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

Rapport sur l'audit interne de la gouvernance de la gestion de l'information et des technologies de l'information

Bureau du surintendant des institutions financières

Novembre 2012

BSIF
OSFI

Canada

Table des matières

1. Contexte

Avant-propos

La Vérification interne obtient un degré donné d'assurance en confirmant que les processus de gestion du risque, de contrôle et de gouvernance du Bureau du surintendant des institutions financières Canada (BSIF), tels qu'ils ont été conçus et présentés par la direction, sont adéquats et fonctionnent de manière à ce que les risques soient bien identifiés et pris en charge, et pour veiller au respect, notamment, des politiques, des plans, des procédures ainsi que des lois et de leurs règlements d'application.

Le Comité de vérification du BSIF et la surintendante ont consenti à ce qu'un audit de la gouvernance de la gestion de l'information (GI) et des technologies de l'information (TI) soit compris dans le plan d'audit interne 2011-2012.

Le présent rapport rend compte des résultats des travaux d'audit achevés à la fin de juillet 2012. La recommandation qu'il contient aidera la Division de la GI-TI à améliorer sa gouvernance.

Le rapport a été présenté au Comité de vérification du BSIF et approuvé par la surintendante le 23 novembre 2012. Il a également fait l'objet d'un examen par le surintendant auxiliaire, Services intégrés, et la dirigeante principale de l'information, et leurs commentaires sont exposés ci-après.

Contexte

Aperçu du bien-fondé de l'audit

Dans les entreprises axées sur le savoir comme le BSIF, la réussite dépend de la sécurité, de l'exactitude, de la fiabilité et de la disponibilité des données ou de l'information que les technologies mettent à la disposition de la direction et des employés au besoin. La gouvernance GI-TI est du ressort de la haute direction et fait partie intégrante de la gouvernance d'entreprise. Elle comprend les structures de direction et d'organisation ainsi que les processus permettant à la haute direction de veiller à ce que la Division de la GI-TI réalise, maintienne et améliore la stratégie, les objectifs de même que l'efficience et l'efficacité des services opérationnels du BSIF.

Il importe d'assurer une bonne gouvernance et une bonne gérance de la fonction GI-TI afin que les investissements dans ce secteur créent de la valeur, et que ces deux qualités permettent d'identifier, de bien comprendre et d'atténuer les risques liés à la GI-TI.

Aperçu de la gouvernance GI-TI au BSIF

La Division de la GI-TI appuie la mission du BSIF en exploitant et en tenant à jour une infrastructure à l'appui des activités de celui-ci, en réduisant les interruptions au minimum et en facilitant le stockage de l'information électronique. Elle a aussi pour fonction d'établir et de tenir à jour un environnement réseau qui soit opérationnellement sûr pour protéger l'information électronique, conformément à la *Politique sur la sécurité du gouvernement* du Secrétariat du Conseil du Trésor (*SCT*) et aux normes s'y rapportant.

Suite à la page suivante

1. Contexte, suite

Aperçu de la gouvernance GI-TI au BSIF (suite)

Le BSIF possède un certain nombre de vieux systèmes qui requièrent une maintenance accrue. Ces systèmes sont remplacés, regroupés, mis à niveau, entretenus ou isolés dans le cadre du Programme de renouvellement de la TI (RTI).

Le programme de RTI, qui consiste en une transformation technologique sur cinq ans, a pour but de renouveler les capacités opérationnelles du BSIF. La stratégie de GI-TI a été approuvée par la haute direction en juin 2009 et a été suivie peu après par un réaménagement des plans de travail et un remaniement organisationnel afin que la Division de la GI-TI soit en mesure de mener à bien le projet de renouvellement. De nouvelles règles de gouvernance la GI-TI ont également été étables pour gérer le changement et prendre les décisions requises tout long du programme RTI. Celui-ci a débuté en 2010-2011 et constitue l'une des plus grandes dépenses annuelles du BSIF.

