

# Contrôles de l'accès aux applications

## Rapport de vérification

### Rapport N° 15/09

### 4 décembre 2009

#### Distribution

Dest : Président et chef de la direction  
Premier vice-président et chef de la direction financière  
Premier vice-président, Solutions technologiques et d'affaires  
Premier vice-président, Ressources humaines  
Premier vice-président, Groupe des produits de financement  
Premier vice-président, Assurances  
Vice-président et contrôleur général  
Vice-président et chef des Services informatiques  
Vice-président, COE-Assurances et CARD  
Vice-président, Services des ressources humaines  
Vice-président, Services aux clients  
Vice-président, Veille commerciale interne et internationale  
Contrôleur adjoint, Finances et contrôle  
Directeur de groupe, Gestion de la trésorerie, fiscalité et assurance d'entreprise  
Directeur de groupe, Prestation de solutions d'affaires  
Directeur de groupe, CARD  
Directeur de groupe, Institutions financières  
Directeur de groupe, COE-Financement & Relations internationales  
Directeur d'exécution de programmes, Finances  
Directeur d'exécution de programmes, Financement  
Directeur d'exécution de programmes, Assurances  
Directeur d'exécution de programmes, RH/Services juridiques/Groupe du président  
Directeur, Centre des services aux clients  
Directeur, Rapports financiers  
Directeur des normes de crédit  
Directeur, Normes de crédit et évaluation par points  
Directeur, Comptes créditeurs  
Chef de l'équipe HRIS  
Analyste des systèmes de gestion, Services des prêts COE  
Analyste des systèmes de gestion, CARD  
Coordonnateur, Comptes créditeurs

#### Équipe de vérification

S. Slechta  
H. Klosevych  
N. Bylen

#### Vice-présidente, Vérification interne

M. Ryan

CC : Premier vice-président, Secrétariat & Services juridiques  
Premier vice-président, Développement des affaires  
Vice-président et trésorier  
Directeur de groupe, Services des prêts  
Directeur d'exécution de programmes, Développement des affaires  
Directeur, Comptabilité des assurances et Compte du Canada  
Chef d'équipe de projet, Services des prêts  
Vice-président, Planification stratégique et Communications  
Directeur de groupe, Planification et Relations avec le gouvernement  
Premier conseiller, Bureau du vérificateur général

## Introduction

Conformément à son plan de vérification de 2009, la Vérification interne d'EDC a réalisé une vérification des contrôles de l'accès aux applications.

## Objectifs et portée de la vérification

L'objectif général de la vérification consistait à évaluer l'efficacité des contrôles mis en place pour restreindre l'accès aux applications de gestion en vue d'assurer l'intégrité constante des données des applications. Plus précisément, l'examen a visé à déterminer si

- ▶ l'accès est autorisé de manière appropriée;
- ▶ l'accès est autorisé selon les besoins et n'est pas excessif par rapport à la fonction de l'employé;
- ▶ la séparation des tâches est maintenue;
- ▶ l'accès est promptement supprimé lorsqu'un employé quitte la Société ou change de rôle;
- ▶ l'accès des administrateurs du système BS&T à l'environnement de production est limité.

En examinant ces aspects, la vérification a tenu compte des éléments de risque suivants dans le cadre de la gestion des risques d'entreprise (ERM) d'EDC : risque lié aux systèmes, risque de non-conformité, risque lié à la sécurité de l'information et risque lié au traitement des transactions. La vérification a englobé les systèmes suivants : PS FIN, CAS, ACBS, Globex, CRS, MBC, FIRM, PS HR, MTIP, C3, GAS et UFS. Le travail de vérification sur le terrain a été effectué aux mois d'octobre et de novembre 2009.

