

Contrôles de l'accès aux applications – Phase II
Rapport de vérification final
Rapport n° 24/10
14 janvier 2011

Distribution

Président et chef de la direction
Premier vice-président et chef de la direction financière
Vice-président et contrôleur général

c.c. : Voir la liste de diffusion ci-jointe

Équipe de vérification :
A. Lowe

Vice-présidente, Vérification interne
Monica Ryan

C.C. : Premier vice-président, Secrétariat et services juridiques
Premier vice-président, Développement des affaires
Premier vice-président, Solutions technologiques et d'affaires
Premier vice-président, Ressources humaines et services généraux
Premier vice-président, Assurances
Vice-président et trésorier
Vice-président, Services aux clients – Ressources humaines
Vice-président et chef des services informatiques
Vice-président, Souscription – CIB et PRI
Vice-président, Souscription en assurance crédit
Vice-président, Renseignements sur la Société et sur le commerce international
Vice-président, Services aux clients
Directeur de groupe, COE – Financement et relations internationales
Directeur de groupe, Prestation de solutions d'affaires
Directeur de groupe, CARD
Directeur de groupe, Services des prêts
Trésorier adjoint
Contrôleur général adjoint
Directeur de groupe, Équipe des institutions financières
Directeur, Solutions d'affaires – Assurances
Analyste pr., Renseignements sur les entreprises, COE – Financement et relations int.
Directeur, Rapports financiers
Directeur, Centre de services aux clients
Directeur, HRIS et actuariat
Directeur, Normes de crédit et évaluation par points
Directeur, Gestion des affaires des TI
Chef de projet, Services des prêts
Directeur de programme, Solutions d'affaires, Assurances
Analyste des renseignements sur les entreprises, Services des prêts
Directeur des normes de crédit
Vice-président, Planification stratégique et Communications
Directeur de groupe, Planification et relations gouvernementales
Directeur principal, Bureau du vérificateur général
Directeur, Bureau du vérificateur général

Introduction

La vérification des contrôles de l'accès aux applications s'est déroulée en deux phases. La première, réalisée en 2009, portait sur l'efficacité de la conception des contrôles d'accès et a fait appel à des sondages détaillés pour établir si les contrôles en question fonctionnaient comme prévu. La vérification a mis au jour des lacunes dans sept des onze applications vérifiées en 2009. La direction a pris des mesures correctives en 2010 pour résoudre ces lacunes. Le plan de vérification de 2010 prévoyait donc une vérification de phase II visant à établir que les nouveaux contrôles mis en place étaient bien conçus et avaient le rendement attendu.

Objectif et portée de la vérification

L'objectif général de cette phase était d'évaluer l'efficacité des contrôles en place pour restreindre de manière efficace l'accès aux applications de gestion afin d'assurer de manière permanente l'intégrité des données de gestion. Notre vérification consistait à évaluer les risques liés à la gestion des risques d'entreprise (ERM) pouvant survenir, à recenser les contrôles en place pour atténuer ces risques et à effectuer des tests afin d'évaluer l'efficacité de leur fonctionnement. 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;
- ▶ 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.

La vérification s'est étendue aux systèmes suivants : CAS, PSFIN, Globex, CRS, MBC, FIRM et UFS. En 2009, nous avons constaté que tous les contrôles s'appliquant au système UFS fonctionnaient comme prévu. Nous avons néanmoins inclus le système UFS dans notre vérification pour appuyer la vérification externe. Nous avons par ailleurs exclu les systèmes MTIP et GAS de la phase II de la vérification, puisque tous les contrôles avaient démontré en 2009 qu'ils fonctionnaient comme prévu. Finalement, nous avons procédé à des sondages limités sur le fonctionnement des systèmes PSHR et ACBS, car nous avons constaté que la plupart des contrôles fonctionnaient comme prévu lors de notre vérification en 2009.

Le travail de vérification sur le terrain requis a été effectué en novembre et en décembre 2010.

Opinion de la Vérification interne

En 2009, nous avons conclu qu'il *existait des possibilités d'améliorer les contrôles*¹ encadrant la gestion des changements apportés aux applications. La direction a depuis mis en place des contrôles efficaces pour corriger les déficiences constatées lors de la phase I, lesquels fonctionnent comme prévu. Par conséquent, nous sommes d'avis que l'accès aux applications de gestion est maintenant bien *contrôlé*. Nous n'avons dès lors aucune recommandation à formuler.

Conclusion

Les constatations et recommandations de la vérification ont été communiquées à la direction. Nous tenons à remercier la direction de son soutien tout au long de la vérification.

¹ 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 sont très probablement atteints.
- **Bien contrôlé** : Des contrôles clés ont été efficacement conçus et fonctionnent comme prévu. Les objectifs du processus vérifié sont probablement atteints.
- **Possibilités d'améliorations** : 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.