Emploi et Développement social Canada
Employment and Social Development Canada

Maintenant et demain, l'excellence dans tout ce que nous entreprenons

Protégé A

Direction générale des services de vérification interne

Audit des contrôles ministériels en matière de système d'information et de technologie de l'information – Phase 1 – Contrôles des applications

Novembre 2014

SP-1084-01-15F

Canada

Vous pouvez télécharger cette publication en ligne à : http://www12.rhdcc.gc.ca.

Ce document est offert sur demande en médias substituts (gros caractères, braille, audio sur cassette, audio sur DC, fichiers de texte sur disquette, fichiers de texte sur DC ou DAISY), en composant le 1 800 O-Canada (1-800-622-6232). Les personnes qui utilisent un téléscripteur (ATS) doivent composer le 1-800-926-9105.

PDF
Cat. nº : Em20-22/2015F-PDF
ISBN : 978-0-660-23152-5

Table des matières

Sommaire exécutif

Les contrôles généraux liés à la technologie de l'information (CGTI) forment un ensemble d'activités de contrôle établi dans l'environnement des technologies de l'information (TI). Ces contrôles peuvent être appliqués à tous les systèmes, applications, processus et ensembles de fichiers de données sur lesquels le Ministère s'appuie pour prendre des décisions dans ses activités courantes. Les CGTI ont été établis pour assurer l'élaboration et la mise en œuvre adéquates des applications, ainsi que l'intégrité des programmes, des fichiers de données et des opérations informatiques. Les CGTI créent l'environnement de TI dans lequel fonctionnent les applications, et ils consistent en deux types de contrôles : les contrôles généraux et les contrôles des applications.

Les contrôles généraux (CGTI) comprennent les contrôles d'accès, les contrôles de sauvegarde et de restauration, et les contrôles des opérations informatiques. Les contrôles des applications, qui sont propres aux programmes informatiques, visent notamment l'exactitude et l'exhaustivité des entrées et des sorties de données, la validité des transactions, et l'établissement de rapports. Les CGTI et les contrôles des applications relèvent du cadre général des contrôles ministériels en matière de système d'information et de technologie de l'information (CMSITI).

Le personnel d'Emploi et Développement social Canada (EDSC) utilise quotidiennement plus de 300 applications pour la réalisation des activités opérationnelles. Une série de critères a été employée pour évaluer ces 300 applications, afin de déterminer celles qui devraient faire l'objet du présent audit. Aussi, puisque le Bureau du vérificateur général (BVG), dans son rapport sur les comptes publics, évalue annuellement les CGTI pour les deux programmes législatifs majeurs d'EDSC (le programme d'assurance-emploi [AE] et le Régime de pensions du Canada [RPC]), les contrôles généraux qui appuient directement ces programmes importants ne font pas partie de notre examen. Pour être sélectionnées, les applications devaient satisfaire aux critères énoncés ci-dessous. Elles devaient :

- être utilisées pour plus d'un programme;
- être en production;
- avoir été développées à l'interne, ou être très personnalisées;
- avoir une forte incidence sur l'exécution d'un programme ou de programmes en particulier;
- faire l'objet de changements complexes;
- ne pas être visées par un remplacement dans un avenir rapproché;
- être liées à un volume élevé de transactions ou d'activités;
- avoir d'importantes répercussions financières;
- avoir une incidence sur les Canadiens et Canadiennes.

Les trois systèmes suivants ont été sélectionnés pour l'audit en fonction de ces critères de sélection et de l'évaluation initiale des risques qui a été effectuée :

- Système ministériel des comptes débiteurs (SMCD)
- Système commun pour les subventions et les contributions (SCSC)
- Numéro d'assurance sociale/Registre d'assurance sociale (NAS/RAS)

Objectif de l'audit

L'objectif est d'évaluer la pertinence des CMSITI pour les applications vérifiées dans la phase 1 de l'audit.

