



Statistique Statistics
Canada Canada

Rapport de vérification

Vérification des Centres de données de recherche Universités de Calgary et de Lethbridge

Décembre 2011

Numéro de projet : 80590-66

Canada 

Table des matières

Sommaire exécutif.....	1
Introduction.....	3
Contexte.....	3
Objectifs de la vérification.....	4
Portée.....	4
Approche.....	4
Autorité.....	5
Constatations, recommandations et réponse de la direction.....	6
Administration des contrats de recherche pour l'utilisation de microdonnées et analyse des risques de divulgation.....	6
Sécurité matérielle.....	12
Sécurité des technologies de l'information.....	14
Annexe.....	18
Annexe A : Critères de vérification.....	18

Sommaire exécutif

Les Centres de données de recherche (CDR) de la région des Prairies sont constitués d'un laboratoire principal situé dans la bibliothèque McKimmie, Université de Calgary (centre de données de recherche d'attache), et à l'Université de Lethbridge (succursale). Ils fournissent des services à environ 122 chercheurs qui travaillent à 51 projets en moyenne chaque mois. Les chercheurs universitaires ont accès à 191 ensembles de données différents de Statistique Canada.

Les mesures de sécurité qui sont mises en œuvre dans les CDR de la région des Prairies doivent permettre d'assurer la confidentialité des données, dans la même mesure que dans les bureaux de Statistique Canada.

Les objectifs de la vérification sont de fournir au statisticien en chef et au Comité ministériel de vérification l'assurance que les CDR de l'Université de Calgary et de l'Université de Lethbridge :

- disposent de pratiques et de mécanismes efficaces, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services.
- respectent les politiques et normes pertinentes du Secrétariat du Conseil du Trésor (SCT) et de Statistique Canada concernant la sécurité des technologies de l'information (TI) et la sécurité matérielle, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services.

La vérification a été effectuée par les Services de vérification interne, en conformité avec la *Politique sur la vérification interne* du gouvernement du Canada.

Principales constatations

Les rôles et responsabilités sont définis et communiqués dans les domaines suivants : contrats de recherche pour l'utilisation de microdonnées (CRM), analyse des risques de divulgation, sécurité matérielle et sécurité des technologies de l'information (TI) dans les CDR. Les pouvoirs sont officiellement délégués au niveau du programme et des opérations. Des processus et procédures sont en place pour l'analyse des risques de divulgation, et les demandes d'analyse des risques de divulgation sont administrées et évaluées avec soin par l'analyste du CDR, afin de veiller à ce que la confidentialité des données ne soit pas compromise. Des mesures de sécurité matérielle et d'accès aux TI pertinentes, ainsi que des mesures de protection de l'identification et de l'authentification, sont en place et sont appliquées pour la sauvegarde et la protection des données confidentielles de Statistique Canada. L'accès aux CDR de la région des Prairies est limité au personnel autorisé, c'est-à-dire les personnes réputées être employées, comme les chercheurs et le personnel de soutien des TI des universités.

La vérification a révélé que les chercheurs ont accès aux CDR et aux fichiers de microdonnées avant que la cote de sécurité soit reçue de la Sécurité ministérielle (SM) et qu'il y existe un malentendu entre le Programme des CDR et la SM concernant la procédure pour le traitement des formulaires d'autorisation de sécurité classifiés et le contrôle des cotes de sécurité. La vérification a révélé que les gains d'efficacité pourraient être maximisés grâce à l'amélioration de la gestion et de l'inventaire des données administratives sur les projets de recherche à la Division de l'accès aux microdonnées (DAM) du bureau central (BC).

L'évaluation des mesures de protection des systèmes et des communications a révélé qu'il existe des possibilités de renforcer l'environnement informatique, grâce à la désactivation de tous les ports de bus série universel (USB) des postes de travail autonomes et à la réduction du délai de fermeture automatique de session des postes de travail.

Conclusion générale

Les mesures de sécurité matérielle et d'accès aux TI, ainsi que les mesures de protection de l'identification et de l'authentification, sont conformes aux politiques et normes pertinentes du SCT et de Statistique Canada. Des processus et des procédures sont en place pour l'analyse des risques de divulgation, et les demandes d'analyse des risques de divulgation sont administrées et évaluées avec soin par l'analyste du CDR, afin de veiller à ce que la confidentialité des données ne soit pas compromise.

Les résultats de la vérification proposent des possibilités d'amélioration des pratiques et des mécanismes en place pour que la confidentialité des données soit protégée lors de la prestation des services. Les domaines à améliorer sont les suivants : 1) désactivation des ports USB et réduction du délai de fermeture automatique de session des postes de travail autonomes; 2) chercheurs autorisés à accéder aux CDR et aux fichiers de microdonnées uniquement après réception de la cote de sécurité de la SM; 3) consultation avec la SM pour clarifier la procédure pour le traitement des formulaires d'autorisation de sécurité classifiés et le contrôle des cotes de sécurité; 4) maximisation des gains d'efficacité grâce à l'amélioration de la gestion et de l'inventaire des données administratives sur les projets de recherche à la DAM du BC.

Conformité aux normes professionnelles

Cette mission de vérification est conforme aux Normes internationales pour la pratique professionnelle de l'audit interne et aux Normes de vérification internes du gouvernement du Canada. Des tests suffisants ont été effectués pour appuyer les constatations et les recommandations connexes.

Patrice Prud'homme
Dirigeant principal de la vérification
Services de vérification interne, Statistique Canada

Introduction

Contexte

Les décideurs doivent avoir une compréhension à jour et approfondie de la société canadienne, non seulement pour répondre aux besoins de l'heure, mais aussi pour prévoir les besoins futurs. Cela entraîne une demande croissante à l'égard des produits analytiques découlant des riches sources de données recueillies par Statistique Canada.