## Opinion de la Vérification interne

À notre avis, *il existe des possibilités d'améliorer les contrôles*<sup>1</sup> encadrant la gestion des changements apportés aux applications. Nous avons constaté que l'accès n'est pas accordé en fonction des besoins pour huit des douze applications visées par notre vérification. Par conséquent un accès excessif est accordé aux profils de superutilisateur et d'administrateur de la sécurité. Les administrateurs de la sécurité n'ont pas toujours l'information requise pour déterminer si les demandes d'accès sont valides. Un examen périodique de l'accès n'est pas effectué uniformément pour toutes les applications de gestion comprises dans notre vérification. Par conséquent, l'accès des utilisateurs est souvent excessif par rapport à leur rôle. Nous recommandons que l'accès des superutilisateurs soit supprimé et accordé temporairement selon les besoins. Le profil d'administrateur de la sécurité ne devrait être accordé qu'aux personnes chargées d'assumer cette fonction. Nous recommandons aussi que le rôle d'administrateur de la sécurité soit assumé par la fonction de gestion. Finalement, l'accès aux applications de gestion essentielles devrait être examiné périodiquement pour qu'il corresponde toujours aux rôles des utilisateurs.

---

<sup>1</sup> Nos opinions standard de vérification sont les suivantes :

- **Contrôles forts** : Des contrôles clés ont été efficacement conçus et fonctionnent comme prévu. Des contrôles internes exemplaires existent. Les objectifs du processus vérifié seront très probablement atteints.
- **Bien contrôlé** : Des contrôles clés ont été efficacement conçus et fonctionnent comme prévu. Les objectifs du processus vérifié seront probablement atteints.
- **Possibilités d'amélioration des contrôles** : Un ou plusieurs contrôles clés n'existent pas, ne sont pas bien conçus ou ne fonctionnent pas comme prévu. Il se peut que les objectifs du processus ne soient pas atteints. Du point de vue des finances et/ou de la réputation, l'incidence sur le processus vérifié est plus qu'insignifiante. De promptes mesures s'imposent.
- **Non contrôlé** : De nombreux contrôles clés n'existent pas, ne sont pas bien conçus ou ne fonctionnent pas comme prévu. Les objectifs du processus ne sont probablement pas atteints. Du point de vue des finances et/ou de la réputation, l'incidence sur le processus vérifié est importante. Des mesures doivent être prises immédiatement.

## Constatations de la vérification et recommandations

### 1. Accès aux comptes privilégiés

Les profils de superutilisateur et d'administrateur permettent aux utilisateurs d'apporter directement des changements aux données de production sans être soumis aux contrôles normaux de traitement des transactions. Nous avons constaté que des comptes privilégiés ont été accordés de façon permanente à des utilisateurs de BS&T dans tous les systèmes, à l'exception de MTIP, UFS, GAS et ACBS. Aucun processus n'a été mis en place pour contrôler les changements effectués par les utilisateurs qui ont ces profils. Nous recommandons que des comptes privilégiés soient attribués temporairement à un nombre limité de personnes de BS&T, selon les besoins. Dans les situations où l'accès permanent ne peut être retiré, les risques et la justification de l'attribution du profil à certains utilisateurs précis doivent être approuvés par la haute direction.

Constatation - Problème majeur<sup>2</sup>

Responsables de l'intervention - Administrateurs de la sécurité et directeurs, BSD

Date d'échéance - 2T2010

### 2. Accès au profil d'administrateur de la sécurité

Le profil d'administrateur de la sécurité permet au détenteur d'accorder à tout utilisateur valide du réseau l'accès aux profils des systèmes dont les profils de type superutilisateur. Nous avons constaté que, dans plusieurs applications, le profil d'administrateur de la sécurité a été accordé de façon permanente à des utilisateurs de BS&T et/ou à des utilisateurs fonctionnels qui ne sont pas responsables de l'administration de la sécurité (PS FIN, CAS, CRS, Globex, MBC, FIRM et PS HR). De plus, pour plusieurs applications, il n'y a pas d'examen périodique des profils d'utilisateurs visant à garantir que l'accès est bien accordé en fonction des besoins. Nous recommandons que le profil d'administrateur de la sécurité soit retiré de tous les utilisateurs qui ne sont pas responsables de l'administration de la sécurité. En outre, nous recommandons que des processus soient mis en œuvre pour examiner périodiquement l'accès aux applications de gestion essentielles.

