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.

Vérification du nettoyage et de la destruction des biens de gestion de l'information (GI) et de technologie de l'information (TI)

Décembre 2012

7053-77 (CS Ex)

Canada

Table des matières

Acronymes et abréviations

ASM	Agent de sécurité du Ministère
BFC	Base des Forces canadiennes
BPR	Bureau de première responsabilité
CCA	Comptes clients d'approvisionnement
CD	Disque compact
CF 779	Certificat de destruction
CS Ex	Chef – Service d'examen
CSTC	Centre de la sécurité des télécommunications Canada
Dir Sécur GI	Directeur – Sécurité de la gestion de l'information
DISSSP	Directeur – Initiatives stratégiques et Services de soutien partagés
DVD	Disque numérique polyvalent
FC	Forces canadiennes
GI	Gestion de l'information
GRC	Gendarmerie royale du Canada
ISDN	Instruction de sécurité de la Défense nationale
MDN	Ministère de la Défense nationale
NSOSI	Normes de sécurité opérationnelle pour les systèmes d'information
OSSI	Officier de la sécurité des systèmes d'information
PGS	Politique du gouvernement sur la sécurité
QGDN	Quartier général de la Défense nationale
RCN	Région de la capitale nationale
RED	Réseau étendu de la Défense
SMA(GI)	Sous-ministre adjoint (Gestion de l'information)
TI	Technologie de l'information
USB	Bus série universel
VCEMD	Vice-chef d'état-major de la Défense

Sommaire des résultats

Les documents classifiés et désignés (définis comme le matériel de gestion de l'information (GI)) et les dispositifs électroniques (définis comme le matériel de technologie de l'information (GI)) sont utilisés de façon régulière au ministère de la Défense nationale (MDN). Selon la politique du gouvernement, lorsque ce matériel et ces dispositifs ne sont plus requis, les ministères doivent mettre en œuvre des processus de nettoyage et de destruction des biens de GI/TI pour prévenir l'accès non autorisé à tout renseignement sensible.

Le Chef – Service d'examen (CS Ex) a mené une vérification du nettoyage et de la destruction des biens de GI/TI afin d'évaluer les processus de gouvernance et de contrôle des activités ministérielles de nettoyage et de destruction des biens, ainsi que la gestion des risques connexes.

Évaluation globale

Un examen des pratiques panministérielles de gestion des biens de GI/TI classifiés et désignés, y compris les processus de nettoyage et de destruction, doit être mené pour vérifier ce qui suit :

- des politiques et des programmes de formation à jour sont en place;
- [redacted]
- [redacted]

Constatations et recommandations

Les processus actuels de gouvernance et de gestion des risques liés aux activités de nettoyage et de destruction des biens de GI/TI [redacted] Voici certains des problèmes décelés à cet égard :

- **Gouvernance.** Les politiques et les documents d'orientation sur le nettoyage et la destruction des biens de GI/TI sont de nature générale et relèvent de nombreuses organisations gouvernementales[1]. De plus, bon nombre de références dans les politiques ne sont plus à jour, et les changements n'ont pas toujours été communiqués efficacement. [redacted]

[1] La Politique du gouvernement sur la sécurité (PGS), entrée en vigueur le 1er avril 2012, confère des responsabilités aux organismes gouvernementaux responsables de la sécurité, comme le Secrétariat du Conseil du Trésor (établir une orientation pangouvernementale), le Centre de la sécurité des télécommunications Canada (CSTC) (protéger les renseignements électroniques) et la Gendarmerie royale du Canada (GRC) (assurer la protection matérielle des biens, des installations et du personnel, et fournir des conseils à cet égard).

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

- **Mécanismes de contrôle interne.** Les processus actuellement utilisés pour gérer les biens [redacted]
- **Gestion des risques.** Bien que les activités de nettoyage et de destruction soient partiellement examinées dans le cadre d’autres procédures ministérielles liées à la TI et à la sécurité, [redacted] par aucune des organisations au sein desquelles des entrevues ont été menées pendant la vérification.

