Bureau du surintendant des institutions financières Canada
Office of the Superintendent of Financial Institutions Canada

Rapport de vérification interne du cadre de contrôle de l'accès aux réseaux informatiques

Janvier 2010

BSIF
OSFI

Canada

Table des matières

Contexte

Introduction

Le Comité de vérification et le surintendant ont accepté que l'infrastructure, les applications, les systèmes et les mécanismes au moyen desquels les BSIF gère l'accès à ses réseaux informatiques (le *Cadre de contrôle de l'accès aux réseaux informatiques*), ainsi que les mesures d'application ce cadre, soient inscrits dans le Plan de vérification interne 2009-2010 du BSIF.

Lors de la préparation de ce plan de vérification, nous avons examiné les politiques, les directives et les pratiques de sécurité en insistant sur l'accès à l'information électronique et sa protection, et sur les pratiques, mesures et outils connexes[1]. En outre, nous avons rencontré le surintendant auxiliaire, Services intégrés, et les directeurs de la Sécurité et de la Division des services d'infrastructure technologique – Gestion de l'information et Technologie de l'information (GI-TI).

Comme on peut le voir au diagramme 1, l'architecture du cadre de contrôle de l'accès aux réseaux informatiques, très élaborée, permet d'en restreindre l'accès aux seules personnes qui doivent pouvoir les consulter pour effectuer leur travail. L'architecture du cadre de contrôle de l'accès aux réseaux informatiques compte deux « zones de sécurité » distinctes : publique, réseau intégré, site de reprise non équipé, et entreposage de bandes hors site.

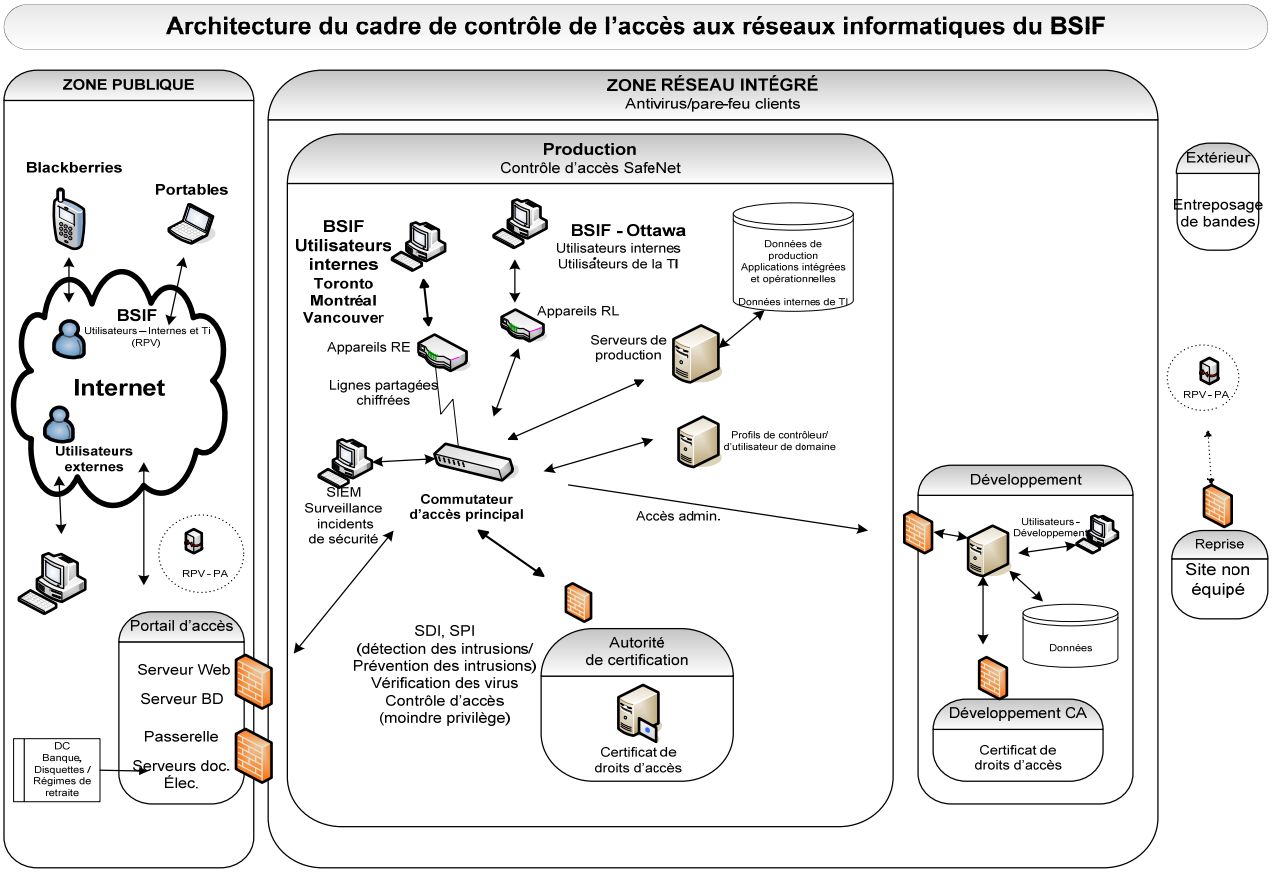
La *zone publique* est située à l'extérieur du réseau intégré du BSIF. Grâce à Internet, les employés[2] ont accès au réseau du BSIF à l'aide d'ordinateurs portables, de *blackberries* et d'ordinateurs personnels. Les services de la zone publique comprennent l'accès au site Web public et aux bases de données du BSIF, ainsi que l'accès à distance aux documents électroniques, au service de courrier électronique externe et aux services du Réseau intégré.

Parmi les mesures de sécurité utilisées, mentionnons l'authentification à deux facteurs (carte à puce), des pare-feu, la prévention et la détection des intrusions, la surveillance dynamique et les appareils de Réseau privé virtuel (les services de RPV utilisent du matériel spécial pour constituer un réseau privé empruntant les lignes du réseau public). Les appareils de RPV offrent une connexion protégée entre deux points de TI (poste de travail à serveur ou serveur à serveur) en chiffrant toutes les données échangées au moyen de cette connexion.

La zone *Réseau intégré* comporte deux *domaines*, un pour le développement et l'autre pour la production. Les employés travaillant dans les bureaux du BSIF ont accès aux services du réseau intégré au moyen de lignes chiffrées d'un réseau local ou d'un réseau étendu. Parmi les mesures de sécurité utilisées, citons l'authentification à deux facteurs (carte à puce), les appareils de RPV, les pare-feu, l'autorité de certification et les profils de contrôleurs et d'utilisateurs, de même que la surveillance des incidents de sécurité.