Objectifs de la Division de la GI-TI et priorités stratégiques du BSIF

La Division de la GI-TI a pour objectifs :

- d'exploiter et d'entretenir l'infrastructure et les services de TI à l'appui des activités du BSIF, de réduire les interruptions au minimum et de faciliter le stockage et la consultation économiques des fonds de renseignements du BSIF;
- d'assurer et d'appuyer l'évolution des systèmes d'information du BSIF pour suivre l'évolution des besoins et demeurer au fait des changements technologiques;
- de mettre en place et d'entretenir un environnement réseau sécuritaire afin de protéger les fonds de renseignements du BSIF conformément aux politiques de l'administration fédérale et en fonction de la nature délicate des renseignements;
- d'entretenir et de tenir à jour des systèmes d'information et des cadres d'exploitation de ces systèmes qui soient sûrs, souples et fiables, afin que les employés puissent créer, recueillir, stocker, protéger et communiquer efficacement l'information dont ils ont besoin pour s'acquitter de leurs obligations;
- de collaborer avec d'autres groupes ou secteurs du BSIF à la production de nouvelles applications ou à la modification ou la mise à nouveau des applications existantes, grandes ou petites, et ce, rapidement, efficacement et en conformité avec les politiques du SCT, le cas échéant.

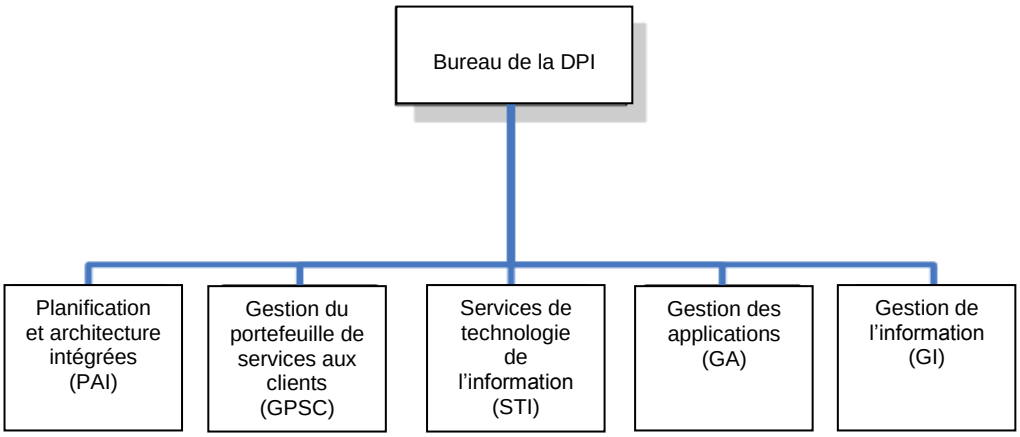
L'amélioration de l'infrastructure intégrée est au nombre des quatre objectifs prioritaires stratégiques ou points de mire du BSIF pour la période 2012-2015, ce qui lui permettra d'accomplir son mandat, d'atténuer ses risques et d'atteindre ses objectifs stratégiques. La Division de la GI-TI appuie la réalisation de cet objectif prioritaire stratégique en continuant à soutenir le programme de RTI afin d'atteindre les objectifs établis, alors que le BSIF se concentre sur le renouvellement des applications après avoir privilégié la mise en œuvre des outils et des services communs.