Sommaire des constatations principales

- Les systèmes de traitement/contrôles automatisés ont été conçus de manière adéquate, et ils fonctionnent efficacement, de manière à ce que les transactions soient exactes, rapides et traitées comme prévu.

- Lorsque les systèmes sont planifiés, conçus et programmés, les mesures et les contrôles d'accès logiques sont pris en considération afin d'empêcher l'accès, la modification ou la divulgation non autorisés des données du système. PROTÉGÉ

- Les sauvegardes sont effectuées fréquemment et systématiquement. Toutefois, le Ministère n'a pas d'entente sur les niveaux de service (ENS) ou de protocole d'entente (PE) avec Services partagés Canada (SPC) qui soit écrit et clair. De plus, les sauvegardes de données système ne sont pas mises à l'essai périodiquement pour vérifier si elles sont exactes et complètes, et le Ministère risque donc de ne pas avoir les registres complets de la « dernière bonne copie » de ses données système.

- Les systèmes de sortie/contrôles automatisés ont été conçus adéquatement et ils fonctionnent efficacement pour que les transactions soient exactes, rapides et traitées comme prévu.

- Les trois applications ont une piste d'audit, et les fichiers du journal d'audit sont tenus à jour. PROTÉGÉ

Conclusion de l'audit

Le Ministère a conçu adéquatement les contrôles automatisés de traitement des applications pour les systèmes d'information ministériels visés par l'audit. Toutefois, il est d'après nous nécessaire d'améliorer les points faibles notés dans le présent rapport PROTÉGÉ de sauvegarde. Cela permettra de perfectionner et de renforcer les contrôles de TI qui sont déjà en place afin de s'assurer que les CMSITI fonctionnent comme prévu.

Recommandations

- La Direction générale de l'innovation, de l'information et de la technologie (DGIIT), en collaboration avec les responsables opérationnels des applications pour le SMCD (Direction générale de l'agent principal des finances, ou DGAPF), le SCSC (Direction générale des opérations de programmes, ou DGOP), et NAS/RAS (Direction générale des services d'intégrité, ou DGSI), devraient avoir une ENS ou un PE avec SPC qui soit clair et écrit, et dans lequel sont définis les rôles et les responsabilités en ce qui a trait à la création et à la gestion des sauvegardes. Plus précisément, la DGIIT devrait

déterminer avec SPC qui est responsable de mettre à l'essai les sauvegardes produites par SPC pour s'assurer qu'elles sont complètes et disponibles dans l'éventualité où les données doivent être restaurées.

- PROTÉGÉ

1.0 Renseignements généraux

1.1 Contexte

Les CGTI forment un ensemble d'activités de contrôle établi dans l'environnement de TI. Ces contrôles peuvent être appliqués à tous les systèmes, applications, processus et ensembles de fichiers de données sur lesquels le Ministère s'appuie pour prendre des décisions dans ses activités courantes. Les CGTI ont été établis pour assurer l'élaboration et la mise en œuvre adéquates des applications, ainsi que l'intégrité des programmes, des fichiers de données et des opérations informatiques. Les CGTI créent l'environnement de TI dans lequel fonctionnent les applications, et ils consistent en deux types de contrôles : les contrôles généraux et les contrôles des applications.

Les contrôles généraux (CGTI) comprennent les contrôles d'accès, les contrôles de sauvegarde et de restauration, et les contrôles des opérations informatiques. Les contrôles des applications, qui sont propres aux programmes informatiques, visent notamment l'exactitude et l'exhaustivité des entrées et des sorties de données, la validité des transactions, et l'établissement de rapports. Les CGTI et les contrôles des applications relèvent du cadre général des CMSITI.

