Les travaux parlementaires

Journal des débats

Commission permanente de l'administration publique

Le mardi 16 novembre 2004 • Vol. 38 N° 15

Audition du secrétaire du Conseil du trésor concernant la gestion de la sécurité informatique

Table des matières

Stratégies du SCT quant à l'authentification dans les ministères et organismes

Travaux du SCT portant sur les normes de sécurité interne s'adressant aux ministères et organismes

Exigences de vérification interne pour chaque ministère

Dépenses assumées par les différents ministères et le SCT pour des services de certification

Fusion des autres services de certification et du service de certification du Secrétariat du Conseil du trésor

Délais concernant la mise en place de l'infrastructure à clé publique

Travaux du SCT sur les normes de sécurité interne s'adressant aux ministères et organismes (suite)

Tests d'intrusion

Cas d'intrusion dans les systèmes informatiques du SCT

Notion du domaine de confiance

Autres intervenants

Mme Rita Dionne-Marsolais, présidente
M. Henri-François Gautrin
Mme Sarah Perreault
M. Raymond Bernier
Mme Cécile Vermette
*** Mme Louise Thiboutot, Secrétariat du Conseil du trésor**
*** M. Raynald Brulotte, idem**
*** M. Marc Laurin, idem**
*** M. Robert Desbiens, idem**
*** M. Martin Lessard, bureau du Vérificateur général**
*** Témoins interrogés par les membres de la commission**

(Dix heures trente-cinq minutes)

La Présidente (Mme Dionne-Marsolais): ...mesdames et messieurs, je constate le quorum et je déclare donc ouverte la séance de la commission qui se réunit aujourd'hui, pour entendre le secrétaire du Conseil du trésor concernant la gestion de la sécurité informatique.

Est-ce qu'il y a des remplacements, Mme la secrétaire?

La Secrétaire: Non, Mme la Présidente, il n'y a pas de remplacement.

La Présidente (Mme Dionne-Marsolais): Alors, nous allons donc débuter nos travaux et demander au Vérificateur général du Québec de faire un exposé bref de quelques remarques. M. le Vérificateur général.

**Exposé du Vérificateur général du Québec,
M. Renaud Lachance**

M. Lachance (Renaud): Mme la Présidente, Mme la vice-présidente, Mmes et MM. les membres de la commission, M. le secrétaire du Conseil du trésor.

L'application de mesures de sécurité informatique adéquates est essentielle à la mise en oeuvre des programmes gouvernementaux. En effet, les atteintes à la sécurité peuvent avoir d'importantes répercussions sur le respect de la vie privée. Elles risquent aussi d'influer sur le maintien des services essentiels, la conduite des activités courantes et la productivité du personnel. Cette vérification visait à nous assurer que la sécurité informatique bénéficie d'un encadrement approprié à l'échelle gouvernementale. Nous cherchions en outre à évaluer si les ministères et les organismes ont mis en place les composantes majeures en vue de protéger leur actif informationnel. Pour ce faire, nos travaux ont porté sur les composantes contribuant le plus à l'atteinte des résultats escomptés et dont l'absence ou la défaillance sont susceptibles d'entraîner la multiplication des incidents. Nos travaux ont été menés principalement auprès du Secrétariat du Conseil du trésor à qui des responsabilités particulières ont été confiées en matière de sécurité informatique.

En ce qui a trait aux moyens de protection déployés, nous avons vérifié les activités menées à cet égard par le ministère du Revenu du Québec, la Société de l'assurance automobile du Québec et la Régie de l'assurance maladie du Québec, ainsi que par deux directions spécialisées du Secrétariat du Conseil du trésor. La présente vérification s'est terminée en mars 2004. L'information numérique et les échanges électroniques du ministère du Revenu, de la SAAQ et de la RAMQ sont généralement bien protégés contre les menaces les plus courantes. Nous avons cependant détecté des failles qui augmentent le risque, puisque le niveau de protection obtenu repose beaucoup plus sur l'expertise et l'implication des employés, ainsi que sur la technologie, que sur des processus bien établis. L'encadrement gouvernemental actuel respecte la plupart des exigences du modèle de référence que nous avons retenu, notamment une description exhaustive des rôles et des responsabilités. Il aborde aussi plusieurs questions fondamentales, telles la classification, la sensibilisation et la formation des effectifs, la sécurité physique de même que la continuité des services.

Certains aspects pourraient cependant être améliorés de façon à mieux baliser la question globale de la sécurité. D'abord, les guides appelés à soutenir l'application des principes énoncés tardent à venir. Ensuite, la notion de domaine de confiance introduite pour mobiliser toutes les parties afin qu'elles répondent aux mêmes exigences de sécurité n'est pas encore intégrée dans la directive sur la sécurité. De plus, le plan gouvernemental de sécurité ne précise pas les résultats attendus. Nous avons aussi constaté que les activités de sensibilisation et de formation de l'effectif ne sont pas encadrées par un programme formel, ce qui favoriserait la satisfaction des besoins communs jugés prioritaires au moment où ils sont ressentis. Enfin, pour procéder à l'authentification des utilisateurs, les services de certification se multiplient sans que la nécessité de chacun d'eux soit démontrée.

En ce qui a trait aux services communs d'infrastructure, le Secrétariat du Conseil du trésor n'a pas officialisé le cadre de gestion de la sécurité du réseau gouvernemental de télécommunications. Il n'exerce pas les contrôles requis pour garantir la présence et l'efficacité des mesures visant à sécuriser ce réseau. Il ne veille pas non plus au maintien des services de traitement informatique sur toutes les plateformes exploitées. Enfin, la planification des services communs que nous avons vérifiée est mal articulée et n'inclut pas l'élaboration d'indicateurs de performance. Par ailleurs, nous avons réalisé des tests d'intrusion dans quatre entités, pour sonder l'efficacité de leurs dispositifs de sécurité. Pour des raisons évidentes, le nom de ces entités, la nature exacte des tests ainsi que les résultats détaillés ne sont pas présentés dans ce rapport. Précisons que nous avons fait appel à des techniques ou à des outils facilement disponibles en cherchant avant tout à simuler des scénarios selon lesquels une personne tentait d'accomplir une action répréhensible souvent à l'intérieur du périmètre de sécurité.

n *(10 h 40)* n

Nos travaux révèlent que la protection des actifs informationnels des quatre entités concernées est adéquate par rapport au flux d'informations qui provient du réseau Internet. Par contre, elle est moins efficace sur d'autres plans, soit la résistance des mécanismes de sécurité, la robustesse des mots de passe choisis, la pertinence des droits d'accès, la configuration des postes de travail et l'aménagement des lieux. Les lacunes détectées pourraient permettre de mener, dans certaines conditions, diverses activités inappropriées. Il est donc important que les entités du gouvernement du Québec évitent qu'un intrus soit capable d'accéder, de façon illégitime, à des systèmes informatiques ou à des données sensibles, de modifier des données ou des programmes, d'installer des programmes malveillants et d'empêcher le bon fonctionnement de plusieurs équipements.

