Vérification de la sécurité des technologies de l'information

Mai 2001

Direction de la vérification et de l'évaluation

Environnement Canada Environment Canada

Canada

Étapes de l'autorisation du rapport

Étape de planification terminée	octobre 2000
Collecte de données terminée	décembre 2000
Rapport terminé	février 2001
Rapport approuvé par le Comité ministériel de vérification et d'évaluation (CMVE)	3 mai 2001

Abréviations utilisées dans le rapport

ASC	Alimentation sans coupure
CAC	Contrôle d'accès et cryptage
CAG	Cadre amélioré pour la gestion
CCTI	Comité consultatif des technologies de l'information
CMC	Centre météorologique canadien
CT	Conseil du Trésor
DGSI	Direction générale des systèmes et de l'informatique
EC	Environnement Canada
EMAF	Essentiel à la mission de l'administration fédérale
GED	Gouvernement en direct
GI	Gestion de l'information
GRC	Gendarmerie royale du Canada
PC	Ordinateur personnel
PRA	Plan de reprise des activités
SCT	Secrétariat du Conseil du Trésor
SMC	Service météorologique du Canada
STI	Sécurité des technologies de l'information

Remerciements

L'équipe de projet de la Direction de la revue, sous la direction d'Elizabeth Murphy-Walsh, était menée par V. Neimanis et comprenait Lucie Héon et Erin Campbell, sous contrat. Une partie des entrevues, ainsi que l'organisation et la facilitation du groupe de discussion ont été réalisées à contrat respectivement par Arnie Frances de Hallux et David Prime de PriceWaterhouseCoopers. L'équipe tient à remercier tous ceux qui ont contribué à la vérification et notamment :

- les employés du Ministère qui ont été interviewés et qui ont apporté une contribution cruciale à cet examen par leurs connaissances spécialisées, leurs points de vue, leurs commentaires et leurs documents;
- les employés qui ont fourni des commentaires détaillés sur la version préliminaire.

Table des matières

Résumé

Contexte

Le Secrétariat du Conseil du Trésor (SCT) exige de chaque ministère qu'il procède à une vérification périodique de la sécurité de ses technologies de l'information (STI) afin de mesurer sa conformité à la politique du SCT sur la sécurité. En outre, le Ministère de l'Environnement avait entrepris d'élaborer une stratégie de GI/TI et devait, ce faisant, évaluer le niveau de STI. Par conséquent, dans le *Plan d'examen de 2000-2001*, le Comité ministériel de la vérification et de l'évaluation a approuvé la réalisation d'une vérification de la STI, conformément à la Politique du SCT sur la sécurité, et en vue d'assurer à la haute direction que la STI soutenait fermement la réalisation des objectifs du Ministère.

Cet examen de la sécurité des technologies de l'information (TI) englobe un examen de l'organisation et de l'administration de la STI, de la sécurité du personnel, de la sécurité matérielle, de la sécurité du matériel informatique, de la sécurité des logiciels, de la sécurité des communications et de la sécurité de l'exploitation dans l'ensemble du Ministère. Le travail effectué dans le cadre de la Stratégie de GI/TI a été pris en compte et intégré aux aspects appropriés. La présente vérification expose donc le niveau de conformité du Ministère par rapport à la politique de STI du Conseil du Trésor, les pratiques exemplaires utilisées par le Ministère et ses points faibles, et formule des recommandations.

Observations

Les conclusions générales de la vérification sont les suivantes :

- EC a un système essentiel à la mission de l'administration fédérale (EMAF) de niveau A pour le Service météorologique du Canada (SMC) qui exige le maintien des activités 24 heures sur 24 et sept jours sur sept, ainsi qu'une solide gestion de la STI. EC satisfait aux exigences de sécurité d'un tel système, comme l'ont démontré l'exercice de préparation à l'An 2000, la tempête de verglas de 1998 et le virus «I luv you».

- Le SMC emmagasine des renseignements de grande valeur et s'occupe de la gestion d'un réseau auquel viennent se greffer les TI du Ministère. Il emploie d'excellentes pratiques et, dans certains cas, dépasse les normes du Conseil du Trésor. Cependant, ces pratiques exemplaires ne sont pas communiquées aux autres services du Ministère, ce qui entraîne des incohérences dans l'application des politiques et des marches à suivre.

- De nombreuses bonnes pratiques ou pratiques exemplaires ont été observées et, si leur emploi était généralisé au Ministère, la STI ne s'en porterait que mieux. Cependant, les marches à suivre pour la STI ne sont pas appliquées, ni surveillées de façon constante au Ministère; certains secteurs accusent des lacunes, tandis que d'autres dépassent les exigences de la politique. Le problème ici se situe au niveau du leadership en matière d'application et de surveillance systématiques des politiques et des marches à suivre, et leur normalisation dans un référentiel aisément accessible.

- En général, le Ministère atteint la plupart des objectifs définis dans le Guide de vérification – Sécurité des technologies de l'information du Conseil du Trésor (1995).

- La formation des utilisateurs et des techniciens, ainsi que l'accroissement de la sensibilisation des utilisateurs ont été définis comme les éléments primordiaux de l'amélioration de la gestion de la STI.

- Le personnel du Ministère qui participe à l'élaboration des documents secrets ou de nature délicate n'a pas les outils protégés nécessaires pour assurer une consultation rapide et appropriée à la grandeur du Ministère, tout en respectant les échéances fixées par la haute direction.

- Les initiatives pangouvernementales, comme Gouvernement en direct, accéléreront l'utilisation des technologies de l'information et pourraient accentuer les faiblesses actuelles de l'application de la STI.

Recommandations

Les conclusions générales et l'analyse ont amené les vérificateurs à présenter les recommandations suivantes dans les catégories de la gestion, des communications et de la formation, ainsi que des outils.

Gestion

1. **Il est recommandé que le SMA, Services ministériels, en collaboration avec le SMA, SMC, examine le rôle du CCTI. Cet examen devrait comprendre: un mandat révisé pour le Comité et ses sous-comités, une modification de la relation de dépendance du Comité, et un examen de la composition et des rôles du Comité en vue de s'assurer que tous les intervenants sont correctement représentés.**

2. **Il est recommandé que le DG, SI, entreprenne de renforcer le cadre de gestion de la STI au Ministère, ce qui comprendrait: une meilleure définition des rôles et des fonctions en matière de STI, une amélioration de la coordination et de la cohérence de l'application des politiques et des marches à suivre, une meilleure planification de la STI et des comptes rendus.**

Communication et formation

3. **Il est recommandé que le DG, SI, en collaboration avec le Directeur de l'informatique au SMC, le DG, RH, et le Bureau de la sécurité du Ministère (BSM), élabore une stratégie de sensibilisation/communication/promotion de la STI.**

Outils

4. **Il est recommandé que le DG, SI, en collaboration avec les membres du CCTI, examine les possibilités de mettre en application des logiciels appropriés pour surveiller les registres de STI au niveau ministériel.**

5. **Il est recommandé que le DG, SI, en collaboration avec le Directeur de l'informatique du SMC et le Bureau de sécurité du Ministère, détermine et distribue de meilleurs outils électroniques pour faciliter les communications protégées.**

Réponse de la direction

Recommandation #1 : D'accord
La DGSI travaille actuellement avec les représentants des Services et des régions à l'évaluation dur rôle de tous les groupes qui relèvent du Comité d'intégration du gouvernement en direct (CIGD). Le rôle du Comité consultatif des technologies de l'information (CCTI)SID sera évalué dans le cadre des travaux du CIGD) On reconnaît l'importance de la participation de tous les intéressés au domaine de la STI à cet exercice; les intérêts des programmes et des tables de concertation seront également pris en compte. Le résultat de ce nouvel alignement des rôles et des rapports hiérarchiques devrait, nous l'espérons, apporter des solutions aux enjeux soulevés dans la vérification.

Échéancier : Juin 2001

Mesures proposées : Le CIGD examinera en détail le rôle des sous-comités qui relèvent du la DGSI.