Le personnel d'Emploi et Développement social Canada (EDSC) utilise quotidiennement plus de 300 applications pour réaliser les activités opérationnelles. Une série de critères a été utilisée pour évaluer ces 300 applications dans le but de déterminer celles qui devraient faire l'objet du présent audit. Aussi, puisque le BVG, dans son rapport sur les comptes publics, évalue annuellement les CGTI pour les deux programmes législatifs majeurs d'EDSC (AE et le RPC), les contrôles généraux qui appuient directement ces programmes importants ne font pas partie de notre examen. Pour être sélectionnées, les applications devaient satisfaire aux critères énoncés ci-dessous. Elles devaient :

- être utilisées pour plus d'un programme;
- être en production;
- avoir été développées à l'interne, ou être très personnalisées;
- avoir une forte incidence sur l'exécution d'un programme ou de programmes en particulier;
- faire l'objet de changements complexes;
- ne pas être visées par un remplacement dans un avenir rapproché;
- être liées à un volume élevé de transactions ou d'activités;
- avoir d'importantes répercussions financières;
- avoir une incidence sur les Canadiens et Canadiennes.

1.2 Objectif de l'audit

L'objectif est d'évaluer la pertinence des CMSITI pour les applications vérifiées dans la phase 1 de l'audit.

1.3 Portée

Les travaux sont effectués sous l'égide des CMSITI en suivant une approche progressive qui s'étalonnera sur quelques années.

Une série de critères, décrits à la section 1.1, ont été utilisés pour sélectionner les applications et les principales interfaces connexes clés à vérifier.

La première phase de l'audit des CMSITI visait les applications sélectionnées et les contrôles généraux associés au NAS/RAS, au SMCD, au SCSC et à leurs principales interfaces choisies. L'annexe C donne un aperçu des applications et des interfaces connexes retenues.

Puisque la DGIIT met actuellement en œuvre le Plan d'action de la direction (PAD), qui a été élaboré pour donner suite au rapport d'évaluation du programme de sécurité de l'information de Gartner, les éléments du rapport Gartner n'ont pas été intégrés au présent audit. De plus, la Direction générale des services de vérification interne (DGSVI) entreprendra une évaluation de la sécurité de la TI afin de fournir un aperçu du niveau de sécurité de la TI au sein du Ministère et de signaler les tendances à cet égard. Cela permettra de cerner et d'évaluer les secteurs de risque, notamment de repérer les lacunes et les chevauchements, en tenant compte de ce qui a déjà été couvert dans les audits, les évaluations et les examens récents, pour déterminer l'orientation future de l'audit. De plus, la DGSVI a des missions prévues qui seront réalisées dans les années subséquentes, conformément aux engagements pris dans le contexte des audits de la sécurité de la TI.

1.4 Méthodologie

La phase 1 de l'audit des CMSITI a été réalisée suivant un certain nombre de méthodologies, notamment des entrevues, des révisions des processus opérationnels, des questionnaires de contrôle, des examens de contrôle, ainsi qu'un examen et une analyse des schémas, des diagrammes, et des documents sur le déroulement des processus.

Des schémas du processus ont aussi été préparés pour le SCSC et le SMCD relativement à leur apport dans les états financiers ministériels.

Le travail d'audit sur le terrain a été réalisé entre juin et septembre 2014.

2.0 Constatations de l'audit

Voici les points forts et les points à améliorer en ce qui a trait aux CMSITI.

2.1 Les données sont traitées avec exactitude et rapidité

Les contrôles de l'entrée de données sont importants, car ils permettent d'assurer le caractère exact, exhaustif et rapide de l'entrée et du transfert de données, ou de leur conversion à partir d'une source originale vers une application informatique. Les données peuvent être entrées dans une application informatique de manière manuelle, en ligne, ou au moyen d'une opération de traitement par lots (opération automatisée). Dans l'examen de contrôles d'entrée, il est important de déterminer le caractère adéquat des contrôles tant manuels qu'automatisés, afin d'assurer l'exactitude des entrées de données grâce à l'utilisation optimale de la validation et de l'édition par ordinateur. Il est aussi important que les procédures de traitement des erreurs facilitent une nouvelle soumission rapide et exacte de toutes les données corrigées. D'après nos procédés d'audit, les contrôles d'entrée des données pour le SMCD, le SCSC, et le NAS/RAS fonctionnent efficacement.