[1] Norme opérationnelle de sécurité du SCT : Gestion de la sécurité des technologies de l'information (GSTI); Politique du SCT sur la sécurité du gouvernement (PSG); Objectifs de contrôle de l'information et des technologies connexes (COBIT)
[2] Y compris les personnes ne faisant pas partie de l'effectif qui possèdent une cote de sécurité.

Architecture du cadre de contrôle de l'accès aux réseaux informatiques ***Diagramme 1***



Terminologie

Composantes physiques du cadre de contrôle de l'accès aux réseaux informatiques	Mesure de sécurité *SafeNet* (carte à puce), l'architecture du cadre de contrôle de l'accès aux réseaux informatiques, etc. Se reporter au diagramme 2, à la page 9.
Biens de TI	Applications opérationnelles, infrastructure de la TI, et logiciels et matériel connexes, appareils de TI personnels, p. ex. les *blackberries*, etc. Se reporter au diagramme 1, à la page 4.
BITI	Bibliothèque d'infrastructure des technologies de l'information, R.-U. (normes *de facto*, pratiques exemplaires pour la gestion des services de TI)
Contrôle de l'accès aux réseaux informatiques	Politiques, directives, processus, activités, mesures et outils de sécurité, et de SIT liés à l'accès à l'information électronique du BSIF et à sa protection.
CCC	Comité consultatif du changement (fait partie du processus de gestion du changement de la GI-TI)
COBIT	Objectifs de contrôle dans les domaines de l'information et des technologies connexes (Cadre de contrôle de la gouvernance et de la gestion de la GI-TI)
COSO	Cadre du *Committee Of Sponsoring Organizations de la Treadway Commission* (cadre de contrôle)
DPI	Dirigeant principal de l'information, GI-TI
EMR	Évaluation de la menace et des risques
GCE	Groupe de la consultation et de l'évaluation (fait partie du processus de gestion du changement de la GI-TI)
GGP	Groupe de la gestion des projets (groupe chargé de l'élaboration de systèmes de GI-TI)
GI-TI	Division de la gestion de l'information / de la technologie de l'information
GSTI	Norme opérationnelle du SCT : Gestion de la sécurité de la technologie de l'information
PGC	Processus de gestion du changement, processus de GI-TI pour la gestion des demandes de changement formulées par les utilisateurs. Le PGC comprend les groupes du CCC et le GCE
PSG	Politique du SCT sur la sécurité du gouvernement
RACI	Modèle de rôles et responsabilités : personne **R**esponsable**, A**visée, **C**onsultée et **I**nformée
RE	Réseau étendu
RL	Réseau local
RPV	Réseau privé virtuel
SafeNet	Technologie / logiciel de carte à puce donnant un accès limitée à des ordinateurs et à l'information électronique grâce à un identifiant et un mot de passe spécifiques et contrôlés.
SIT	Services d'infrastructure technologique, groupe des opérations de TI (GI-TI)
SS	Services de sécurité (groupe de la sécurité au BSIF)
Utilisateurs	Secteurs de la surveillance, de la réglementation et des Services intégrés, Division des

(Applications)	régimes de retraite et Bureau de l'actuaire en chef (applications)

Fournir des garanties

Afin de pouvoir gérer ses travaux dans un contexte complexe et en constante évolution, le BSIF élabore et met en place des politiques, des directives et des processus spéciaux que l'on qualifie généralement de « cadres de contrôle interne ». Ces cadres donnent au surintendant et à la haute direction l'assurance que la nature et la portée des tâches requises pour mener à bien les activités du BSIF sont bien définies et que la cohérence et la qualité des travaux sont assurées.

Ces cadres et leur application sont essentiels pour le surintendant et le Comité de vérification, car ils leur permettent de s'acquitter de leurs responsabilités aux termes de la Politique de vérification interne du Conseil du Trésor en ce qui touche les processus de gouvernance, de contrôle et de gestion des risques du BSIF. En vertu de cette politique, les Services de vérification et de consultation doivent procéder à des vérifications d'assurance relativement à la qualité de la conception des activités du BSIF et des rapports intégrés connexes (structure du cadre de contrôle interne) et à leur fonctionnement (l'application des cadres pour respecter les objectifs opérationnels).

Objet de la vérification

La vérification a pour objet :

- de produire une évaluation du cadre de contrôle interne (*Cadre de contrôle de l'accès aux réseaux informatiques*) en vertu duquel la sécurité du BSIF et l'infrastructure de contrôle de l'accès aux réseaux informatiques donnent un accès limité à l'information électronique et la protègent;
- d'évaluer la qualité et le niveau d'application des mesures de sécurité du réseau accessible au moyen de la carte à puce *SafeNet*;
- de déterminer les possibilités d'amélioration, s'il y a lieu.

Portée de la vérification

La vérification porte sur le **Contrôle de l'accès aux réseaux informatiques** (politiques, directives et pratiques de sécurité et de SIT associés à l'accès limité à l'information électronique du BSIF et sa protection) pour l'exercice 2009-2010 au mois de *décembre 2009*, de même que les améliorations en cours au troisième trimestre de 2009-2010 et prévus. Les travaux comprendront la mise à l'essai des mesures de sécurité *SafeNet*, entre *le premier trimestre de 2009 et la fin du deuxième trimestre, à la fin de septembre 2009*.

Le présent examen ne porte pas sur :

- le niveau d'application des mesures de contrôle de l'accès aux réseaux informatiques au BSIF, exception faite de la récapitulation des structures, activités, processus et outils existants et prévus qui ont trait au contrôle de l'accès aux réseaux informatiques, et des tests détaillés appliqués à la sécurité du réseau, comme il a été susmentionné;
- l'architecture de l'infrastructure technologique du BSIF, sauf si elle s'applique à l'architecture du cadre de contrôle de l'accès aux réseaux informatiques;
- l'élaboration des application/systèmes, sauf en ce qui touche l'administration de leur accès limité au contrôle de l'accès aux réseaux informatiques;
- les mesures de protection non liées à la TI, notamment les locaux et installations, la classification de l'information, et les vérifications de sécurité des employeurs et des entrepreneurs.

Approche en matière de vérification

La vérification a été effectuée conformément aux *Normes internationales pour la pratique professionnelle de la vérification interne* de l'Institut des vérificateurs internes, conformément à la politique du Conseil du Trésor sur la vérification interne, pour en confirmer les constatations, l'analyse, les observations et les recommandations.