Recommandation #2 : D'accord
Dans le cadre du processus de développement de la Stratégie de la gestion de l'information et des technologies de l'information, la DGSI a examiné les rôles et responsabilités reliés au cadre de gestion de la STI. Nous reconnaissons qu'il y a plusieurs carences relatives aux activités fonctionnelles et opérationnelles dans ce domaine. Nous avons demandé et nous recevrons des fonds dans le cadre de l'Intégrité de programmes qui nous permettront d'aborder ces carences.

Échéancier : Mars 2002

Mesures proposées : Nous prendrons les mesures pour clarifier les rôles, améliorer l'application des politiques en la rendant plus cohérente, améliorer la planification et les rapports de la STI. Les mesures précises comprendront: 1) le renforcement de l'équipe de la STI en créant plus de postes afin d'appuyer le programme dans la RCN; 2) le développement et la mise à jour des guides et politiques ministériels en tant que coordonnateur national de la STI; 3)l'acquisition d'outils pour améliorer les opérations. Le Directeur général de la DGSI sera responsable de ces mesures.

Recommandation #3 : D'accord
Nous appuyons entièrement une campagne de sensibilisation à la STI. Jusqu'à maintenant nous avons pris des mesures limitées (bulletins réguliers au personnel, message spéciaux lorsque des menaces précises ont été identifiées, etc.). Le CCTI nous a demandé de faire davantage. Dans les mois à venir nous publierons des produits plus importants.

Échéancier : Mars 2002

Mesures proposées : Nous prendrons des mesures pour accroître l'impact de l'information qui est diffusée au personnel. Du matériel de formation à l'intention du personnel sera également développé au besoin. Les coordonnateurs nationaux et régionaux de la STI préparent actuellement un plan de communication afin d'informer les usagers du rôle de la STI et de la nécessité de mettre en place certaines mesures de sécurité pour le réseau. Afin

de rendre le plan plus cohérent, les activités de la RCN et des régions seront intégées. C'est le DG, DGSI, qui sera responsable de cette mesure.

Recommandation #4 : D'accord
Cette recommandation soulève certains problèmes techniques qui seront traités d'ici les prochaines semaines avec le personnel des TI des Services et des régions (matériel, logiciel, compétences techniques et personnel requis). À la suite de ces discussions, nous fournirons davantage d'information.

Échéancier : Juin 2001

Mesures proposées : Sous la direction du DG, SGSI, examiner cette recommandation avec le personnel technique et fournir une réponse plus officielle à la Direction de la revue.

Recommandation #5 : D'accord
Nous participons actuellement à la planification d'un projet-pilote sur la transmission sécuritaire. Comme vous le savez sans doute, les efforts faits à l'échelle du gouvernement dans ce domaine ne permettront seulement la transmission de documents de niveau B. Les résultats de ce projet-pilote nous permettront de mieux comprendre les coûts et avantages relatifs reliés à la mise en place de ces outils et processus nécessaires pour transmettre des documents nécessitant un niveau de sécurité B.

Échéancier : Septembre 2001

Mesures proposées : La DGSI travaillera avec les régions à un projet-pilote permettant de transmettre des courriels codés ou signés électroniquement, et ce jusqu'au niveau B. Il y aura d'autres décisions relatives à la faisabilité et à la mise en oeuvre. Le DG, DGSI, sera responsables de ces mesures.

Introduction

Contexte de la vérification

Le Secrétariat du Conseil du Trésor (SCT) exige de chaque ministère qu'il procède à une vérification périodique de la sécurité de ses technologies de l'information (STI) afin de mesurer sa conformité à la politique du SCT sur la sécurité. En outre, le Ministère de l'Environnement avait entrepris d'élaborer une stratégie de GI/TI et devait, ce faisant, évaluer le niveau de STI. Par conséquent, dans le *Plan d'examen de 2000-2001*, le Comité ministériel de la vérification et de l'évaluation a approuvé la réalisation d'une vérification de la STI, conformément à la Politique du SCT sur la sécurité, et en vue d'assurer à la haute direction que la STI soutenait fermement la réalisation des objectifs du Ministère.

Contexte de la STI

Le consensus à tous les échelons est que personne n'est jamais totalement protégé. L'art véritable de la sécurité de réseau consiste à comprendre la nature de l'exposition, les risques inhérents et, mieux encore, la valeur des données que l'on tente de protéger.[1]

La STI désigne les mesures qui sont prises par une entité pour garantir l'intégrité de l'information traitée au moyen des systèmes informatiques. L'organisation doit accepter un certain niveau de risque inhérent lorsqu'elle met en œuvre des TI dans le cadre de ses activités, risque qui s'accentue dans un monde où les technologies deviennent désuètes très rapidement. Bien qu'un certain nombre de marches à suivre et de pratiques soient employées pour protéger les TI, il est impossible de les protéger contre toutes les menaces, accidentelles ou délibérées et ce, avec une totale certitude.

Gérer le risque peut aider à mieux utiliser le budget et les ressources. Très souvent, on voit des gens ériger des clôtures à coût de millions de dollars pour protéger des biens de quelques dollars, mais on voit aussi des biens considérables autour desquels la sécurité laisse grandement à désirer.[2]

Environnement Canada (EC) tente d'arriver à un équilibre entre les mesures considérées diligentes et raisonnablement pratiques, et celles qui sont inutilement coûteuses ou difficiles à appliquer. La STI est gérée conformément au degré de risque et à sa probabilité par rapport à la valeur de l'information pour le Ministère. La politique sur la sécurité du Conseil du Trésor contient des lignes directrices pour garantir une STI ministérielle appropriée; même lorsqu'elles sont suivies à la lettre, ces lignes directrices ne protègent pas l'organisation avec une certitude absolue. L'objectif visé est donc de prendre des mesures raisonnables pour gérer et minimiser le risque.

---

[1] Deveau, Denise, When to say "no access", *Computing Canada*, vol 26, n° 26, 15 décembre 2000, p. 14.

[2] Ibid., p. 15

De plus, EC est un ministère à vocation scientifique, ce qui suppose qu'il faut établir un équilibre entre les besoins de STI et la nécessité de communiquer de l'information à ses partenaires et intervenants. Certains domaines de programme, comme la Protection de l'environnement (application de la loi), la Conservation de l'environnement, les Politiques et les communications et les Ressources humaines emmagasinent de l'information de nature délicate et exigent un niveau élevé de sécurité. Par ailleurs, le Service météorologique du Canada (SMC) qui accomplit une fonction essentielle à la mission de l'administration fédérale (EMAF) doit travailler en temps réel chaque jour de l'année afin de pouvoir assurer la sécurité du public. Cette fonction exige des mesures de sécurité élevées de façon à protéger les réseaux contre tout dommage. Ainsi, Environnement Canada dispose de toute une gamme de mesures de sécurité qui résultent de la nature diversifiée de ses activités et doit établir un équilibre approprié pour gérer la STI.

Portée et méthodologie

L'objectif de la présente vérification était de mesurer la conformité du Ministère au Guide de vérification – Sécurité des technologies de l'information (STI) du Conseil du Trésor (1995); d'identifier les pratiques exemplaires et les points vulnérables; et de faire des recommandations. La vérification a aussi tenu compte de cinq initiatives ministérielles complémentaires, réalisées dans le cadre de l'établissement de la stratégie de GI/TI :

- la vérification de la capacité de mettre en œuvre l'initiative de Gouvernement en direct, une étude réalisée par KPMG;
- le recensement de tous les comités s'occupant de questions relatives à Internet, réalisé par CGI;
- l'évaluation de la capacité actuelle du Ministère en vue de déterminer les points de vulnérabilité en GI/TI, effectuée par EDS;
- une étude sur les télécommunications donnée à contrat par le SMC, et dont le rapport doit être présenté en mars 2001;
- une analyse anti-intrusion effectuée sur la Voie verte.