Suite à la page suivante

1. Contexte, suite

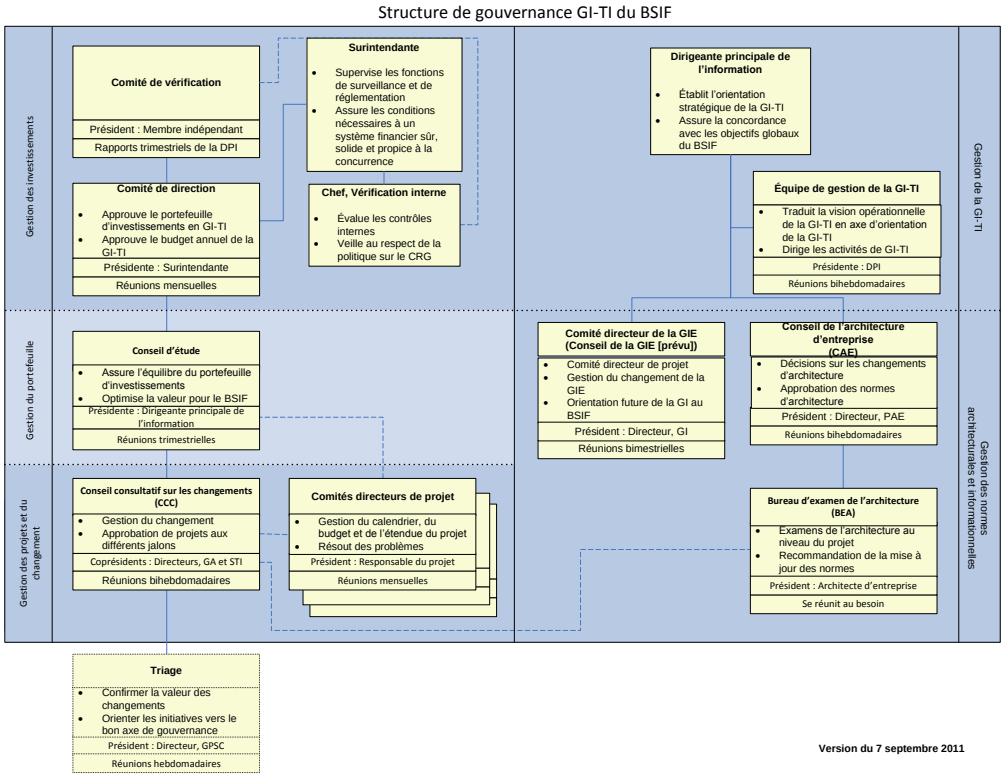
Organigramme de la fonction GI-TI

La Division de la GI-TI fait partie du Secteur des services intégrés, dont la direction est assurée par le surintendant auxiliaire. C'est la dirigeante principale de l'information (DPI) qui est responsable de la Division, laquelle est composée de près de 80 employés à temps plein et de consultants répartis entre les cinq groupes suivants :



Structure de gouvernance GI-TI

La structure de gouvernance GI-TI fait partie intégrante de la gouvernance d'entreprise et se présente comme il suit :



Source : Division de la GI-TI, exposé du 15 septembre 2011.

Suite à la page suivante

1. Contexte, suite

Aperçu du cadre stratégique

Le BSIF a mis en place un certain nombre de procédures et de politiques de GI-TI à l'appui de la gouvernance GI-TI générale, qui s'inspirent en grande partie des cadres, des directives et des politiques du SCT en la matière qui s'appliquent au BSIF. Se reporter à l'***annexe 1 : Liste de référence des politiques du SCT et des bonnes pratiques dans l'industrie***.

Le BSIF a aussi instauré diverses politiques et procédures en matière de sécurité en réponse aux exigences de l'administration fédérale, pour atténuer les risques connus et pour appliquer de bonnes pratiques. Le plan de sécurité ministérielle (PSM) qu'exige la *Directive sur la gestion de la sécurité ministérielle* du SCT sera le principal instrument d'identification des risques nouveaux ou supplémentaires et des mesures à prendre pour les atténuer, ce qui comprend d'autres politiques et procédures à l'appui du programme de RTI. Le premier jet du PSM est achevé mais n'a pas encore été soumis à l'examen et à l'approbation de la haute direction. Dans sa *Directive sur la gestion de la sécurité ministérielle*, le SCT avait exigé de l'ensemble des ministères la mise en place d'un PSM au plus tard le 30 juin 2012.

2. Objectif, délimitation et stratégie

Objectif de l'audit

L'audit avait pour but de fournir l'assurance raisonnable que le BSIF a mis en place une structure de gouvernance GI-TI et un contrôle de supervision adéquats, en déterminant si :

1. la structure organisationnelle de la fonction GI-TI est appropriée et les fonctions et attributions sont clairement définies, notamment en matière de sécurité, de décision et d'investissement;
2. le plan stratégique GI-TI s'inscrit dans les plans et les priorités stratégiques du BSIF;
3. le plan d'investissement en GI-TI permet d'appuyer la stratégie générale de l'entreprise;
4. la planification stratégique en matière de GI-TI s'effectue d'une façon structurée pouvant être gérée et mesurée;
5. les budgets et les dépenses de GI-TI font l'objet d'un suivi adéquat.

Suite à la page suivante

2. Objectif, délimitation et stratégie, suite

Délimitation de l'audit

L'audit couvrait la période du 1er avril 2011 au 31 mars 2012 et portait sur :

- la structure organisationnelle de la fonction GI-TI et les fonctions clés qui soutiennent la Division de la GI-TI dans l'exécution de sa mission et qui étaient en place pendant cette période;
- le plan stratégique GI-TI et le programme de RTI, et leur concordance avec les plans et les priorités stratégiques du BSIF;
- la supervision par la direction des mesures de rendement en matière de GI-TI, y compris les coûts.

Stratégie d'audit

L'audit a été réalisé selon les Normes internationales pour la pratique professionnelle de la vérification interne de l'Institut des vérificateurs internes, conformément à la *Politique sur la vérification interne* du Conseil du Trésor.