Les travaux de vérification du *contrôle de l'accès aux renseignements électroniques* :

- examen et récapitulation des structures, activités, processus et mesures/outils existants, en application et prévus par rapport à la *structure du contrôle de l'accès du contrôle de l'accès aux réseaux informatiques*, y compris la surveillance, l'analyse, l'évaluation et la déclaration en matière de sécurité, notamment le suivi par impartition du périmètre de réseau et la réaction aux incidents;
- examen et récapitulation de l'*architecture du cadre du contrôle de l'accès aux réseaux informatiques* et des structures, activités, processus et mesures/outils connexes;
- examen et récapitulation des structures, activités, processus et mesures/outils existants, en application et prévus de l'utilisation de *SafeNet* à la grandeur du BSIF, de même que des essais relatifs à l'utilisation de *SafeNet* par les employés dans l'exercice de leurs fonctions. Un échantillon représentatif de 20 à 40 utilisateurs du BSIF et des services de TI sera établi pour examiner l'utilisation de *SafeNet*;
- entrevues avec les membres de la direction et le personnel des Services de sécurité et des SIT, de même qu'un échantillon d'utilisateurs des services de TI du BSIF et des services de TI.
- recensement et application de pratiques et méthodes comparables relatives à l'accès du contrôle de l'accès aux réseaux informatiques à l'information électronique, à sa protection, y compris la GSTI, la PSG, le BITI, l'Institut de la gestion de projets – Manuel de connaissance de la gestion de projet, et l'information et les évaluations offertes par le biais d'associations responsables, comme l'ISACA.

Cadre de contrôle interne

Le cadre de contrôle interne de l'accès aux réseaux informatiques (éléments de critères et composantes connexes) énoncé à l'*Annexe A – Cadre de contrôle interne* a été utilisé pour évaluer la politique, les directives, les processus, les activités, les mesures/outils de contrôle interne de l'accès protégé à la TI.

Les critères ont été élaborés à partir de sources diverses de politique et directives de sécurité et de contrôle de l'accès aux réseaux informatiques, et de pratiques exemplaires[3], après consultation du directeur de la Sécurité, du DPI et du directeur des Services d'infrastructure technologique, GI-TI. La portée et la complexité du contexte de la TI au BSIF, de même que l'information qui le caractérise et les risques qu'il comporte, ont été prises en compte aux fins de l'élaboration des critères de contrôle interne.

Les critères de contrôle interne ont été acceptés par le surintendant auxiliaire, Services intégrés, aux fins d'évaluation et de rapport concernant l'accès protégé de la TI à l'information électronique.

[3] Ces critères proviennent des cadres de contrôle et y correspondent : COSO (Committee of Sponsoring Organizations of Treadway Commission, GSTI (Norme opérationnelle du SCT en matière de sécurité : Gestion de la sécurité de la technologie de l'information), et COBIT (Objectifs de contrôle dans les domaines de l'information et des technologies connexes).

Observations, évaluation et recommandations

Aperçu

Notre vérification a porté sur le *cadre interne de gestion de l'accès aux renseignements électroniques* en date de *décembre 2009* et sur les améliorations qui ont été apportées pendant le troisième trimestre de 2009-2010, de même que sur l'examen de l'application de la mesure de sécurité *SafeNet* (accès limité à l'information de TI du BSIF) *entre avril et la fin de septembre 2009*.

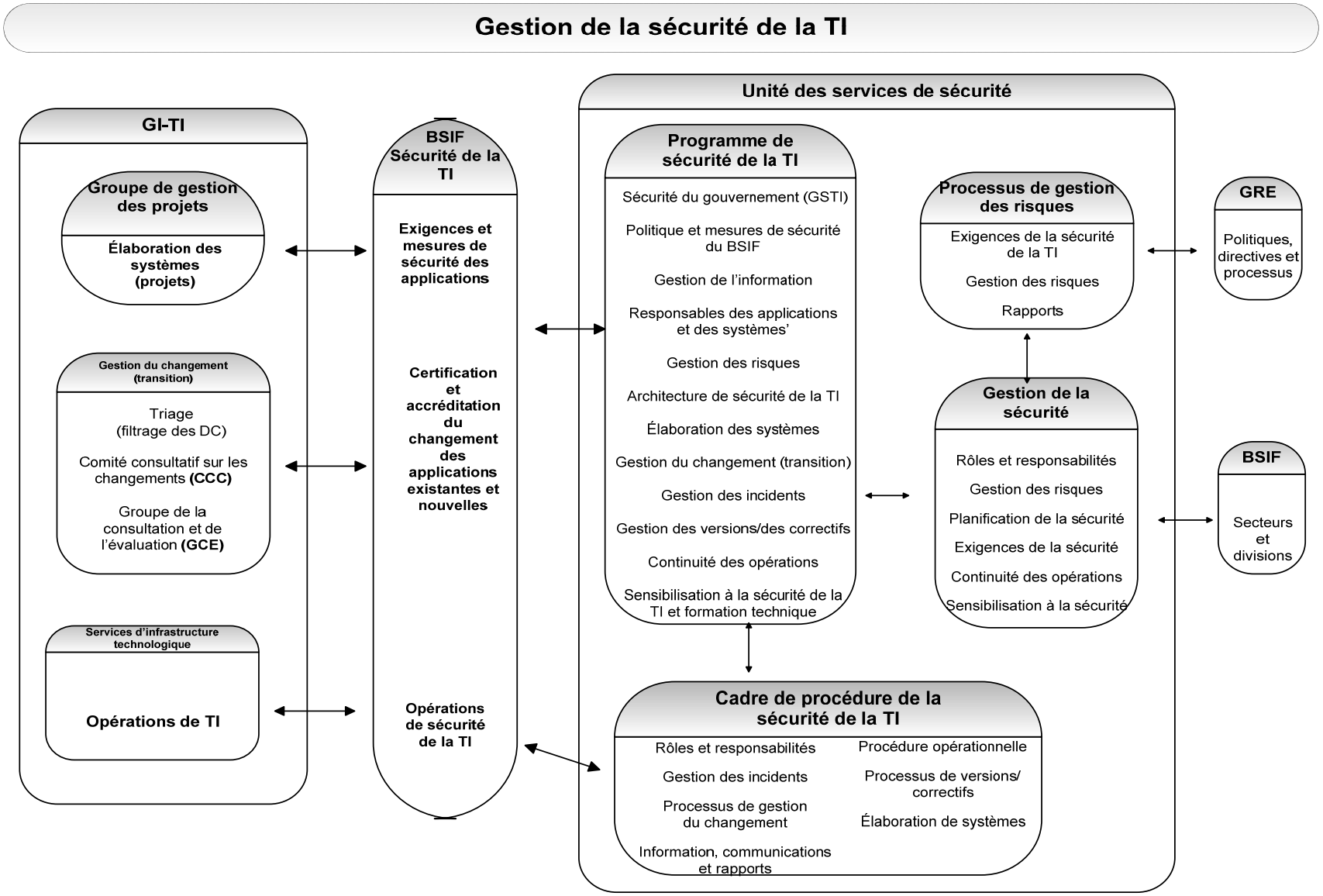
Les travaux ont été effectués en collaboration, car l'amélioration de la TI et de la sécurité avait déjà eu lieu, ou était déjà en cours pendant ces travaux. Des discussions continues se sont déroulées avec le directeur des Services de l'infrastructure technologique, GI-TI, et avec les principaux employés qui tiennent à jour et fournissent les services de sécurité et de contrôle de l'accès aux réseaux informatiques.