Le Guide de vérification – Sécurité des technologies de l'information (1995) du SCT a été utilisé pour définir les critères de la vérification. Ces critères ont servi de base d'analyse aux observations et à la formulation des conclusions. Trois sources de données ont permis d'établir les conclusions de la vérification, soit plus de 50 entrevues, un examen exhaustif des dossiers et un groupe de discussion. Des membres du personnel chargé de la gestion et de l'administration de la STI et un échantillon d'employés travaillant au soutien de chacun des quatre secteurs d'activité du Ministère ont été sélectionnés dans les cinq Régions et à l'administration centrale pour constituer le groupe de personnes interviewées. Tout au long du processus de collecte de données, on s'est efforcé de recueillir des documents concernant la STI. Enfin, les conclusions initiales, tirées des deux premières méthodes de collecte de données, ont été présentées à un groupe de discussion tenu dans le cadre d'une réunion du Comité consultatif des technologies de l'information (CCTI). Les activités du groupe de discussion consistaient entre autre à appuyer et à classer les énoncés de risques, ainsi qu'à définir certaines stratégies initiales de gestion en vue d'y donner suite. Pour plus de détails, se reporter à l'annexe 1.

Des renseignements supplémentaires concernant la stratégie de Gouvernement en direct (GED) et l'utilisation des langues officielles dans le domaine de la STI ont aussi été recueillis et seront étudiés ultérieurement dans le rapport sous la rubrique «Autres sujets».

Observations

Les conclusions générales de la vérification sont les suivantes :

- EC a un système essentiel à la mission de l'administration fédérale (EMAF) de niveau A pour le Service météorologique du Canada (SMC) qui exige le maintien des activités 24 heures sur 24 et sept jours sur sept, ainsi qu'une solide gestion de la STI. EC satisfait aux exigences de sécurité d'un tel système, comme l'ont démontré l'exercice de préparation à l'An 2000, la tempête de verglas de 1998 et le virus «I luv you».

- Le SMC emmagasine des renseignements de grande valeur et s'occupe de la gestion d'un réseau auquel viennent se greffer les TI du Ministère. Il emploie d'excellentes pratiques et, dans certains cas, dépasse les normes du Conseil du Trésor. Cependant, ces pratiques exemplaires ne sont pas communiquées aux autres services du Ministère, ce qui entraîne des incohérences dans l'application des politiques et des marches à suivre.

- De nombreuses bonnes pratiques ou pratiques exemplaires ont été observées et, si leur emploi était généralisé au Ministère, la STI ne s'en porterait que mieux. Cependant, les marches à suivre pour la STI ne sont pas appliquées, ni surveillées de façon constante au Ministère; certains secteurs accusent des lacunes, tandis que d'autres dépassent les exigences de la politique. Le problème ici se situe au niveau du leadership en matière d'application et de surveillance systématiques des politiques et des marches à suivre, et leur normalisation dans un référentiel aisément accessible.

- En général, le Ministère atteint la plupart des objectifs définis dans le Guide de vérification – Sécurité des technologies de l'information du Conseil du Trésor (1995).

- La formation des utilisateurs et des techniciens, ainsi que l'accroissement de la sensibilisation des utilisateurs ont été définis comme les éléments primordiaux de l'amélioration de la gestion de la STI.

- Le personnel du Ministère qui participe à l'élaboration des documents secrets ou de nature délicate n'a pas les outils protégés nécessaires pour assurer une consultation rapide et appropriée à la grandeur du Ministère, tout en respectant les échéances fixées par la haute direction.

- Les initiatives pangouvernementales, comme Gouvernement en direct, accéléreront l'utilisation des technologies de l'information et pourraient accentuer les faiblesses actuelles de l'application de la STI.

Les observations sont regroupées dans sept grandes catégories qui touchent les 15 objectifs du Guide de vérification de la STI du SCT.

L'étude a permis de déterminer que trois objectifs du Guide de vérification de la STI du Conseil du Trésor ne s'appliquaient pas à EC. Ce sont :
- La gestion du matériel cryptographique; EC n'utilise pas la cryptographie pour coder l'information.

- Les exigences relatives à l'autorisation et à l'authentification des signatures numériques; EC a très peu recours à l'autorisation électronique actuellement, sauf dans le cas d'un projet pilote mis sur pied dans la Région de l'Atlantique, relativement aux formulaires de congé et aux autorisations de voyage.
- Les exigences relatives à la sécurité des signaux de valeur pour les systèmes liés aux TI qui traitent ou transmettent des renseignements désignés de nature très secrète ou extrêmement délicate; cette exigence ne s'applique pas à EC.

1. Organisation et administration

Les observations sur la structure de gestion de la STI, le cadre de gestion du risque, l'accès aux TI et le contrôle des STI font partie de cette catégorie.

Gestion

La vérification a porté sur la façon dont les fonctions de gestion sont définies et assignées, sur l'existence d'un processus de planification et la manière de communiquer les politiques et marches à suivre au personnel.

La vérification a permis de déterminer que les attributions en matière de STI sont assignées à la DGSI et la gestion de réseau au CMC/SMC. Les relations sont définies dans un document d'organisation qui est actuellement mis à jour, conformément à l'objectif de la politique du SCT concernant l'assignation des fonctions de gestion. Les attributions nationales en matière de STI sont assignées à la DGSI et 1,5 ETP est consacré à la coordination de cette fonction. Le CMC/SMC joue un rôle crucial sur le plan de la STI par l'exploitation d'ECONet, qui est le fondement du système du Ministère et son personnel possède des connaissances techniques et opérationnelles poussées.

Cependant, l'application et la gestion de la STI dans les services et les Régions est dispersée sur le plan **organisationnel** parmi de nombreux employés qui ont recours à différentes pratiques. Il en résulte des incohérences dans l'application des mesures de la STI au Ministère et dans l'accomplissement des rôles et des fonctions détaillées assignés au personnel chargé de s'occuper de STI.

Le Ministère dispose d'un Comité consultatif des technologies de l'information (CCTI) pour donner des conseils à la DGSI. Cependant, ce Comité n'est pas lié aux tables de concertation et, par conséquent, au processus de prise de décisions et de gestion du Ministère. On a observé que si le CMC/SMC gère le réseau du Ministère, son rôle et sa place au sein du Comité ne semblent toutefois pas correspondre à ses responsabilités en tant que gestionnaire du réseau.

En ce qui concerne la **planification**, il n'y a pas de plan national de STI officiel et intégré, ni de fonds réservés à cette fin au Ministère, comme l'exige la politique du CT. Bien que certains domaines de programme aient des plans bien établis, ils ne sont pas mentionnés et intégrés dans le processus de planification annuel, ni élaboré en collaboration avec d'autres au Ministère. L'exercice de préparation à l'An 2000 a renforcé la planification des interventions d'urgence et de la reprise des activités; cependant, le processus de mise à jour n'a pas été appliqué comme il est également signalé dans la Vérification de la sécurité (2000) effectuée par la Direction de la revue.

Il existe des **liens** au sein du Ministère entre la fonction de STI et d'autres fonctions administratives, ce qui est conforme à cet aspect des exigences de la politique du SCT. Cependant, ces liens ne sont pas aussi officiels qu'ils devraient l'être pour que toutes les dimensions de la STI soient systématiquement envisagées. L'absence de liens officiels au Ministère est partiellement démontrée par l'incohérence des rôles et attributions fonctionnels et organisationnels et l'absence de plan ministériel de la STI. Les liens extérieurs avec la GRC et le Centre de la sécurité des télécommunications sont appropriés et maintenus à partir d'un point de contact central à la DGSI.

Certaines politiques et marches à suivre du Ministère sont affichées sur l'intranet; EC satisfait donc partiellement aux exigences de la politique du SCT. Cependant, elles ne sont pas communiquées de manière très efficace. Ainsi, à moins que le personnel n'ait à consulter fréquemment les politiques et les normes de STI, il les connaît généralement peu même si des bulletins et des directives sont fréquemment transmis par courrier électronique. En résumé, le Ministère n'a pas d'approche stratégique pour communiquer, promouvoir et diffuser l'information concernant la STI, et en assurer un effet maximal.