Pour faire en sorte que les problèmes soulevés en ce qui a trait à la gouvernance et au contrôle des processus actuels de nettoyage et de destruction soient corrigés, on recommande que l’agent de sécurité du Ministère (ASM) effectue [redacted] activités de nettoyage et de destruction des biens de GI/TI en collaboration avec le Directeur – Sécurité de la gestion de l’information (Dir Sécur GI). Les résultats de [redacted] devraient ensuite être utilisés pour revoir la politique, les processus et la formation [redacted]

Remarque : Pour une liste plus détaillée des recommandations du CS Ex et la réponse de la direction, veuillez consulter l’annexe A – Plan d’action de la direction.

Introduction

La présente vérification était prévue dans le Plan de vérification axé sur les risques du CS Ex pour les années financières 2012-2013 à 2014-2015. La sécurité nationale est une priorité du gouvernement du Canada et du Ministère. Elle joue un rôle déterminant dans les opérations du MDN et des Forces canadiennes (FC) et elle est considérée comme un facteur de risque ministériel important. Il est donc essentiel de protéger et de détruire les biens de GI/TI de façon appropriée pour garantir la confidentialité et la sécurité des renseignements sensibles. Les biens de GI comprennent les copies papier de dossiers personnels, les rapports classifiés et désignés et les disques compacts (CD) et les disques numériques polyvalents (DVD). Les biens de TI comprennent les disques durs, les clés USB et d'autres dispositifs électroniques.

Les biens de GI/TI doivent être adéquatement nettoyés ou détruits à la fin de leur vie utile pour prévenir la récupération, la reproduction et l'utilisation d'information classifiée ou désignée par des tiers non autorisés. Des moyens technologiques permettent de récupérer l'information contenue dans des dispositifs de stockage électronique si ceux-ci n'ont pas été correctement nettoyés ou détruits. Des logiciels, allant de programmes sophistiqués à de simples gratuiciels, peuvent être utilisés pour récupérer des données qui n'ont pas été épurées ou détruites correctement. Il existe également des logiciels de reconnaissance numérique capables de reconstituer le matériel de GI qui n'a pas été déchiqueté assez finement. [redacted][2].

Contexte

Exigences de la politique. La PGS stipule que la sécurité consiste en l'assurance que l'information, les biens et les services ne sont pas compromis et exige une évaluation continue des risques. La sécurité requiert également la mise en place, la surveillance et le maintien de mécanismes appropriés de contrôle de gestion interne en matière de prévention (atténuation), de détection, d'intervention et de rétablissement. Les administrateurs généraux sont responsables de la mise en œuvre et de l'administration efficace de la gestion de la sécurité[3]. Le MDN a établi des consignes et des directives en matière de sécurité afin de respecter cette exigence[4].

[2] Pratiques relatives au retrait des renseignements personnels de certaines institutions fédérales – Rapport de vérification de la commissaire à la protection de la vie privée du Canada (2012).
[3] PGS (2012) – Article 3.6.
[4] Par exemple : chapitres 11 et 72 des Instructions de sécurité de la Défense nationale (ISDN); NSOSI; Ordonnances de sécurité des systèmes d'information de la région de la capitale nationale (RCN).

Tel qu'indiqué dans le document du Ministère intitulé « Règlement et instructions de sécurité relatifs aux systèmes classifiés », les biens de GI/TI comprennent le matériel informatique, les logiciels, les copies papier et électroniques, les dispositifs de stockage, les périphériques et les liens et les dispositifs de communication. Les Normes de sécurité opérationnelle pour les systèmes d'information (NSOSI) précisent que les rebuts classifiés ou désignés qui doivent être détruits doivent être brûlés, déchiquetés ou désintégrés. Les rebuts classifiés, y compris l'équipement qui ne peut être détruit adéquatement par ces méthodes, doivent être traités par tout moyen efficace pouvant garantir que nul ne pourra extraire l'information classifiée des résidus.

