Correctional Service Canada | Service correctionnel Canada

Safety, Respect and Dignity for All

La sécurité, la dignité et le respect pour tous

LA VÉRIFICATION DES CONTRÔLES D'ACCÈS LOGIQUE

Direction de la vérification interne

378-1-240

Approuvé par le Comité de vérification

Le 20 mai 2008

Canada

SOMMAIRE EXÉCUTIF

Le Service correctionnel du Canada, en tant que composante du système de justice pénale et dans la reconnaissance de la primauté du droit, contribue à la sécurité publique en incitant activement et en aidant les délinquants à devenir des citoyens respectueux des lois, tout en exerçant sur eux un contrôle raisonnable, sûr, sécuritaire et humain. Afin d'atteindre ses objectifs, le SCC utilise divers systèmes informatiques internes qui contiennent de l'information de nature délicate et (ou) qui sont considérés essentiels à la mission du Service. Étant donné que les mécanismes de contrôle d'accès logique (p. ex. les codes d'utilisateur et les mots de passe qui donnent aux utilisateurs l'accès au réseau ou aux applications de l'organisation) constituent le fondement de la sécurité de la TI, ces mécanismes doivent être considérés comme le principal moyen de protéger le SCC contre l'accès non autorisé à ses systèmes et à l'information de nature sensible qu'ils renferment.

Dans le cadre du plan de vérification interne de 2007-2008, une vérification des mécanismes de contrôle d'accès logique du Service correctionnel du Canada (SCC) a été effectuée par la Direction de la vérification interne, avec l'assistance de la firme Deloitte.

La présente vérification comportait une évaluation des mécanismes de contrôle d'accès logique pour certaines applications clés du SCC, y compris : le SGD – Système de gestion des délinquant(e)s, le SIGFM – Système intégré de gestion des finances et du matériel, le SGRH (PeopleSoft) et l'entrepôt des données (ED). Elle comportait également une évaluation de la plate-forme Active Directory de Microsoft et de l'accès à distance (réseau privé virtuel), puisque ces systèmes sont des « passerelles » qui mènent à d'autres applications.

Les mécanismes de contrôle d'accès logique ont été évalués selon les objectifs de contrôle COBIT « Planifier et organiser » et « Assurer la sécurité des systèmes ». On a notamment évalué les objectifs suivants :

- *Planifier et organiser – Un cadre de gestion des risques et un processus d'évaluation des risques en matière de TI ont été élaborés et mis en œuvre pour gérer et évaluer les risques liés au contrôle d'accès logique;*
- *Assurer la sécurité des systèmes – Les applications sont suffisamment protégées pour prévenir l'utilisation, les divulgations et les modifications non autorisées, ainsi que les dommages et la perte de données.*

Conclusion générale

Planifier et organiser – Le SCC a conçu et mis en œuvre des mécanismes de contrôles clés qui aident à cerner et à évaluer les risques liés à la sécurité de la TI. Ces contrôles comprennent des évaluations de la menace et du risque (EMR) qui permettent de déterminer les risques, ainsi qu'une norme d'évaluation de la GSTI dont la direction s'est servie pour identifier les lacunes. Cependant, le SCC ne possède pas

de cadre global de gestion des risques de la TI pour l'ensemble du SCC, ni de processus d'évaluation des risques qui permet à identifier et à établir la liste des priorités pour les besoins de sécurité de la TI. De plus, les EMR pour les applications visées par la présente vérification, devraient être mises à jour.

Assurer la sécurité des systèmes – En ce qui a trait aux applications examinées dans le cadre de la vérification, des contrôles sont en place pour assurer que l'accès des nouveaux utilisateurs est dûment autorisé et que les politiques et les procédures liées à la sécurité de la TI sont communiquées à ces nouveaux utilisateurs. En outre, des contrôles liés aux activités de surveillance et aux incidents de sécurité ont été conçus et mis en œuvre pour le système SGD. Cependant, davantage d'efforts doivent être consacrés à la conception et (ou) à la mise en œuvre de mesures de contrôle visant à empêcher l'accès non autorisé aux applications du SCC. [redacted]. De plus, on devrait aussi envisager une intégration accrue des responsabilités en matière de sécurité ainsi que [redacted]. Ces mesures pourraient améliorer la sécurité de la TI et permettraient de réaliser des économies si celles-ci sont mises en place.

Des recommandations ont été formulées sur les secteurs à améliorer.

La haute direction a examiné les constatations du présent rapport et y souscrit. Le plan d'action de la direction qui porte sur les recommandations figure à l'annexe C.