Nous avons scruté et examiné toutes les composantes du *cadre interne de gestion de l'accès aux réseaux informatiques*. Pour suivre le cours des observations issues de la vérification, veuillez consulter le *Diagramme 2 – Gestion du contrôle de l'accès aux réseaux informatiques*, qui présente l'interaction du Groupe des services de sécurité et des principaux groupes du BSIF, de même que les cadres et activités portant sur la gestion du contrôle de l'accès aux réseaux informatiques. Le cas échéant, nous avons tenu compte du nombre d'améliorations apportées et lancées pendant notre vérification. Ces mesures exigeront un effort de coordination ciblé entre les Services de sécurité et la GI-TI, les gestionnaires axiaux et fonctionnels, et la direction.

Même si nous avons dégagé les principales composantes d'un cadre de contrôle interne efficace, nous avons décelé d'autres éléments à améliorer. Nos observations et recommandations portent plus particulièrement sur :

- l'officialisation et le raffermissement des politiques et procédures inhérentes afférentes au programme global d'accès aux réseaux informatiques;
- la mise au point d'un processus de gestion du risque de sécurité au niveau opérationnel;
- le raffermissement du contrôle de l'accès aux renseignements découlant d'un exercice de concertation de Services de sécurité, de Services d'infrastructure technologique et d'autres groupes chargés de la GI-TI.

Gestion du contrôle de l'accès aux réseaux informatiques ***Diagramme 2***



Contrôle de l'accès aux réseaux informatiques

Éléments/composantes du contrôle interne	Observations, évaluation et recommandations
Gouvernance : établissement des objectifs et contexte opérationnel	
▪ *L'obligation de rendre compte de la supervision existe* ▪ *Les rôles et responsabilités sont définis, communiqués et compris* ▪ *La politique et les pratiques d'accès protégé à la TI sont bien établis* *Recommandation* Officialiser et raffermir les politiques et procédures de contrôle de l'accès aux réseaux informatiques dans le cadre d'un programme fondamental de gestion de l'accès aux réseaux informatiques englobant la Politique sur la sécurité du gouvernement et les normes, directives exigences de pratique de GSTI.	Les groupes des Services de sécurité (**SS**) et des Services d'infrastructure technologique (**SIT**) gèrent et offrent des services de sécurité à l'échelle du BSIF. Selon la Politique sur la sécurité du gouvernement (**PSG**) et les directives concernant la Gestion de la sécurité de la technologie de l'information (**GSTI**), les rôles et responsabilités respectifs en matière de contrôle de l'accès aux réseaux informatiques ont été établis à l'aide d'un modèle de *responsabilité* conforme au RACI[1] reposant sur la PSG et les directives sur la GSTI, selon le contexte de TI du BSIF. D'après l'analyse du RACI, les groupes respectifs mettent en place de façon prioritaire les politiques, directives et processus opérationnels nécessaires pour intégrer et coordonner les travaux liés au contrôle de l'accès aux réseaux informatiques. *Note 1 : RACI: personne **R**esponsable, **A**visée, **C**onsultée et **I**nformée. Une matrice RACI est un type d'outil d'affectation de responsabilité qui indique le lien entre les activités et les employés. La description intégrale de cet outil figure à la rubrique Organization Charts and Position Descriptions du PMBOK (quatrième édition) – Develop Human Resource Plan process.* À titre de membre du Comité consultatif du changement (**CCC**) et du Groupe de la consultation et de l'évaluation (**GCE**), les Services de sécurité font partie intégrante du processus de gestion du changement (**PGC**) de la GI-TI. Un de les principaux rôles à ce titre consiste à gérer l'évaluation et l'acheminement des demandes de changement (**DC**) au processus de changement ou d'élaboration pertinent – un changement standard mineur, un changement important, un projet d'élaboration de système ou un projet opérationnel de TI. Une DC relative à l'élaboration d'un système ou à un projet opérationnel de TI est gérée au moyen de processus distincts. Les Services de sécurité sont membres signataires de projets d'élaboration de systèmes en ce qui a trait à la sécurité et au contrôle de l'accès aux réseaux informatiques. Le PGC doit informer les Services de sécurité des projets opérationnels de TI, de sorte que les besoins en matière en sécurité puissent être déterminés dès que possible. À la suite de l'examen externe de la gouvernance de la sécurité au sein du BSIF, on a recommandé de mettre sur pied une *tribune de gestion de la sécurité*. Les Services de sécurité ont indiqué que la création d'une telle tribune est à l'étude. Nous appuyons fermement cette initiative. Une tribune permet d'adapter la PSG et les exigences de GSTI en fonction des besoins du BSIF, de la structure du programme de sécurité du BSIF, y compris les exigences et mesures de sécurité des applications opérationnelles, et de l'élaboration de plans de sécurité pour l'ensemble de l'organisme. Les directives du SCT concernant la planification de la sécurité, qui seront diffusées bientôt, prévoient l'élaboration, la mise en œuvre et la tenue à jour de plans de sécurité ministériels (BSIF) qui renferment des détails sur les décisions de gestion des risques de sécurité et qui énoncent les stratégies, les buts, les objectifs, les priorités et les échéances qui permettront de resserrer la sécurité au BSIF. Il est important que tous les intervenants, secteurs et divisions participent directement à l'élaboration et à la tenue à jour de politiques, de directives et de programmes de sécurité (et de contrôle de l'accès aux réseaux informatiques). Les documents de gestion de l'accès aux réseaux informatiques que nous utilisons présentement renferment des éléments de la politique, des normes et des procédures, mais ils ne sont pas toujours complets. Par exemple, une analyse interne des lacunes de la politique a révélé que nous avions besoin de politiques et de directives en matière de gestion des biens, de gestion de la vulnérabilité et des incidents, de normes de sécurité des