Structure organisationnelle. Au MDN, la gouvernance et la surveillance des politiques et des activités du Ministère en matière de sécurité ont été confiées à l'ASM. Le Sous-ministre adjoint (Gestion de l'information) (SMA(GI)), par l'entremise du Dir Sécur GI, est chargé de veiller à l'application des politiques et des normes ministérielles relatives à la sécurité des TI, y compris la politique et les directives sur le nettoyage et la destruction des biens de GI/TI. Il est également responsable de la gestion du cycle de vie des biens de GI/TI pour l'organisation. Selon la classification de sécurité de l'information, des organisations du SMA(GI) telles que la Direction – Services à l'utilisateur final (Gestion de l'information) et le 76e Groupe des communications, pourraient participer au processus de nettoyage et de destruction des biens de GI/TI. Un officier de la sécurité des systèmes d'information (OSSI) devrait être en poste dans chaque organisation ministérielle pour assurer la liaison avec ces groupes et leur fournir des conseils.

Le processus de nettoyage et de destruction matériels des biens de GI/TI ne dépend pas uniquement de la classification ou de la désignation de sécurité, mais également du lieu géographique. Dans la région de la capitale nationale (RCN), la plupart des activités de destruction des biens de GI/TI sont menées par le Directeur – Initiatives stratégiques et Services de soutien partagés (DISSSP) (de nombreuses organisations du MDN utilisent des déchiqueteuses approuvées par la GRC pour leurs propres besoins en GI). Au niveau des bases, les activités de nettoyage et de destruction des biens de GI/TI sont souvent menées sur place par le personnel affecté à l'approvisionnement, et des déchiqueteuses sont utilisées pour la destruction du matériel de GI.

Objectif

L'objectif de la vérification était d'évaluer les processus de gouvernance et de contrôle des activités de nettoyage et de destruction des biens de GI/TI, ainsi que la gestion des risques connexes.

Portée

La vérification a porté sur les biens de GI/TI protégés et classifiés, dans la RCN et les bases.

Méthodologie

Les résultats de la vérification sont fondés sur ce qui suit :

- des entrevues menées auprès d'intervenants en GI/TI occupant diverses fonctions dans la RCN, allant de l'approvisionnement, de la certification et de l'accréditation à la destruction et à l'archivage des biens de GI/TI, en passant par la manipulation des biens;
- des examens des lois, des politiques et directives, des instructions et des documents d'orientation;
- des visites sur place ou des entrevues téléphoniques menées auprès d'intervenants de trois grandes installations du MDN et des FC : la Base des Forces canadiennes (BFC) Petawawa, la 1re Division aérienne du Canada/BFC Winnipeg et la BFC Halifax.

Déclaration de conformité

Les constatations et les conclusions de la vérification formulées dans le présent rapport reposent sur des preuves de vérification suffisantes et appropriées qui ont été recueillies au moyen de procédures conformes aux Normes internationales pour la pratique professionnelle de la vérification interne de l'Institut des vérificateurs internes. La vérification est donc conforme aux Normes relatives à la vérification interne au sein du gouvernement du Canada, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité. Les opinions exprimées dans le présent rapport sont fondées sur les conditions qui existaient lors de la vérification et elles ne s'appliquent qu'à l'entité examinée.

Constatations et recommandations

[redacted]

- Gouvernance
  - Politiques désuètes [redacted]
  - [redacted]
- Contôles internes
  - [redacted]
  - [redacted]
- Gestion des risques
  - [redacted]

Gouvernance

Polique et programme. La politique actuelle relative au nettoyage et à la destruction des biens de GI/TI est énoncée dans la Politique de sécurité du ministère de la Défense nationale, l'ISDN, les NSOSI et d'autres directives ministérielles en matière de sécurité[5]. Ces documents, ainsi que les lignes directrices émises dans les bulletins sur la sécurité de la GRC et les Lignes directrices en matière de sécurité des technologies de l'information du CSTC, offrent aux OSSI et aux employés du Ministère des directives sur la façon de nettoyer et de détruire adéquatement les biens de GI/TI. [redacted]

