus afin de limiter les risques d'inconsistances dans les actions posées et prévient des contournements d'accès et des abus de privilèges.

Une *Politique de gestion des accès* comprend en général des règles concernant l'octroi, le retrait, la modification et la révision périodique des droits accès.

Nous avons constaté qu'il existe uniquement un guide pour les demandes d'accès à l'application SBA sous la forme d'un encadré sur l'intranet de la Ville. Nous considérons que cela ne constitue pas une procédure formelle de gestion des accès.

L'octroi, la modification et le retrait des accès se font selon les étapes appropriées suivantes:

- Des responsables dans les unités d'affaires et les arrondissements font des demandes d'accès directement dans l'application DASI (Demande d'accès aux systèmes informatiques);
- Ensuite, ces demandes sont transmises à l'équipe du Centre d'expertise au STI;
- Celle-ci crée les codes d'accès au niveau de l'ordinateur central IBM;
- Lorsque les demandes d'accès sont validées, le pilote<sup>2</sup> de l'application SBA donne l'accès selon les profils et les unités d'affaires demandés.

Afin de valider que les demandes d'accès suivent les étapes expliquées ci-dessus, des tests d'efficacité ont été effectués sur un échantillon (4 demandes sélectionnées sur un total de 33 entre octobre 2019 et novembre 2020) de demandes d'accès. Le résultat de ces tests démontre que les demandes d'accès suivent adéquatement ces étapes.

Une révision des droits d'accès adéquate est effectuée annuellement. En effet, nous avons examiné, sur base d'échantillon, les révisions des accès de 5 unités administratives sur un total de 43 pour les années 2018 et 2019. Les demandes de révision et les changements afférents ont bien été effectués.

Nous avons analysé les sept comptes administrateurs et les trois comptes génériques. Ceux-ci sont justifiés et sont adéquatement gérés.

Sans gestion des accès formalisée et documentée, la Ville ferait face aux risques suivants:

- Des erreurs dues à la mauvaise interprétation des directives informelles;
- Des droits d'accès inappropriés octroyés.

### 3.2.1.A. Recommandation

Nous recommandons au Service des finances, en collaboration avec le Service des technologies de l'information, de créer une procédure pour la gestion des accès spécifique à l'application système budgétaire automatisé et de s'assurer de sa diffusion auprès des parties prenantes.

<sup>2</sup> Un pilote est un superutilisateur avec des connaissances techniques approfondies qui agit comme un intermédiaire entre l'unité d'affaires et le STI pour assurer le bon fonctionnement de l'application.

### 3.2.2. Gestion de mots de passe

La clé d'accès dans une application, soit la combinaison d'un code d'utilisateur et d'un mot de passe, se doit d'être robuste et assez contraignante afin de limiter les risques d'accès non autorisés. Les paramètres d'authentification de mots de passe doivent être alignés avec la politique de la Ville (p. ex. la longueur minimale du mot de passe, l'inclusion de majuscules et de caractères spéciaux, l'impossibilité de réutiliser les précédents mots de passe).

L'application SBA est hébergée sur l'ordinateur central IBM (*mainframe*) comme plusieurs autres applications. L'utilisateur n'a pas accès directement à l'application, il doit d'abord s'authentifier au réseau de la Ville puis s'authentifier à SBA. Les paramètres de mots de passe sont les mêmes pour l'ensemble des applications de l'ordinateur central IBM.

La Ville a diffusé très récemment de nouveaux encadrements adéquats sur la gestion des accès, en l'occurrence concernant :

- la directive sur la gestion des accès (émise en juillet 2020);
- le standard sur la gestion des accès (émise en novembre 2020).

En comparant les paramètres de mots de passe du système IBM avec les exigences des encadrements, nous avons relevé certaines disparités.

Des accès non autorisés pourraient survenir dans le cas où des usagers utiliseraient des mots de passe qui ne seraient pas en adéquation avec les exigences des nouveaux encadrements sur la gestion des accès.

#### 3.2.2.A. Recommandation

Nous recommandons au Service des technologies de l'information de se conformer aux nouveaux encadrements sur la gestion des accès.