Dans l'ensemble, deux grandes organisations sont responsables des TI, soit la DGSI et le SMC; les rôles et attributions de ces groupes sont définis dans un document d'architecture actuellement mis à jour; ainsi, il est peu probable qu'on omette des lacunes en matière de STI et qu'il y ait violation des systèmes. En ce qui concerne la planification, les activités de STI ne sont pas toujours appliquées de façon stratégique et cohérente dans l'ordre des priorités en raison de l'absence d'un plan ministériel de STI. En outre, l'opportunité de l'intervention du Ministère risque d'être ralentie en situation d'urgence à cause des faiblesses et du manque de fiabilité des processus de reprise des activités et d'intervention d'urgence. Le Ministère a toutefois en place l'infrastructure de planification et de prise de décisions nécessaire à cet aspect, notamment le CCTI et les tables de concertation.

Gestion du risque

Le but de la gestion du risque dans le domaine de la STI est de mettre en place une méthode de gestion appropriée, des marches à suivre et la capacité nécessaire pour s'assurer que les décisions sont fondées sur une information valable et que les nouvelles TI sont implantées dans un cadre commun au Ministère.

La vérification a permis de constater que la DGSI avait mis au point un cadre de gestion du risque basé sur le Cadre amélioré pour la gestion (CAG) du Conseil du Trésor qui doit être utilisé pour tous les nouveaux systèmes. Cette marche à suivre officielle de gestion du risque au Ministère n'est cependant pas appliquée uniformément pour tous les nouveaux systèmes qui sont mis au point au Ministère, ni utilisée pour corriger les systèmes actuellement en place. Plusieurs domaines de programme ont une excellente stratégie de gestion du risque, y compris des méthodes, des marches à suivre et une capacité de gestion, et l'appliquent rigoureusement. Ainsi, certains secteurs sont en mesure de prendre des décisions basées sur une information valable. Bien que la plupart des programmes aient mentionné utiliser une démarche de gestion du risque de façon informelle, les secteurs qui ont des systèmes essentiels appliquent une gestion du risque officielle.

Accès aux TI

La vérification visait à évaluer si le Ministère avait des marches à suivre lui permettant de vérifier les autorisations et l'accès aux systèmes de TI. Cela comprend des privilèges d'accès accordés au personnel, l'utilisation de codes, de mots clés et de mots de passe.

L'étude a révélé que les politiques et marches à suivre du Ministère en matière d'accès sont bien définies et mises en œuvre. Toutefois, les marches à suivre concernant la gestion des comptes ne sont pas uniformes dans l'ensemble du Ministère. Certains secteurs surveillent les comptes inactifs et exigent un renouvellement périodique des mots de passe, tandis que d'autres le font moins régulièrement. De plus, le personnel n'utilise pas de façon uniforme la protection des mots de passe pour empêcher un accès irrégulier aux ordinateurs personnels. On a aussi pu déterminer que les caractéristiques des mots de passe pour les sauve-écrans, les ordinateurs de poche comme les Palm Pilot et les Blackberry, etc. sont fréquemment laissées à la discrétion de l'utilisateur et, par conséquent, ne sont souvent pas appliquées. En ce qui concerne l'accès aux TI à partir du domicile ou de l'extérieur des immeubles du Ministère en passant par le réseau, il existe une marche à suivre officielle qui est appliquée dans tout le Ministère et qui dépasse les exigences du SCT. Cette marche à suivre comporte l'utilisation d'un mot de passe pour l'identification personnelle, associée à une carte de contrôle d'accès (CCA). Dans l'ensemble, les marches à suivre en place dépassent les exigences du SCT. Néanmoins, les marches à suivre de gestion des comptes pourraient être appliquées de façon plus cohérente. On trouvera à ce sujet d'autres détails sous la rubrique *Sécurité des communications*.

Il est donc possible d'apporter une plus grande assurance en appliquant de façon constante les protocoles d'utilisation de mot de passe dans tout le Ministère. Les services qui ont de l'information essentielle et de grande valeur, assurant la permanence 24 heures sur 24 et sept jours sur sept, appliquent effectivement des marches à suivre pour l'accès sévères et dépassent les exigences d'accès externe.

Surveillance de la sécurité

Selon les objectifs de la politique du SCT, la STI des ministères devrait faire l'objet d'une surveillance et d'un d'examen réguliers, et même d'un examen par l'EIES de la GRC. EC a demandé à la GRC d'intervenir dans des cas particuliers : par exemple, la GRC a fait un examen du Centre canadien des eaux intérieures, lors de l'installation de nouvel équipement d'application de la loi, au moment d'une réinstallation. L'établissement de Dorval du SMC fait l'objet d'une évaluation annuelle par la gestion des installations et, tous les cinq ans, par la division de l'EIES de la GRC. En outre, certains examens internes de la STI ont déjà été réalisés. Le Service des glaces a fait une vérification menée par la direction l'année dernière pour ses unités. En 1991, la Direction de la revue a aussi effectué une vérification ciblée touchant certains aspects de la STI. Néanmoins, aucun examen officiel par l'EIES/GRC n'a été entrepris au cours des dix dernières années, ni n'a été sollicité. Bien que la surveillance passée de la STI n'ait pas été exhaustive et ne respecte pas les exigences de la politique du SCT, la combinaison des examens de certains établissements importants, ainsi que la réalisation de la présente vérification devraient fournir au Ministère les éléments nécessaires pour mettre à jour la STI.

2. Sécurité du personnel

En examinant la sécurité du personnel, nous avons demandé aux personnes interviewées de commenter les aspects suivants :

- la mesure dans laquelle les Déclarations de la nature délicate sont faites et mises à leur disposition pour les TI;
- les processus en place pour l'examen préliminaire des nouveaux membres du personnel et la révocation des privilèges d'accès à ceux qui quittent le Ministère;

- les mesures qui sont prises pour s'assurer que les usagers ont une connaissance suffisante des politiques et marches à suivre en matière de STI;
- la qualité de la formation reçue par le personnel qui s'occupe de l'application et de la mise à jour de la STI.

Déclarations de la nature délicate

Les Déclarations de la nature délicate sont des documents qui contiennent les exigences concernant le caractère confidentiel, l'intégrité et l'accessibilité et qui servent à déterminer les privilèges d'accès du personnel aux systèmes de TI. L'application officielle de ce processus fournit une assurance quant aux privilèges d'accès. On a pu établir que la plupart des domaines de programme n'appliquent pas de façon uniforme ou systématique les Déclarations de la nature délicate, à l'exception du CMC/SMC. Par conséquent, EC ne respecte pas la politique du SCT à cet égard. L'absence de cadre de contrôle officiel qui donnerait l'assurance que des Déclarations de la nature délicate ont été préparées pour les systèmes, les réseaux et les applications peut expliquer cette situation. Bien qu'aucun incident n'ait été signalé, on bénéficierait d'une plus grande assurance si ce genre de processus était appliqué.

Processus d'examen préliminaire et d'établissement des droits d'accès aux systèmes

Le personnel qui a accès aux systèmes de TI devrait faire l'objet d'un examen préliminaire approprié et ses privilèges d'accès devraient être établis en fonction de sa situation. Les processus d'examen permettant de donner et de retirer les privilèges d'accès à un utilisateur sont appliqués et sont conformes à la politique du SCT. Il existe une certaine confusion quant à l'application des vérifications de base et approfondie de la fiabilité aux fins de l'attribution des privilèges d'accès aux nouveaux utilisateurs ou aux utilisateurs à caractère spécial comme les chercheurs invités. En outre, il n'existe aucun processus officiel pour le personnel qui quitte temporairement l'organisation en raison d'une affectation. Dans l'ensemble, ces processus pourraient être améliorés si l'on établissait un lien automatique avec les Systèmes des ressources humaines, afin de s'assurer que l'information sur le statut de l'utilisateur et ses privilèges d'accès demeure constamment à jour.