Somme toute, notre vérification fait ressortir que les entités vérifiées s'appliquent à assurer la sécurité de la ressource informationnelle. Elle indique aussi que des gestes concrets devront être accomplis pour que leur action soit conforme aux

meilleures pratiques en vigueur. Bien que nos constatations ne puissent être généralisées à l'ensemble de l'appareil gouvernemental, il n'en demeure pas moins que la sécurité informatique soulève certaines préoccupations au moment où l'État s'engage à se rapprocher des citoyens en misant sur une utilisation plus intensive des technologies de l'information et des communications. Je vous remercie.

La Présidente (Mme Dionne-Marsolais): Merci, M. le Vérificateur général. Donc, vous avez entendu, M. le secrétaire du Conseil du trésor, que nous n'avions pas d'inquiétude tant qu'à la protection de nos systèmes contre les menaces les plus courantes. Je pense que c'est le constat le plus important du Vérificateur général. Par contre, il y a des améliorations à apporter, et on souhaiterait vous entendre aujourd'hui, quant à ces améliorations-là. Je vous laisse donc la parole. Vous voudrez peut-être présenter vos collaborateurs.

Exposé du secrétaire du Conseil du trésor, M. Luc Meunier

M. Meunier (Luc): Merci beaucoup. Mme la Présidente, Mmes et MM. les membres de la commission, M. le Vérificateur général, mesdames et messieurs. Ma présence, aujourd'hui, devant cette commission, vise à vous présenter la position du Secrétariat du Conseil du trésor à l'égard du rapport du Vérificateur général sur la gestion de la sécurité informatique.

Tout d'abord, j'aimerais souligner la présence à mes côtés de M. Robert Desbiens, secrétaire associé à l'inforoute gouvernementale et aux ressources informationnelles, de M. Gordon Smith, secrétaire associé aux services administratifs, de M. Raynald Brulotte, directeur général des technologies de l'information et des communications, et de Mme Louise Thiboutot, coordonnatrice gouvernementale de la sécurité de l'information et des échanges électroniques. Avec votre permission, Mme la Présidente, et celle des membres de la commission, mes collègues seront en mesure de me seconder afin de vous présenter le travail du secrétariat ainsi que pour répondre aux questions et aux préoccupations qui pourraient être soulevées. Avant de rendre compte de la position du secrétariat sur les recommandations du Vérificateur général, j'aimerais effectuer un bref retour sur la démarche de notre organisation en matière de gestion de la sécurité informatique.

La sécurité informatique est une priorité pour le secrétariat, et nous le véhiculons et le faisons valoir auprès des ministères et des organismes, par des actions de gouverne et de soutien. Nous croyons au rôle de premier plan que doit exercer le secrétariat afin d'implanter une véritable culture de la sécurité au sein de l'ensemble de l'appareil gouvernemental. C'est d'ailleurs dans cette optique que le secrétariat a mis en place une équipe dédiée à cette fonction et qui s'affaire à cette tâche depuis déjà quelques années. Le Vérificateur général a d'ailleurs indiqué, dans son rapport, que l'encadrement offert aux ministères et organismes était plutôt satisfaisant. Il a également jugé que le cadre actuel respectait la plupart des exigences du modèle de référence retenu pour fins de comparaison. D'entrée de jeu, je tiens à dire que le secrétariat est d'accord avec les constats du rapport du Vérificateur général et qu'il a déjà pris en considération les recommandations qui en découlent. Je vous ferai donc part des réalisations et des intentions du secrétariat à propos des bilans et des plans gouvernementaux, de la directive sur la sécurité, du cadre de gestion et de la gestion des infrastructures communes de traitement.

L'action du secrétariat en matière d'encadrement de la sécurité informatique repose principalement sur l'application de la directive sur la sécurité de l'information numérique et des échanges électroniques dont le contenu est le reflet de pratiques internationales adaptées au contexte de l'administration québécoise. Ainsi, chaque année, le secrétariat produit, en collaboration avec près de 70 ministères et organismes, un état de situation gouvernemental. Pour réaliser ce travail important, le secrétariat a mis en place un concept novateur de mesures pour lequel le gouvernement du Québec fait figure de précurseur. À cette fin, les ministères et organismes doivent évaluer annuellement leur positionnement par rapport aux bonnes pratiques en matière de sécurité. Le secrétariat dresse par la suite un portrait global de la situation avant d'établir une stratégie et un plan d'action qui sont soumis au Conseil du trésor pour approbation. Trois états de situation ont été produits à ce jour. Le dernier est en cours de validation.

Selon le Vérificateur général, la mesure de la performance des ministères et organismes et le délai de production de l'état de situation gouvernemental pourraient être améliorés. À cet égard, il est bon de noter qu'au cours des dernières années le secrétariat a agi en priorité sur les mécanismes de production des bilans et sur l'analyse de risques, afin de favoriser une prise en charge par les ministères et organismes. Le secrétariat peut ainsi désormais porter une attention plus particulière à la gestion du suivi et de la performance.

D'ici mars 2005, le secrétariat se positionnera sur la façon d'intégrer à son processus la gestion par résultats et l'élaboration d'indicateurs de gestion. Dans sa réflexion, il prendra en considération l'imputabilité des ministères et des organismes et fera l'arrimage avec les mesures adoptées dans le cadre du gouvernement en ligne. En ce qui a trait aux délais de production de l'état de situation gouvernemental, le secrétariat a dû faire face à quelques impondérables qui en ont retardé la production. Le secrétariat entend faire un suivi attentif de cette situation en vue de produire les documents dans les délais attendus. De plus, tel que

recommandé par le Vérificateur général, l'évaluation et l'actualisation de la directive sur la sécurité de l'information numérique et des échanges électroniques sont actuellement en cours et devraient être complétées pour février 2005. La directive refondue intégrera la notion de domaine de confiance, notion qui a fait l'objet de sessions de formation auprès du personnel des ministères et organismes, au cours des derniers mois.