### 3.2.3. Surveillance des accès

Afin de prévenir des tentatives d'accès non autorisées ou de détecter des incidents relatifs aux accès des utilisateurs, il est nécessaire de disposer d'un processus de surveillance des accès. Cette surveillance permettra également une analyse plus efficace en cas d'incident sur la gestion des accès.

Nous avons constaté qu'il n'y a pas de journalisation ni de surveillance des accès dans l'application SBA.

Sans surveillance des accès, il ne serait pas possible de prévenir de manière efficace les tentatives d'accès non autorisés. Également, l'absence de registre des accès rendrait difficile de retracer les événements en cas d'incident.

### 3.2.3.A. Recommandation

Nous recommandons au Service des technologies de l'information de mettre en place un processus récurrent de journalisation et de surveillance des accès sur l'application système budgétaire automatisé.

### 3.2.4. Ségrégation des tâches

Afin de prévenir des accès non autorisés dans l'application SBA, il est important de maintenir une ségrégation des droits entre les profils et les droits accordés. Dans ce contexte, les attributions de comptes à hauts privilèges doivent être réglementées et suivies.

Nous avons examiné les différents types de profils d'accès et nous concluons qu'il n'y a pas de conflits ni de tâches incompatibles dans les profils préétablis ce qui confirme que ces derniers sont gérés de façon satisfaisante dans l'application SBA.

Aucune recommandation n'est nécessaire.

## 3.3. Gestion des changements

Toute modification dans un environnement de production doit suivre un certain nombre de réglementations, de processus et de validations. En effet, sans processus et de contrôles adaptés, l'intégrité et la stabilité de l'application seraient à risque. L'utilisation d'outils appropriés pour le suivi, le contrôle et la surveillance est primordiale.

Il est commun de voir des erreurs de changements, dans un environnement de production au lieu d'un environnement de tests, par l'équipe de programmeurs, car ces derniers ont des droits d'écriture dans ces deux environnements. Il devient également possible pour un programmeur de contourner les processus officiels lorsqu'il dispose d'un accès direct en production.

Nous avons obtenu un fichier qui décrit sommairement les différentes étapes de la mise en production d'un changement, soit :

- les analyses fonctionnelles par les pilotes et les analyses techniques et d'impacts faites par les développeurs;
- l'approbation par les pilotes et le chef de division;
- le développement par le développeur;
- les tests unitaires par les développeurs, les tests d'acceptation par les pilotes et les tests des utilisateurs-experts;
- la mise en production par l'équipe de production au STI.

Cependant, cela ne constitue pas une procédure formellement documentée, approuvée et connue par les parties prenantes.

Afin de valider que les demandes de changements suivent les étapes recommandées jusqu'à la mise en production, des tests d'efficacité ont été

effectués sur une base d'échantillon. Nous avons remarqué que pour toute l'année 2020, il n'y avait que quatre demandes de changement inscrites dans l'outil de billet CA Service Desk alors que selon nos discussions avec les parties prenantes, d'autres changements auraient eu lieu, mais ils n'auraient pas été systématiquement documentés.

Nous avons quand même analysé les quatre seules demandes de changements et nous avons constaté qu'elles ne suivent pas les saines pratiques de gestion des changements (p. ex. l'absence d'analyse, d'approbation, de tests et d'autorisations de mise en production).

Néanmoins, selon nos travaux, le seul programmeur de l'application SBA n'a pas accès à l'environnement de production, ce qui est adéquat.

L'absence d'une procédure formellement documentée de gestion des changements augmente les risques de mise en production de changements non autorisés et indésirables ce qui pourrait avoir des conséquences sur l'intégrité et la disponibilité de l'application SBA et de ses données.

### 3.3.A. Recommandation

Nous recommandons au Service des finances, en collaboration avec le Service des technologies de l'information, de mettre en place une procédure formelle sur la gestion des changements.

## 3.4. Pérennité humaine et technique

Pour une application développée à l'interne qui date du début des années 90 et qui utilise une vieille technologie, il est très important :

- d'appliquer des mises à jour afin d'assurer une évolution technologique adéquate (étant donné que le SBA est une application maison, les mises à jour se font par des demandes de changement, voir section du rapport 3.3.);
- de prévoir les ressources humaines adéquates et suffisantes tant au niveau opérationnel qu'aux fins de relève pour en assurer sa pérennité.