Formation en STI (formation des utilisateurs, maintien et application de la STI)

Bien qu'une certaine formation officielle soit offerte au personnel qui s'occupe du maintien et de l'application de la STI, la plupart des secteurs n'ont pas de plan de formation officiel pour leur personnel des TI et les cours offerts ne sont pas uniformes d'une région ou d'un programme à l'autre. Un nombre important des employés interviewés ont exprimé des préoccupations à propos du niveau de sensibilisation des utilisateurs à la STI. En particulier, on a noté qu'à cause du caractère limité de la formation, la sensibilisation aux menaces éventuelles est généralement faible. Cependant, le personnel de certains domaines, comme les Services de l'aviation et de la défense (SMC), les Politiques et communications (AC) et l'Application de la loi sont davantage conscients des questions de sécurité en général et, en conséquence, ont une meilleure connaissance des questions de STI. Étant donné que les secteurs traitant directement de l'information de nature délicate bénéficient d'une formation en sensibilisation appropriée, la politique du SCT est en partie respectée. Cependant, le manque de sensibilisation et le peu de compréhension des questions de SI dans d'autres secteurs du Ministère pourraient représenter un risque potentiel en matière de STI.

3. Sécurité matérielle

La vérification de la sécurité matérielle a porté sur les preuves de mesures appropriées de sécurité matérielle associées à la STI, y compris les systèmes de gicleurs, les extincteurs d'incendie, les mécanismes de sécurité pour les portes (p. ex., cartes magnétiques ou serrures), le contrôle d'accès périmétrique, des planchers surélevés, etc.

Exigences relatives à la STI matérielle et du milieu

Les mesures de sécurité matérielle, telles qu'observées par l'équipe de vérification, sont généralement suffisantes et le Ministère se conforme à la politique du SCT. Néanmoins, les zones de TI du Ministère ne sont pas uniformément sûres, puisque les mesures de sécurité matérielle varient selon les régions et les programmes. Certaines préoccupations ont été exprimées à propos de l'état actuel de la sécurité matérielle au Ministère. Cependant, les risques de pertes ou de dommages relatifs à des biens de TI, attribuables au manque d'uniformité de la sécurité matérielle pour les infrastructures importantes sont jugés faibles parce que les mesures appropriées sont prises aux endroits cruciaux. Le CMC/SMC (Dorval) est considéré comme un emplacement critique au Ministère, ainsi que sur le plan fédéral dans la Région du Québec, puisqu'on y emmagasine de l'information et du matériel de grande valeur pour la préparation des prévisions météorologiques. Ainsi, les mesures de sécurité matérielle utilisées à Dorval correspondent aux exigences d'un système EMAF.

4. Sécurité du matériel informatique

Les questions relatives à l'aliénation, à l'entretien, à l'acquisition, à l'alimentation sans coupure (UPS) et aux politiques et marches à suivre connexes sont les critères utilisés pour évaluer la sécurité du matériel informatique.

Exigences en matière de sécurité du matériel informatique et de STI

L'équipe de vérification a pu déterminer que le Ministère avait des politiques et des marches à suivre concernant la sécurité du matériel informatique et qu'elles étaient appliquées, y compris des dispositifs opérationnels d'alimentation sans coupure (UPS) pour tous les emplacements du SMC où ils sont nécessaires.

Les achats et les stocks de matériel informatique ne sont pas contrôlés ou planifiés de façon centrale et uniforme dans tout le Ministère. La consignation des biens de TI dans les répertoires de stocks n'est pas cohérente. Certaines unités, y compris le Service des glaces (SMC), les Services de l'aviation et de la défense (SMC), le CMC à Dorval (SMC), l'Institut national de recherche sur les eaux, le Centre national de recherche en hydrologie, la Région de l'Atlantique et Politiques et communications (AC) ont du matériel normalisé au sein de leur organisation, tandis que d'autres n'en ont pas. Néanmoins, il existe des spécifications types pour les ordinateurs personnels, définies par la DGSI, afin de garantir la compatibilité des systèmes. Ce manque de normalisation peut avoir une incidence sur la capacité de la direction de tirer le meilleur parti possible du matériel informatique. La normalisation est aussi un moyen d'atténuer les besoins de soutien technique.

Le respect des politiques d'aliénation et d'entretien est généralement bon, bien que les attestations de sécurité ne soient pas toujours requises pour les systèmes qui sont réparés à l'extérieur et à l'interne. Cependant, les risques de problèmes sont jugés faibles, puisque la quantité d'information protégée qui est laissée sur le matériel est minime et que les entreprises du secteur privé ont quand même une réputation à protéger. En outre, la

consigne de nettoyage des disques durs avant l'élimination au moyen du logiciel de la GRC n'est pas appliquée de façon universelle dans toutes les régions et tous les programmes. Étant donné que d'autres logiciels sont utilisés, la possibilité de divulguer des renseignements de nature délicate semble toutefois peu probable. Dans l'ensemble, on peut dire que le Ministère se conforme partiellement à la politique du SCT concernant la sécurité du matériel informatique.

5. Sécurité des logiciels

Les critères utilisés pour examiner la sécurité des logiciels comprennent la vérification de l'activation constante des logiciels de détection de virus, de l'existence de mesures de contrôle pour empêcher l'installation de logiciels non autorisés, ainsi que de l'existence et de l'application des politiques et marches à suivre connexes.

Les politiques et les marches à suivre concernant la sécurité des logiciels existent et sont appliquées. Les procédés d'acquisition, de contrôle, d'autorisation et d'installation des logiciels sur les postes de travail sont peu sévères dans certains secteurs et très rigoureux dans d'autres, dont le Service des glaces (SMC), les Services de l'aviation et de la défense (SMC) et Politiques et communications (AC).

Certaines préoccupations ont été exprimées à propos du niveau actuel de sécurité des logiciels pour ce qui est de la protection contre les virus et de la capacité des utilisateurs d'installer des logiciels non autorisés. Bien que les logiciels de détection et de nettoyage de virus soient largement disponibles, ils ne sont pas mis à jour et utilisés uniformément pour tout le matériel, surtout dans les systèmes éloignés. On a noté que les utilisateurs ne mettaient pas à jour leur logiciel antivirus sur les ordinateurs portatifs et les PC à domicile avec le même degré de diligence qu'ils le font au bureau. Il n'y a pas de vérification ministérielle concernant les PC et aucun suivi systématique des licences d'utilisation, sauf au Centre national de recherche en hydrologie. En outre, le personnel dans bien des domaines a la possibilité de télécharger, d'acquérir et d'installer des logiciels qui n'ont pas été antérieurement approuvés.

La sécurité des logiciels au Ministère satisfait donc partiellement à la politique du SCT. Pourtant, des téléchargements non autorisés, surtout à partir d'Internet, peuvent poser des problèmes puisqu'un seul utilisateur peut infecter tous les réseaux. Afin de réduire les risques de ce genre, le Ministère a présentement un logiciel de détection de virus sur les PC, de même qu'au niveau des serveurs de réseau. On aurait une plus grande assurance en informant les utilisateurs des risques ou en limitant davantage la capacité de téléchargement. Vu les risques de plus en plus grands qu'un logiciel accessible par Internet puisse être porteur d'un nouveau virus qui échapperait à la protection antivirus, la responsabilité de l'utilisation appropriée du système revient à l'utilisateur. Les utilisateurs à distance qui ne mettent pas à jour leur système et qui téléchargent des logiciels sont plus vulnérables aux virus et, à leur tour, peuvent soumettre le réseau à un niveau de risque inutile. Le CMC/SMC surveille de façon constante l'ECONet, mais les risques d'infection à partir de serveurs de réseau d'échange subsistent toujours.

6. Sécurité des communications

Les critères utilisés pour évaluer la conformité au regard de la sécurité des communications comprennent un réseau de télécopieurs protégé, l'absence d'information protégée de niveau supérieur à A sur le réseau et l'utilisation des cartes de CAC pour accès à distance.

Bien que les Régions et les programmes n'aient pas tous eu des télécopieurs protégés au moment de la vérification, les examinateurs ont été informés que la mise en place d'appareils était prévue pour le 15 décembre 2000. En ce qui concerne l'accès à distance, on a pu déterminer que les cartes de CAC sont utilisées de façon uniforme au sein des programmes et des Régions.

