Health Canada Santé Canada

Rapport de vérification Final

Vérification de l'intégrité des données
Interface entre le système source du SGCC et le SAP

avril 2008

Table des matières

Sommaire ..... **ii**

Introduction. . .....…….....…….……..1

Contexte 1
Objectifs de la vérification 1
Portée et approche 2

Constatations, recommandations et réaction de la direction **2**

Exhaustivité et fiabilité des données …..... 2
Mise en concordance des données de sortie et rapprochement 2
Environnement des contrôles en général 3
Examen des comptes d'utilisateurs par la direction 3
Droits d'accès des utilisateurs 4
Dispositions relatives à l'intégrité des données 6
Centre de sauvegarde extérieur 7
Procédures relatives au cycle chronologique de l'élaboration des systèmes 8

Sommaire

Le Système de gestion des contrats et des contributions (SGCC) a été intégré dans toutes les régions de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI) de Santé Canada en décembre 2001, et sa mise en œuvre a été terminée en avril 2002. Le SGCC est un système électronique mis en œuvre à l'échelle du pays pour aider la Direction générale à effectuer la surveillance et la vérification de ses contrats et accords de contribution (CAC), et à rendre des comptes à ce sujet. Le Système d'applications de gestion intégrée des ressources (SAGIR) de Santé Canada utilise la version 3 du SAP pour les demandes de transaction et l'interface avec divers systèmes internes. Le SGCC est l'un des systèmes sources qui fournit des données au SAP. Au cours de l'exercice 2006-2007, le SGCC a permis de traiter l'équivalent d'environ 827 millions de dollars en subventions et en contributions.

La vérification visait les deux objectifs suivants :

- déterminer la qualité des données, en matière d'exactitude et d'exhaustivité, dans les systèmes qui jouent le rôle d'interface avec le SAGIR et le SAP;
- évaluer de façon générale les mesures de contrôle interne qui touchent le SGCC.

L'examen a été mené par le Bureau de la vérification et de la responsabilisation conformément à la *Politique sur la vérification interne* du gouvernement du Canada.

Les résultats des essais détaillés du SGCC et du système SAP ont permis de déterminer que les données transmises au SAP par l'entremise d'interfaces avec d'autres systèmes sont exactes. Il a été impossible de déterminer si ces données sont exhaustives parce que le SGCC ne fournit pas de sommes de contrôle qui permettraient de comparer les données qui entrent dans le SAP et qui en sortent. Cette mesure est requise pour évaluer les données échangées par le SGCC et le SAP. On court donc le risque de ne pas savoir si toutes les données ont été échangées avec le SAP. Au moment d'effectuer la vérification, la DGSTNI ajoutait cette fonctionnalité au SGCC. De façon générale, le contrôle fonctionne de façon satisfaisante, mais il faudra améliorer la documentation des procédures d'exploitation si l'on veut garantir l'uniformité des données.

Introduction

Contexte

Le Système de gestion des contrats et des contributions (SGCC) a été intégré dans toutes les régions de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI) de Santé Canada en décembre 2001, et sa mise en œuvre a été terminée en avril 2002. Le SGCC est un système électronique mis en œuvre à l'échelle du pays pour aider la Direction générale à effectuer la surveillance et la vérification de ses contrats et accords de contribution, et à rendre des comptes à ce sujet.

Le Système d'applications de gestion intégrée des ressources (SAGIR) de Santé Canada utilise le SAP pour les demandes de transaction et les interfaces avec divers systèmes internes, comme le Système de gestion des contrats et des contributions (SGCC). Les données du SAP permettent de générer des rapports financiers et de gestion afin de fournir à la haute direction des renseignements lui permettant de gérer efficacement les ressources financières du Ministère.

La vérification a été entreprise par le Bureau de la vérification et de la responsabilisation conformément au Cadre de vérification fondé sur les risques de Santé Canada et doit couvrir la période allant de 2006-2007 à 2008-2009. Elle a été approuvée le 4 octobre 2006 par le Comité de vérification et d'évaluation du Ministère. La vérification est effectuée conformément à la *Politique sur la vérification interne* du gouvernement du Canada.