- **Politique désuète.** La politique et les directives sur le nettoyage et la destruction des biens de GI/TI sont désuètes et ont perdu de leur pertinence. Certaines consignes de sécurité ministérielles ont plus de cinq ans, [redacted] Bon nombre des politiques de sécurité du Ministère remontent à 1998 et font encore référence à des technologies qui ne sont plus couramment utilisées depuis

[5] ISDN, chapitre 11 (Destruction de documents classifiés), ISDN, chapitre 72 (Supports d'enregistrement magnétique).

plus de dix ans (comme les disquettes de 5 po)[6]. [redacted]

- **Communication.** Les intervenants ne sont pas toujours informés en temps opportun des mises à jour ou des changements apportés aux politiques. Les mises à jour ou les changements apportés aux politiques pertinentes sur le nettoyage et la destruction des biens de GI/TI sont principalement communiqués par l’entremise de courriels ou du site Web sur la sécurité des TI. Les intervenants ont indiqué que les listes d’adresses courriel du personnel de sécurité clé, comme les OSSI et les surveillants de la sécurité des unités, ne sont pas toujours complètes. [redacted]
- **Références.** Les intervenants ont mentionné que les diverses références aux activités de nettoyage et de destruction des biens de GI/TI dans les politiques et les directives [redacted] Les utilisateurs ont indiqué qu’ils se sentaient dépassés par la quantité de documents et le nombre de sources qu’ils devaient consulter pour trouver de l’information pertinente. [redacted] C’est pourquoi beaucoup d’utilisateurs misent sur les communications informelles avec des personnes-ressources pour obtenir des conseils sur les procédures de destruction approuvées.
- **Orientation.** Les politiques et documents d’orientation sur la GI/TI ne se prêtent pas à la création d’un processus normalisé de nettoyage et de destruction des biens de GI/TI. Les intervenants ont indiqué que les documents actuels [redacted] Dans certains cas, les disques durs étaient détruits au moyen de diverses méthodes, [redacted]

[redacted] les employés ont indiqué qu’ils croyaient bien que leur processus de nettoyage et de destruction du matériel de GI/TI était adéquat. Les organisations ont établi leurs propres instructions permanentes d’opération en misant sur des approches sensées pour s’assurer qu’une fois le matériel de TI détruit, l’information contenue dans ce matériel ne puisse être récupérée. Tous les employés interrogés ont affirmé ne pas hésiter à consulter des personnes-ressources comme les officiers responsables des OSSI de la RCN lorsqu’ils avaient des questions.

[6] Le chapitre 72 des ISDN a été publié en mai 1999, les NSOSI, en mai 1998, et les Ordonnances de sécurité des systèmes d’information de la RCN, en 2005.

Formation et dotation en personnel

Formation. Les OSSI jouent un rôle essentiel dans le processus de nettoyage et de destruction des biens de GI/TI. Ils sont généralement les premières personnes que les employés consultent au sein de leur organisation lorsqu'ils ont des questions sur la façon de nettoyer ou de détruire adéquatement les biens de GI/TI. Il est donc important que ces personnes reçoivent le niveau de formation nécessaire pour s'acquitter de leurs tâches.

Il existe des programmes de formation de base pour les OSSI. Le Ministère tient régulièrement des séminaires à leur intention et a offert des cours de formation aux OSSI dans le passé[7]. De plus, des institutions privées offrent des cours de formation qui mènent à une accréditation professionnelle. Toutefois, les OSSI ont indiqué que le nettoyage et la destruction des biens de GI/TI ne représentaient qu'un faible pourcentage de leur travail et que, par conséquent, [redacted]

Les qualifications des OSSI interrogés au cours de la vérification variaient grandement. Certains OSSI étaient des militaires ou d'anciens militaires possédant de l'expérience dans le domaine des communications et des TI, et d'autres étaient des employés civils n'ayant reçu qu'une formation de base en administration. Les OSSI ont indiqué qu'ils misaient sur leurs réseaux de communication officiel et non officiel pour obtenir l'information requise. Les officiers responsables des OSSI de la RCN et les OSSI des bases qui ont été interrogés pendant la vérification se sont révélés bien formés et renseignés, et facilement accessibles pour les OSSI de la RCN.