Environ 47 p. 100 des personnes interviewées ont exprimé des préoccupations à propos de la sécurité des communications au Ministère. Le problème primordial était l'existence d'information dont la désignation était supérieure au niveau A sur le réseau. Plusieurs des personnes interrogées ont signalé avoir vu de l'information de nature délicate sur le réseau à cause de l'absence d'autres possibilités de consultation en temps suffisamment opportun pour respecter les échéances de la haute direction. La transmission d'information secrète et protégée de niveau B a aussi été signalée au cours de la Vérification de la sécurité 2000 réalisée par la Direction de la revue. Puisque l'information de nature délicate sur le réseau semble constituer un problème, le Ministère est considéré comme se conformant seulement partiellement à la politique du SCT. La pratique qui consiste à utiliser le réseau pour transmettre de l'information protégée accroît les risques de fuites ou d'interception.

7. Sécurité de l'exploitation

Cette section de la vérification porte sur les politiques relatives au réseau, à sa structure et aux marches à suivre opérationnelles, y compris la surveillance et les autres protections du système. Il convient de noter que l'étude sur les télécommunications du SMC, actuellement en cours et dont les résultats sont prévus en mars 2001, devrait fournir plus de renseignements sur ce point.

Réseaux et applications réseau

Le réseau EcoNet qui soutient les programmes du SMC et de l'ensemble du Ministère est exploité et géré par le SMC. L'installation du CMC/SMC, à Dorval, exploite un système EMAF et est aussi désignée comme emplacement essentiel à la mission de l'administration fédérale dans la Région du Québec. Le SMC fournit les connaissances techniques et opérationnelles nécessaires pour assurer l'efficacité de l'application de son programme météorologique à l'échelle nationale et surveille l'utilisation du réseau et les irrégularités du système 24 heures sur 24, sept jours sur sept. Puisque les activités régionales sont accomplies à partir de nombreux bureaux dispersés au Canada et fournissent des analyses et des données météorologiques, le réseau constitue une infrastructure cruciale pour les activités du SMC. Les résultats de la vérification ont révélé que, dans l'ensemble, des politiques et des marches à suivre existent pour le réseau et sont appropriées.

La surveillance des journaux de réseau constitue un outil de diagnostic et de gestion de système/réseau. Ils peuvent servir à déceler les tentatives d'intrusion, ainsi que les utilisations non autorisées du système. La surveillance est sporadique et varie selon les services, les régions et les endroits. Il n'y a pas de surveillance globale continue pour l'ensemble du Ministère qui engloberait tous les niveaux du système (réseau longue portée,

réseau métropolitain, réseau local). La surveillance des journaux de réseau permet aux administrateurs du système de faire des inspections. Celles-ci comprennent la vérification de l'étiquette de réseau ou des contraintes d'usage du Ministère, tâche qui n'a pas été vraiment entreprise par les administrateurs, ni ne leur a été assignée. Ce genre de contrôle est effectué de façon exceptionnelle lorsqu'on soupçonne une mauvaise utilisation. La surveillance des intrusions au niveau de l'ECONet seulement est effectuée à l'échelle du Ministère au CMC/SMC, à Dorval, afin de garantir la sécurité et l'intégrité du système. Le CMC surveille le réseau et exerce son pouvoir de prendre des mesures correctives lorsque des menaces semblent imminentes. Un contrôle semblable est en place pour les activités des Services de l'aviation et de la défense (SMC).

La vérification a signalé d'autres faiblesses. Des modems sont installés sur des PC reliés au réseau, ce qui va à l'encontre des politiques ministérielles. Certains modems sont utilisés à des fins légitimes, par exemple pour communiquer avec du matériel de contrôle des données, et sont en activité seulement pendant la durée du transfert des données. Les préoccupations viennent plutôt de ce qu'avec un PC et un modem en activité, d'autres pourraient s'introduire dans la connexion et l'utiliser comme passerelle vers le système. En outre, des cas ont été signalés où une configuration inappropriée du PC a créé des brèches dans le garde-barrière, constituant une passerelle ouverte vers le réseau. Heureusement, aucun incident du genre n'a été rapporté. Le problème est qu'il n'y a pas de contrôle cohérent de la configuration des modems et des ports ouverts, et une application peu rigoureuse des politiques du Ministère. Cependant, il y a des exceptions, comme dans les établissements de recherche ou au sein de Politiques et communications, qui surveillent étroitement ou, comme dans le cas du CNRH, qui régissent les configurations. Il y a certainement là une possibilité de renforcer et d'améliorer l'uniformité des activités réseau puisqu'elles ne sont pas conformes actuellement à la politique du SCT. Cependant, le rôle actif joué par le SMC sur le plan de la surveillance globale du réseau fournit un niveau raisonnable de sécurité aux activités actuelles du Ministère sur l'ECONet.

Planification des interventions d'urgence en TI et des besoins du Ministère

Cette partie de la vérification visait à examiner les politiques et les pratiques relatives à la reprise des activités et à la planification des interventions d'urgence.

Les conclusions révèlent qu'un plan de reprise des activités (PRA), axé sur les systèmes de TI importants d'EC, a été établi avant l'An 2000. Les résultats de cet effort ont permis de créer un PRA relativement complet; malheureusement, aucune mesure n'a été prise pour s'assurer que l'information serait tenue à jour. Or, la mise à jour de ce genre de plan au moyen de sa base d'information devient de plus en plus coûteuse à mesure que le temps passe. Cependant, certains services/régions ont commencé à déployer des efforts en ce sens, mais seulement pour leurs propres secteurs; aucun effort n'a été fait à l'égard d'un plan d'ensemble.

En outre, il n'y a pas de processus ministériel pour le contrôle et l'évaluation des interventions d'urgence et des PRA. La planification des interventions d'urgence est en grande partie propre au programme du SMC, ce qui est attribuable à sa situation de système EMAF. Le SMC dispose de plans courants d'intervention d'urgence, ainsi que de marches à suivre. Ses besoins opérationnels exigent qu'il emploie des sources appropriées d'alimentation sans coupure (UPS), et que des mesures d'intervention d'urgence soient prévues pour des sites miroirs au cas où des problèmes techniques entraîneraient

l'interruption des activités à un centre météorologique. Des conclusions semblables ont été exposées dans la Vérification de la sécurité 2000 réalisée par la Direction de la revue.

Il est possible de tenir à jour les plans d'intervention d'urgence et de reprise des activités puisque, à l'heure actuelle, le Ministère se conforme seulement partiellement à la politique du SCT. Cependant, le rôle joué par le SMC pour l'application des plans d'intervention d'urgence comme élément courant de ses activités quotidiennes assure le niveau de sécurité correspondant à sa fonction. De nombreuses régions et de nombreux services ont des marches à suivre d'intervention d'urgence moins formelles et ne sont donc pas entièrement sans protection. Politiques et communications a mis au point ses propres plans d'intervention d'urgence opérationnels, indépendamment de ceux du Ministère.

D'après les conclusions antérieures et la réponse de la direction indiquée dans la Vérification de la sécurité 2000, l'agent de sécurité du Ministère désignera une personne-ressource centrale qui sera chargée de surveiller et de tenir à jour les plans de reprise et de continuité des activités, annuellement. Cette mesure devrait abaisser le niveau de risque en garantissant un effort continu à la grandeur du Ministère.

Autres enjeux

Pendant la vérification, des renseignements ont été recueillis à propos des efforts déployés par le Ministère dans le cadre de **l'initiative de Gouvernement en direct** (GED). Fait intéressant à noter, la sécurité est un point qui a été fréquemment soulevé.

> *La nécessité du cybergouvernement est maintenant largement acceptée. Les gouvernements sont aux prises avec les détails d'application pratique, comme les priorités, les coûts, la rapidité, l'assignation des tâches, les répercussions organisationnelles et en matière de RH, et leur image auprès du public*.[3]

Nos entrevues nous ont permis de noter que la sécurité est de plus en plus importante parce que l'information courante de certains ministères exigera une protection accrue. Il faudra rechercher l'équilibre entre sécurité et accès des clients. De même, il faudra intégrer un certain niveau d'authentification des données pour garantir les sources et la validité de l'information. La question du renouvellement du personnel exigera une attention particulière en ce qui concerne l'accroissement des contacts avec les clients et des connexions au système. Il faudra donc des investissements plus importants du côté aussi bien du personnel que de l'infrastructure. Les autres commentaires ont porté sur la nature encore très théorique du GED dont on comprend mal les liens et les répercussions sur le plan opérationnel. Les rôles des secteurs public et privé devront être précisés et les politiques des organismes centraux comme le Conseil du Trésor devront être modifiées pour qu'elles soient compatibles avec ce « nouveau mode de travail ». Les scientifiques devront aussi s'adapter aux nouvelles orientations et modifier leurs opinions sur la propriété des données.