En 1998, dans le cadre de l'Initiative canadienne sur les statistiques sociales, on a examiné les défis auxquels fait face la collectivité des chercheurs au Canada. Dans son rapport sur l'avancement de la recherche utilisant les statistiques sociales, le groupe de travail national recommandait notamment de créer des installations de recherche pour améliorer l'accès des chercheurs universitaires aux fichiers de microdonnées de Statistique Canada.

Les CDR font partie d'une initiative de Statistique Canada, du Conseil de recherches en sciences humaines (CRSH), des Instituts de recherche en santé du Canada (IRSC) et de consortiums d'universités, en vue de renforcer la capacité du Canada dans le domaine de la recherche sociale et d'appuyer la collectivité de chercheurs stratégiques. Le CRSH est l'organisme fédéral qui assure la promotion et le soutien de la recherche universitaire et de la formation en sciences sociales et humaines. Les IRSC sont le principal organisme fédéral chargé du financement de la recherche en santé au Canada.

Au total, 24 CDR sont installés dans un environnement protégé sur les campus universitaires et permettent aux chercheurs d'accéder à des microdonnées découlant d'enquêtes sur la population et auprès des ménages. Les chercheurs n'ont pas à se rendre à Ottawa pour accéder aux microdonnées de Statistique Canada. Il existe aussi un Centre fédéral de données de recherche à Ottawa, qui permet aux chercheurs d'avoir accès aux microdonnées de ministères stratégiques fédéraux.

Le CDR de la région des Prairies a ouvert ses portes en 2001 et est situé dans l'immeuble de la bibliothèque du campus de l'Université de Calgary. Il s'agit d'un établissement de taille moyenne, ouvert à temps plein, qui comporte 14 postes de travail qui sont mis à la disposition des chercheurs pour leurs recherches, du lundi au vendredi, de 8 h 30 à 16 h 30. On y retrouve un analyste de Statistique Canada à temps plein et un à temps partiel. En octobre 2010, une succursale de CDR a été inaugurée dans l'immeuble de la bibliothèque du campus de l'Université de Lethbridge. Tous les nouveaux emplacements de CDR sont d'abord des succursales d'un centre existant et demeurent ainsi jusqu'à ce que leur niveau d'activité justifie leur transformation en centre à part entière. La succursale de CDR compte un adjoint statistique à temps partiel de Statistique Canada, qui est chargé d'assurer la sécurité pendant les heures d'ouverture, soit 12,5 heures par semaine, et travaille en collaboration avec les analystes de l'Université de Calgary, qui est le CDR d'attache.

Les CDR de la région des Prairies sont exploités en vertu des dispositions de la *Loi sur la statistique* et sont administrés en conformité avec toutes les règles de confidentialité. Ils ne sont accessibles qu'aux chercheurs dont les projets ont été approuvés et qui ont prêté serment en vertu de la *Loi sur la statistique*, en tant que personnes réputées être employées.

Objectifs de la vérification

Les objectifs de la vérification sont de fournir au statisticien en chef et au Comité ministériel de vérification l'assurance que les CDR de l'Université de Calgary et de l'Université de Lethbridge :

- disposent de pratiques et de mécanismes efficaces, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services.
- respectent les politiques et normes pertinentes du SCT et de Statistique Canada concernant la sécurité des technologies de l'information (TI) et la sécurité matérielle, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services.

Portée

La portée de la présente vérification comprenait un examen des systèmes et des pratiques des CDR de la région des Prairies, à l'Université de Calgary et à l'Université de Lethbridge, dans le contexte de la protection des données, de l'utilisation des technologies et de la sécurité matérielle.

La vérification a été axée sur l'analyse des risques de divulgation et le contrôle de confidentialité des données par les employés de Statistique Canada sur place, le statut de personne réputée être employée et les exigences en matière d'autorisation de sécurité pour l'accès aux microdonnées, le processus de propositions de recherche des CDR, les contrats de recherche pour l'utilisation de microdonnées, la sécurité matérielle des emplacements de CDR, conformément aux politiques et normes pertinentes du SCT ou de Statistique Canada, et la protection des TI, conformément aux politiques et normes pertinentes du SCT et de Statistique Canada.

Approche

Le travail sur le terrain a été exécuté en deux étapes : la première étape a consisté à passer en revue et à évaluer les processus et procédures relatifs à la sécurité matérielle, à l'utilisation des technologies et à la protection des données. La deuxième étape a pris la forme de visites sur place dans les CDR de la région des Prairies, afin de vérifier les contrôles de protection des fichiers de microdonnées, y compris l'accès logique et les contrôles de sécurité informatique, et de mener des tests de conformité des centres, afin d'évaluer les mesures de sécurité matérielle en place.

Autorité

La vérification a été menée en vertu du Plan pluriannuel de vérification axé sur les risques de Statistique Canada, pour 2011-2012 et 2013-2014, approuvé au mois de mars 2011 par le Comité ministériel de vérification.

Constatations, recommandations et réponse de la direction

Champ d'enquête n° 1 : Les Centres de données de recherche disposent de pratiques et de mécanismes efficaces, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services au Centres de données de recherche régional.

Administration des contrats de recherche pour l'utilisation de microdonnées et analyse des risques de divulgation

Les pouvoirs requis pour l'administration des CRM et l'analyse des risques de divulgation sont officiellement délégués au niveau du programme et des opérations, et les rôles et responsabilités sont définis et communiqués.

Des processus et des procédures sont en place pour l'analyse des risques de divulgation, et les demandes d'analyse des risques de divulgation sont administrées et évaluées avec soin par l'analyste du CDR, afin de veiller à ce que la confidentialité des données ne soit pas compromise.