Objectifs de la vérification

La vérification visait les deux objectifs suivants :

- déterminer la qualité des données, en matière d'exactitude et d'exhaustivité, dans les systèmes qui jouent le rôle d'interface avec le SAGIR et le SAP;
- évaluer de façon générale les mesures de contrôle interne qui touchent le SGCC.

La vérification portait sur les éléments suivants :

- la mise à jour automatisée de champs dans le SGCC;
- les mesures de contrôle qui permettent de s'assurer que la transmission de toutes les données a été réalisée;
- les mesures de contrôle des transactions;
- le traitement des erreurs;
- la répartition des responsabilités;
- les contrôles d'accès;
- la gestion des problèmes.

Portée et approche

La portée de la vérification mettait l'accent sur l'intégrité des données dans le SGCC, qui possède une interface avec le SAP. La vérification inclut aussi une évaluation des mesures de contrôle internes liées au SGCC. Il a été établi que, pour la période allant du 1er avril 2005 au 31 mars 2006, la valeur totale de toutes les S et C qui sont passées par l'interface entre le SGCC et le SAGIR atteignait environ 827 millions de dollars.

La vérification de l'interface du SGCC a été menée dans la région de la capitale nationale. La vérification a été effectuée principalement sous la forme d'entrevues entre des responsables de Santé Canada, d'un examen des documents pertinents, et de la mise à l'essai des contrôles informatisés en général et des contrôles des applications associées à l'interface entre le SGCC et le SAP. Comme la vérification a été menée au début de 2007, on ne disposait pas de données pour l'intégralité de l'exercice 2006-2007. On a donc décidé de procéder à un examen des fichiers de l'interface pour la période allant du 1er janvier au 31 décembre 2006.

Les données recueillies et analysées provenaient des fichiers de données transférés du SGCC au SAP pendant l'année civile 2006. Des tests spécifiques ont été menés dans la région de l'Ontario. Les fichiers de l'interface ont été comparés aux données figurant dans les fichiers actuels des finances et des programmes.

Le projet a été mené conformément à la *Politique sur la vérification interne* du gouvernement du Canada. La vérification a été effectuée à l'aide des COBIT (objectifs de contrôle pour les technologies de l'information et les technologies connexes) de l'APVCSI, qui est un modèle de régie de la TI.

On a effectué un examen général des contrôles dans le but d'avoir un aperçu général des contrôles qui font partie de l'environnement du SGCC. L'examen des contrôles des applications incluait la validation des saisies de données, le contrôle de l'accès logique, ainsi que l'enregistrement et le traitement des exceptions et des autorisations.

Constatations, recommandations et réaction de la direction

Exhaustivité et fiabilité des données

Mise en concordance des données de sortie et rapprochement

Il faudrait mettre sur pied des procédures permettant de s'assurer que les données de sortie font couramment l'objet d'une mise en concordance avec les sommes de contrôle pertinentes. Il faudrait aussi prévoir des pistes de vérification, qui permettraient un suivi plus facile du

traitement des transactions et le rapprochement des données dans les cas où la transmission a été interrompue.

Nous avons tenté de choisir un échantillon de fichiers d'interface afin d'obtenir une somme de contrôle pour chaque fichier. Nous avons ensuite tenté de valider la somme de contrôle calculée par rapport à la véritable somme de contrôle de l'interface avec le SAP pour les dates en question. Le rapprochement n'a pas pu être effectué parce que le SGCC et le SAP ne sont pas programmés de façon à ce qu'il soit possible de générer des sommes de contrôle pour l'interface.

En l'absence de somme de contrôle, la direction risque de ne pas pouvoir savoir si toutes les données du SGCC ont véritablement été transmises au SAP. Il y a toutefois une mesure de contrôle compensatoire puisqu'un destinataire qui n'a pas reçu le bon paiement dans le délai approprié en informera probablement le Ministère.

Recommandation n° 1

Nous recommandons que le directeur général de la Direction générale de la planification et de la gestion des affaires (DPGA) de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI) élabore un processus de rapprochement des données du SGCC et du SAP.

Réaction de la direction

Recommandation acceptée. La direction est au courant de la situation et tente actuellement d'élaborer un processus automatisé de rapprochement des données du SGCC et du SAP. Le processus a été mis en œuvre le 26 octobre 2007.