Le secrétariat a également mis en oeuvre ou intégré à son plan d'action différentes mesures en ce qui concerne le cadre de gestion et plus spécifiquement les guides et outils nécessaires à l'application de la directive, le développement d'un programme de sensibilisation et de formation, l'indication de clauses relatives à la sécurité dans les ententes contractuelles et finalement la certification et l'authentification. En effet, la production de guides et outils est désormais évolutive et ajustée aux besoins des ministères et organismes: un programme de sensibilisation et de formation est actuellement en cours de validation et sera mis en application à partir d'avril 2005; un inventaire des clauses de sécurité à prendre en considération dans la rédaction d'ententes contractuelles sera disponible dès mars 2005; de nouvelles orientations en matière de certification seront disponibles en mars 2005; et la fusion des deux services de certification, soit celui du ministère de la Justice et du Secrétariat du Conseil du trésor, sera complétée à la même période.

De nouvelles orientations en matière d'authentification ont été approuvées en août 2004, et le développement du Service québécois d'authentification gouvernementale qui a débuté en septembre 2004 sera graduellement implanté à compter de l'automne 2005. À ce sujet, il est important de noter que ce système sera compatible avec le système du gouvernement du Canada, ce qui permettra aux citoyens d'utiliser le même code pour les deux gouvernements. Par ailleurs, le secrétariat offre des services communs d'infrastructure à plusieurs ministères et organismes. Dans son rapport, le Vérificateur général a évalué le réseau de télécommunications multimédia de l'administration publique québécoise, le RETEM, et les services de traitement informatique multiplateforme offerts à l'aide d'ordinateurs de moyenne et grande puissance. En ce qui concerne le RETEM, le cadre de gestion est maintenant officialisé depuis juin 2004, et une politique de sécurité qui définit les orientations et les obligations des partenaires est également disponible. Également, depuis juin 2004, le secrétariat procède régulièrement à des analyses de vulnérabilité sur les équipements névralgiques du RETEM.

Concernant les infrastructures de traitement informatique multiplateforme, le Vérificateur général demande que le secrétariat poursuive l'élaboration de son architecture de sécurité, qu'il mette au point un processus assurant l'évaluation périodique et indépendante de la vulnérabilité des infrastructures et qu'il complète la mise en place des mesures de reprise afférentes. En ce qui concerne l'architecture de sécurité, elle sera complétée pour mars 2005 et sera conforme au cadre de référence gouvernemental. Par la suite, le secrétariat amorcera la conception d'un cadre de gestion de la sécurité pour avril 2006. En ce qui a trait à l'évaluation de la vulnérabilité des infrastructures, le secrétariat a mis en place un processus d'évaluation périodique et indépendant qui fait en sorte que des évaluations sont effectuées par composante, sur une base annuelle. Exceptionnellement, en 2003-2004, aucune évaluation de ce type n'a été effectuée. Pour 2004-2005, le secrétariat a déjà prévu procéder à l'évaluation d'une composante considérée parmi les plus sensibles.

n *(10 h 50)* n

Concernant les mesures de reprise, le secrétariat vérifie biannuellement celles relatives aux infrastructures communes. De plus, chaque année, au moment du renouvellement des ententes avec ses clients, le secrétariat sensibilise ces derniers à l'importance de ces vérifications. Concernant l'intégration d'indicateurs de performance à la planification des activités de sécurité, le secrétariat effectuera des travaux à ce sujet pour mars 2005.

Mme la Présidente, j'ose croire que l'ensemble des mesures et des actions exposées, qu'elles soient en cours ou à venir, répondront aux préoccupations soulevées par le Vérificateur général. En terminant, j'aimerais insister sur le fait que le Secrétariat du Conseil du trésor, à l'instar des autres administrations, est bien au fait des dangers qui le menacent. Et je tiens à réaffirmer que toutes les mesures possibles pour contrer ces dangers seront mises de l'avant, car, comme gestionnaires de l'État, nous avons l'obligation d'utiliser les meilleurs moyens disponibles afin de s'assurer que la sécurité de nos systèmes informatiques et de la protection des renseignements personnels et confidentiels. Le défi est immense, mais nous sommes déterminer à le relever. Merci.

La Présidente (Mme Dionne-Marsolais): Je vous remercie beaucoup, M. le secrétaire général... le secrétaire, pardon, du conseil. Effectivement, vos commentaires sont très intéressants par rapport à ce qu'on a étudié dans le rapport du Vérificateur. Et ça sert à quelque chose, qu'il y ait une vérification régulière, à ce qu'on voit. Puis vous vous y conformez bien.

Discussion générale

On va donc commencer les échanges. Comme d'habitude, on va faire 10 minutes-10 minutes. Et je vais passer la parole au député de Verdun.

Validation des risques résiduels pour chaque ministère et organisme par le Secrétariat du Conseil du trésor (SCT)

M. Gautrin: Je vous remercie, Mme la Présidente. Alors, je voudrais aussi, Mme la Présidente, affirmer ici l'article 4.27 du rapport du Vérificateur général qui tient à rappeler ici que, dans le cadre actuel, le cadre actuel de gestion respecte la plupart des exigences du modèle de référence que nous avons retenu, c'est-à-dire, en un mot simple, c'est-à-dire que la sécurité informatique est globalement, en général, dans l'ensemble, bien protégée au niveau du gouvernement du Québec.

Néanmoins, moi, j'aurais trois questions à vous poser. La première, c'est ce qu'on appelle le risque acceptable ou le risque résiduel. Vous savez que, dans la stratégie actuellement, la responsabilité des risques appartient à chaque ministère et chaque organisme, mais évidemment le niveau de risque acceptable est différent d'un organisme à un autre organisme. On appelle ça le risque résiduel ou risque acceptable, enfin comme vous voulez l'utiliser. Je n'ai pas vu nulle part le rôle, préciser le rôle du Secrétariat du Conseil du trésor dans la démarche de validation du risque acceptable pour chacun des ministères et organismes.