Il a été fondé en grande partie sur le document reconnu internationalement intitulé *Le management des risques de l'entreprise – Cadre de référence*, produit par le Committee of Sponsoring Organizations of the Treadway Commission (COSO), et il est inspiré d'une partie des objectifs de contrôle COBIT 4.1 de l'APVCSI qui sont liés aux bonnes pratiques de la troisième version de la Bibliothèque d'infrastructure des technologies de l'information.

La Vérification interne a aussi tiré parti :

- des cadres, directives et politiques du SCT en la matière qui s'appliquent au BSIF;
- d'autres normes de gouvernance GI-TI observées dans le secteur ou d'autres pratiques exemplaires ou cadres de contrôle, selon le cas.

Se reporter à l'***annexe 1 : Liste de référence des politiques du SCT et des bonnes pratiques dans l'industrie***.

La méthode d'audit comportait :

- un examen de la documentation pertinente, telle que les politiques et procédures applicables du BSIF et du SCT, et des organigrammes, des fonctions et attributions, des ordres du jour et procès-verbaux de réunions, des plans d'investissement, et des plans et priorités stratégiques;
- l'observation directe de plusieurs réunions importantes du comité de gouvernance GI-TI;
- des tests de cheminement des principaux processus à l'appui de la GI-TI;
- des entretiens avec le personnel clé et des parties prenantes.

Suite à la page suivante

3. Conclusion

Conclusion

La direction a mis en place une structure de gouvernance et des processus adéquats en matière de GI-TI qui sont comparables aux bonnes pratiques de ministères et organismes fédéraux similaires.

La Division de la GI-TI a établi de solides assises pour la gouvernance GI-TI en prévoyant un apprentissage continu et des capacités d'intervention. Au fur et à mesure que la gouvernance GI-TI au BSIF gagnera en maturité, elle sera mieux en mesure de tirer parti de ces solides assises pour améliorer l'analyse des besoins du BSIF en matière de protection des renseignements personnels et de sécurité de l'information à l'égard de ses applications et de ses données.

D'après mon jugement professionnel de dirigeant principal de la vérification, les procédures d'audit appliquées et les éléments probants recueillis sont suffisants et adéquats pour confirmer l'exactitude de l'opinion formulée dans le présent rapport. Pour formuler cette opinion, nous avons établi une comparaison entre la situation, telle qu'elle était au moment de l'audit, et les critères d'audit définis au préalable et approuvés par la direction. L'opinion ne vise que l'entité à l'étude. Les éléments probants ont été recueillis conformément à la politique, aux directives et aux normes d'audit interne du Conseil du Trésor, et les procédures utilisées sont conformes aux normes professionnelles de l'Institut des vérificateurs internes. Les éléments probants recueillis sont suffisants pour démontrer, à l'intention des cadres supérieurs, le bien-fondé de l'opinion découlant de l'audit interne.

Nous tenons à souligner l'excellente collaboration et l'échange de points de vue avec tous ceux ayant participé à l'audit. Nous n'aurions pu effectuer un examen aussi approfondi et nous concentrer sur les élément d'importance sans le soutien dont nous avons bénéficié tout au long de l'audit.

_____ _____

Dirigeant principal de la vérification, VI Date

4. Observations et recommandations

La fonction GI-TI possède une structure organisation-nelle adéquate

a. Il existe un cadre de gouvernance GI-TI en matière de décision, de direction et de responsabilisation, qui correspond aux bonnes pratiques observées dans certains ministères et organismes fédéraux de taille similaire.

b. Des comités de gouvernance stratégiques et tactiques en matière de GI-TI sont investis d'une mission efficace ainsi que d'un mandat et de fonctions et attributions clairement définis. Leur structure hiérarchique est bien définie et leur composition adéquate.

c. La structure organisationnelle de la fonction GI-TI est adéquate compte tenu de la taille et de la nature du BSIF, et elle prévoit des rôles et des responsabilités bien définis des fonctions de GI-TI, des pouvoirs et une structure hiérarchique.

d. Les cadres supérieurs du BSIF, la Division de la GI-TI et les Services de sécurité et de l'administration sont adéquatement représentés aux principaux comités opérationnels GI-TI.

e. La dirigeante principale de l'information (DPI) fait rapport périodiquement à la haute direction et au Comité de vérification.

f. La DPI bénéficie de l'appui de la haute direction et dispose donc des pouvoirs et des ressources pour mettre à exécution le plan stratégique GI-TI.

