National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Revu par le CS Ex conformément à la *Loi sur l'accès à l'information* (LAI). Renseignements NON CLASSIFIÉS.

Suivi de la vérification de la sécurité de la technologie de l'information : Certification et accréditation

Juillet 2009

7050-33-6 (CS Ex)



Canada

Mise en garde

Le résultat de ce travail ne constitue pas une vérification du processus de certification et d'accréditation de la TI. En fait, le rapport dresse un bilan des progrès accomplis à l'égard du plan d'action de la direction figurant dans la Vérification de la sécurité de la TI : Certification et accréditation de septembre 2007.

Revu par le CS Ex conformément à la *Loi sur l'accès à l'information* (LAI). Renseignements NON CLASSIFIÉS.

Table des matières

Acronymes et abréviations

AF	Année financière
AS	Adjoint spécial
C&A	Certification et accréditation
CEM(GI)	Chef d'état-major (Gestion de l'information)
CS Ex	Chef – Service d'examen
Dir Sécur GI	Directeur – Sécurité (Gestion de l'information)
FC	Forces canadiennes
Gp GI	Groupe de gestion de l'information
MDN	Ministère de la Défense nationale
N1	Niveau 1
PAD	Plan d'action de la direction
PGS	Politique du gouvernement sur la sécurité
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
TI	Technologie de l'information
VCEMD	Vice-chef d'état-major de la Défense

Introduction

Comme l'exige la Politique sur la vérification interne du Conseil du Trésor, le Chef – Service d'examen (CS Ex) a procédé à un suivi afin d'évaluer la mise en œuvre du plan d'action de la direction (PAD) fourni par le Vice-chef d'état-major de la Défense (VCEMD) et le Chef d'état-major (Gestion de l'information) (CEM(GI)) par suite de la *Vérification de la sécurité de la technologie de l'information (TI) : Certification et accréditation (C&A)* (septembre 2007).

La Politique du gouvernement sur la sécurité (PGS) exige que « les ministères aient des contrôles sécuritaires de base, surveillent continuellement leurs niveaux de prestation de services, identifient et analysent les menaces à leurs propres systèmes et établissent des mécanismes efficaces de réponse aux incidents et de continuité opérationnelle [1]. » Le processus de C&A est le principal mécanisme utilisé pour faire en sorte que des contrôles sécuritaires de base soient exercés et que des contrôles supplémentaires soient mis en oeuvre afin de protéger la confidentialité, l'intégrité et la disponibilité de l'information du ministère de la Défense nationale (MDN) et des Forces canadiennes (FC) contre les menaces internes et externes. Le Directeur – Sécurité (Gestion de l'information) (Dir Sécur GI) agit comme coordonnateur de la sécurité de la TI du MDN et des FC et est chargé de s'assurer que les systèmes de TI du MDN et des FC ont été convenablement certifiés et accrédités avant d'être mis en état de fonctionnement.

L'aptitude du Ministère à conserver la confiance du public et de la communauté internationale, à se conformer aux lois fédérales telles que la *Loi sur la protection de l'information* et la *Loi sur la protection des renseignements personnels* et à appuyer la réussite des opérations militaires et des initiatives gouvernementales comme le Projet des états financiers vérifiés dépend beaucoup de la confidentialité, de l'intégrité et de la disponibilité de nombreux systèmes d'information. Au sein du MDN et des FC, la sensibilité de l'information est très diversifiée – il peut s'agir de renseignements publics et commerciaux, de données personnelles, d'opérations militaires et de renseignement national et international – et sa confidentialité, son intégrité, sa disponibilité et sa valeur pour le Ministère doivent être préservées.

Méthodologie

Le présent suivi n'est pas une autre vérification des mêmes questions. Il consiste plutôt à examiner la documentation et les éléments de preuve afin d'évaluer les progrès de la mise en œuvre du PAD en date du 15 avril 2009. Les méthodes suivantes ont servi à déterminer les progrès du PAD :

- entrevues avec le Dir Sécur GI et son personnel;
- entrevues avec l'AS2/VCEMD;
- examen des documents de politique, des plans et des rapports touchant le processus de C&A.

[1] *Politique du gouvernement sur la sécurité*, section 10.12, février 2002.