Les gains d'efficacité pourraient être maximisés grâce à l'amélioration de la gestion et de l'inventaire des données administratives sur les projets de recherche à la DAM du BC. L'accès aux CDR et l'accès aux fichiers de microdonnées sont accordés aux chercheurs par la SM. Il existe un malentendu entre le Programme des CDR et la SM concernant la procédure pour le traitement des formulaires d'autorisation de sécurité classifiés et le contrôle des cotes de sécurité.

Administration des contrats de recherche pour l'utilisation de microdonnées et analyse des risques de divulgation

L'administration des contrats de recherche pour l'utilisation de microdonnées (CRM) c'est-à-dire le contrôle et la protection des données désignées conservées dans les CDR, l'établissement et le maintien de répertoires de données administratives sur les projets de recherche, et l'accès aux CDR accordé uniquement aux chercheurs détenant une cote de sécurité valide, représente une combinaison de responsabilités, de procédures et de contrôles utilisés pour gérer efficacement les CRM et assurer la confidentialité des données.

Autorité

Les CDR sont exploités en vertu des dispositions de la *Loi sur la statistique* et sont administrés en conformité avec toutes les règles de confidentialité. Ils ne sont accessibles qu'aux chercheurs dont les projets ont été approuvés et qui ont prêté serment en vertu de la *Loi sur la statistique*, en tant que personnes réputées être employées.

Rôles et responsabilités

Les rôles et responsabilités relativement à la gestion des CRM, à l'accès aux microdonnées confidentielles et à l'analyse des risques de divulgation sont définis et communiqués à tous les

intervenants, dans des politiques, normes, documents de procédures et guides détaillés. Au niveau du programme, les pouvoirs sont officiellement délégués au gestionnaire du Programme des CDR dans le *Manuel des pratiques de sécurité* de Statistique Canada qui exige l'attestation que les formalités prescrites pour les données administratives, les propositions de recherche et les autres renseignements sont suivies, tout au long du cycle de vie du projet. La vérification a révélé que le processus d'« attestation » n'est pas défini et qu'il existe une ambiguïté à l'intérieur du Programme des CDR quant à ce qu'il signifie exactement.

Procédures de traitement des contrats

Au début d'un projet de recherche, l'analyste du CDR détermine les besoins d'accès aux données. Si l'accès à un CDR représente la voie appropriée d'accès aux données, le chercheur prépare une proposition d'accès aux données, avec l'aide de l'analyste du CDR au besoin. Cette proposition est soumise en ligne au CRSH. Elle fait l'objet d'une évaluation par les pairs, c'est-à-dire que la proposition est évaluée selon son mérite scientifique, et d'une révision institutionnelle par le secteur spécialisé, afin de déterminer si des données analytiques sont nécessaires et si les données peuvent appuyer le projet. Sur réception de l'avis d'approbation du projet par la Division de l'accès aux microdonnées du bureau central, l'analyste du CDR rédige le contrat que le ou les chercheurs doivent signer et invite ces derniers à une séance d'orientation et de signature du contrat. À la séance d'orientation, de la formation relative aux stratégies d'analyse des risques de divulgation, ainsi qu'aux mesures de sécurité des technologies de l'information et de sécurité matérielle, est fournie aux chercheurs. Le *Guide des chercheurs*, qui décrit les rôles et responsabilités des chercheurs et des analystes de CDR, dans les CDR, et le *Code de valeurs et d'éthique de la fonction publique* de Statistique Canada sont fournis aux chercheurs, qui signent pour en accuser réception.

La vérification a permis de vérifier la conformité aux procédures de traitement des contrats, grâce à l'examen d'un échantillon de contrats sélectionnés au hasard, soit 21 des 182 contrats (11 %) en date de décembre 2010, pour les CDR de la région des Prairies. La vérification a révélé que pour 20 contrats, la proposition de projet et une liste d'ensembles de données, le courriel d'approbation du projet et des copies signées du CRM et de ses modifications et révisions figuraient dans le dossier et étaient complets. On n'a pas pu localiser la documentation d'un contrat parce que celui-ci n'avait pas été conclu dans le CDR des Prairies.

En tant que personnes réputées être employées, les chercheurs doivent faire l'objet d'une enquête de sécurité, afin d'obtenir une cote de fiabilité, en vertu des paragraphes 5(2) et 5(3) de la *Loi sur la statistique*, et ils doivent prêter serment ou affirmation d'office et de discrétion, en vertu du paragraphe 6(1) de la *Loi sur la statistique*. La vérification a permis de déterminer que les formulaires de sécurité sont remplis et que le serment ou l'affirmation d'office a été traité lorsque le ou les chercheurs signent le CRM. Les formulaires de sécurité originaux sont envoyés par messenger à la DAM du BC par l'analyste du CDR, en vue d'être soumis à la SM pour traitement. Toutefois, dans notre échantillon de 21 contrats concernant 37 chercheurs, seulement 7 des 37 copies de serment signé et 13 des 37 documents d'autorisation de sécurité ont pu être localisées par la DAM du BC pour notre examen.

L'accès aux CDR et l'accès aux données devraient être accordés aux chercheurs par l'analyste du CDR, sur réception du courriel de la DAM du BC concernant les dates de début et de fin de l'autorisation de sécurité délivrée par la SM. Cela est conforme au document de procédures « *Formalités de vérification de sécurité pour les chercheurs des CDR* » préparé par la DAM et confirmé par la SM. La vérification a révélé que, dans les CDR de la région des Prairies, l'accès aux CDR et aux données commence dès qu'un chercheur a soumis les documents remplis pour l'autorisation de sécurité, et indiqué ne pas avoir de dossier criminel. La demande d'analyse des risques de divulgation, toutefois, est autorisée uniquement lorsque l'analyste du CDR reçoit un courriel de la DAM du BC concernant les dates de début et de fin de l'autorisation de sécurité délivrée par la SM. Ces directives contradictoires figurent dans une présentation intitulée *Autorisation de sécurité – Cheminement des données* préparée par la DAM du BC.