Alors, ma question à vous: Est-ce que, dans les ententes que vous avez avec les ministères et organismes, est inclus ce que je pourrais appeler la validation du risque acceptable pour chaque ministère et chaque organisme?

La Présidente (Mme Dionne-Marsolais): M. le secrétaire.

M. Meunier (Luc): Je passerais peut-être la parole à Mme Thiboutot, qui est notre spécialiste dans le domaine.

La Présidente (Mme Dionne-Marsolais): Alors, Mme Thiboutot, on vous écoute.

Mme Thiboutot (Louise): Bonjour. Oui, M. Gautrin, pour répondre à votre question...

La Présidente (Mme Dionne-Marsolais): Vous devez référer au député de Verdun.

Mme Thiboutot (Louise): Oui, excusez; député de Verdun. Excusez-moi, je suis novice.

M. Gautrin: Ah, ce n'est pas grave. On apprend vite, vous savez.

La Présidente (Mme Dionne-Marsolais): Vous êtes toute pardonnée, madame. Ne vous inquiétez pas.

Mme Thiboutot (Louise): Voilà. Alors, le secrétaire du Conseil du trésor, comme on le mentionnait, on travaille à deux niveaux, tant au niveau de la gouverne et au niveau du soutien auprès des ministères et organismes. Dans le cas de l'évaluation des risques, les ministères sont les premiers responsables à réaliser des analyses de risques dans leur organisation et ils sont responsables par la suite d'établir un plan d'action pour corriger et arriver justement à contrôler, là, ces risques résiduels le mieux possible.

Dans le cadre de nos validations, à travers le bilan, annuellement, on évalue globalement les résultats des grandes pratiques en sécurité, mais nous n'allons pas au niveau détaillé de chacun des ministères, donc de chacun des plans d'action des ministères et organismes. Par contre, cette année, nous avons proposé • et c'est en évaluation présentement • nous avons proposé d'avoir un suivi à cet effet à partir de l'an prochain. Alors, nécessairement, il y aura des changements à ce niveau-là, et ce qu'on propose, c'est que les ministères réalisent officiellement une analyse de risques en 2005 et qu'ils nous présentent le résultat en décembre 2006.

M. Gautrin: Et qu'il y ait, à ce moment-là, une validation par le conseil...

Mme Thiboutot (Louise): Une validation de ces risques résiduels.

Échéancier des travaux sur l'évaluation de l'application de la directive sur la sécurité informatique

M. Gautrin: Vous avez abordé la question de l'évaluation globale. J'en viens à l'élément 4.37 et à l'article 20 de la directive. Rappelez-vous, en 1999, le Conseil du trésor avait confié au secrétariat la responsabilité d'application de la nouvelle directive, et le secrétariat devait, trois ans après, en faire l'analyse. Alors, si j'ai bien compris, le Secrétariat du Conseil du trésor a décidé de

surseoir à cette exigence, considérant que l'information présentée dans les états de situation qu'il prépare était suffisante.

Et là il y a une espèce de divergence entre le Vérificateur général et vous-même quant au fait qu'il n'y a pas une évaluation globale. Vous avez une suite d'évaluations individuelles, comme vous l'avez rappelé. Est-ce que je dois comprendre de la réponse qui m'est donnée à la question précédente qu'en 2006 il y aurait donc, à ce moment-là, une évaluation globale?

La Présidente (Mme Dionne-Marsolais): Madame ou M. le secrétaire... Mme Thiboutot.

Mme Thiboutot (Louise): Alors, M. le député Gautrin, la réponse est encore en deux volets.

M. Gautrin: J'espère qu'un jour peut-être il y aura un comté portant mon nom...

Mme Thiboutot (Louise): Ah oui, vraiment?

M. Gautrin: ...mais pour l'instant ce n'est pas encore le cas.

Mme Thiboutot (Louise): Alors, la réponse est aussi en deux volets. Effectivement, après trois ans, nous devions évaluer l'application de la directive et proposer des recommandations à cet effet. Ce que nous avons fait dès le départ, par nos bilans annuels, c'est de vérifier, à tous les ans, l'application de chaque responsabilité des ministères et organismes à l'intérieur de la directive. Alors, nous, nous considérons que ce volet-là nous permettait d'évaluer cette application de la directive au fil des ans. Donc, on a une progression à tous les ans et on voit comment les ministères rencontrent leurs responsabilités à cet effet.

Et naturellement c'est que, l'an dernier, nous avons décidé de planifier, pour l'année 2004-2005, la révision de la directive et l'évaluation complète avec les ministères et organismes. Le travail est en cours; les travaux ont débuté en juin dernier. On s'est associé, le Comité d'orientation stratégique en sécurité, donc plusieurs ministères. Il y a 22 personnes, là, qui font partie du Comité d'orientation stratégique, et également on a créé un sous-groupe de travail pour travailler plus en profondeur les éléments de modification qu'on pourrait apporter à la directive. Les résultats devraient être présentés en février prochain.

M. Gautrin: ...à ce moment-là, globale de la situation.

Mme Thiboutot (Louise): Globale de l'application de la directive.

M. Gautrin: Il nous reste du temps?

La Présidente (Mme Dionne-Marsolais): ...M. le député de Verdun.

Certification des services gouvernementaux en ligne par un organisme externe

M. Gautrin: Merci. Alors, j'ai une autre question. Le Vérificateur général aborde la question éventuellement de la certification par un organisme externe. Vous savez parce que vous l'avez en partie financé. Le CRIM veut actuellement constituer un organisme de certification. Est-ce que c'est quelque chose qui pourrait être associé à la démarche du Secrétariat du Conseil du trésor pour certifier, par cet organisme externe, la sécurité de chacun des systèmes et des architectures?

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot.

Mme Thiboutot (Louise): Oui. Alors, effectivement, depuis un an, nous travaillons avec le Centre de recherche en informatique de Montréal, le CRIM, pour évaluer la possibilité de certifier l'ensemble des services qui sont mis en ligne. Alors, nous, on focusse, par rapport au gouvernement électronique, le volet spécifique des services qui sont mis en ligne.