Éléments/composantes du contrôle interne	Observations, évaluation et recommandations
	applications, et de planification de la reprise après une catastrophe. La politique et les directives en matière de gestion de l'accès aux réseaux informatiques existent et sont communiquées à l'interne. Aucun programme essentiel de sécurité (et de contrôle de l'accès aux réseaux informatiques) n'est lié à la PSG, à la GSTI et aux besoins internes de sécurité à l'intérieur d'un ensemble intégré de politiques, de directives, de processus et d'outils. À défaut d'une telle structure globale, il serait difficile de savoir si les activités courantes décrites jusqu'ici seront exécutées de façon coordonnée et consolidée. *Nous recommandons au BSIF d'officialiser et de raffermir en priorité les politiques et procédures de contrôle de l'accès aux réseaux informatiques à l'intérieur d'un programme fondamental de sécurité englobant la Politique de sécurité du gouvernement et les normes, pratiques et exigences de la GSTI adaptées au contexte de TI du BSIF.*
Gestion des risques	
▪ *Le risque et la tolérance au risque est conforme aux pratiques de GRE* ▪ *La détermination des exigences en matière de risque de TI repose sur l'évaluation du contexte de la TI* ▪ *Les risques relatifs au contrôle de l'accès aux réseaux informatiques sont détectés et évalués, et des contrôles d'atténuation sont effectués.*	Au BSIF, la politique et les processus de gestion du risque global sont utilisés pour déterminer, évaluer et atténuer les risques qu'encourent les secteurs et des groupes. Au Secteur des services intégrés, les risques afférents à la sécurité et à l'accès aux réseaux informatiques sont déterminés, évalués et, le cas échéant, intégrés aux plans d'action de la GRE. Même si les risques de sécurité sont intégrés aux évaluations de la GRE du BSIF, il n'existe pas de processus propre à la gestion du risque de sécurité pour déterminer, évaluer, atténuer et gérer les risques opérationnels afférents à la sécurité et à l'accès aux réseaux informatiques. Un processus de gestion du risque afférent à la sécurité établi en vertu de la PSG et de la GSTI, conformément à la GRE, est essentiel pour la détermination, l'évaluation des exigences en matière de sécurité et le signalement des risques afférents à l'accès aux réseaux informatiques aux responsables de la GRE et à la direction. Un processus de gestion des risques de ce type correspondrait aux fonctions et processus principaux de GI-TI, notamment la gestion de portefeuille, l'élaboration de systèmes, les opérations de TI, les versions d'applications et de systèmes, et la gestion de la mise à jour des incidents et versions/correctifs.
Recommandation Établir un processus de gestion du risque de sécurité à un niveau opérationnel qui englobe les exigences de TI, la détermination et l'évaluation du risque relatif au contrôle de l'accès aux réseaux informatiques, la gestion et les rapports sur le risque de sécurité conforme aux pratiques de GRE	Les Services de sécurité évaluent périodiquement les risques afférents à l'accès aux réseaux informatiques (vulnérabilité, menaces et risques), de même que des rapports destinés à la direction au sujet des principaux facteurs de risques et de principales sources de préoccupations. Les résultats de ces évaluations sont analysés sous l'angle de l'impact sur le BSIF, et des mesures et des recommandations sont proposées. Les mesures sont placées en ordre de priorité et des ressources sont déterminées. En outre, les SIT surveillent de façon continue les contextes interne et externe, et ils exécutent des évaluations quotidiennes des menaces et des risques. Le processus de partage des résultats de ces évaluations doit être officialisé. Les Services de sécurité formulent des demandes de renseignements et assurent le suivi de leurs évaluations et des évaluations des SIT au chapitre du risque des opérations de TI, notamment le refus éventuel de service et des attaques de pénétration. Il n'existe pas de processus de répertoriage, de suivi et de rapport pour déterminer si ces problèmes de sécurité ont été abordés. Ce processus de suivi des évaluations et recommandations relatives au contrôle de l'accès aux réseaux informatiques est essentiel pour maintenir le contexte du contrôle de l'accès aux réseaux informatiques au BSIF. Selon de récentes évaluations du contrôle de l'accès aux réseaux informatiques, les risques externes sont contrôlés pas de rigoureux contrôles périmétriques. Les processus

Éléments/composantes du contrôle interne	Observations, évaluation et recommandations
	internes de surveillance du contrôle de l'accès aux réseaux informatiques sont toutefois moins stricts. Il s'agit de processus informels et de pratiques non conformes se rapportant aux versions et correctifs de sécurité, à la vulnérabilité et à la gestion des incidents. Les SIT ont amorcé le processus de mise en œuvre des correctifs de sécurité des systèmes opérationnels. Parallèlement à notre recommandation pour que le BSIF officialise et raffermisse les politiques et procédures de contrôle de l'accès aux réseaux informatiques afin de les intégrer à un programme fondamental de sécurité relevant de la section Gouvernance et responsabilité, nous recommandons aux Services de sécurité d'établir un processus de gestion du risque de sécurité pour enchâsser la gestion du risque de TI et les politiques et mesures sous-jacentes de sécurité et de contrôle de l'accès aux réseaux informatiques dans un programme de contrôle de l'accès aux réseaux informatiques. Le processus de gestion du risque de sécurité fournirait de précieux renseignements et des évaluations du contrôle de l'accès aux réseaux informatiques servant à déterminer la tolérance globale du BSIF au risque, la structure du contexte de la TI au BSIF, de même que celle des politiques et mesures de sécurité des applications opérationnelles. *Nous recommandons l'établissement d'un processus de gestion du risque de sécurité au niveau opérationnel qui intègre les mesures de sécurité du contrôle de l'accès aux réseaux informatiques, l'identification et l'évaluation des risques auxquels le contrôle de l'accès aux renseignements électronique est exposé, et la gestion et le signalement du risque de sécurité, conformément aux pratiques de GRE.*
Processus de contrôle	
▪ *La planification et les ressources de sécurité englobent les mesures de sécurité du contrôle de l'accès aux réseaux informatiques* ▪ *Établissement d'un programme de protection qui comprend les mesures du contrôle de l'accès aux réseaux informatiques* ▪ *Il existe une fonction de gestion des incidents* ▪ *L'élaboration des systèmes et la gestion du changement renferment les exigences de contrôle de l'accès aux réseaux informatiques* ▪ *La planification de la continuité et de la reprise renferment les*	La norme de gestion du contrôle de l'accès aux réseaux informatiques (GSTI), qui relève du SCT, invite spécifiquement les ministères et organismes à adopter une stratégie de défense active qui comprend des activités de prévention, de détection, de réaction et de reprise. Il existe un programme de protection de la sécurité au BSIF, ainsi qu'une architecture solide d'accès aux réseaux informatiques, (Diagramme 1 – Architecture du cadre du contrôle de l'accès aux réseaux informatiques). Cette architecture prévoit l'accès limité à l'information électronique du BSIF grâce à des mesures de sécurité qui englobent l'authentification à deux facteurs dans le contexte interne de la TI au BSIF (réseau intégré), les communications chiffrées du réseau privé virtuel, les pare-feu, l'autorisation de certification et les privilèges d'accès, de même que le chiffrement complet des données sur ordinateurs personnels et portables. Des mesures actives de surveillance des risques et de sauvegarde sont en place. Le personnel responsable de la TI dispose de deux comptes d'accès, un compte utilisateurs pour les tâches administratives normales et un compte de surveillance et d'administration distinct pour les tâches opérationnelles. Le BSIF a mis en place nombre de composantes d'un cadre de procédure de la sécurité. Ce cadre est toutefois informel et de portée limitée, et les travaux des Services de sécurité et des SIT ne sont pas bien intégrés pour constituer une architecture du cadre de contrôle de l'accès aux réseaux informatiques. Par exemple, même si le réseau est surveillé par le personnel de la TI, l'information, les enjeux et les évaluations touchant la sécurité sont transmis de façon informelle aux Services de sécurité. D'après le RACI, les groupes mettent en place des politiques, des directives et des processus opérationnels sous-jacents qui répartissent les rôles et responsabilité afférentes au contrôle de l'accès aux réseaux informatiques entre les deux groupes. Les critères d'évaluation du contrôle de l'accès aux réseaux informatiques et l'information transmise aux Services de sécurité au sujet des