La vérification a aussi révélé que le document de procédures « *Formalités de vérification de sécurité pour les chercheurs des CDR* » n'est pas conforme aux directives et à l'interprétation de la SM concernant le traitement approprié des documents d'autorisation de sécurité classifiés et la date de contrôle appropriée des cotes de sécurité. Par conséquent, il existe un malentendu entre la DAM du BC, l'analyste du CDR et la SM. Cela augmente le risque de pratiques incorrectes et de décisions erronées. Il n'existe pas non plus de directive propre au Programme des CDR sur la période de conservation des documents d'autorisation de sécurité originaux.

Il n'existe pas de directive propre au Programme des CDR sur la période de conservation des répertoires archivés des chercheurs (c.-à-d., zippés, chiffrés et mis sur des disques compacts ou des lecteurs de disque dur externes; et les fichiers sur papier de l'analyse des risques de divulgation des chercheurs). Des données archivées remontant au moment de l'ouverture du CDR de l'Université de Calgary sont entreposées dans des classeurs fermés à clé dans la salle de serveur sécurisée et dans les classeurs fermés à clé des postes de travail.

Recommandations :

Il est recommandé que le statisticien en chef adjoint, Secteur de la statistique sociale, de la santé et du travail, s'assure que :

- *le « processus de certification » compris dans le Manuel des pratiques de sécurité est clarifié;*
- *des fichiers complets pour les CRM, y compris des copies des documents d'autorisation de sécurité et des serments signés par les personnes réputées être employées, sont conservés au BC;*
- *en consultation avec la SM, les éléments suivants sont clarifiés, grâce à la mise à jour du document de procédures « Formalités de vérification de sécurité pour les chercheurs des CDR », pour les éléments suivants :*
 - ✓ *responsabilités de l'analyste du CDR et du BC concernant le traitement des documents d'autorisation de sécurité originaux;*

- ✓ *procédures concernant le moment où l'accès au CDR est accordé au chercheur et celui où un chercheur peut demander une analyse des risques de divulgation avant de sortir des données du CDR;*
- ✓ *procédures concernant la date de fin devant être contrôlée par le BC pour les autorisations de sécurité des étudiants canadiens et étrangers (intégrer un « écran d'impression » dans le champ de données sur la sécurité du Système de gestion des relations avec la clientèle et mettre en évidence la « date de fin » pour le contrôle par le personnel du BC);*
- ✓ *période de conservation des documents d'autorisation de sécurité originaux par le BC.*
- *des directives concernant la période de conservation des documents archivés et des fichiers sur papier des chercheurs sont fournies.*

Réponse de la direction :

La direction est d'accord avec toutes les recommandations.

- Le gestionnaire de la DAM a veillé à ce que la documentation du programme soit passée en revue, et les changements recommandés ont été apportés pour clarifier le « processus de certification ». Les changements ont été communiqués à tous les analystes travaillant dans les CDR.
Produit livrable et échéance : Mise à jour du document de procédures « *Formalités de vérification de sécurité pour les chercheurs des CDR* » terminée.
- Le gestionnaire de la DAM a veillé à ce que la structure de classement soit modifiée, afin d'améliorer l'actualité de la recherche des données historiques sur papier, et à ce que toutes les données soient classées sous le nom du chercheur principal.
Produit livrable et échéance : Structure de classement modifiée à la DAM du BC d'ici le 31 mars 2012.
- Le gestionnaire de la DAM a veillé à ce que la SM soit consultée, afin de clarifier le document de procédures « *Formalités de vérification de sécurité pour les chercheurs des CDR* », relativement aux aspects suivants :
 - Responsabilités de l'analyste du CDR et du BC concernant le traitement des documents d'autorisation de sécurité originaux.
Produit livrable et échéance : Mise à jour d'ici le 31 décembre 2011.
 - Procédures concernant le moment où l'accès au CDR est accordé à un chercheur et celui où un chercheur peut demander une analyse des risques de divulgation, en vue de sortir des données du CDR.
Produit livrable et échéance : Mise à jour du document de procédures terminée et compréhension par les analystes du CDR confirmée.
 - Procédures concernant la date de fin devant être contrôlée par le BC pour les autorisations de sécurité des étudiants canadiens et étrangers.

Produit livrable et échéance : Écran d'impression du document de procédures inclus.

- Période de conservation des documents d'autorisation de sécurité originaux par le BC clarifiée par la SM.

Produit livrable et échéance : Mise à jour du « *Guide des opérations internes* », d'ici le 31 mars 2012.

- Le gestionnaire de la DAM a veillé à ce que les gestionnaires de CDR rencontrent la Division de la gestion de l'information pour contribuer à la directive sur l'archivage et les périodes de conservation.

Produit livrable et échéance : Plan de mise en œuvre pour l'archivage des dossiers des CDR, d'ici le 31 mars 2012.

Analyse des risques de divulgation

Les CDR sont les dépositaires des fichiers de microdonnées principaux de Statistique Canada, qui sont accessibles pour les chercheurs dont les projets sont approuvés. Des processus et des procédures efficaces et appropriées pour l'analyse des risques de divulgation devraient être en place et appliqués, afin de réduire de façon significative les risques de divulgation non désirée. Les demandes d'analyse des risques de divulgation devraient être administrées et vérifiées soigneusement par l'analyste du CDR, conformément aux protocoles établis, afin de veiller à ce que la confidentialité des données ne soit pas compromise.