Alors, cette démarche-là, qui a débuté en mars dernier, on a fait un premier regard de qu'est-ce qui se passe à travers les grands gouvernements en France, aux États-Unis, un peu partout, en Nouvelle-Zélande, en Grande-Bretagne. Et qu'est-ce qui est ressorti de tout ça? C'est qu'effectivement, en Europe, il y a un volet de certification très fort qui est basé sur l'ISO 17799, là • c'est des volets techniques pour vous • mais tout ça pour vous dire que le volet de certification des entreprises particulièrement est très fort à ce niveau-là. Sur le plan des gouvernements, c'est beaucoup plus au niveau des analyses de risques que les gouvernements travaillent afin de valider et d'évaluer, là, si les services qui sont mis en place sont fonctionnels et sécuritaires.

Alors, notre première approche nous donne ça comme portrait. À partir de ça, nous, on continue à travailler avec eux pour évaluer quel serait le modèle applicable. Dans un premier temps, parce qu'on veut faire assez rapidement, on veut évaluer une approche d'autoévaluation avec des outils qui vont permettre aux ministères et organismes de s'autoévaluer lors de la mise en place, là, et du développement d'un service qui sera mis en ligne. Par après, pour des services beaucoup plus critiques, bien, là, il y aura un volet beaucoup plus d'audit, par exemple, qui sera amené pour valider, là, beaucoup plus en profondeur le volet de la sécurité.

La Présidente (Mme Dionne-Marsolais): M. le député de Verdun.

n *(11 heures)* n

M. Gautrin: Donc, vous n'avez pas d'objection à travailler avec le CRIM...

Mme Thiboutot (Louise): Pas du tout.

M. Gautrin: ...au terme du processus, d'arriver réellement à un mécanisme d'audit.

Mme Thiboutot (Louise): Non, parce qu'effectivement ça prend un tiers pour nous certifier; on ne peut pas se certifier nous-mêmes. Alors, le fait d'avoir l'ISIQ • on peut nommer l'organisme... pas l'organisme, mais il va exister un jour...

M. Gautrin: ...début décembre. Bien, au début décembre, si j'ai compris.

Mme Thiboutot (Louise): ...il sera mis au monde prochainement, il sera annoncé du moins • oui, effectivement la solution, c'est d'avoir des tiers pour pouvoir certifier l'ensemble de ces services-là.

M. Gautrin: Alors, je vous remercie. Mme la Présidente...

Adoption du cadre de gestion du Réseau de télécommunications multimédia de l'administration publique québécoise (RETEM)

La Présidente (Mme Dionne-Marsolais): Oui, puis on reviendra. Alors, Mme la députée de Marie-Victorin. Ah, d'accord. Alors, moi, j'ai des questions, si vous me permettez, à ce moment-là.

On dit, à l'article 4.92, dans le rapport du Vérificateur général • peut-être que vous l'avez dit, mais je ne l'ai pas saisi • on dit: «Dans le contexte d'une prestation de services communs d'infrastructure, il est essentiel d'établir les principes de sécurité, d'attribuer clairement les responsabilités et [...] communiquer le tout aux diverses parties concernées pour qu'il y ait cohésion. Or, près de deux ans après la mise sur pied du RETEM, le cadre de gestion traitant de la sécurité n'est pas officiellement adopté.»

M. le secrétaire, est-ce qu'on comprend qu'il est adopté maintenant ou s'il ne l'est pas encore? Et, sinon, pourquoi?

M. Meunier (Luc): M. Brulotte pourra renchérir, mais le cadre de gestion du RETEM a été approuvé en juin 2004, et une politique de sécurité qui officialise les orientations et les obligations des partenaires a été approuvée en octobre 2004.

La Présidente (Mme Dionne-Marsolais): Donc, cette critique-là ou ce commentaire-là a été corrigé.

M. Brulotte (Raynald): Il était valide au moment où le Vérificateur général a fait son intervention, et, l'été dernier, on a procédé aux corrections.

La Présidente (Mme Dionne-Marsolais): D'accord. Quand vous dites: Il était valide, mais il n'avait pas été officiellement adopté, c'est ce que le Vérificateur dit.

M. Brulotte (Raynald): C'est-à-dire, oui. C'est parce que le Vérificateur général a fait son intervention le printemps dernier, et nous, le cadre de gestion du RETEM, il faut quand même rappeler aux membres de cette commission que le Secrétariat du Conseil du trésor travaille avec un partenaire privé pour la dispensation des services de télécommunications. Et donc, effectivement, ça aura pris deux ans, avec notre partenaire privé, pour bien établir les rôles et les responsabilités. C'est la fonction d'un cadre de gestion.

Donc, il aura fallu deux ans pour bien établir les rôles et les responsabilités de chacun des partenaires, c'est-à-dire le partenaire privé et nous. Et ça a été finalisé en juin 2004.

La Présidente (Mme Dionne-Marsolais): M. Brulotte, est-ce que vous trouvez que c'est normal, deux ans, pour négocier avec un privé pour établir ces conditions-là?

M. Brulotte (Raynald): Oui, dans les circonstances, c'est tout à fait normal. Je rappelle...

La Présidente (Mme Dionne-Marsolais): Qu'est-ce que vous voulez dire par «les circonstances»?

M. Brulotte (Raynald): C'est qu'encore une fois le dossier du réseau de télécommunications du gouvernement du Québec, c'est quand même quelque chose de gigantesque. C'est d'une ampleur et d'une complexité absolument importantes. C'est une entente contractuelle, voyez-vous, qui tourne autour de 250 millions de dollars. Et, là-dedans, comme on fait affaire avec un partenaire qui est un télécommunicateur reconnu, il y a déjà une prime à la sécurité, si je peux dire, parce que la société Bell Canada, pour ne pas la nommer, qui est le partenaire qui a été retenu là-dedans, bien vous connaissez la longue tradition, si je peux dire, en matière de sécurité des entreprises dans le domaine de la téléphonie. Alors, ce n'est pas parce que le cadre de gestion a pris deux ans à être finalisé avec notre partenaire que la sécurité, si je peux dire, n'était pas assurée, étant entendu qu'on fait affaire avec une entreprise de la taille et l'envergure comme Bell Canada.