Éléments/composantes du contrôle interne	Observations, évaluation et recommandations
exigences de contrôle de l'accès aux réseaux informatiques *Recommandation* Raffermir le cadre de procédure du contrôle de l'accès aux réseaux informatiques pour y intégrer des procédures concernant la gestion des incidents, les mises à jour des version et des correctifs, la certification et l'accréditation de la technologie, et la planification de la continuité et de la reprise, de même que la planification connexe de la sécurité et des ressources	enjeux et des évaluations touchant la contrôle de l'accès aux réseaux informatiques sont mis au point par les deux groupes qui œuvrent côte à côte. Une nouvelle politique anticipée du SCT sur la planification de la sécurité insiste sur le regroupement de toutes les composantes de la sécurité (y compris la contrôle de l'accès aux réseaux informatiques) dans un plan de sécurité global aux fins de la planification intégrée et de la détermination des ressources. Ce plan engloberait des politiques, des exigences de sécurité, des directives et un soutien administratif et de la TI, la sensibilisation des employés et la formation technique appliquée à la sécurité globale et à sa composante, la contrôle de l'accès aux réseaux informatiques. Il faudra intégrer les plans de sécurité aux plans opérationnels et de TI, et aux activités et aux fonctions d'appui. L'établissement d'un *processus de gestion du risque de sécurité* (se reporter à la section « Gestion du risque » des observations) et la mise au point d'un cadre de *procédure* de la sécurité sont des éléments essentiels pour favoriser un tel effort de planification. À titre de membre du groupe chargé de l'élaboration au SCT, les Services de sécurité connaissent déjà ces exigences et ils sont donc bien placés pour concevoir et mettre en œuvre la nouvelle politique de planification. Le BSIF prévoit d'appliquer la nouvelle politique en 2010-2011. Une composante clé de la mise en place d'un programme de gestion de la sécurité, énoncée à la section Gouvernance et responsabilité, consiste à déterminer la propriété et la responsabilité des biens de TI (applications opérationnelles, infrastructure de TI, appareils personnels de TI, notamment des *blackberries*, etc.). Puisque qu'environ la moitié seulement des applications opérationnelles ont un « propriétaire désigné », il est difficile de savoir si la politique et les mesures de sécurité satisfont aux besoins opérationnels et s'il y a juste équilibre entre le risque de TI et les besoins opérationnels. La participation insuffisante des propriétaires à la politique de TI, à la tolérance de la TI au risque et à la sélection des mesures de sécurité pourrait influer sur la conception des applications opérationnelles et la convivialité des mesures. En vertu de l'initiative RACI, les Services de sécurité sont actuellement le propriétaire désigné des biens de contrôle de l'accès aux réseaux informatiques du BSIF, notamment la mesure de sécurité de carte à puce *SafeNet*, et la structure de l'architecture du cadre de contrôle de l'accès aux réseaux informatiques. À titre de propriétaire de l'infrastructure de TI, les SIT offriront un soutien technique en matière de conception de la sécurité, de même que des services liés aux activités de TI. Par exemple, la carte à puce constitue la pierre angulaire de l'architecture du cadre du contrôle de l'accès aux réseaux informatiques du BSIF, au sein de laquelle l'accès à l'information électronique se retreint aux personnes autorisées selon un système d'authentification à deux facteurs (une carte à puce (l'outil) et un mot de passe (le savoir)). Les composantes clés de cette mesure de sécurité sont en place. Toutefois, elles doivent être fusionnées sur le plan de la surveillance et des énoncés de responsabilité, de politique et d'orientation émanant de la gestion, des exigences des utilisateurs et en matière de TI, et de la sensibilisation et de la formation technique des employés. D'autres composantes essentielles d'un *programme de gestion de la sécurité* sont la gestion du changement, l'élaboration de systèmes et le passage de logiciels au stade de production (gestion de la transition). L'un des défis de la sécurité consiste définir son rôle et ses responsabilités dans la gestion de la transition (passage des applications et systèmes au stade de la production de la TI). En se joignant au CCC et au GCE GI-TI (se reporter à la section Gouvernance et responsabilité des observations), les Services de sécurité