Dotation en personnel. Les OSSI jouent un rôle important pour assurer le respect des exigences ministérielles en matière de sécurité. Les organisations qui traitaient régulièrement de questions de sécurité comptaient en leur sein des OSSI compétents et bien renseignés sur les exigences en matière de nettoyage et de destruction des biens de GI/TI.

[redacted]

[redacted]

[7] Le Dir Sécur GI tient actuellement un symposium annuel à l'intention des OSSI et travaille également à l'élaboration d'un cours d'OSSI.

Conclusion

Contrôles internes

Processus de destruction des rebuts de GI classifiés en vrac dans la RCN

Dans la RCN, le DISSSP offre un service de destruction des rebuts de GI classifiés en vrac. Les organisations du MDN dans la RCN peuvent remplir de grands sacs papier de matériel de GI classifié et demander que des employés du DISSSP les ramassent et les détruisent au centre industriel de destruction du matériel papier

[redacted][8]

Gestion des biens de TI

Pour avoir l'assurance que les biens sont adéquatement nettoyés et détruits, le Ministère doit d'abord tenir un inventaire exact des biens. Cet inventaire doit comprendre l'information requise pour identifier les biens de TI et déterminer leur emplacement et leur état. Pour garantir un processus de nettoyage et de destruction adéquat, les biens doivent être suivis correctement de l'approvisionnement jusqu'à la destruction.

Les organisations ministérielles assurent le suivi des biens au moyen des comptes clients d'approvisionnement (CCA). Plus précisément, les articles à porter aux CCA d'une organisation sont ceux dont le coût unitaire est égal ou supérieur à 1 000 $ ou ceux qui sont restreints ou attrayants[9]. Pour maintenir l'exactitude des listes d'inventaire, les articles doivent être comptés régulièrement. L'inventaire doit se faire normalement tous les quatre ans pour valider les stocks des CCA.

Biens non classifiés

Selon les vérifications menées précédemment par le CS Ex, les listes d'inventaire des biens de TI non classifiés sont inexactes et non fiables[10]. Par exemple, les gestionnaires des biens du SMA(GI) ont indiqué qu'au sein de la RCN, les inventaires organisationnels des CCA n'étaient exacts qu'à [redacted] De plus, selon les réponses données lors des entrevues, les inventaires des CCA [redacted][11].

Disques durs. Bien que les disques durs non classifiés puissent être utilisés pour traiter de l'information jusqu'au niveau Protégé B (si celle-ci est cryptée), [redacted] Dans le cadre du suivi des biens de TI, comme les ordinateurs non classifiés connectés au Réseau étendu de la Défense (RED), un numéro d'inventaire est attribué à la tour de l'ordinateur et ce bien est inscrit dans un CCA. [redacted]

[8] Il a été mentionné que les employés du DISSSP possèdent une cote de sécurité de niveau secret, au minimum.
[9] Selon le Manuel d'approvisionnement des FC (Section B – Politiques de catalogage), les articles attrayants sont ceux qu'il est facile de convertir à un usage personnel ou qui peuvent faire l'objet d'abus, p. ex. les boîtes à outils, le matériel électronique, les caméras, les assistants numériques, les ordinateurs, etc. Les articles restreints comprennent les munitions.
[10] Rapports du CS Ex : Vérification de la gestion des stocks : Excédents et élimination, août 2009; Vérification de la gestion des stocks : Inventaire, rajustements et radiations, octobre 2008.
[11] Selon le Manuel d'approvisionnement des FC de 2011, l'inventaire doit se faire lors des passations de commandement ou au minimum tous les quatre ans.

Le personnel note le numéro de série de chaque disque dur qu'il détruit,

Dispositifs de stockage amovibles. Les CD/DVD et les clés USB ont une très grande capacité de stockage.