L'analyse des risques de divulgation prend la forme d'un examen ou d'un contrôle de confidentialité des produits statistiques par les employés de Statistique Canada. Pour ce faire, on tente de déterminer s'il est possible d'inférer ou de déduire des données d'identification évidentes de cas individuels ou des renseignements concernant des cas individuels, à partir des produits statistiques. Il existe trois types de divulgation : divulgation d'identité; divulgation d'attribut; et divulgation par recoupement.

Rôles et responsabilités

La vérification a confirmé que l'analyste à temps plein du CDR de l'Université de Calgary s'acquitte de cette fonction pour les CDR de la région des Prairies. Il a des connaissances et de l'expérience concernant les techniques et les logiciels d'échantillonnage statistique. Le contrôle de confidentialité se fait au moyen des lignes directrices propres aux enquêtes pour 60 enquêtes dans le site Web du CDR. Les questions ou préoccupations concernant le processus de contrôle de confidentialité sont réglées par le gestionnaire régional de CDR, sur une base hebdomadaire; à la réunion annuelle des CDR; et par le Comité de la confidentialité du CDR, dont le mandat consiste à superviser à la fois les analystes de CDR et le Programme des CDR concernant l'analyse des risques de divulgation.

Les chercheurs reçoivent de la formation pendant leur séance d'orientation concernant le processus d'analyse des risques de divulgation, les diverses méthodes d'analyse et la façon de remplir le formulaire de demande de divulgation pour chaque demande de produits.

Processus et procédures

Une ébauche de document détaillé et exhaustif intitulé *Guide de l'analyse des risques de divulgation à l'intention des analystes des CDR* fournit à l'analyste du CDR des instructions détaillées étape par étape, ainsi que des illustrations et des diagrammes, sur la façon de procéder à une analyse des risques de divulgation. Des lignes directrices sur l'analyse des risques de divulgation pour les divers types de données et produits descriptifs ou tabulaires, ainsi que des matrices de variance-covariance et de corrélation, des graphiques, des modèles et un exemple de « formulaire de demande de divulgation » sont aussi inclus.

Une partie importante du processus consiste pour les chercheurs à remplir le « *Formulaire de demande d'analyse de divulgation* », dans lequel ils doivent dresser une liste de données d'échantillonnage statistique. Si l'analyste du CDR ne comprend pas une « variable », la demande est rejetée. Il est du ressort de l'analyste du CDR de s'assurer qu'il comprend ce que signifient les variables, ainsi que leur importance. Les lignes directrices de contrôle de confidentialité sont affichées dans le CDR et sont disponibles sous forme électronique à partir des postes de travail, afin de veiller à ce que les chercheurs remplissent toutes les sections pertinentes du formulaire. L'impression est acheminée à l'imprimante de réseau, qui est contrôlée par l'analyste du CDR. Du papier de couleur est utilisé pour les dossiers qui ont été approuvés et dont la sortie est autorisée. Ce contrôle permet aux analystes de vérifier visuellement ce qui sort des CDR.

La vérification a permis de conclure que des processus et procédures pour l'analyse des risques de divulgation sont en place et sont communiqués aux CDR par la DAM du BC, afin de réduire les risques de divulgation non désirée. Un échantillon de contrats sélectionnés au hasard a été vérifié en ce qui a trait à l'analyse des risques de divulgation. À cette fin, on a passé en revue le formulaire de demande de divulgation, les fichiers de produits connexes créés, ainsi que les résultats de l'analyse des risques de divulgation dans le sous-répertoire de demandes d'autorisation créé par l'analyste du CDR pour examen avec le chercheur, en vue de la création et de la diffusion du produit.

La vérification a permis de déterminer que l'analyste du CDR s'assure que les données confidentielles de Statistique Canada ne sont pas compromises en administrant et en évaluant avec soin toutes les demandes d'analyse des risques de divulgation.

Champ d'enquête n° 2 : Les Centres de données de recherche respectent les politiques et normes pertinentes du Secrétariat du Conseil du Trésor et de Statistique Canada concernant la sécurité des technologies de l'information et la sécurité matérielle, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services au Centres de données de recherche régional.

Sécurité matérielle

Des rôles et responsabilités au niveau du programme et de la région sont définis et communiqués, et les pouvoirs sont officiellement délégués au niveau du programme et des opérations.

Des mesures de sécurité matérielle conformes aux politiques et normes pertinentes du SCT et de Statistique Canada sont en place et appliquées pour la sauvegarde et la protection des données confidentielles de Statistique Canada. L'accès aux CDR de la région des Prairies est limité au personnel autorisé, c'est-à-dire les personnes réputées être employées, comme les chercheurs et le personnel de soutien des TI des universités.

La sécurité matérielle dans le CDR doit être conforme aux politiques pertinentes du SCT, comme la *Politique sur la sécurité du gouvernement* et le *Manuel des pratiques de sécurité* de Statistique Canada. Les rôles et responsabilités doivent être définis, clairs et communiqués. Dans le contexte des CDR, la sécurité matérielle devrait inclure des contrôles concernant l'accès aux locaux, la détection des intrusions et les activités de suivi.