Bien que selon le STI et le SF, la disponibilité des ressources humaines spécialisées sur le marché est un enjeu majeur, ils n'ont pas mis en place un plan formel pour assurer la relève des ressources existantes et le transfert des connaissances. Nous avons remarqué qu'il y a un seul développeur programmeur du côté du STI et trois pilotes du côté du SF, sans aucune relève désignée. De plus, ces derniers pourraient être éligibles à la retraite d'ici quatre à six ans.

Le PDI 2021-2030<sup>3</sup> prévoit le remplacement de l'application SBA dans le cadre du projet « Système budgétaire » à partir de 2024.

<sup>3</sup> Fiche du projet « Système budgétaire » au PDI 2021-2030: 21\_4204\_068.



La Ville fait donc face à un manque de ressources humaines spécialisées et à une dette technologique importante, en l'occurrence:

- le manque d'un plan de relève humaine incluant le transfert de connaissances;
- l'indisponibilité des ressources compétentes (p. ex. la maîtrise d'anciennes technologies et la connaissance en comptabilité) sur le marché.

Les problématiques de pérennité humaine et technique pourraient causer une perte de connaissances et de maîtrise de l'application. Ainsi, il serait difficile de maintenir l'application SBA opérationnelle jusqu'à son projet de remplacement et rendrait difficile une gestion budgétaire adéquate de la Ville.

### 3.4.A. Recommandation

Nous recommandons au Service des finances et au Service des technologies de l'information de mettre en place un plan de relève humaine en incluant le transfert de connaissances.

## 3.5. Gestion des opérations

### 3.5.1. Documentations

Afin d'assurer une efficacité opérationnelle et une maintenabilité de l'application, il est important de disposer d'une documentation claire et mise à jour périodiquement.

Nous avons constaté que les procédures et les guides à la disposition des utilisateurs et des pilotes sont adéquats. En effet, nous retrouvons, entre autres, la description des tâches et activités à réaliser par les pilotes ainsi que les différentes procédures de l'application SBA pour la réalisation du budget (p. ex. le changement d'exercice, l'acceptation du budget, les transferts de données).

Aucune recommandation n'est nécessaire.

### 3.5.2. Gestion des incidents et des problèmes

Chaque incident détecté doit être correctement documenté dans une application de billetterie facilitant l'identification unique de l'incident en documentant l'origine du problème, les impacts et sa résolution.

Un processus de suivi des incidents nécessitant un plan d'action doit être mis en place afin de s'assurer que des mesures d'atténuation ont été implantées.

Mis à part un document de formation et un diagramme de processus qui relatent les différentes étapes de l'utilisation et de la création de billets d'incidents dans l'outil CA Service Desk, il n'existe pas de procédure documentée complète, approuvée et diffusée pour la gestion des incidents propre à l'application SBA.

Certains utilisateurs créent un billet dans l'outil CA Service Desk géré par le STI. Par contre, la majorité des utilisateurs appellent directement le pilote de l'application au SF pour signaler un incident. Nous avons remarqué qu'entre janvier 2019 et septembre 2020, il n'y avait que quatre incidents documentés dans l'outil, ce qui confirme que les incidents ne sont pas systématiquement documentés dans l'outil CA Service Desk. Lors de nos travaux, nous avons pu valider pour les quatre incidents documentés, l'existence des informations pertinentes suivantes :

- La date de création du billet;
- La priorité;
- L'impact;
- La description,
- L'état de l'incident;
- La résolution.

En l'absence d'une procédure formelle, les différentes étapes de la gestion des incidents ne sont pas balisées ni uniformisées, ayant pour conséquences que les incidents ne sont pas systématiquement documentés. Le SF ferait face aux risques suivants :

- Les incidents pourraient ne pas être réglés en temps opportun;
- L'absence d'historique des incidents ne permettrait pas de prévenir les événements récurrents ce qui entraînerait des coûts inutiles et des pertes de temps.

### 3.5.2.A. Recommandation

Nous recommandons au Service des finances, en collaboration avec le Service des technologies de l'information de :

- créer une procédure pour la gestion des incidents du système budgétaire automatisé;
- documenter systématiquement les incidents.