Selon les directives du Ministère sur l'utilisation acceptable des clés USB, le gestionnaire des biens de GI/TI d'une organisation est responsable de la coordination de toutes les exigences liées aux clés USB. Il doit à tout le moins conserver un répertoire des clés remises et rendues. Les réponses données lors des entrevues ont permis de conclure

Délais de destruction

Aucune limite de temps n'a été relevée dans les documents de politique ministériels applicables en ce qui a trait à la destruction des biens de GI/TI. Bien que la majorité des intervenants interrogés aient indiqué qu'ils essayaient de mener les activités de destruction à intervalles réguliers, des cas ont été recensés où des disques durs étaient empilés pendant une période pouvant aller jusqu'à deux ans avant d'être détruits. Ces cas ont surtout été décelés dans des organisations et dont les besoins en matière de nettoyage et de destruction de biens de TI sont beaucoup moins importants.

Registres de destruction

De nombreuses politiques du MDN précisent que le certificat de destruction (CF 779) est le document requis pour fournir une confirmation écrite de la destruction de tout matériel sensible (sauf les documents Protégé A). Ces registres doivent être conservés dans un dossier pour une période minimale de trois ans et doivent être remplis par l'organisation qui a procédé à la destruction du matériel et par l'organisation qui possédait le matériel. Les intervenants interrogés [redacted]

[redacted] le centre de destruction du QGDN n'offre des certificats de destruction aux clients de la RCN [redacted]

En ce qui concerne la destruction des biens de GI, le chapitre 11 des ISDN du MDN stipule que les certificats de destruction devraient s'appliquer aux rebuts officiels et à tous les documents portant la mention TRÈS SECRET et SECRET. [redacted] Le déchiquetage est la façon la plus efficace de détruire ces documents et permet de garantir que les rebuts classifiés seront détruits rapidement, près de leur point d'origine et sans l'aide d'un intermédiaire. [redacted]

Conclusion

[redacted]

Évaluation des risques

Processus et lignes directrices

Les activités de nettoyage et de destruction des biens de GI/TI menées par les organisations interrogées consistaient en une simple application de la politique ministérielle, jugée trop générale et désuète, [redacted] Bien que ces politiques soient fondées sur des normes acceptées par l'industrie pour ce qui est de la destruction matérielle des biens de

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

GI/TI (p. ex. les normes de la GRC) ou des étapes à suivre pour envoyer le matériel à un centre de destruction centralisé (DISSSP), [redacted]

Les processus de nettoyage et de destruction des biens de GI/TI ne sont pas les mêmes dans les organisations de la RCN et dans celles situées ailleurs au pays. [redacted] Par exemple, une organisation de la RCN peut faire appel aux services [redacted] pour détruire ses disques durs et son matériel de GI classifié, une base située à l'extérieur de la RCN peut posséder son propre désintégrateur de disques durs et sa propre déchiqueteuse industrielle, et une troisième organisation peut demander à son équipe d'experts en explosifs de détruire ses disques durs au moyen d'explosifs. Toutes ces méthodes de destruction ont leurs avantages et leurs inconvénients, mais chacune d'elle respecte l'exigence selon laquelle le matériel doit être détruit de façon à prévenir la reproduction d'information classifiée ou désignée. [redacted] les employés de chaque organisation ont indiqué qu'ils croyaient bien que leur processus permettait de détruire le matériel de GI/TI d'une manière acceptable et complète.

Le nettoyage et la destruction des biens de GI/TI n'est qu'une des nombreuses responsabilités assumées par les OSSI. Les OSSI organisationnels interrogés durant la vérification ont indiqué [redacted]

Conclusion

[redacted]

Recommandation

1. [redacted] on recommande que l'ASM, en collaboration avec le Dir Sécur GI, prenne les mesures suivantes :

- [redacted]
- [redacted]

BPR : VCEMD

Conclusion générale

Les activités ministérielles de nettoyage et de destruction des biens de GI/TI ont évolué au fil du temps

Annexe A – Plan d'action de la direction

Évaluation des risques

Recommandation du CS Ex (Importance élevée)

1. [redacted]
- [redacted]
- [redacted]