Lorsque des données sont envoyées dans le SMCD, le SCSC et NAS/RAS, le système vérifie automatiquement le fichier séquentiel pour s'assurer d'obtenir le bon numéro de séquence. Par exemple, des contrôles de validation sont en place afin qu'un lot traité ait un numéro de séquence qui suit celui du dernier lot traité. De plus, un rapprochement annuel est effectué par le personnel d'EDSC du bureau de Bathurst, au Nouveau-Brunswick, avec les données du système d'application du RPC, afin de s'assurer que les données transférées à partir du programme concordent avec celles de NAS/RAS. Des contrôles sont aussi en place pour les entrées de données dans les champs (p. ex., nombre établi de chiffres par champ, vérification du NAS, lettres seulement, données numériques seulement, séparation des tâches dans le SCSC, tableaux pré-remplis et menus déroulants).

Pour l'interface du SMCD avec le système du programme canadien de prêts aux étudiants (PCPE), les taux d'intérêt sont pré-établis dans le système afin que les utilisateurs ne puissent pas les changer. Les taux sont saisis dans le SMCD par le personnel des Systèmes financiers, qui n'a pas la capacité de modifier ou d'approuver les transactions dans le SMCD. Ces taux sont changés uniquement lorsque le secteur de programme (p. ex., PCPE) l'avertit d'un changement de taux.

Les rapports de contrôle de la qualité sont produits par les trois systèmes pour le traitement par lots, afin de détecter et d'identifier les anomalies. Ces rapports sont examinés par l'équipe d'assurance de la qualité des applications respectives après chaque traitement de lot. En plus des séquences de dossier utilisées pour la validation de données, l'application vérifiera les enregistrements d'en-tête[1] pour l'identification de la source, et les enregistrements de fin[2] pour confirmer le nombre d'enregistrements. En ce qui a trait au SMCD, les rapports de contrôle de la

1 Les enregistrements d'en-têtes sont des structures d'information. Elles identifient l'information qui suit, par exemple, un bloc d'octets dans un flux de communication.

2 Les enregistrements de fin sont les informations qui occupent plusieurs octets à la fin d'un bloc de données transmises. Les enregistrements d'en-tête et les enregistrements de fin contiennent des données de contrôle d'erreur qui sont utiles pour confirmer l'exactitude et le statut de la transmission.

qualité contiennent aussi un total de contrôle[3], pour vérifier la somme d'un champ particulier pour toutes les données transférées et le comparer avec le même total de contrôle du fichier d'entrée avant les entrées dans le SMCD.

En ce qui concerne les transactions rejetées, par exemple un échec de validation électronique (p. ex., mauvais NAS transféré à partir du système d'application du PCPE et de la base de données provinciale sur l'état civil), les agents de Bathurst effectuent une vérification manuelle des données à l'écran pour s'assurer que les données transférées à partir du PCPE vers NAS/RAS sont exactes. Ces écrans « en ligne » comportent divers contrôles de validation pour les entrées invalides, et ils affichent des messages d'erreur en conséquence. De plus, l'écran « en ligne » demandera aussi aux agents de revérifier l'information saisie, afin qu'aucune erreur de saisie de données n'ait été faite avant la poursuite des procédures.

Les trois systèmes ont aussi des contrôles adéquats par rapport à la séparation des tâches. Par exemple, dans le SMCD, un utilisateur ne peut pas avoir un profil lui permettant à la fois de modifier et d'approuver une transaction. D'une façon similaire, dans le SCSC, des contrôles automatisés des applications empêchent les utilisateurs d'avoir en même temps des profils pour l'entrée de données et l'approbation.

Par conséquent, à la lumière des contrôles mis à l'essai pour le traitement, nous concluons que les contrôles automatisés ont été conçus adéquatement et fonctionnent efficacement pour veiller à ce que les transactions soient traitées avec exactitude et rapidité.