Évaluation de l'efficacité du dispositif de sécurité protégeant le RETEM

La Présidente (Mme Dionne-Marsolais): Pourtant, à 4.93, le Vérificateur dit: «Pour ce qui est des aspects clés de la sécurité, nous avons noté que la [Direction générale des télécoms] dispose de peu d'informations sur la vulnérabilité et l'efficacité du dispositif de sécurité protégeant le RETEM, même si toute l'infrastructure propre à ce réseau est en place depuis l'automne 2002.»

Est-ce que vous pouvez commenter cela et nous dire exactement comment vous interprétez ce commentaire et comment vous y avez donné suite?

M. Brulotte (Raynald): Oui. Voici, Mme la Présidente, le commentaire que j'ai à faire là-dessus. C'est que d'abord il ne faut jamais oublier qu'on a mis en place, il y a environ un an et demi, j'appelle ça une cellule de sécurité. Il y a une appellation contrôlée, si je peux dire, dans cet univers-là, ça s'appelle un CERT, pour Computer Emergency Response Team. Et cette cellule de sécurité là qu'on a mise en place il y a environ un an et demi • bon, le temps de doter en personnel cette minicellule de sécurité • et, depuis que cette cellule de sécurité là est en place, effectivement on a confié à cette cellule-là le mandat de procéder à certaines analyses de vulnérabilité périodiquement.

Et, aujourd'hui, je peux me permettre d'affirmer, devant les membres de la commission, qu'on est en relative maîtrise des vulnérabilités de notre infrastructure de télécommunications. Et cette cellule de sécurité nous procure quotidiennement, si je peux dire, cette assurance-là qu'on maîtrise les vulnérabilités. D'abord, on les identifie systématiquement, périodiquement, et, deuxièmement, on prend les mesures correctives qui s'imposent.

La Présidente (Mme Dionne-Marsolais): Est-ce que je pourrais demander au Vérificateur général si cette réponse-là satisfait les inquiétudes de ce paragraphe-là?

M. Lachance (Renaud): Oui, je vais laisser M. Martin Lessard répondre à la question.

La Présidente (Mme Dionne-Marsolais): Monsieur?

M. Lachance (Renaud): Martin.

La Présidente (Mme Dionne-Marsolais): Martin, d'accord.

M. Lessard (Martin): Oui, effectivement.

Fréquence des évaluations des composantes de la stratégie de sécurité informatique de la Direction générale des services

informatiques gouvernementaux

La Présidente (Mme Dionne-Marsolais): Oui, d'accord. Ça nous rassure aussi alors dans ce cas. J'ai une autre question.

À 4.94, le Vérificateur parle que la DGSIG, là, la Direction générale des services informatiques... a «apprécié globalement, en 2001, la vulnérabilité [encore là] et l'efficacité de sa stratégie de sécurité en fonction d'une norme reconnue et, depuis, procède à des travaux complémentaires [pour] répondre à des besoins ponctuels. Par ailleurs, elle est en train de s'approprier de nouveaux outils pour poser de meilleurs diagnostics...» Et, un peu plus tard, on dit: «Il lui reste à prendre les mesures nécessaires afin que les évaluations soient dorénavant conduites de façon périodique et indépendante. Elle devra en outre se doter d'outils qui assurent la prise en charge de toutes les vulnérabilités.»

À votre avis, à la suite de ça, vous jugeriez quelle périodicité pour vous assurer de ces évaluations régulières? À quelle période, à quelle fréquence est-ce que ça devrait être fait?

M. Brulotte (Raynald): Mme la Présidente, je dirais, au fond, dans un monde idéal, il n'y a pas de périodicité, ce seraient toutes les composantes, à chaque année, qui devraient faire l'objet d'une, j'allais dire d'une révision en profondeur. Mais vous comprendrez qu'avec, je veux dire, on a quand même des moyens limités, alors ce qu'on essaie de faire, c'est de prendre au moins une composante dans nos infrastructures et d'en faire l'analyse. Au moment où on se parle, la composante qui fait l'objet de nos préoccupations, si je peux dire...

La Présidente (Mme Dionne-Marsolais): Cette année?

M. Brulotte (Raynald): ...cette année, en 2004-2005, c'est le réseau local, parce que vous savez que souvent les vulnérabilités, souvent ça arrive de l'interne. Alors, on est en mesure...

La Présidente (Mme Dionne-Marsolais): Le réseau local étant dans un ministère...

M. Brulotte (Raynald): Oui, oui, oui, oui, oui.

La Présidente (Mme Dionne-Marsolais): ...du gouvernement ou du conseil?

M. Brulotte (Raynald): Non, non, non, le réseau local du serveur gouvernemental, la direction générale des technologies d'informatique et des communications.

Stratégie de gestion du SCT en regard de la sécurité informatique gouvernementale

La Présidente (Mme Dionne-Marsolais): O.K. Dans les commentaires du Secrétariat du Conseil du trésor concernant l'encadrement central, il y a une phrase qui m'a étonnée, et j'aimerais ça qu'on me l'explique. À la page 99 du rapport, bon, on parle évidemment de l'encadrement, on parle du domaine de confiance et on dit: «...le secrétariat travaille actuellement à soutenir les ministères et les organismes dans la mise en place d'une méthode et d'un outil permettant de mesurer les risques auxquels ils feront face pour mieux les suivre ultérieurement.» On en a parlé avec le député de Verdun. Et on dit: «Une fois ce travail terminé, l'étape suivante serait l'élaboration et l'implantation graduelle d'un modèle de gestion de la performance de sécurité. Cependant • et c'est cette phrase-là qui me préoccupe • il faut noter que l'élaboration d'un tel modèle constitue un défi de taille, puisqu'il s'agit d'une nouveauté sur la scène internationale.»

Expliquez-moi ça parce que ça a attiré mon attention, ça. En quoi est-ce que c'est une nouveauté? On n'est pas les seuls à se préoccuper de ça, j'imagine? Mme Thiboutot.

n *(11 h 10)* n

Mme Thiboutot (Louise): Oui, Mme la Présidente. Alors, effectivement, nous ne sommes pas les seules à se préoccuper de l'évaluation de la performance et d'amener aussi des indicateurs de gestion pour mesurer cette performance-là, sauf que présentement nous sommes tous en même temps à faire cette évaluation-là. Il n'y a pas d'outil actuel qui généralise des objets et qui nous permettrait de dire: Oui, c'est tel indicateur qui devrait être évalué ou tel indicateur. Et chacun aussi doit s'approprier, dépendant des résultats des analyses de risques, qu'est-ce qu'on va vouloir évaluer. Alors, on ne veut pas évaluer tout. Il faut préciser qu'est-ce qui est le plus important à évaluer, dans quelle mesure on peut la mesurer.