Éléments/composantes du contrôle interne	Observations, évaluation et recommandations
	participent maintenant directement à la discussion portant sur la sécurité et la contrôle de l'accès aux réseaux informatiques qui relèvent d'une demande de changement de la part des utilisateurs. Ainsi, les exigences du contrôle de l'accès aux réseaux informatiques, les risques et les exigences de sécurité sont identifiés et pris en compte dans un contexte proactif. Même si les Services de sécurité participent à l'examen et à la diffusion d'applications nouvelles et de changement d'applications existantes, le processus de gestion de la transition de la GI-TI ne réclame pas un examen officiel et une approbation définitive par les Services de sécurité avant que les applications et les systèmes passent au stade de la production dans le cadre d'une vérification de certification et d'accréditation. Cette vérification doit être intégrée aux listes de vérification et aux pratiques actuelles de gestion de la transition. En vertu de l'initiative RACI, le rôle des Services de sécurité aux fins de l'évaluation de l'impact et de la priorité des mises à jour du contrôle de l'accès aux réseaux informatiques (correctifs) a été intégré à la gestion des versions et des correctifs. Un ordre de priorité des correctifs de sécurité est établi et des plans de mise en œuvre sont appliqués. La planification de la continuité des activités (PCA) est reconnue comme prioritaire. La mise à jour du plan de continuité des activités et du plan de reprise des activités (PRA) est en cours. Il est nécessaire d'établir un processus officiel raffermi de PCA afin de l'intégrer à la planification de la reprise des activités. *Nous recommandons de raffermir le contrôle de l'accès aux réseaux informatiques en y intégrant des procédures de gestion des incidents, des mises à jour des version et des correctifs, la certification et l'accréditation de la technologie, et la planification de la continuité et de la reprise, de même que la planification connexe de la sécurité et des ressources.*
Gouvernance : Information, communication et signalement	
▪ *L'information sur l'accès aux réseaux informatiques est :* ▪ *définie, recueillie, évaluée et intégrée à des rapports* ▪ *communiquée de façon continue entre les autorités de la sécurité et les intervenants* ▪ *intégrée à la sensibilisation à la sécurité des employés et à la formation du personnel de la sécurité et de la TI* *Recommandations* Raffermir le cadre de procédure du contrôle de	Comme on l'a vu à la section Gestion des risques, les Services de sécurité évaluent les menaces et les risques et les SIT surveillent en permanence les contextes interne et externe de la TI. L'information et les évaluations sont partagées de façon informelle et officieuse. Par conséquent, les rapports concernant la sécurité ou la constance de la communication de l'information, de ses destinataires et des échéances ne sont pas déposés de façon routinière. Il est essentiel que l'information de sécurité exacte soit communiquée aux bons intervenants au bon moment. Jusqu'à ce que les principaux processus opérationnels et de sécurité, notamment la gestion des incidents, la gestion des versions et des correctifs et la diffusion des logiciels soient complètement établis, l'information sur la contrôle de l'accès aux réseaux informatiques ne sera pas divulguée aux fins des évaluations et des rapports périodiques. Les rapports sur les risques liés au contrôle de l'accès aux réseaux informatiques, sur la vulnérabilité, sur les incidents, sur les événements et sur les mesures d'atténuation destinées aux personnes compétentes et qui doivent prendre des mesures, ne sont pas garantis; il n'est pas non plus certain si l'information sera reçue à temps. Il existe des pratiques *opérationnelles* informelles en matière de contrôle de l'accès aux réseaux informatiques aux Services de sécurité et aux SIT dans les domaines de l'EMR, de la surveillance réseau et de la gestion des versions et des correctifs. En outre, on note des lacunes su plan des directives et procédures de contrôle de l'accès aux réseaux informatiques, comme il est précisé à la section Processus de contrôle. En vertu de

Éléments/composantes du contrôle interne	Observations, évaluation et recommandations
l'accès aux réseaux informatiques qui englobe des procédures touchant l'information, la communication et les rapports de contrôle de l'accès aux réseaux informatiques. Officialiser et raffermir les politiques et procédures de contrôle de l'accès aux réseaux informatiques pour les intégrer à un programme fondamental de sécurité prévoyant la formation à la sensibilisation des employés et la formation du personnel de la sécurité et de la GI-TI.	l'initiative RACI, les Services de sécurité et les SIT s'affairent à classer ces lacunes en donnant la priorité à la définition de l'information sur la contrôle de l'accès aux réseaux informatiques, et à la nature, à la portée et à la présentation des rapports sur la contrôle de l'accès aux réseaux informatiques, y compris la transmission des questions de contrôle de l'accès aux réseaux informatiques à la haute direction. Il importe que ces améliorations soient apportées au cadre de gestion de la sécurité de l'accès aux réseaux informatiques. Les entrevues révèlent que la politique et les exigences de sécurité, en particulier du contrôle de l'accès aux réseaux informatiques, ne sont pas toujours bien communiquées. Les entrevues avec les utilisateurs de la carte à puce *SafeNet* indiquent une variation considérable de la connaissance des mesures de sécurité à observer, de l'importance de ranger la carte en lieu sûr lorsqu'ils s'absentent de leur poste de travail et des conséquences que pourrait devoir essuyer les BSIF si une carte devait être utilisée à mauvais escient. En 2009, les Services de sécurité ont appliqué un programme de sensibilisation destiné à tous les employés. Tous les employés devraient suivre une séance de sensibilisation à la sécurité informatique dans le cadre d'un programme global de formation en gestion de l'information électronique, de même que des séances sur leurs rôles et responsabilités au titre de l'accès aux réseaux informatiques et de l'utilisation de *SafeNet*, des portables, des *blackberries*, du courrier électronique et des réseaux. Du point de vue technique et du contrôle de l'accès aux réseaux informatiques, nous encourageons la formation interdisciplinaire, de sorte que les analystes de l'accès aux réseaux informatiques soient à l'aise avec le BITI et que les analystes de la TI soient à l'aise avec le contrôle de l'accès aux réseaux informatiques et les exigences connexes de la GSTI en matière de sécurité. Il est essentiel que les Services de sécurité et le personnel de la GI-TI partagent une même vision. *Nous recommandons de raffermir le contrôle de l'accès aux réseaux informatiques qui englobe des procédures touchant l'information, la communication et les rapports de contrôle de l'accès aux réseaux informatiques.* *Nous recommandons d'officialiser et de raffermir les politiques et procédures d'accès aux réseaux informatiques pour les intégrer à un programme global de sécurité prévoyant la formation à la sensibilisation des employés et la formation du personnel de la sécurité et de la GI-TI.*

Conclusion

Aperçu

Notre vérification a porté sur le *contrôle de l'accès aux réseaux informatiques* (*décembre 2009*), sur les améliorations qui lui ont été apportées pendant le troisième trimestre de 2009-2010, et sur la carte à puce *SafeNet* (accès restreint à l'information du BSIF sur la TI) pour la période comprise entre *avril 2009 et la fin de septembre 2009.*

Les vérifications ont été effectuées en collaboration, y compris la collecte des renseignements et les évaluations, les entrevues auprès des cadres et du personnel des Services de sécurité et des Services d'infrastructure technologique, GI-TI, et l'utilisation de *SafeNet* dans l'ensemble du BSIF. Nous avons constaté un engagement global et concerté envers l'établissement d'un vaste cadre de contrôle interne de l'accès aux réseaux informatiques.

Conclusion

D'après notre évaluation du *contrôle de l'accès aux réseaux informatiques*, nous avons conclu que :

> *Bien des composantes du cadre de contrôle interne sont en place; toutefois, l'amélioration d'éléments clés s'impose. Le BSIF a lancé des initiatives et pris des mesures en vue d'établir un vaste cadre de contrôle interne de l'accès aux réseaux informatiques. Nous reconnaissons les efforts déployés à cette fin.*
>
> *Pour apporter les améliorations nécessaires, il est nécessaire de compter sur la participation des gestionnaires et de la direction dans l'ensemble du BSIF, car les améliorations influent sur tous les secteurs et divisions.*
>
> Un effort ciblé devra être déployé pour :
>
> - officialiser et raffermir les politiques et procédures de contrôle de l'accès aux réseaux informatiques dans le cadre d'un programme global d'accès aux réseaux informatiques;
> - établir un processus de gestion des risques de sécurité au niveau opérationnel, conformément aux pratiques de GRE;
> - raffermir les procédures inhérentes au contrôle de l'accès aux réseaux informatiques entre les Services de sécurité, le Services de l'infrastructure technologique et d'autres groupes de la GI-TI.