Évaluation globale

Au moment du suivi, le Sous-ministre adjoint (Gestion de l'information) (SMA(GI)) était sur le point de publier son plan de revitalisation de la C&A visant à réduire l'arriéré de C&A ..... ……..... du processus actuel. En plus d'indiquer clairement les responsabilités de l'État-major interarmées stratégique, des autorités opérationnelles des systèmes de niveau 1 (N1), des responsables techniques et des entités du Groupe de gestion de l'information (Gp GI) en ce qui a trait au « processus de C&A », le document classe les priorités de C&A (réseaux, installations et applications) selon quatre niveaux allant du plus prioritaire au moins prioritaire, l'intention étant de traiter les éléments les plus prioritaires au cours des 12 à 18 prochains mois.

Bien que le plan de revitalisation de la C&A soit un bon pas en avant, les progrès .....
.....
.....
.....
.....
..... toutefois, on n'a pas réussi à embaucher un entrepreneur pour effectuer tel que prévu l'étude approfondie du processus de C&A. .....
.....
.....
.....

.....
.....
.....

Progrès de la mise en œuvre du PAD

Certification et accréditation

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

..... du processus de C&A afin d'en .....
..... à la PGS et aux normes et lignes directrices connexes, ...
.....

..... On a également recommandé que les politiques ministérielles soient mises à jour et que les ressources nécessaires soient déterminées, financées et obtenues afin de mettre en œuvre .... Les politiques mises à jour et les besoins en ressources additionnelles seraient fondés sur les résultats de cette analyse, et le travail connexe devait être terminé avant juin 2008. ....

L'étude approfondie du processus de C&A devait être confiée à un entrepreneur, mais l'offre du seul soumissionnaire a été jugée non conforme en janvier 2009. Le Dir Sécur GI examine actuellement d'autres solutions pour remplir cet engagement.

En décembre 2008, le Dir Sécur GI a affecté une ressource à temps plein afin d'obtenir une vue d'ensemble des processus internes et des rapports mutuels avec d'autres organisations du Gp GI. .... Les résultats de ces évaluations doivent être coordonnés avec le personnel de C&A et intégrés dans l'étude de la C&A. Parallèlement, les responsables du Projet d'environnement de sécurité de l'information d'entreprise explorent des options à plus long terme en ce qui a trait à une méthode de C&A automatisée, en commençant par l'élaboration d'une architecture de sécurité approuvée pour ensuite mettre en place un logiciel capable de repérer et de signaler les configurations non approuvées. Cette solution à plus long terme est envisagée dans le but d'améliorer considérablement le traitement et la productivité. ....

À l'heure actuelle, l'attention est portée sur l'accréditation de tous les systèmes d'information du MDN et des FC qui figurent sur la liste des systèmes aux fins de C&A du Dir Sécur GI .... L'exactitude de l'état de la C&A a été vérifiée à l'égard de tous les systèmes d'information du domaine désigné qui se trouvent sur la liste du Dir Sécur GI, ...

....

.....
.....
.....
.....
.....
.....

D'autres progrès ont eu lieu à l'égard des recommandations liées aux ressources. Le Dir Sécur GI a doté la plupart des postes de l'effectif actuel, et 17 postes supplémentaires ont été approuvés par le biais du processus de planification des activités et de l'initiative de revitalisation de la C&A .....
.....
.....
.....
.....
..... Cette augmentation financerait les salaires additionnels et un contrat pour l'embauche de neuf agents de la sécurité des systèmes d'information qui aideraient les autorités opérationnelles à rédiger les documents de C&A requis. Toutefois, comme le plan d'activités de l'AF 2009-2010 n'a pas encore reçu l'approbation finale, l'état de la demande de financement est inconnu.

Risque résiduel

Un système d'information est accrédité dès que l'autorité opérationnelle accepte le risque résiduel. .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
..... Le VCEMD était d'accord et prévoyait que les mesures initiales visant à quantifier et à formuler des recommandations pour la haute direction sur la gestion du risque résiduel lié à la C&A de la TI seraient prises d'ici la fin de mars 2008; le personnel du Gp GI devait apporter son aide au besoin.

Bien que la politique actuelle du MDN et des FC sur la gestion des risques mentionne l'établissement de niveaux de tolérance à l'égard du risque, et que les efforts se poursuivent afin d'intégrer les pratiques de gestion des risques dans le processus de planification et de gestion de la Défense, ... Des représentants du Grand prévôt adjoint (Sécurité), du Dir Sécur GI, de l'État-major interarmées stratégique (Plans) et du Directeur – Gestion de l'information (Renseignement) ont en effet élaboré une proposition et une matrice de gestion des risques qui répondaient à la majeure partie de la recommandation du rapport, ... Le groupe du VCEMD s'affaire à déterminer la meilleure façon de répondre à cette recommandation, mais il l'envisagera du point de vue de l'acceptation des risques en général plutôt que simplement comme un besoin en matière de TI.