Le plan stratégique GI-TI est aligné sur le plan stratégique général du BSIF

a. Le plan stratégique GI-TI s'inscrit dans l'orientation stratégique du BSIF et tient compte des principaux besoins opérationnels et des priorités stratégiques.

b. Les services opérationnels guident et aident la Division de la GI-TI dans ses décisions d'investissement, laquelle en tient compte dans son plan stratégique.

Le plan d'investis-sement en GI-TI appuie la stratégie du BSIF

a. Le plan d'investissement en GI-TI appuie la stratégie du BSIF et correspond aux bonnes pratiques observées dans certains ministères et organismes fédéraux de plus grande taille.

b. Les objectifs des activités de planification stratégique et de planification des investissements en matière de GI-TI sont bien définis, ils sont alignés sur les plans et priorités stratégiques du BSIF et les appuient, ils sont priorisés et ils sont communiqués aux parties concernées.

La planification stratégique en matière de GI-TI s'effectue de façon structurée

a. Le BSIF a mis en place un processus de planification stratégique bien défini en matière de GI-TI qui prévoit des points de décision et de contrôle adéquats.

b. Les politiques, pratiques et procédures liées aux processus de planification stratégique et de planification des investissements sont communiquées aux parties concernées.

c. Les objectifs des activités de planification stratégique et de planification des investissements sont communiqués aux parties concernées.

Suite à la page suivante

4. Observations et recommandations, suite

Les investissements en GI-TI font l'objet d'un suivi

a. Le BSIF a mis en place un processus de gouvernance efficace pour préparer, évaluer et contrôler les analyses de rentabilité, de façon à pouvoir bien analyser les projets d'investissement technologique en fonction d'un compromis entre les risques, les coûts et les avantages.

b. La gestion du programme de RTI correspond aux bonnes pratiques observées dans certains ministères et organismes fédéraux de taille similaire.

c. Les pratiques de communication de l'information à la direction sont adéquates et permettent de suivre l'évolution des activités par rapport aux plans.

d. La direction exerce une supervision sur l'exécution du plan stratégique GI-TI.

Observation n° 1 :

Possibilité d'améliorer la stratégie GI-TI et la méthode de gestion du risque

Tandis que le programme de RTI est en bonne voie, la Division de la GI-TI peut améliorer davantage sa stratégie et sa méthode de gestion du risque en élaborant et en instaurant, en collaboration avec l'agent de sécurité ministériel, un plan économique prévoyant une analyse périodique des risques liés aux applications et aux données du BSIF, afin de s'assurer que celles-ci répondent toujours aux exigences en matière de sécurité et de protection des renseignements personnels.

Le BSIF a réalisé en 2007 sa dernière mesure des risques et des menaces liés à ses applications. Or, le programme de RTI est en train de modifier certains des éléments communs de l'infrastructure informatique globale du BSIF. Bien que le BSIF effectue une certaine forme d'analyse des risques lorsqu'un projet de modification passe par les diverses étapes du développement de l'application avant son déploiement dans l'environnement de production (en passant par le processus d'examen et d'approbation du comité de triage et du Conseil consultatif sur les changements) :

- il n'existe aucune obligation de procéder à une analyse des risques liés à la protection des renseignements personnels ou à la sécurité de la GI-TI;
- il ne semble exister aucune méthode systématique et économique pour procéder à une analyse périodique des risques liés aux applications et aux données, afin de s'assurer que celles-ci répondent toujours aux exigences en matière de sécurité et de protection des renseignements personnels.

Recommandation n° 1

Afin de se conformer aux bonnes pratiques de certains des ministères et organismes fédéraux ainsi qu'aux instructions des politiques et des normes applicables du SCT, le BSIF devrait élaborer et mettre en application une méthode d'analyse des risques liés aux applications et aux données pour confirmer que celles-ci répondent toujours aux exigences en matière de sécurité et de protection des renseignements personnels.

Suite à la page suivante

4. Observations et recommandations, suite

Recommandation n° 1 (suite)

Pour réaliser des gains d'efficience, le BSIF n'aurait qu'à inscrire ces exigences dans un répertoire central, puis tirer parti de cette information pour effectuer une analyse des risques à l'égard des éléments communs de l'infrastructure informatique. Le cas échéant, les risques résiduels liés aux applications et aux données seraient ensuite évalués par le Conseil consultatif sur les changements, conjointement avec les responsables des services opérationnels.