2.2 Les contrôles liés à PROTÉGÉ aux sauvegardes doivent être renforcés

PROTÉGÉ

3 Méthode pour assurer l'exactitude des données traitées. Il s'agit du total de plusieurs champs de données dans un fichier, y compris les champs qui ne sont pas normalement utilisés dans les calculs, par exemple le numéro de compte. Aux diverses étapes de traitement, le total de contrôle est recalculé et comparé avec l'original. Si une donnée a été perdue ou modifiée, une non-concordance indique une erreur.

Sauvegardes

L'objectif principal des sauvegardes est de pouvoir récupérer des données perdues à la suite de leur suppression, de leur corruption ou même d'un sinistre. La perte de données peut être une expérience courante pour les utilisateurs d'ordinateurs ou dans les applications, et les contrôles de reprise après sinistre et de planification de la continuité des opérations sont donc nécessaires. Pour que le processus de sauvegarde soit fiable et fonctionne comme prévu, il faut effectuer régulièrement des essais de sauvegarde.

Les essais de sauvegarde présentent des avantages. Premièrement, ils permettent de vérifier l'intégrité des données sans se référer aux fichiers originaux. Deuxièmement, ils permettent d'éviter d'avoir à faire des copies superflues de fichiers, ce qui améliore la vitesse de sauvegarde. Un grand nombre d'organisations font appel à des tiers pour mettre à l'essai, valider et optimiser leurs opérations de sauvegarde.

Dans le présent audit, il a été constaté durant les entrevues que les trois applications sélectionnées respectent les procédures de sauvegarde normalisées, particulièrement en ce qui a trait à la fréquence du processus de synchronisation des fichiers. À l'heure actuelle, EDSC s'appuie sur SPC pour les opérations de sauvegarde du SMCD, du SCSC et de NAS/RAS. À la lumière des entrevues réalisées, EDSC utilisait les sauvegardes dans le passé pour régler de manière sélective les problèmes cernés dans les trois systèmes d'application; toutefois, EDSC n'a pas eu à effectuer de restauration complète de la base de données. La capacité de restaurer la base de données complète de l'un ou l'autre de ces systèmes n'a pas encore été vérifiée.

De plus, il n'existe aucun PE et aucune ENS entre EDSC et SPC pour ce qui est des services de sauvegarde fournis par SPC. Toutefois, les ENS qui étaient en place avant la création de SPC sont respectées. Avec une ENS ou un PE, il sera plus facile de comprendre les rôles et les responsabilités relativement à la création et à la gestion des sauvegardes, et EDSC pourra s'assurer que les contrôles de sauvegarde adéquats sont en place.

Une sauvegarde complète est créée quotidiennement pour le SMCD. Chaque semaine, les renseignements provenant des sauvegardes quotidiennes sont compilés et enregistrés dans une

autre base de données. Avant chaque nouvelle version ou mise à jour du SMCD, une sauvegarde séparée est effectuée au cas où il y aurait, après-coup, un pépin dans le système.

En ce qui concerne le SCSC, les sauvegardes de données pour le système d'application des Ententes sur le développement du marché du travail (EDMT Web) et l'interface SMCD sont traitées par SPC, qui effectue les sauvegardes quotidiennes. Le SCSC conserve également pendant quatre semaines une sauvegarde du fichier séquentiel qu'il a envoyé au SMCD par l'intermédiaire de son fichier séquentiel SMCD. De plus, le SCSC effectue des vérifications de la qualité une fois que tous les fichiers ont été traités, afin de s'assurer que les données sont sauvegardées adéquatement.

En ce qui a trait à NAS/RAS, ses données sont hébergées sur PROTÉGÉ. Dans ce cas, PROTÉGÉ sont responsables des services d'intégrité et de récupération des données.

Recommandation

La DGIIT, en collaboration avec les responsables opérationnels des applications pour le SMCD (DGAPF), le SCSC (DGOP) et NAS/RAS (DGSI) devraient avoir une ENS ou un PE avec SPC qui soit clair et écrit, et dans lequel sont définis les rôles et les responsabilités en en ce qui a trait à la création et à la gestion des sauvegardes. Plus précisément, la DGIIT devrait déterminer avec SPC qui est responsable de mettre à l'essai les sauvegardes produites par SPC pour s'assurer qu'elles sont complètes et disponibles dans l'éventualité où les données doivent être restaurées.