### 3.5.3. Gestion des sauvegardes

Advenant un incident, le processus de copies de sauvegarde assure que les données perdues peuvent être restaurées dans leur intégralité. Celui-ci doit être documenté et doit faire l'objet de tests de récupération sur une base régulière afin d'en tester son bon fonctionnement.

Mentionnons d'emblée qu'il n'existe pas de procédure formelle pour la gestion des copies de sauvegarde de l'application SBA. D'après les informations recueillies, les copies de sauvegardes se réalisent à deux niveaux, dont les suivants :

- La base de données: c'est la sauvegarde de l'ensemble des bases de données dans l'ordinateur central IBM (incluant l'application SBA) dont la fréquence est:
  - hebdomadaire pour les disques de toutes les applications IBM;
  - hebdomadaire et journalière pour les bases de données ainsi que tous les journaux;
  - hebdomadaire et incrémentaux pour les fichiers séquentiels<sup>4</sup>;
- L'applicatif: c'est la sauvegarde journalière de toutes les données de l'application SBA.

Mis à part les restaurations sur demande, le STI ne procède pas à des tests de restauration réguliers au niveau applicatif SBA.

Il existe aussi des tests globaux une fois par année sur l'ensemble de la base de données IBM (incluant l'application SBA), mais ils sont effectués dans un contexte de relève informatique dont l'objectif principal est de restaurer les services de la plateforme et de ses données, mais pas spécifiquement pour un ensemble de données comme l'application SBA.

L'absence d'une procédure formelle de gestion des copies de sauvegarde de l'application SBA et des tests de restauration réguliers des données de l'application SBA aurait un impact sur la capacité de restaurer le système en temps opportun. Cela pourrait occasionner des pertes de données et de temps.

### 3.5.3.A. Recommandation

Nous recommandons au Service des technologies de l'information de :

- documenter la procédure pour la gestion des copies de sauvegarde de l'application système budgétaire automatisé;
- procéder à des tests réguliers de restauration de sauvegarde de l'application système budgétaire automatisé.

<sup>4</sup> Ce sont des enregistrements traités les uns à la suite des autres.

## 4. Conclusion

Le système budgétaire intégré (SBA) est la principale application budgétaire de la Ville de Montréal (la Ville). Cette application développée à l'interne dans le début des années 90 contient toutes les données budgétaires de la Ville (autant les dépenses que les revenus). Le budget de fonctionnement 2021 se chiffre à 6,17 G\$.

Bien que le projet de changement de cette application désuète soit prévu pour débiter en 2024, nos recommandations permettront à la Ville de palier aux risques afférents aux lacunes constatées d'ici le remplacement de SBA.

Selon nos travaux d'audit, nous concluons que certains mécanismes de contrôles nécessiteraient des améliorations afin d'atténuer les risques liés à la confidentialité, l'intégrité et la disponibilité des données dans l'application SBA. En effet :

- les rôles et les responsabilités ne sont pas adéquatement documentés. De plus, le propriétaire de l'application SBA n'est pas identifié formellement. Par conséquent, certaines tâches risqueraient de ne pas être réalisées et d'autres pourraient avoir plusieurs responsables ce qui pourrait engendrer de la confusion, des omissions et des actions inégales quant à la gestion de l'application.
- pour la gestion des accès, il n'y a pas de procédure formelle spécifique à l'application SBA, les paramètres de mots de passe ne sont pas conformes aux encadrements de la Ville et il n'y a pas de journalisation ni de surveillance des accès. L'absence de ces éléments pourrait augmenter les risques de modification des données par des personnes non autorisées.
- l'absence d'une procédure formellement documentée de gestion des changements augmenterait les risques de mise en production de changements non autorisés et indésirables, ce qui pourrait avoir un impact sur l'intégrité et la disponibilité des données et de l'application SBA.
- en l'absence d'un plan formel pour assurer la relève des ressources humaines existantes et le transfert des connaissances, l'équipe SBA ne serait pas en mesure d'assurer une bonne gestion de l'application ce qui pourrait impacter la qualité des services offerts aux utilisateurs.