Alors, on ne fait pas d'indicateur pour faire des indicateurs, il faut être capable d'aller sur le terrain et de pouvoir vérifier cette mesure qui va nous donner, là, les résultats de notre vérification. Alors, quand on dit qu'à l'échelle internationale il n'y pas d'élément pour nous aider présentement, c'est dans le sens que ce n'est pas tout fait. Il n'y a rien de fait d'avance. On ne peut pas partir puis dire: Oui, on va utiliser ça ou on va utiliser ça. Alors, il faut vraiment faire l'évaluation de qu'est-ce qu'on veut mesurer, valider le type d'indicateurs qu'on va pouvoir mettre en place et par après les mesures qu'on va prendre pour évaluer ces mesures-là.

La Présidente (Mme Dionne-Marsolais): C'est un peu ce que vous avez dit dans vos commentaires. Où en êtes-vous dans les études d'impact de ces outils de gestion, d'indicateurs, en fait?

Mme Thiboutot (Louise): En fait, le projet en soi va démarrer au mois de décembre, ce qui veut dire qu'au mois de mars on devrait avoir beaucoup plus d'informations à cet effet-là. C'est sûr qu'on fait une vigie régulière, hein? On est sur tous les sites des gouvernements américains, des gouvernements européens pour voir, même dans l'entreprise privée, qu'est-ce qui se fait. Alors, on récupère ces informations-là, mais le projet en tant que tel va démarrer seulement qu'en décembre de cette année.

La Présidente (Mme Dionne-Marsolais): Qui sont les leaders dans l'industrie?

Mme Thiboutot (Louise): En termes de sécurité?

La Présidente (Mme Dionne-Marsolais): Oui. Bien, par rapport à ces indicateurs de performance de... informatique.

Mme Thiboutot (Louise): Bien, on voit que, du côté de la Grande-Bretagne, du côté de la sécurité, ils sont quand même assez bien organisés. La Nouvelle-Zélande aussi s'organise...

La Présidente (Mme Dionne-Marsolais): Au niveau des gouvernements.

Mme Thiboutot (Louise): Au niveau des gouvernements. Mais les banques aussi se donnent les moyens beaucoup pour le volet financier et le renseignement personnel. Mais, nous, dans le fond, nos comparaisons, on les fait beaucoup avec les gouvernements plutôt.

La Présidente (Mme Dionne-Marsolais): D'accord. Mme la députée de Chauveau.

Nombre de services de certification gouvernementaux

Mme Perreault: Oui. Alors, merci beaucoup, Mme la Présidente. Moi, d'abord je vous souhaite la bienvenue. Et je vous réfère au paragraphe 4.39 du rapport du Vérificateur général qui concerne l'instauration des premiers services de certification. Il est dit, là-dedans, que la lenteur, la mise en place de ces services-là a fait en sorte qu'il y a une multiplication de ces mêmes services là. Et, tout à l'heure, à la page 6 de votre allocution, M. le secrétaire du Conseil du trésor, vous nous dites qu'il y a une fusion entre deux services, soit celui du ministère de la Justice et celui du secrétariat.

Alors, ma question a deux volets. D'une part, est-ce qu'il existe actuellement d'autres services à l'intérieur même du gouvernement ou en fait dans les sociétés connexes au gouvernement? Et, oui, dans le fond c'est ça, ma question: Est-ce qu'il en existe d'autres? Puis, s'il en existe d'autres, pourquoi ne pas les fusionner, parce que, tout à l'heure, on a discuté avec le Vérificateur général et on se posait la question?

M. Meunier (Luc): ...

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot.

Mme Thiboutot (Louise): Oui. Il n'y en a que deux. Il n'y a que deux services de certification, que l'on retrouve au ministère de la Justice et à la Direction générale des télécommunications, et il y a eu décision de les fusionner. Et c'est ce qui est en train de se faire présentement.

La Présidente (Mme Dionne-Marsolais): Mme la députée de Chauveau.

Possibilité d'utilisation des services gouvernementaux de certification actuels

**par la Société de l'assurance automobile
et la Chambre des notaires**

Mme Perreault: Merci, Mme la Présidente. Tout à l'heure, lors d'une discussion avec le bureau du Vérificateur général, il a été question de la Société de l'assurance automobile du Québec de même que de la Chambre des notaires, pour citer ces deux exemples-là, qui ont accès peut-être aux services gouvernementaux et qui pourraient peut-être • et je pose la question • fusionner aux services actuels ou peut-être que ce n'est pas possible de le faire. Parce que peut-être que, concernant la Société de l'assurance automobile du Québec, il est peut-être question des mandataires de la Société de l'assurance automobile du Québec. Mais j'aimerais que vous répondiez à cette question-là.

La Présidente (Mme Dionne-Marsolais): Oui, Mme Thiboutot ou M. Brulotte.

M. Brulotte (Raynald): Oui, effectivement la Société de l'assurance auto nous a contactés il y a déjà, je dirais, peut-être une année, une année et demie, en vue effectivement d'utiliser les services de certification que la direction générale a développés, services de certification qui vont être fusionnés avec les services de certification du ministère de la Justice. Donc, il n'y aura plus qu'une seule autorité de certification au sein de l'administration gouvernementale. Mais effectivement la Société de l'assurance auto, pour effectivement sécuriser les échanges électroniques entre elle-même et ses mandataires, je veux dire, explore actuellement la possibilité d'utiliser l'infrastructure à clé publique, là, qui est une technologie de sécurisation des échanges électroniques qui requiert effectivement des certificats. Donc, la Société de l'assurance auto explore la possibilité d'utiliser ce service-là pour sécuriser ses échanges.

La Présidente (Mme Dionne-Marsolais): Mme la députée de Chauveau.

Mme Perreault: Donc, ce que je comprends de vos propos, c'est qu'il n'est pas exclu qu'éventuellement la Société de l'assurance automobile du Québec puisse être certifiée par le même système, là.

M. Brulotte (Raynald): Ah, non, non, absolument pas. Absolument pas.

Mme Perreault: Ou utilise le même système, là.