Rôles et responsabilités

La vérification a permis de déterminer qu'au niveau du programme, les pouvoirs fonctionnels sont officiellement délégués au gestionnaire du Programme des CDR, et qu'au niveau régional, l'analyste du CDR et l'adjoint statistique sont responsables de la sécurité matérielle. L'analyste du CDR relève du gestionnaire régional de CDR. L'adjoint statistique de Lethbridge relève de l'analyste à temps plein du CDR de l'Université de Calgary. L'entente financière actuelle entre Statistique Canada et l'Université de Calgary stipule que Statistique Canada est responsable d'assurer un accès sécuritaire aux données de Statistique Canada à l'université, y compris la sécurité matérielle du centre et la sécurité électronique des données, les vérifications de sécurité et les autorisations d'accès. La SM du BC fournit des lignes directrices et des directives sur les exigences en matière de sécurité matérielle. La SM procède aux inspections de sécurité matérielle et de sécurité des TI des emplacements de CDR et fournit des recommandations au gestionnaire. Des inspections de sécurité des TI et de sécurité matérielle ont eu lieu en avril 2002 au CDR de l'Université de Calgary et en octobre 2009 au CDR de l'Université de Lethbridge, par la SM, avant que ces centres deviennent opérationnels.

Évaluation des contrôles de sécurité matérielle dans les Centres de données de recherche de la région des Prairies

Afin d'évaluer si les CDR de la région des Prairies se conforment à la *Politique sur la sécurité du gouvernement* du SCT et au *Manuel des pratiques de sécurité* de Statistique Canada, une inspection physique des CDR de la région des Prairies a été effectuée, afin de vérifier les pratiques de sécurité des locaux opérationnels situés à l'extérieur du complexe de Statistique Canada, au BC.

Contrôle de la sécurité du périmètre

Les deux CDR sont situés dans l'immeuble de la bibliothèque du campus. La vérification a révélé que les deux installations sont conformes aux exigences du SCT et de Statistique Canada en ce qui a trait à la sécurité du périmètre, pour ce qui est des « étages partagés », c'est-à-dire la séparation et la construction des murs, ainsi que des portes pleines en bois dotées de quincaillerie et d'accessoires robustes.

Contrôles de sécurité à l'entrée

L'accès aux deux CDR de la région des Prairies se fait par un point d'entrée unique, afin de permettre un filtrage et des contrôles efficaces par le personnel de ces CDR. Chaque porte d'entrée est équipée d'une alarme électronique en cas d'intrusion et d'un cadenas dont seuls le personnel des CDR et la sécurité du campus ont les clés. Cela est conforme aux exigences du SCT et de Statistique Canada.

Contrôles de la sécurité de l'accès

Afin de se conformer aux exigences du SCT et de Statistique Canada, un système d'accès avec carte à bande magnétique, c'est-à-dire une carte d'identité renfermant des données électroniques permettant d'identifier le détenteur, est en place dans les deux CDR, afin de contrôler l'accès aux installations. Le système enregistre tous les accès au CDR, et le personnel du CDR peut obtenir une copie sur papier du registre d'accès au moyen des cartes à bande magnétique auprès de la sécurité du campus, au besoin. Les visiteurs non autorisés ne peuvent pas aller au-delà de la porte d'entrée des installations des CDR.

Contrôles du câblage de télécommunications et des zones à accès restreint

La vérification a confirmé que le câblage des TI passe dans les murs et les plafonds des deux CDR. Au CDR de l'Université de Calgary, il y a une salle de serveur sécurisée, qui comporte des classeurs verrouillés pour l'entreposage des disques compacts et des fichiers archivés des chercheurs, afin de protéger les données confidentielles, classifiées et protégées. L'accès au réseau B est disponible uniquement dans une salle de réunions distincte dotée d'un poste de travail. Comme le CDR de l'Université de Lethbridge est beaucoup plus petit, son serveur et son accès au réseau B sont sécurisés dans le bureau de l'adjoint statistique. Tous les postes de travail des deux CDR comportent des classeurs pouvant être fermés à clé, dont les clés sont conservées dans les bureaux de l'analyste du CDR et de l'adjoint statistique. Cela est conforme aux exigences du SCT et de Statistique Canada.

Contrôles des activités de nettoyage et d'entretien

En conformité avec les exigences du SCT et de Statistique Canada, le personnel d'entretien et de nettoyage n'a pas de carte d'accès aux CDR. Le personnel de nettoyage peut accéder uniquement au CDR pendant les heures d'ouverture normales et est escorté par le personnel du CDR. Si un accès est requis en dehors des heures normales d'activité, le personnel de nettoyage et d'entretien doit être accompagné par les responsables de la sécurité du campus.

Contrôles de la détection des intrusions et des activités de suivi

Les responsables de la sécurité du campus assurent un contrôle 24 heures par jour et 7 jours par semaine des installations de CDR. Ces responsables ont une carte d'accès et un code de sécurité pour le système d'alarme. Un système de surveillance par caméra est installé dans les deux CDR, afin d'améliorer la sécurité, et fait l'objet d'un contrôle par l'analyste à temps plein du CDR de l'Université de Calgary et par l'adjoint statistique de l'Université de Lethbridge.

Les CDR ne peuvent être laissés sans surveillance. Si l'analyste du CDR doit quitter le CDR pendant les heures régulières, les chercheurs doivent aussi le faire, la porte doit être fermée à clé et une affiche doit être placée sur la porte.

À partir de l'inspection physique des CDR de la région des Prairies, la vérification a permis de déterminer que des mesures pertinentes de sécurité matérielle sont en place et sont appliquées pour la sauvegarde et la protection des données confidentielles de Statistique Canada et que l'accès aux CDR de la région des Prairies est limité au personnel autorisé, c'est-à-dire les personnes réputées être employées, comme les chercheurs et le personnel de soutien des TI des universités.

Sécurité des technologies de l'information

Les rôles et responsabilités au niveau du programme et de la région sont définis et communiqués.

Des tests concernant les mesures de protection de l'accès, de l'identification et de l'authentification, à partir d'un échantillon de contrats sélectionnés au hasard, ont révélé que des mesures sont en place et fonctionnent comme prévu.