Mesures de la direction

L'organisation du VCEMD, avec l'aide des praticiens de la sécurité de la GI/TI du Groupe GI, veillera à ce qui suit :

- Rédiger des bulletins provisoires et des clarifications de politique pour sensibiliser les employés du MDN et des FC [redacted]
- Dans le cadre de l'initiative de transformation de la sécurité menée par le Directeur général – Transformation de la sécurité, [redacted] politiques, aux processus et à la formation connexes dans le but suivant :
  - déceler les lacunes, les incohérences et les besoins de mises à jour de la politique du MDN et des FC, et en tenir compte dans la nouvelle version de la politique sur la sécurité;
  - dans le cadre de la restructuration de la sécurité, déterminer si des changements organisationnels sont requis;
  - dans le cadre de la restructuration de la sécurité, déterminer si des changements aux processus et l'attribution de rôles et de responsabilités connexes sont requis;
  - cerner tout besoin en matière de formation et de sensibilisation au sein du MDN et des FC;
  - repérer tout instrument de politique d'autres ministères responsables de la sécurité qui pourrait offrir une orientation ou des avis inadéquats ou problématiques.
- Rédiger d'autres bulletins provisoires et des clarifications de politique [redacted]
- Dans le cadre de l'initiative de transformation de la sécurité en cours, mener les activités suivantes :
  - mettre en œuvre tout changement ou ajout nécessaire à la Politique de sécurité du MDN et au Manuel de sécurité de la Défense;

- intégrer tout changement organisationnel requis [redacted]
- intégrer les besoins en matière de formation et de sensibilisation associés à la destruction appropriée des biens de GI/TI au Programme de sensibilisation et de formation en matière de sécurité du MDN et des FC;
- participer à des groupes de travail interministériels pour apporter des changements aux politiques et aux programmes du gouvernement du Canada en matière de sécurité.

Mesures provisoires

Le VCEMD prendra les mesures suivantes avant la date cible de septembre 2014 :

- Mise à jour de la politique sur l'élimination des rebuts classifiés : le Directeur – Sécurité de la Défense ira de l'avant avec la mise à jour de cette importante politique. Une ébauche sera produite d'ici le 30 juin 2013.
- Le Directeur – Sécurité de la Dérense publiera des bulletins sur la sécurité à compter d'avril 2013. Un lien sera établi avec les responsabilités confiées à l'ASM en ce qui a trait à la promotion de la sensibilisation aux questions de sécurité. Les bulletins s'adresseront aux officiers de la sécurité des unités et aux officiers de la sécurité des systèmes d'information en particulier, et aux employés du MDN en général. Les numéros mensuels comprendront ce qui suit :
  - Avril : Le Dir Sécur GI fera le point sur les questions liées aux Conseils en matière de sécurité des technologies de l'information 06.
  - Mai : Le Dir Sécur GI fera le point sur l'élimination des rebuts classifiés.
- [redacted]

BPR : VCEMD
Date cible : Septembre 2014

Annexe B – Critères de vérification

Objectif

Évaluer les processus de gouvernance et de contrôle des activités de nettoyage et de destruction des biens de GI/TI, ainsi que la gestion des risques connexes.

Critères

- Des politiques et une structure de gouvernance assorties d'objectifs, de rôles et de responsabilités clairs sont en place pour garantir le nettoyage et la destruction efficaces des biens de GI/TI.
- Les risques liés au nettoyage et à la destruction des biens de GI/TI ont été cernés, documentés et atténués.
- Des mécanismes de contrôle sont en place et ils fonctionnent comme prévu pour garantir que les biens de GI/TI sont nettoyés et détruits de façon sécuritaire, uniforme et appropriée.

Sources des critères

- ISDN, chapitre 72 – Instructions de manipulation sécuritaire des supports d'enregistrement magnétique
- ISDN, chapitre 11 – Destruction de documents classifiés et désignés
- Critères de vérification liés au Cadre de responsabilisation de gestion : outil à l'intention des vérificateurs internes (Secteur de la vérification interne – Bureau du contrôleur général).