Environnement des contrôles en général

Examen des comptes d'utilisateurs par la direction

La direction devrait disposer d'un processus de contrôle lui permettant d'examiner les comptes et d'en confirmer les droits d'accès de façon périodique. Une comparaison périodique des ressources, incluant les responsabilités inscrites, devrait être effectuée dans le but d'en réduire les risques d'erreur, de fraude, d'utilisation abusive ou de modification non autorisée.

Nous n'avons trouvé aucune politique établissant des procédures officielles normatives de fonctionnement en ce qui concerne les examens de l'accès au système par les administrateurs de base de données et les super-utilisateurs :

- les procédures officielles pour l'examen par la direction de l'accès des administrateurs de base de données et des super-utilisateurs du système d'exploitation ne sont pas disponibles ni documentées;

- onze des dix-sept demandes de changement d'un compte d'utilisateur ne mentionnaient pas la raison du changement. Seule les tâches professionnelles liées au privilège de l'utilisateur étaient mentionnées.

Comme aucune politique d'examen de l'accès n'est documentée, le Ministère court le risque que certains privilèges d'accès qui ne sont plus utiles soient encore en vigueur, ce qui peut entraîner des cas d'utilisation abusive. La direction risque aussi de ne pas savoir pourquoi des privilèges d'accès sont accordés ou modifiés.

Recommandation n° 2

On recommande que le directeur général de la Direction de la planification et de la gestion des affaires (DPGA) de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI) :

a) demande au dirigeant principal de l'information (DPI) d'établir et de documenter des procédures d'exploitation normative pour la surveillance des activités des administrateurs de base de données et des super-utilisateurs du SGCC qui ont accès au système d'exploitation;

b) veille à ce que le formulaire de demande d'accès pour les utilisateurs du SGCC soit amélioré de façon à inclure la raison pour laquelle les privilèges relatifs à un compte existant du SGCC sont modifiés.

Réaction de la direction

a) Recommandation acceptée. Le directeur général de la DPGA a consulté le DPI de Santé Canada, qui fournira des procédures normatives d'exploitation pour la surveillance des activités des administrateurs de base de données et des super-utilisateurs du SGCC.

b) Recommandation acceptée. Le formulaire de demande concernant un compte du SGCC sera amélioré de façon à inclure la raison qui explique la modification des privilèges.

Droits d'accès des utilisateurs

Les droits d'accès des utilisateurs aux systèmes doivent être gérés à partir d'un point central et être fondés sur les exigences de leur emploi et les besoins organisationnels documentés et définis. Les droits d'accès des utilisateurs sont demandés et approuvés par les gestionnaires de l'utilisateur et mis en œuvre par l'administrateur du compte du SGCC (et, en partie, par un administrateur du réseau local Novell de Santé Canada). Des procédures devraient aussi être créées pour garantir que seuls les employés autorisés effectuent de la saisie des données.

Les droits d'accès des utilisateurs au SGCC sont gérés à partir d'un point central par l'équipe de soutien du SGCC de la Direction de la planification et de la gestion des affaires (DPGA) de la

DGSPNI. Ils sont établis en fonction des besoins opérationnels définis et documentés et des exigences professionnelles. Le gestionnaire de l'utilisateur s'occupe de demander et d'approuver ces droits, qui sont mis en œuvre par l'équipe de soutien du SGCC. Tous les six mois, l'équipe de soutien du SGCC produit un relevé qui mentionne les utilisateurs actuels du SGCC. Ce relevé est envoyé aux gestionnaires régionaux afin qu'ils l'examinent. Nous avons examiné le relevé pour la région de l'Ontario et avons constaté que quatorze des vingt-sept utilisateurs de l'Ontario ne s'étaient pas connectés au SGCC depuis 2005.

En outre, aucune procédure ne semblait exister en ce qui concerne l'octroi et l'approbation des privilèges pour les administrateurs de base de données ou les super-utilisateurs en ce qui concerne l'accès au système d'exploitation. Les comptes des administrateurs de base de données sont administrés par le DPI, et non par la DPGA, et ne font pas l'objet d'une supervision équivalente à celle des comptes des utilisateurs du SGCC. Cet écart s'explique par le fait que les administrateurs de base de données ont besoin d'un accès direct à la base de données Oracle du SGCC, tandis que les utilisateurs du SGCC n'ont pas accès à cette base de données. Le Ministère court le risque qu'un membre de l'équipe des administrateurs de base de données ou un super-utilisateur exécute une tâche qui ne sera pas détectée et ne fera pas partie des attentes de l'équipe de gestion du SGCC. Il existe aussi un risque d'accès non autorisé à la base de données du SGCC.