Constatation - Problème majeur

Responsables de l'intervention - Administrateurs de la sécurité et directeurs, BSD

Date d'échéance - 2T2010

### 3. Examen périodique de l'accès aux systèmes d'application

Il existe des processus de révision périodique visant à déterminer si l'accès aux systèmes suivants est approprié : UFS, PS FIN, MTIP, ACBS, CAS et C3. Cependant, il n'y a pas d'examen périodique du bien-fondé de l'accès aux systèmes Globex, CRS, MBC, FIRM, PSHR et GAS. Par conséquent, on a constaté plusieurs cas où l'accès de l'utilisateur n'est plus requis, est excessif ou crée une séparation inappropriée des tâches. Nous recommandons la mise en œuvre d'un examen périodique de l'accès à l'environnement de production. Celui-ci devrait inclure la validation de l'accès des utilisateurs/de BS&T auprès des directeurs des utilisateurs et des responsables des systèmes.

---

<sup>2</sup> Cotes attribuées aux résultats de la vérification :

**Problème majeur** - Un contrôle clé n'existe pas, est mal conçu ou ne fonctionne pas comme prévu et le risque financier et/ou de réputation est plus qu'insignifiant. L'objectif du processus sur lequel porte le contrôle ne sera probablement pas atteint. Des mesures correctives sont requises pour que les contrôles soient rentables et/ou que les objectifs du processus soient atteints.

**Problème modéré** - Un contrôle clé n'existe pas, est mal conçu ou ne fonctionne pas comme prévu et le risque financier et/ou de réputation pour le processus est plus qu'insignifiant. Cependant, un contrôle compensatoire existe. Des mesures correctives sont requises pour éviter de compter uniquement sur les contrôles compensatoires et/ou pour s'assurer que les contrôles sont rentables.

**Problème mineur** - Faiblesse dans la conception et/ou dans le fonctionnement d'un contrôle qui n'est pas un contrôle clé. Il est peu probable qu'il y ait des répercussions sur la capacité d'atteindre les objectifs. Des mesures correctives sont suggérées pour s'assurer que les contrôles soient rentables.

Constatation - Problème majeur  
Responsables de l'intervention - Administrateurs de la sécurité  
Date d'échéance - 2T2010

#### **4. Centre des services à la clientèle - facilitateur vs administrateur de la sécurité**

Le Centre des services à la clientèle (CSC) fait fonction de facilitateur en accordant l'accès aux systèmes d'application, c'est-à-dire en servant de point de contact unique pour les demandes d'accès et en obtenant les approbations nécessaires. En plus de ce rôle de facilitateur, le CSC assume également le rôle d'administrateur de la sécurité pour les systèmes CRS, Globex, FIRM et MBC. En tant qu'administrateur de la sécurité, le CSC a la responsabilité de déterminer si un utilisateur devrait recevoir l'accès demandé et si cet accès est approprié par rapport à sa fonction. Toutefois, nous avons constaté que le CSC ne reçoit pas toujours l'information requise pour prendre cette décision. Lorsqu'il agit à titre de facilitateur, le CSC n'obtient pas toujours les approbations à fournir aux administrateurs de la sécurité. Nous recommandons que le rôle du CSC soit limité à la facilitation de l'administration de la sécurité. Les approbations explicites devraient être données par courriel ou par une signature sur le formulaire de demande d'accès. Toute approbation devrait être envoyée à l'administrateur de sécurité de la fonction concernée pour être consignée avant que l'accès ne soit accordé.

Constatation - Problème majeur  
Responsables de l'intervention - Centre de services à la clientèle et administrateurs des systèmes  
Date d'échéance - 2T2010

### **Conclusion**

Les constatations et recommandations de la vérification ont été communiquées à la direction et acceptées par celle-ci, qui a élaboré des plans d'action, dont la mise en œuvre devrait se faire pas plus tard qu'au 2<sup>e</sup> trimestre de 2010.

Nous tenons à remercier la direction de son soutien tout au long de la vérification.