Le respect des exigences relatives aux **langues officielles** fait partie de toute vérification ou tout examen. Bien que de nombreux services/Régions n'aient signalé aucun problème important, certains points ont été soulevés. Une des faiblesses mentionnées était la rareté

[3] David Prime , *Auditing and risk in a e-business world*, IIA, section d'Ottawa, Conférence sur les vérificateurs internes dans l'administration publique, 16 octobre 2000

de l'utilisation du français dans les communications internes au sein de la Région du Québec. Par exemple, certaines annonces ministérielles de virus ne sont pas bilingues lorsqu'elles sont distribuées dans la Région du Québec; certains courriels destinés à la Région du Québec arrivent en anglais seulement, indiquant que la version française suivra, mais elle ne suit pas toujours.

Internet crée des pressions pour la production de rapports entièrement bilingues, capacité qui n'est pas facile à appliquer pour les chercheurs, de sorte qu'il en découle des besoins de traduction coûteux avec les délais correspondants. Cette situation a été notée de façon générale, que la langue d'origine soit l'anglais ou le français.

Les autres préoccupations potentielles dans ce domaine comprennent : le nombre d'employés bilingues dans la Région de l'Atlantique (seulement le poste de directeur); la demande de services du SMC en français à Iqaluit qui devrait augmenter les demandes faites à la RPN, puisque cet emplacement était antérieurement desservi par le bureau de Montréal.

Recommandations

EC exploite efficacement un système EMAF au sein du SMC et a bâti son réseau sur ce système, ce qui lui donne un niveau de STI correspondant aux exigences opérationnelles de ce genre de système. Bien que le Ministère atteigne en partie à la plupart des objectifs de la politique du SCT, les améliorations recommandées ci-dessous permettraient d'améliorer le niveau de conformité à la politique tout en appuyant encore mieux les objectifs d'EC. Les conclusions générales et l'analyse ont amené les vérificateurs à présenter les recommandations qui suivent dans les catégories de la gestion, des communications et de la formation, ainsi que des outils.

Gestion

Recommandation n^{o} 1

L'infrastructure décisionnelle est déjà en place au Ministère, notamment les tables de concertation et le CCTI, pour améliorer la gestion et l'administration de la STI, ainsi que pour assurer l'uniformité de l'application des politiques et des marches à suivre et de la surveillance dans tout le Ministère. Les tables de concertation sont des points décisionnels clés du Ministère et le CCTI est composé de conseillers, de spécialistes et de gestionnaires de très haut niveau en informatique. Cependant, actuellement, le CCTI n'est pas tenu de rendre compte à la table de la Gestion, de l'administration et des politiques (GAP). Étant donné que le CMC/SMC joue un rôle important dans la structure du réseau, une réorganisation de son rôle au sein du CCTI devrait être envisagée. Le rajustement de la relation de dépendance a déjà été noté dans l'*Examen de la bureautique* réalisée par la Direction de la revue en 1999.

Il est recommandé que le SMA, Services ministériels, en collaboration avec le SMA, SMC, examine le rôle du CCTI. Cet examen devrait comprendre : un mandat révisé pour le Comité et ses sous-comités, une modification de la relation de dépendance du Comité, et un examen de la composition et des rôles du Comité en vue de s'assurer que tous les intervenants sont correctement représentés.

Cette recommandation devrait être mise en œuvre en 2000-2001 à peu de frais.

Recommandation n^{o} 2

Bien que les rôles et attributions de la DGSI et du SMC soient définis et tenus à jour, l'étalement des responsabilités à la grandeur du Ministère a amené une fragmentation de la gestion et de l'administration de la STI au Ministère, de sorte que les politiques et marches à suivre ne sont pas appliquées de façon cohérente. Un examen et une redéfinition des rôles et attributions détaillés seraient avantageux pour améliorer l'uniformité et l'efficacité des politiques. La structure de responsabilisation des postes et organisations qui suivent devrait faire partie de cet examen :

- la Sécurité TI à l'administration centrale et dans les Régions;
- les secteurs d'activité à l'administration centrale;
- la DGSI et les Régions;
- le Secrétariat de Gouvernement en direct;
- la DGSI et l'agent de sécurité du Ministère.

On a établi que certains programmes ou régions utilisent d'excellentes pratiques tandis que d'autres ne satisfont que partiellement aux exigences des politiques. Si toutes les pratiques exemplaires actuellement employées dans certaines parties du Ministère (définies à l'annexe 2) devaient devenir universelles, elles contribueraient grandement à améliorer la STI, ainsi qu'à accroître le respect par le Ministère de la politique du CT.

Il est recommandé que le DG, SI, entreprenne de renforcer le cadre de gestion de la STI au Ministère, ce qui comprendrait : une meilleure définition des rôles et des fonctions en matière de STI, une amélioration de la coordination et de la cohérence de l'application des politiques et des marches à suivre, une meilleure planification de la STI et des comptes rendus.

Cette recommandation devrait être mise en œuvre en 2000-2001 à peu de frais.

Communications et formation

Recommandation n^{o} 3

Au sein du Ministère, un des principaux facteurs de l'application de bonnes pratiques en matière de STI est la collectivité des utilisateurs. À l'exception de certains secteurs choisis, la sensibilisation des utilisateurs a été signalée parmi les principaux éléments qui permettront d'améliorer la STI. Les utilisateurs ont tendance à avoir peu si ce n'est aucune formation en STI et leur sensibilisation aux menaces potentielles est généralement faible. En outre, les politiques et marches à suivre existantes ont dans bien des cas peu d'effet sur les utilisateurs, ce qui est principalement attribuable à un manque de communication / promotion de la STI.

Un programme global de sensibilisation aux TI à l'échelle du Ministère, associé à une stratégie de communication / promotion comprendrait les caractéristiques suivantes :

- un site Web où seraient regroupées toutes les politiques et marches à suivre en matière de STI;

- un dossier d'information amélioré et des messages visant à accroître la sensibilisation des utilisateurs et à assurer la transmission d'un message cohérent dans tout le Ministère (rappels périodiques; mises à jour régulières concernant les nouvelles technologies en association avec d'autres séances de formation; module informatisé sur la formation en direct);
- formation obligatoire de tous les employés (p. ex. trousse spécialisée pour les chercheurs/étudiants invités; séance d'orientation).

Toutes ces mesures devraient être liées à la concrétisation de l'engagement à l'égard du lancement, par le Bureau de sécurité du Ministère, d'un programme de sensibilisation sur la sécurité à l'échelle du Ministère. Étant donné l'étendue des fonctions, il serait prudent que toutes les parties soient consultées aux différentes étapes de préparation.

Il est recommandé que le DG, SI, en collaboration avec le Directeur de l'informatique au SMC, le DG, RH, et le Bureau de la sécurité du Ministère (BSM), élabore une stratégie de sensibilisation / communication / promotion de la STI.

Cette recommandation devrait être mise en œuvre en 2000-2001; le coût devrait être évalué par le DG, SI, ainsi que par le BSM.

Outils

Recommandation n^{o} 4

Il faut assurer une certaine surveillance afin que les procédés et les marches à suivre soient respectés et appliqués uniformément dans tout le Ministère et faciliter le dépistage des lacunes en STI. Pour arriver à un degré élevé d'assurance, la surveillance doit être accrue dans les domaines suivants :

- journaux de STI;
- mécanismes intégrés, liés à la mise en œuvre des politiques et des marches à suivre comme des feuilles d'approbation pour les évaluations de menaces et de risques.