Recommandation n° 3

On recommande que le directeur général de la Direction de la planification et de la gestion des affaires (DPGA) de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI) :

a) demande à la DPI de mettre en œuvre et de documenter des procédures normatives d'exploitation pour les administrateurs de données concernant l'approbation des privilèges des administrateurs de base de données et des super-utilisateurs qui ont accès au système d'exploitation;

b) demande que toutes les régions examinent attentivement la date à laquelle chaque utilisateur a accédé pour la dernière fois au SGCC, et désactivent les comptes des utilisateurs qui n'ont pas accédé au SGCC depuis un nombre préétabli de mois.

Réaction de la direction

a) Recommandation acceptée. Le directeur général de la DPGA a consulté le DPI, et ils s'occuperont de mettre en œuvre et de documenter des procédures normatives d'exploitation permettant d'approuver les privilèges des administrateurs de base de données et des super-utilisateurs.

b) Recommandation acceptée. Les gestionnaires de comptes, dans les régions, continueront d'effectuer, tous les six mois, un examen de tous les comptes de leur région, et porteront une attention particulière à la date du dernier accès.

Dispositions relatives à l'intégrité des données

Il faudrait prévoir des procédures qui permettraient de s'assurer que, le cas échéant, les programmes d'application contiennent des dispositions qui prévoient une vérification automatique des tâches effectuées par le logiciel afin de garantir l'intégrité des données, et de permettre le rétablissement de l'intégrité grâce à une reprise au point de contrôle (une fonction d'un logiciel de gestion de base de données qui permet de renverser une transaction de façon à ce que les données retournent à leur état d'avant la transaction). Une reprise au point de contrôle est effectuée quand une transaction prend fin de façon anormale et qu'il faut recommencer. Les procédures automatiques qui permettent de garantir l'intégrité des données devraient être documentées.

Les procédures de maintien de l'intégrité des données ne sont pas documentées parce que le Ministère n'a pas de politique obligeant la documentation des procédures normatives d'exploitation pour les administrateurs de base de données. Il existe un risque que, si un administrateur de base de données ou son remplaçant n'est pas disponible, il faudra beaucoup de temps à la personne qui les remplacera pour savoir quelles procédures de maintenance de la base de données elle doit effectuer, et la façon dont elle doit le faire. Cela pourrait entrainer des retards dans la restauration de la base de données.

Recommandation n° 4

On recommande que le directeur général de la Direction de la planification et de la gestion des affaires (DPGA), au sein de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI), demande au DPI de documenter toutes les procédures afin de garantir l'intégrité des données et de corriger les problèmes liés aux bases de données.

Réaction de la direction

Recommandation acceptée. Le directeur général de la DPGA a consulté le DPI, et ils prépareront des procédures permettant de garantir l'intégrité des données et de corriger les problèmes des bases de données.

Centre de sauvegarde extérieur

L'entreposage à l'extérieur des supports de sauvegarde, des documents et des autres ressources de PI essentiels doit être organisé de façon à faciliter leur récupération et à appuyer les plans de poursuite des activités.

Il n'existe pas de procédures normatives officielles d'exploitation concernant les centres de sauvegarde extérieurs. Nous avons interrogé des administrateurs de base de données Oracle pour le SGCC, ainsi que des employés du groupe responsable du serveur du Centre de services du réseau et des systèmes (CSRS). Nous avons appris que des sauvegardes sur bande magnétique sont effectuées de façon quotidienne, hebdomadaire, mensuelle et annuelle et font l'objet d'une rotation. Les rotations quotidiennes et hebdomadaires sont conservées sur place, au centre de traitement. Les bandes mensuelles et annuelles sont conservées à l'extérieur. Le CSRS effectue un contrôle des bandes envoyées par le centre de traitement vers le lieu de sauvegarde extérieur ou reçu par le centre de traitement en provenance du lieu de sauvegarde.