Réponse de la direction

La DGIIT ne croit pas qu'elle doive mettre en place des ENS pour des détails aussi précis que les sauvegardes par application – les tâches nécessaires pour les créer initialement et maintenir un tel niveau de détails dans les ENS entraîneraient des coûts prohibitifs. Toutefois, nous nous efforçons d'accroître la rigueur. La DGIIT élabore actuellement un protocole de fonctionnement qui décrira les secteurs où des PE et des ENS sont requis, le niveau attendu de rendement opérationnel ainsi que les procédures de renvoi aux paliers supérieurs. La date d'achèvement estimée est le 31 mars 2015.

2.3 Les contrôles des extrants ont été conçus adéquatement et ils fonctionnent efficacement

Les contrôles de sortie de données sont utilisés pour assurer l'intégrité des données transmises ainsi que la diffusion adéquate, exhaustive et rapide de tous les extrants produits. Les extrants peuvent être des documents papier, des fichiers utilisés comme intrants dans d'autres systèmes, ou des renseignements diffusés aux fins de consultation en ligne. Le caractère adéquat des contrôles d'extrants a été évalué pour s'assurer que les résultats du traitement des données sont exacts et fiables, que les totaux des contrôles d'extrants sont précis et vérifiés, et que les renseignements qui en découlent sont transmis aux utilisateurs finaux de manière opportune et cohérente.

Le SMCD génère des renseignements financiers qu'il transmet par l'intermédiaire de l'interface du Système d'aide à la décision (SAD), laquelle reçoit les renseignements financiers aux fins de la préparation des états financiers et des rapports de comptes publics du Ministère. D'une manière similaire à celle des contrôles d'extrants pour le SCSC, les fichiers séquentiels transférés du SMCD vers le SAD passent par un processus automatique de validation des données. Le SMCD vérifie le numéro de séquence pour s'assurer qu'il suit la bonne séquence, en plus de valider le dossier et les totaux de contrôle avant traitement.

Le SCSC transmet dans le SMCD l'information sur tout trop-payé ou montant dû par les clients, par l'intermédiaire d'une sortie de fichier séquentiel. La sortie de fichier séquentiel dans le SMCD passe par un processus automatique de validation des données. Le SCSC vérifie le numéro de séquence pour s'assurer qu'il suit la bonne séquence, en plus de valider le dossier et les totaux de contrôle avant traitement. D'autres extrants sont générés en temps réel, par exemple SCSC et EDMT-Web, et par le fait même, ils n'ont besoin d'aucun contrôle sur les fichiers d'interface.

En ce qui a trait à NAS/RAS, s'il y a des problèmes avec des transactions particulières, les données peuvent être réenvoyées pour validation par le système du PCPE, ou les NAS individuels peuvent être validés et extraits de nouveau à partir du système du RPC.

Des rapports de contrôle de la qualité sont aussi produits pour les trois applications afin de montrer le comptage des enregistrements des données extraites, dans le but de valider que la sortie de données est terminée. De plus, les trois applications effectuent des contrôles de validation automatique[4] pour s'assurer que le numéro de séquence d'un lot traité suit celui du précédent.

2.4 Les pistes d'audit sont maintenues, PROTÉGÉ

Une piste d'audit est un dossier chronologique, un ensemble de dossiers, et/ou une destination et une source de dossiers liés à la sécurité qui fournit une preuve documentaire de la séquence des activités. Les dossiers d'audit découlent des activités ou des transactions qui sont traitées au moyen des applications. Les pistes d'audit peuvent mettre en évidence tous les renseignements liés à une entrée, modification, création ou suppression particulière de transaction dans une application précise.

Tous les accès NAS et les mises à jour de compte sont enregistrés dans une piste d'audit en ligne tenue à jour par l'application du RAS. La piste d'audit **PROTÉGÉ** est utilisée à des fins d'enquête. **PROTÉGÉ**.