Cette approche devrait comporter un examen et une révision de la politique de gestion du changement, afin que les listes de contrôle du Conseil consultatif sur les changements et des divers comités de soutien soient modifiées comme il se doit et qu'elles exigent que les risques liés à la protection des renseignements personnels ou à la sécurité de la GI-TI soient évalués et fassent l'objet d'un accord formalisé avec les services opérationnels, avant de passer à l'étape de la production.

5. Réponse de la direction et plan d'action

Aperçu

Le présent rapport a été revu par la DPI et le surintendant auxiliaire, Services intégrés, qui ont pris bonne note de l'observation et de la recommandation.

La Division de la GI-TI se référera à cette recommandation de la Vérification interne pour améliorer sa gouvernance.

Réponse et commentaires de la direction

La direction accepte la recommandation découlant de l'audit. Les commentaires qui suivent sont pertinents au vu de la recommandation et de la capacité de la fonction GI-TI à s'y conformer.

En 2009, en réponse à l'analyse des risques et des menaces effectuée en 2007, le BSIF a procédé à un exercice de classification de sécurité et a donc acquis une bonne connaissance de son fonds documentaire. Près de 90 % de cette information est classée confidentielle, ce qui, pour le gouvernement du Canada, correspond à la cote « Protégé B » selon la *Politique sur la sécurité du gouvernement* du SCT. Le BSIF détient aussi des renseignements personnels qui sont classés « Protégé A » ou « Protégé B ». Avant leur collecte, ces renseignements doivent être spécifiquement définis par une évaluation des facteurs relatifs à la vie privée, puis protégés et conservés dans une ou plusieurs banques de données personnelles, une fois obtenus. Vu qu'il n'existe pratiquement pas d'information « Protégé C » dans le fonds documentaire, le BSIF possède des données qui sont relativement homogènes et bien comprises du point de vue de la sécurité et de la protection des renseignements personnels.

En 2011-2012, dans le cadre du programme de gestion du cycle de vie de la fonction de GI-TI, plusieurs composants du réseau de données « en fin de vie » ont été remplacés, en même temps que la refonte de la structure du réseau, afin de suivre les

Suite à la page suivante

5. Réponse de la direction et plan d'action, suite

Réponse et commentaires de la direction (suite)

bonnes pratiques du gouvernement du Canada telles que la norme sur la gestion de la sécurité des technologies de l'information (GSTI). Le réseau du BSIF est donc sûr et entièrement prêt pour la mise en application de la recommandation découlant de l'audit.

Les détails de la mise en application sont explicités ci-après.

Plan d'action de la direction

En réponse à la recommandation, la Division de la GI-TI, en collaboration avec les Services de sécurité et de l'administration, apportera des modifications aux politiques et aux procédures en vigueur et au système concerné (GSI), afin de pouvoir créer et tenir à jour un inventaire des applications et des données, y compris les risques s'y rapportant liés à la sécurité de l'information et à la protection des renseignements personnels. Les responsables des services opérationnels seront mis au courant et informés des questions les concernant, et des rapports seront déposés dans le GSI pour rendre compte des progrès accomplis. Ces mesures seront achevées vers la fin de 2013-2014.

Annexe 1 : Liste de référence des politiques du SCT et des bonnes pratiques du secteur

Liste de référence des politiques du SCT

Voici la liste des cadres, directives, politiques et normes du SCT qui s'appliquent à la gouvernance GI-TI au BSIF :

- *Cadre de responsabilisation de gestion* (CRG)
- *Cadre stratégique pour l'information et la technologie*
- *Politique sur la gestion de l'information*
- *Politique sur la gestion des technologies de l'information*
- *Directive sur la gestion des technologies de l'information*
- *Politique de planification des investissements – Actifs et services acquis*
- *Politique sur la sécurité du gouvernement*
- *Directive sur la gestion de la sécurité ministérielle*
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)*

Liste de référence des bonnes pratiques du secteur

Voici maintenant la liste des normes, bonnes pratiques et dispositifs de contrôle observés dans le secteur :

Appellation	Catégorie	Adresse URL
Val IT, APVCSI	Référentiel de gouvernance de la TI	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx
COBIT, APVCSI	Cadre de contrôle GI-TI	http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx
Bibliothèque d'infrastructure des technologies de l'information (BITI)	Bonnes pratiques	http://www.itil-officialsite.com/
Référentiel des connaissances en gestion de projet (PMBoK)	Normes de gestion de projet	http://www.pmi.org/PMBOK-Guide-and-Standards.aspx
Le cadre amélioré de la gestion	Bonne pratique du SCT	http://www.tbs-sct.gc.ca/emf-cag/index-fra.asp