L'équipe chargée de la vérification tient à souligner la qualité des échanges et de l'appui qu'elle a reçu durant cet exercice.

_____
Directeur principal,
Services de vérification et de consultation

_____
Date

Réponse de la direction

Les Services de sécurité et les SIT estiment tous deux que cette vérification a contribué positivement à nos mandats. Nous remercions l'équipe chargée de la vérification de son approche de collaboration et de la rigueur dont elle a fait preuve. Nous sommes entièrement d'accord avec les constatations issues de cet exercice. Elles attestent fidèlement des progrès réalisés jusqu'à présent et du chemin qu'il nous reste à parcourir. Bien qu'ils soient d'ores et déjà encadrés par de solides mécanismes et protocoles de protection, la direction reconnaît que certaines améliorations devront être apportées au cadre interne de contrôle de l'accès à ses réseaux informatiques.

Comme nous l'avons vu ici et en témoigne le *diagramme 1*, l'architecture du cadre de contrôle de l'accès aux réseaux informatiques du BSIF est très élaborée. Elle procède de mesures de sécurité, telles que le contrôle en deux volets de l'identité de l'utilisateur (c.-à-d. la carte à puce *SafeNet*) et le chiffrement électronique des communications et de la totalité des données qui se trouvent dans les ordinateurs de bureau et les portables pour restreindre l'accès aux renseignements électroniques. C'est d'ailleurs ce que confirment des évaluations indépendantes des menaces et des risques, le programme de surveillance continue des réseaux informatiques du BSIF et nos évaluations quotidiennes des risques et de la vulnérabilité. À la lumière de ce qui précède et du fait qu'à ce que nous sachions, personne ne soit parvenu à consulter nos renseignements électroniques sans autorisation à ce jour, la direction estime que les mesures de sécurité entourant ses réseaux informatiques sont efficaces.

Nous notons également que les recommandations qui se trouvent dans ce rapport font état des défis qui attendent le BSIF au chapitre du raffermissement du cadre de contrôle interne de l'accès aux réseaux informatiques. Nombre d'initiatives sont déjà en cours pour relever ces défis. C'est d'ailleurs dans cette démarche que s'inscrit notre groupe de travail sur le perfectionnement de la matrice RACI et l'amélioration du cadre de contrôle interne à partir de ses composantes actuelles.

Nous nous engageons à établir une approche équilibrée pour raffermir le programme de sécurité du BSIF, selon un niveau de risque acceptable, de sorte que notre organisme puisse devenir un modèle d'efficience et d'efficacité pour les autres organismes fédéraux. Toutes les recommandations comprises dans le rapport seront prises en compte dans les quatorze mois qui nous séparent de la fin de l'exercice 2010-2011.

Annexe A – Critères de contrôle interne

Critères de contrôle interne (utilisés pour évaluer la vérification)	
Éléments	**Composantes**
Gouvernance : Établissement des objectifs et du contexte opérationnel	▪ Les responsabilités en matière de gouvernance, d'objectifs et de supervision, de même que les structures organisationnelles, existent déjà au BSIF. ▪ Les rôles et responsabilités conformes aux compétences sous-jacentes, et les interactions des intervenants (haute direction, GRE, secteurs/divisions, vérification et examen, et ceux qui fournissent et appuient les services de sécurité) sont définis, communiqués et compris. ▪ Les politiques et pratiques de sécurité au BSIF renferment une politique sur la sécurité du gouvernement (PSG), et des normes sur la gestion de la sécurité de la technologie de l'information (GSTI) adaptées pour tenir compte de la situation du BSIF. ▪ La politique et les directives de sécurité en place prévoient l'accès limité à l'information électronique et la protection de cette dernière (définie, documentée et communiquée); ces instruments sont examinés et modifiés au besoin, d'après la PSG, les exigences et les normes de sécurité sur la GSTI. ▪ La politique et les directives de sécurité portant sur l'information électronique correspondent bien et appuient la mise en œuvre de plans et priorités intégrés
Gestion des risques	▪ Les risques internes et externes relatifs à l'accès aux réseaux informatiques et leur protection sont déterminés, évalués, atténués et intégrés à la politique et aux directives de sécurité. ▪ La détermination des exigences en matière de sécurité et de TI, et le choix, la vérification et la mise en œuvre de mesures et d'outils de sécurité reposent sur l'identification et l'évaluation des risques. ▪ Le contexte interne et externe de la TI est continuellement surveillé et évalué pour détecter les menaces et la vulnérabilité, et il est intégré à la gestion du risque de sécurité. ▪ La gestion du risque au BSIF et les directives touchant la tolérance au risque sont intégrées à la gestion du risque de sécurité.
Processus de contrôle	▪ La *planification et* les *ressources* de sécurité à la grandeur du BSIF renferment des exigences pour donner à la sécurité l'accès à l'information électronique et en assurer la protection.
	▪ Il existe un *programme de protection de la sécurité* qui renferme la surveillance et l'appui des mesures et outils de sécurité, notamment des cartes à puce, des pare-feu, le chiffrement, la sécurité des applications, et la protection antivirus et contre les codes malveillants, l'autoévaluation et les vérifications indépendantes de la sécurité, le contrôle de l'accès et les mesures de sécurité physique.
	▪ Il existe des mesures de *gestion des incidents* servant à détecter et à gérer les incidents de sécurité de TI qui donnent accès aux mesures de sécurité, les modifient, les désorganisent ou les contournent.

	▪ Les exigences de sécurité sont intégrées à l'*élaboration des systèmes* et couvrent le cycle de vie des applications et des systèmes, ou des services.
	▪ La *planification continue de la reprise* et les plans comprennent les exigences pour donner à la sécurité l'accès à l'information électronique et en assurer la protection.
Gouvernance : Information, communications et rapports	▪ L'information sur la sécurité touchant l'accès à l'information électronique et sa protection est définie, recueillie, évaluée et intégrée dans la gestion, la sécurité et les rapports sur les activités. ▪ L'information sur la sécurité traitant de la surveillance, les évaluations des risques et de la vulnérabilité, la gestion des incidents et les mesures d'atténuation sont communiquées de façon continue aux services de sécurité et aux intervenants d'une manière conforme aux obligations respectives en matière de gouvernance et de supervision. ▪ La sensibilisation et la formation des employés (et des intervenants du domaine de la sécurité) en matière de sécurité sont déterminées, établies et communiquées.