PROTÉGÉ

En ce qui concerne le SMCD, une piste d'audit est maintenue pour les transactions effectuées dans le SMCD. **PROTÉGÉ** peuvent être utilisés à des fins d'enquête. **PROTÉGÉ**.

4 La validation de données est le processus consistant à s'assurer que les données avec lesquelles une application fonctionne sont épurées, correctes et utiles.

En ce qui a trait au SCSC, tous les écrans consultés par les utilisateurs sont surveillés, en plus de tous les comptes NAS consultés. La piste d'audit retient de telles informations, qui pourront être utilisées dans le cadre d'une enquête, PROTÉGÉ.

PROTÉGÉ

Recommandation

PROTÉGÉ

Réponse de la direction

Le SMA, DGSI, accepte cette recommandation, et il mobilisera des partenaires et fera l'analyse nécessaire PROTÉGÉ. Ces mesures devraient être réalisées d'ici septembre 2015.

3.0 Conclusion

Le Ministère a conçu adéquatement les contrôles automatisés de traitement des applications pour les systèmes d'information ministériels visés par l'audit. Toutefois, il est d'après nous nécessaire d'améliorer les points faibles notés dans le présent rapport **PROTÉGÉ** de sauvegarde. Cela permettra de perfectionner et de renforcer les contrôles de TI qui sont déjà en place afin de s'assurer que les CMSITI fonctionnent comme prévu.

4.0 Énoncé d'assurance

Selon notre jugement professionnel, les procédures d'audit appliquées et les éléments probants recueillis sont suffisants et appropriés pour confirmer l'exactitude des constatations présentées dans ce rapport. Ces dernières sont fondées sur les observations et les analyses faites lors de l'audit. Elles s'appliquent uniquement à l'évaluation des CMSITI pour les interfaces vérifiées du SMCD, du SCSC et de NAS/RAS. Les éléments probants ont été recueillis conformément aux *Normes relatives à la vérification interne au sein du gouvernement du Canada* et aux *Normes internationales pour la pratique professionnelle de l'audit interne*.

Annexe A : Évaluation des critères d'audit

PROTÉGÉ

Annexe B : Glossaire

AE	Assurance-emploi
ARC	Agence du revenu du Canada
ARNAS	Accès rapide au numéro d'assurance sociale
BVG	Bureau du vérificateur général du Canada
CGTI	Contrôles généraux liés à la technologie de l'information
CMSITI	Contrôles ministériels en matière de système d'information et de technologie de l'information
CPRP	Chef de la protection des renseignements personnels
DGAPF	Direction générale de l'agent principal des finances
DGIIT	Direction générale de l'innovation, de l'information et de la technologie
DGOP	Direction générale des opérations de programmes
DGSI	Direction générale des services d'intégrité
DGSVI	Direction générale des services de vérification interne
EDMT	Ententes sur le développement du marché du travail
EDSC	Emploi et Développement social Canada
ENS	Entente sur les niveaux de service
GSTI	Gestion de la sécurité des technologies de l'information
NAS	Numéro d'assurance sociale
NAS/RAS	Numéro d'assurance sociale/Registre d'assurance sociale
PAD	Plan d'action de la direction
PCPE	Programme canadien de prêts aux étudiants
PE	Protocole d'entente
RPC	Régime de pensions du Canada
SAD	Système d'aide à la décision
SAP	Systèmes, applications et produits de traitement de données
SCSC	Système commun pour les subventions et les contributions
SERTI	Système d'exécution du renouvellement de la technologie de l'information
SMCD	Système ministériel des comptes débiteurs
SMCDCOM	SMCD - interface de communication
SPC	Services partagés Canada
TI	Technologie de l'information

Annexe C : Aperçu des applications et des interfaces sélectionnées

NAS/RAS

Le NAS/RAS joue un rôle essentiel dans le fonctionnement des programmes tels l'AE, le RPC, la SV et le PCPE. Il contient des renseignements sur chaque personne ayant reçu un NAS, ce qui comprend les informations fournies dans la demande originale par le client. Le RAS conserve les dossiers liés aux changements de nom, aux autres modifications, aux demandes de remplacement de carte et aux renseignements sur les comptes spéciaux.