L'évaluation des mesures de protection des systèmes et des communications a révélé qu'il existe des possibilités de renforcer l'environnement informatique, grâce à la désactivation de tous les ports USB des postes de travail autonomes et à la réduction du délai de fermeture automatique de session des postes de travail.

La sécurité des technologies de l'information dans les CDR doit être conforme aux politiques pertinentes du SCT, comme les *Normes de sécurité opérationnelle : Gestion de la sécurité des technologies de l'information* et le *Manuel des pratiques de sécurité* de Statistique Canada. Les rôles et responsabilités doivent être définis, clairs et communiqués. Dans le contexte des CDR, la sécurité des TI devrait inclure la protection des systèmes et des communications : des contrôles de sécurité qui appuient la protection du système d'information proprement dit, ainsi que les communications avec ce système; le contrôle de l'accès : des contrôles de sécurité qui permettent d'accorder ou de refuser aux utilisateurs l'accès aux ressources d'un système d'information; et l'identification et l'authentification : des contrôles de sécurité qui appuient l'identification des utilisateurs et l'authentification de ces utilisateurs lorsqu'ils tentent d'accéder au système d'information.

Rôles et responsabilités

La vérification a révélé que la structure de responsabilisation de la sécurité des TI dans les CDR de la région des Prairies est la même que pour la sécurité matérielle.

Mesures de protection du système et des communications

L'environnement informatique à l'intérieur des CDR est constitué de postes de travail autonomes devant être utilisés par les chercheurs. Ces postes ne sont pas reliés à Internet. L'accès Internet est disponible uniquement pour les employés du CDR et à partir du poste de travail situé dans la salle de réunions du CDR de l'Université de Calgary. Les postes de travail utilisent le système d'exploitation courant de Statistique Canada, ainsi que la configuration de logiciel de bureau et des logiciels statistiques approuvés, comme SPSS, Stata ou SAS. La vérification a révélé que les logiciels particuliers demandés par les chercheurs sont installés par l'analyste du CDR, après approbation par la Division des services de technologie informatique du BC. Cela est autorisé par le Programme des CDR.

Au CDR de l'Université de Calgary, les ports USB de 11 des 14 postes de travail étaient activés, ce qui augmente de façon significative le risque de retrait non détecté de microdonnées confidentielles de Statistique Canada au moyen d'une clé USB. La vérification a permis de déterminer qu'il n'y a pas eu de violations de la sécurité ou d'incidents déclarés concernant le retrait non autorisé de microdonnées confidentielles au CDR. La fermeture automatique de session des postes de travail était fixée à 45 minutes ou ne fonctionnait pas de façon uniforme, ce qui augmente le risque d'accès non autorisé à des microdonnées confidentielles de Statistique Canada ou à des postes de travail sans surveillance.

Un télécopieur se trouve dans la salle de réunions du CDR de l'Université de Calgary et est mis à la disposition des chercheurs, ce qui augmente le risque de transmission non détectée ou non autorisée de données confidentielles de Statistique Canada par les chercheurs.

Mesures de protection de l'accès, de l'identification et de l'authentification

Un échantillon de contrats sélectionnés au hasard comprenant 26 des 182 contrats (14 %) en date de décembre 2010, pour les CDR de la région des Prairies, ont fait l'objet d'une vérification au chapitre des contrôles de l'accès, de l'identification et de l'authentification. À cette fin, on a passé en revue le contenu du répertoire de l'échantillon par rapport au fichier principal, afin de s'assurer que tous les noms de fichiers faisaient partie des ensembles de données originaux; on a passé en revue le registre des événements, en vue de déterminer les numéros d'identification d'utilisateurs supprimés de l'échantillon, pour s'assurer qu'ils n'avaient pas accès; et on a passé en revue le répertoire actif des noms d'utilisateurs et des autorisations d'ensembles de données, pour s'assurer qu'ils touchaient uniquement des contrats actifs dans notre échantillon.

Les tests de vérification ont révélé que l'accès aux systèmes, aux fichiers de microdonnées et aux programmes est limité aux chercheurs qui ont des contrats actifs. Au total, sept des contrats terminés récemment ont été vérifiés dans le registre des événements, afin de s'assurer qu'il n'y

avait pas eu d'accès aux fichiers de microdonnées connexes depuis la date d'achèvement. Les résultats ont révélé qu'aucun accès n'a eu lieu. La vérification a confirmé que les fichiers de microdonnées ne sont pas retirés du serveur une fois que sont terminés tous les contrats connexes reposant sur ces fichiers. Cette pratique est appuyée par le Programme des CDR, afin de permettre à ces derniers de maintenir une bibliothèque locale de tous les fichiers auxquels on accède dans les CDR.

Les procédures précisent que des comptes d'utilisateurs devraient être créés uniquement lorsqu'un contrat est approuvé et devient actif; l'accès devrait être supprimé si le compte est inactif. La création de comptes d'utilisateur et l'octroi de l'accès aux fichiers de microdonnées étaient étayés par des contrats actifs approuvés dans tous les contrats échantillonnés. Les mots de passe respectent les normes de Statistique Canada, mais demeurent les mêmes pour toute la durée du contrat, qui peut aller d'un an à plusieurs années. Le *Manuel des pratiques de sécurité* de Statistique Canada exige que les mots de passe soient valides pendant 90 jours au maximum.