Plus précisément, voici les détails selon les critères d'évaluation :

### Critère d'évaluation – 1. Rôles et responsabilités

Les rôles et les responsabilités et le propriétaire de l'application SBA ne sont pas formellement identifiés dans une documentation telle une matrice RACI (Réalisateur, Approbateur, Consulté et Informé).

## **Critère d'évaluation – 2. Gestion des accès**

Il n'y a pas de procédure formelle concernant la gestion des accès à l'application SBA. La configuration des mots de passe n'est pas conforme au nouveau standard de la Ville. Il n'y a pas de journalisation ni de surveillance des accès dans l'application SBA.

Par contre, les profils d'accès sont gérés de façon satisfaisante pour cette application. Aussi, la révision annuelle et la gestion des comptes génériques et à hauts privilèges sont adéquates.

## **Critère d'évaluation – 3. Gestion des changements**

Il n'y a pas de procédure formelle sur la gestion des changements. Les demandes de changements ne sont pas systématiquement documentées. Pour celles qui le sont, elles ne suivent pas les étapes de mise en production d'un changement ci-dessous :

- Les analyses fonctionnelles par les pilotes et les analyses techniques et d'impacts faites par les développeurs;
- L'approbation par les pilotes et le chef de division;
- Le développement par le développeur;
- Les tests unitaires par les développeurs, les tests d'acceptation par les pilotes et les tests des utilisateurs-experts;
- La mise en production par l'équipe de production au STI.

## **Critère d'évaluation – 4. Pérennité humaine et technique**

Bien que la disponibilité des ressources humaines spécialisées sur le marché soit un enjeu majeur pour les parties prenantes, aucun plan de relève humaine avec un transfert de connaissances n'a été développé. L'application SBA, datant des années 90, fait face à une désuétude technologique.

## **Critère d'évaluation – 5. Gestion des opérations**

La documentation de gestion des opérations de l'application SBA à la disposition des utilisateurs et des pilotes est adéquate.

La gestion des incidents ne fait pas l'objet d'une procédure formelle et ceux-ci ne sont pas documentés systématiquement.

Les copies de sauvegarde de l'application SBA sont effectuées de façon régulière et systématique. Cependant, il n'y a pas de procédure formelle de gestion des copies de sauvegarde propre à l'application SBA ni de tests périodiques de restauration sur ces dernières.

## 5. Annexe

### 5.1. Objectif et critères d'évaluation

#### Objectif

Déterminer si les mécanismes de contrôle mis en place pour l'application système budgétaire automatisé (SBA) permettent de s'assurer que celle-ci ne présente aucun risque majeur de confidentialité, d'intégrité et de disponibilité des données.

#### Critères d'évaluation

##### 1. Rôles et responsabilités

Les rôles et les responsabilités sont définis, approuvés, communiqués et permettent une imputabilité claire. Le propriétaire de l'application est formellement identifié.

##### 2. Gestion des accès

Une procédure de création, de modification, de suppression et de révision des droits d'accès à l'application SBA est adéquatement documentée. L'application utilise des paramètres d'authentification assez robustes pour maintenir un environnement sûr. Les profils et les droits accordés permettent une ségrégation des tâches adéquate afin de prévenir les accès non autorisés et les modifications de données. Des activités de surveillance sont mises en place afin de détecter des incidents en temps opportun.

##### 3. Gestion des changements

Les changements en production sont proprement documentés, tracés, testés et validés par les autorités compétentes. L'accès des programmeurs à l'environnement de production est restreint et contrôlé.

##### 4. Pérennité humaine et technique

Des mises à jour sont appliquées périodiquement permettant d'assurer une évolution technologique adéquate, du personnel qualifié ainsi qu'une relève suffisante tout au long du cycle de vie de l'application.

##### 5. Gestion des opérations

L'application dispose d'une documentation permettant de minimiser les risques opérationnels. Chaque incident en production fait part d'un billet unique qui retrace l'origine, le problème et sa résolution. Un plan d'action est associé aux problèmes et aux incidents de type majeur. Un plan de sauvegarde est documenté et respecté correctement. De plus, des tests de récupération sur les copies de sauvegarde sont effectués sur une base régulière.