Les interfaces associées au NAS/RAS ont été examinées sur la base des critères énoncés à la page 4 du présent rapport, afin de déterminer celles qui seraient visées par l'audit. Par conséquent, les contrôles des applications de NAS/RAS et ses interfaces clés avec le PCPE, le RPC, l'état civil et l'application Web d'accès rapide au NAS (ARNAS), qui permet aux agents des bureaux locaux de servir les clients à l'aide de pages Web personnalisées donnant l'accès au RAS, ont été examinés durant la phase de réalisation de l'audit.

SMCD

Un grand nombre de programmes du Ministère génèrent des comptes débiteurs, par exemple l'AE, le RPC et le PCPE. Le SMCD est un système générique national en ligne conçu pour conserver et gérer divers types de comptes débiteurs au sein du Ministère. Par l'intermédiaire de systèmes d'interface, le SMCD recueille des renseignements sur les comptes liés à divers programmes législatifs, notamment les trop-payés du RPC et de l'AE, ainsi que les pénalités. Le SMCD a été établi à partir du concept d'un client ayant potentiellement de nombreux comptes, et d'un agent de recouvrement responsable de recouvrer la dette du client. Le SMCD est aussi utilisé pour l'exécution de fonctions de comptabilité dans les comptes impayés associés au Programme canadien de prêts aux étudiants et d'autres comptes débiteurs. Le SMCD fonctionne avec PROTÉGÉ, et il est administré par la DGAPF.

Les interfaces associées au SMCD ont été examinées sur la base des critères énoncés à la page 4 du présent rapport, afin de déterminer celles qui seraient visées par l'audit. Les contrôles des applications du SMCD et ses interfaces clés, c'est-à-dire le RPC (Système d'exécution du renouvellement de la technologie de l'information [SERTI]), le PCPE, le SMCD - interface de communication (SMCDCOM), et le SAD ont été vérifiés durant la phase de réalisation. Les interfaces avec l'Agence du revenu du Canada (ARC) et les systèmes, applications et produits de traitement de données (SAP) ne seront pas visés. Compte tenu du

stade précoce de la mise en œuvre SAP et de l'élaboration en cours d'une interface entre SAP et le SMCD, la vérification de ce dernier sera effectuée dans des audits subséquents.

PROTÉGÉ

SCSC

Le SCSC est une application bilingue qui a été développée à l'interne pour gérer les programmes de subventions et de contributions du Ministère. Le SCSC a été lancé dans l'ensemble du Ministère au troisième trimestre de 2001, et il fonctionne sur une plateforme Oracle. Il permet aux utilisateurs de documenter par voie électronique toutes les étapes du cycle de vie d'un projet, de la demande jusqu'à la fermeture du dossier, et de gérer les dossiers de chaque client. Le SCSC a mis en place une capacité de production de rapports qui permet aussi aux utilisateurs de générer divers rapports concernant la base des bénéficiaires du Ministère et les projets au titre desquels ces bénéficiaires touchent des fonds. Le SCSC est géré par le Portefeuille de traitement de transactions de la DGIIT. Le système traite annuellement (estimations de 2010-2011) environ deux milliards de dollars de subventions et de contributions administrées par l'intermédiaire des bureaux régionaux et de la DGOP.

Les interfaces associées au SCSC ont été examinées sur la base des critères énoncés à la page 4 du présent rapport, afin de déterminer celles qui seraient visées par l'audit. Les contrôles des applications du SCSC, ainsi que les interfaces clés telles le SMCD et EDMT Web, ont été examinés durant la phase de réalisation. Les interfaces externes avec l'ARC et Travaux publics et Services gouvernementaux Canada n'ont pas été vérifiées.