L'analyste du CDR détient les privilèges administratifs. De ce fait, il est chargé de créer un répertoire pour chaque projet approuvé, ainsi qu'un compte d'utilisateur et un mot de passe connexes pour chaque chercheur, en vue d'un accès à lecture seule au répertoire. Par conséquent, les chercheurs ne peuvent pas : accéder aux fichiers de microdonnées pour lesquels ils n'ont pas un projet approuvé; consulter le contenu des ensembles de données qui ne sont pas précisés dans leur proposition; et transférer des fichiers (documents, ensembles de données, syntaxe ou produit) d'un projet de recherche à un autre. Une fois qu'un compte d'utilisateur est créé, l'analyste du CDR informe les responsables de la sécurité du campus universitaire d'émettre une carte d'identité de membre du corps professoral/d'étudiant, ce qui permet d'accéder au CDR.

La vérification a permis de déterminer que des mesures de sécurité des TI pertinentes sont en place et sont appliquées pour la sauvegarde et la protection des données confidentielles de Statistique Canada. Des mesures de protection de l'accès, de l'identification et de l'authentification sont en place dans les CDR et fonctionnent comme prévu.

Recommandations :

Il est recommandé que le statisticien en chef adjoint, Secteur de la statistique sociale, de la santé et du travail, s'assure que :

- *les mots de passe et les délais de fermeture automatique de session des postes de travail respectent le Manuel des pratiques de sécurité de Statistique Canada;*
- *les ports USB des postes de travail sont désactivés;*
- *le télécopieur soit enlevé de la salle de réunions des chercheurs du CDR de l'Université de Calgary.*

Réponse de la direction :

La direction est d'accord avec toutes les recommandations.

- Le gestionnaire de la DAM a soumis les normes relatives aux mots de passe et à la fermeture automatique de session des postes de travail au Comité de la technologie du CDR, afin qu'il les intègre dans le processus d'authentification centralisé qui est actuellement mis en place.

Produit livrable et échéance : Prototype d'authentification centralisée, d'ici le 31 mars 2012, et adoption par les CDR, tout au long de 2012-2013.

- Le gestionnaire de la DAM a veillé à ce que tous les ports USB soient désactivés à nouveau et à ce qu'une liste de contrôle mensuelle soit préparée par le Comité de la technologie à l'intention des analystes, afin de vérifier les pratiques de sécurité en vigueur.

Produit livrable et échéance : Liste de contrôle mensuelle. Terminée.

- Le gestionnaire de la DAM a veillé à ce que le télécopieur soit installé dans le bureau de l'analyste.

Produit livrable et échéance : Terminée.

Annexe

Annexe A : Critères de vérification

Champ d'enquête/Contrôle clé	Critère
<i>1) Les Centres de données de recherche disposent de pratiques et de mécanismes efficaces, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services au Centres de données de recherche régional.</i>	
Responsabilisation	<p>1) Les responsabilités sont officiellement définies et communiquées.</p> <p>2) Les pouvoirs sont officiellement délégués et correspondent aux responsabilités des personnes, et les fonctions incompatibles ne sont pas combinées.</p>
Gestion des risques	<p>1) Les risques sont déterminés et tiennent compte des environnements interne et externe du Programme des CDR.</p> <p>2) Des processus et des lignes directrices officiels existent pour évaluer les contrôles et gérer les risques déterminés.</p>
Valeurs de la fonction publique	<p>1) Les employés attestent qu'ils se conforment aux valeurs, à l'éthique et au code de conduite de Statistique Canada.</p>
Résultats et rendement	<p>1) La responsabilité du contrôle est claire et communiquée et les résultats sont communiqués aux niveaux d'autorisation requis.</p> <p>2) Le contrôle actif est manifeste.</p>
<i>2) Les Centres de données de recherche respectent les politiques et normes pertinentes du Secrétariat du Conseil du Trésor et de Statistique Canada concernant la sécurité des technologies de l'information et la sécurité matérielle, afin de veiller à ce que la confidentialité des données soit protégée lors de la prestation des services au Centres de données de recherche régional.</i>	
Responsabilisation	<p>1) Les pouvoirs fonctionnels de la sécurité des TI et de la sécurité matérielle, dans le contexte du programme des CDR, font l'objet d'une approbation appropriée et sont exercés par les chefs fonctionnels.</p> <p>2) La structure d'organisation comporte des voies de communications et des rapports clairs et efficaces.</p>
Gestion des risques	<p>1) Il existe des évaluations de contrôle de la sécurité de TI et de la sécurité matérielle, auxquelles contribuent les fonctions des services intégrés pertinentes.</p>
Gérance	<p>Sécurité des TI :</p> <p>1) Les processus, procédures et contrôles pour la protection des</p>

Gérance (suite)	<p>fichiers de microdonnées de Statistique Canada comprennent :</p> <ul style="list-style-type: none">➤ <i>des contrôles d'accès logique</i> – pour contrôler l'accès aux fichiers de microdonnées, conformément aux modalités des contrats de recherche pour l'utilisation de microdonnées➤ <i>la sécurité des systèmes informatiques</i> – pour assurer la protection électronique des données et prévenir et déceler les vulnérabilités au chapitre de la sécurité. <p>2) Des procédures et des mécanismes d'authentification et d'accès sont en place.</p> <p>3) Les contrôles des TI comprennent un mélange de contrôles automatisés et manuels, et leur efficacité opérationnelle est vérifiée périodiquement.</p> <p>4) Les processus régissant l'accès aux données respectent les politiques des TI pertinentes du SCT et de Statistique Canada en matière de sécurité, les exceptions sont déterminées et des mesures appropriées sont prises.</p> <p>Sécurité matérielle :</p> <p>1) Les mesures de sécurité matérielle respectent les politiques et procédures pertinentes du SCT et de Statistique Canada.</p> <p>2) L'accès physique au CDR est restreint pour la protection des biens de nature délicate, et des procédures pour sauvegarder et protéger l'utilisation des biens existent et sont appliquées.</p>
------------------------	--