Nous n'avons découvert aucune preuve de la création de relevés ou de registres permettant de s'assurer que des sauvegardes réussies étaient vraiment effectuées. L'absence de relevé ou de registre est attribuable à l'absence d'exigences concernant la documentation des procédures de sauvegarde. Il existe un risque que des archives de données en particulier ne se trouvent pas au centre de sauvegarde extérieur ou ne soient pas disponibles pour être restaurées quand on en aura besoin.

Recommandation n° 5

On recommande que le directeur général de la Direction de la planification et de la gestion des affaires (DPGA), au sein de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI), demande au DPI de documenter les procédures d'entreposage à l'extérieur et de sauvegarde. Ces procédures devraient inclure, au moins, les éléments suivants :

- *des directives sur la façon d'effectuer les sauvegardes;*
- *des directives sur la façon de s'assurer que la sauvegarde a bel et bien fonctionné;*
- *des directives permettant de s'assurer que le dispositif de stockage de fichier de sauvegarde peut être utilisé pour restaurer la base de données avec succès;*
- *des directives concernant l'étiquetage adéquat des dispositifs de stockage de fichiers de sauvegarde;*
- *des directives pour l'expédition des dispositifs de stockage de fichiers de sauvegarde vers le centre de sauvegarde extérieur;*
- *des directives concernant la réception des dispositifs de stockage de fichiers de sauvegarde en provenance du centre de sauvegarde extérieur;*
- *la durée de conservation des dispositifs de stockage de fichiers de sauvegarde;*

- *des directives concernant la surveillance du processus de sauvegarde et la transmission des moyens de sauvegarde entre le centre de données et les installations de sauvegarde extérieure.*

Réaction de la direction

Recommandation acceptée. Le directeur général de la DPGA a consulté le DPI, et ils fourniront de la documentation concernant les procédures de sauvegarde des bases de données et d'entreposage extérieur.

Procédures relatives au cycle chronologique de l'élaboration des systèmes

La méthode relative au cycle chronologique de l'élaboration des systèmes (CCES) de Santé Canada s'appuie sur les éléments suivants :

- des mécanismes adéquats de définition et de documentation des exigences en matière d'entrée de données concernant tout projet de modification, d'élaboration de système ou d'application;
- des mesures adéquates de définition, de conception et de documentation de toutes les interfaces externes et internes;
- des mécanismes adéquats de définition et de documentation des exigences en matière de sortie en ce qui concerne tout projet de modification, d'élaboration de système ou d'application.

Il n'existe aucune méthode officielle documentée concernant le CCES. Des mécanismes de définition et de documentation des exigences en matière d'entrée ou des changements en matière d'entrée utilisent la base de données de suivi du SGCC. Le SGCC est une application standard disponible sur le marché (COTS) adaptée à l'origine pour répondre aux besoins de la DGSPNI. Le fournisseur doit s'occuper d'apporter tout changement aux tableaux ou au code source. L'équipe de soutien du SGCC ne peut apporter que des changements limités aux valeurs de certains champs de données modifiables. Aucun changement ne peut être apporté aux champs d'entrée ou de sortie puisque les champs de saisie requis du SAP ne peuvent être modifiés, et que le format des fichiers de sortie du SGCC est incorporé au programme du SGCC et ne peut être modifié que par le fournisseur.

Même si le format de l'interface externe du SAP a été déterminé au préalable et mis en place, il n'existe pas de méthode ni de lignes directrices générales précisant de quelle façon les interfaces externes et internes du SGCC doivent être définies, conçues ou documentées dans l'avenir. Il n'existe pas, non plus, de mécanisme de définition et de documentation des exigences relatives aux fonctions de sortie du SGCC vers le SAP. En l'absence d'un CCES documenté, il existe un risque que, dans le cadre d'un projet de maintien ou de développement du SGCC, des exigences

opérationnelles ou des fonctionnalités concernant les interfaces de données ne soient pas prises en compte ou soient mises en œuvre de façon erronée.

Recommandation n° 6

On recommande que le directeur général de la Direction de la planification et de la gestion des affaires (DPGA), au sein de la Direction générale de la santé des Premières nations et des Inuits (DGSPNI), utilise une méthode axée sur le CCES pour documenter l'interface SGCC-SAP.

Réaction de la direction

Recommandation acceptée. Un document sera élaboré afin de cerner et de décrire le processus actuel d'interface entre le SGCC et le SAP.