La nécessité de vérifications externes (GRC) devrait être évaluée par le CCTI et une décision devrait être prise à la table de GAP.

Il est recommandé que le DG, SI, en collaboration avec les membres du CCTI, examine les possibilités de mettre en application des logiciels appropriés pour surveiller les registres de STI au niveau ministériel.

Cette évaluation devrait avoir lieu tous les deux ans, à compter de 2002-2003, ce qui donnerait suffisamment de temps pour mettre en œuvre les recommandations de la présente vérification. Le coût serait évalué par le DG, SI.

Recommandation n^{o} 5

Le Ministère n'a pas les outils numériques efficaces et rentables nécessaires pour la manipulation d'information de nature délicate. Le personnel qui traite de l'information de nature délicate n'est pas toujours conscient des autres moyens de communication dont il dispose et n'a peut-être pas la formation nécessaire pour prendre une décision éclairée lorsqu'il transmet électroniquement de l'information de cette nature. De plus, les autres moyens de communication, comme les télécopieurs protégés sont opérationnels depuis peu

de temps, ce qui a entraîné des situations où des renseignements de nature délicate ont été transmis par des moyens non protégés. Le personnel a besoin d'outils protégés et efficaces pour consulter rapidement ses collègues du Ministère et respecter les échéances serrées imposées par la haute direction. Il devrait disposer d'outils pour communiquer l'information de nature délicate aussi efficacement qu'il le fait pour les documents ordinaires. Le projet pilote visant à mettre en œuvre la transmission de messages protégés en 2001 au moyen de l'infrastructure à clés publiques (ICP) est certainement un pas dans la bonne direction vers une solution à long terme. Cependant, la prise de mesures d'amélioration de la sécurité, après un examen de ce qui se fait dans les autres ministères, ainsi que la sensibilisation des utilisateurs aux possibilités d'éviter les risques, pourraient, à court terme, entraîner une amélioration tangible.

Il est recommandé que le DG, SI, en collaboration avec le Directeur de l'informatique du SMC et le Bureau de sécurité du Ministère, détermine et distribue de meilleurs outils électroniques pour faciliter les communications protégées.

La recommandation devrait être mise en œuvre en 2000-2001; le coût devrait être évalué par le DG, SI, et le BSM.

Réponse de la direction ***(Se référer au Résumé)***

Conclusion

Dans l'ensemble, Environnement Canada atteint partiellement les objectifs définis dans le Guide de vérification – Sécurité des technologies de l'information du Conseil du Trésor (1995). À EC, les TI font maintenant partie intégrante des activités, mais l'importance et l'attention accordées à la STI correspondante n'ont pas suivi le même rythme. Le Ministère a appliqué des mesures de sécurité, mais pas de façon aussi uniforme et exhaustive que l'indiquent ses politiques. Certains secteurs accusent des faiblesses, tandis que d'autres dépassent les exigences. La sensibilisation à la sécurité à tous les niveaux, ainsi qu'une responsabilisation bien claire masquent un bon nombre des problèmes de STI et empêchent de les régler efficacement.

Tandis qu'augmente la dépendance à l'égard de l'électronique par la multiplication des sites Web et l'amélioration de GED, il importe de se pencher sur les faiblesses et les incohérences du réseau et de ses utilisateurs. Le réseau ne sera jamais plus solide que son maillon le plus faible et son élément primordial est l'utilisateur. Pour cette raison, il sera très important d'accorder une attention particulière en temps opportun aux domaines d'amélioration signalés. Les efforts devraient porter sur les points suivants :

- Améliorer la STI du Ministère – réduire efficacement les faiblesses actuelles qui ont été décelées avant qu'elles deviennent de plus en plus coûteuses à corriger.
- Amener le Ministère à se conformer encore mieux à la politique du SCT sur la sécurité.
- Placer le Ministère dans une meilleure position pour mettre en œuvre l'initiative de GED tout en étant bien protégé.

Annexe 1 Liste des documents supplémentaires pour la vérification de la sécurité des TI

Nota : Ces documents peuvent n'être disponibles qu'en anglais.

1. Méthodologie de la vérification de la STI
2. Bibliographie de la vérification de la STI
3. Liste des personnes interrogées pour la vérification de la STI
4. Résultats du groupe de discussion – Énoncés des risques

Annexe 2 Liste des pratiques exemplaires

Rôles et attributions

Les attributions en matière de gestion de la sécurité sont clairement établies, définies et assignées, aussi bien en ce qui concerne la structure que la fonction, aux gestionnaires de réseau.

La STI est assignée à un membre du personnel qui est chargé d'élaborer un ensemble cohérent de politiques et de marches à suivre qui seront appliquées dans toutes les Régions, et d'établir un plan de mise en œuvre. Ces attributions figurent dans la description de travail de l'agent de sécurité des TI.

Sensibilisation à la sécurité des TI

Des séances de sensibilisation à la sécurité des TI ont lieu plusieurs fois par année, parallèlement à des envois périodiques, et les politiques de sécurité sont regroupées dans un emplacement central.

Le personnel des TI participe aux équipes de gestion de programme, ce qui favorise la communication des questions de sécurité.

Un dossier d'introduction écrit à l'intention de l'utilisateur est remis à tous les nouveaux utilisateurs du système.

Une trousse d'information générale (vidéo et CD-ROM) décrivant tous les aspects de la sécurité des TI a été constituée et présentée à la réunion du CCTI de novembre 2000.

Planification

L'information sur la politique est actuellement recueillie auprès de toutes les Régions en vue de créer un plan uniforme qui sera tenu à jour. Le membre du personnel chargé de la STI élabore ce plan.

Les TI et la STI sont coordonnés et planifiés en tant que service central commun à toute la collectivité des utilisateurs, et relèvent d'un comité de gestion qui fournit des orientations / mesures de contrôle.

Pour tous les nouveaux projets, un arrêté de projet est élaboré, comprenant les exigences en matière de sécurité des TI. Un projet ne peut être mis en œuvre avant que l'arrêté de projet ait été préparé.

Planification des interventions d'urgence et de la reprise des activités

Un plan complet d'intervention d'urgence a été élaboré, mis à l'essai et tenu à jour.

Gestion du risque

Une évaluation obligatoire de la gestion du risque est effectuée sur tous les systèmes. La démarche du cycle de vie est toujours employée et suivie par le groupe d'élaboration.

Sécurité matérielle

Les serveurs et les systèmes importants sont gardés dans une salle des ordinateurs protégée où la température et l'humidité sont réglées, et où l'accès est limité par carte une magnétique qui enregistre l'arrivée du propriétaire de la carte et son heure d'entrée. La salle des ordinateurs comporte un système d'UPS empêchant les fluctuations ou les pannes de courant. Une protection contre l'incendie appropriée (gicleurs, extincteurs) est en place et fonctionnelle.

Sécurité des réseaux et des logiciels

L'utilisation des logiciels est limitée aux configurations du système. Ce processus permet de s'assurer qu'aucun logiciel non autorisé ne pourra être installé sur le système. Cette mesure est aussi une protection pour le réseau.

Surveillance

Des vérifications de sécurité périodiques sont effectuées. Lorsque des problèmes sont décelés (p. ex. ordinateurs laissés en marche, documents non protégés ou téléphones cellulaires ouverts), la personne en cause reçoit une formation additionnelle.

Les inspections de STI par la GRC ou par une entreprise privée sont prévues afin de vérifier les configurations d'ordinateur et de réseau; tout rajustement nécessaire est effectué.

Des examens périodiques sont entrepris pour contrôler le journal du serveur de façon à dépister toute activité suspecte.

Réparation et aliénation du matériel

L'information protégée est seulement stockée sur le système et non sur les PC ou les ordinateurs portatifs.

Un système d'étiquettes de propriété est en place et toute tentative de modifier le matériel (p. ex. retirer la puce de mémoire vive) entraîne l'activation d'un système d'alarme.

Les réparateurs de l'extérieur sont accompagnés et supervisés jusqu'à ce qu'ils aient terminé leur travail. On ne leur fournit ni les mots de passe ni les numéros d'identification personnelle.