M. Brulotte (Raynald): C'est ça. C'est ça. On se comprend bien quand même: la Société de l'assurance auto ne serait pas une autorité de certification. C'est un client, un ministère ou un organisme comme un autre qui a des besoins de sécurisation qui requièrent l'utilisation d'un dispositif, j'allais dire de sécurité de niveau moyen ou plus élevé. À ce moment-là, donc c'est un client comme les autres ministères et les organismes.

La Présidente (Mme Dionne-Marsolais): Mme la députée de Chauveau.

Mme Perreault: Maintenant, quant à la Chambre des notaires, est-ce que c'est aussi le même cas que la Société de l'assurance automobile du Québec?

La Présidente (Mme Dionne-Marsolais): M. Brulotte.

M. Brulotte (Raynald): Oui, c'est-à-dire que la Chambre des notaires, en rapport avec le ministère de la Justice, a déjà, j'allais dire • ça s'appelle Notarius, notamment • alors le... C'est-à-dire, le ministère de la Justice, vous le savez peut-être que le ministère de la Justice, quelque part comme en 1998, a implanté le RDPRM, le Registre des droits personnels et réels mobiliers, et ce service-là, cette application-là requérait justement l'utilisation de la technologie qu'on appelle l'infrastructure à clé publique. Et donc, dans le service du RDPRM qui a été développé, il y a l'utilisation imbriquée donc dans l'application, il y a utilisation d'un service de certification. C'est pourquoi le ministère de la Justice, dès 1998, a mis en place un service de certification.

Et effectivement la Chambre des notaires, il y a quelque temps, a été contactée par justement nos collègues du Secrétariat du Conseil du trésor, et il y aurait possibilité de, j'allais dire d'utiliser la Chambre des notaires comme une sorte de partenaire dans la gestion du service de certification du ministère de la Justice. Mais ces pourparlers-là, c'est davantage du côté du ministère de la Justice, je crois, que ces pourparlers-là ont cours actuellement.

Mme Perreault: Mais excusez ma...

Mme Thiboutot (Louise): ...complément d'information.

La Présidente (Mme Dionne-Marsolais): Oui, Mme Thiboutot.

Mme Perreault: Parce que ce n'est pas facile à comprendre.

Mme Thiboutot (Louise): Bien, oui, c'est compliqué, effectivement. On s'y perd facilement. Alors, bien, premièrement, la Chambre des notaires, on travaille avec eux pour la vérification d'identité, on s'entend? Donc, c'est pourquoi on entend souvent parler de la Chambre des notaires dans le cadre de l'infrastructure à clé publique gouvernementale. C'est qu'ils sont utilisés pour faire la vérification d'identité pour la délivrance des certificats.

Pour ce qui est de leur infrastructure à clé publique dont c'est Notarius, là, qui en a la responsabilité, c'est avec le registre foncier que le volet de certification est utilisé. Nous n'utilisons pas, nous, en tant qu'infrastructure à clé publique, l'infrastructure de Notarius.

La Présidente (Mme Dionne-Marsolais): Bien, ça n'a pas l'air, là, Mme la députée de Chauveau. Non, mais je suis d'accord avec elle. D'accord. M. le député de Montmorency.

M. Bernier: Alors, bonjour. Merci d'être ici, ce matin... Vérificateur général, les gens du secrétariat. Mais justement, en complément là-dessus, vous mentionnez, au niveau des orientations en matière d'authentification qui ont été approuvées en août 2004: Et le développement du Service québécois d'authentification gouvernementale qui a débuté en septembre 2004 sera grandement implanté à compter de l'automne 2005. C'est ce que le secrétaire mentionne. On sait qu'au niveau authentification il y a beaucoup d'investissements qui sont faits par des ministères et des organismes. Pensons au ministère du Revenu, hein, qui investit beaucoup d'argent dans ce sens-là; pensons à la Société de l'assurance automobile aussi, hein, où il y a beaucoup d'éléments qui sont utilisés pour contacter l'information, pour transiger au niveau de l'information.

n *(11 h 20)* n

Moi, j'aimerais vous entendre là-dessus parce que c'est quand même des sommes importantes, là. Puis j'aimerais voir de quelle façon on va développer l'authentification. Parce que souvenons-nous que le NAS, le fameux NAS du gouvernement canadien, hein, qui, à un moment donné, a été la clé dans plusieurs, pendant plusieurs années • je remonte dans mes années passées au gouvernement...

Une voix: ...

Stratégies du SCT quant à l'authentification dans les ministères et organismes

M. Bernier: ...oui, je suis jeune • mais il reste qu'avec le temps ça s'est estompé, bon, on a découvert toutes sortes de problèmes, toutes sortes de choses. Donc, on s'en va où avec ça, en ce qui regarde l'authentification par rapport au développement de chacun des ministères et organismes au niveau de leurs besoins, transiger avec le public, puis, quand on parle de gouvernement en ligne, bien d'autant plus, hein? Donc, j'aimerais vous entendre sur ça, là. Et ça pourra peut-être renseigner en partie de ce que vous avez besoin.

La Présidente (Mme Dionne-Marsolais): M. le secrétaire.

M. Meunier (Luc): C'est toute la question du service québécois d'authentification que Mme Thiboutot pilote.

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot, on vous écoute.

Mme Thiboutot (Louise): D'accord.

La Présidente (Mme Dionne-Marsolais): On va prendre un cours d'authentification.

Mme Thiboutot (Louise): D'authentification. Alors, on a répondu, M. Meunier répondait dans le sens que tout d'abord, cette année, on s'est dotés d'une stratégie d'authentification sur l'ensemble des ministères et organismes. La stratégie en fait donne les grandes balises d'authentification, les façon de vérifier l'identité, dépendant du niveau de confiance qu'on veut donner ou que les ministères doivent donner aux services, là, qu'ils vont mettre en ligne. Également, ça comprend le guide pour savoir les mesures

qui seront nécessaires pour assurer le niveau de confiance désiré et également, si on fait de la vérification d'identité à distance ou sur place, donc de rencontrer les gens pour vérifier leur identité.

Donc, toutes ces grandes orientations-là viennent baliser, auprès des ministères et organismes, la façon dont eux doivent réaliser l'authentification dans leur ministère et organisme. Ils ont ces balises-là. On s'est aussi donné une stratégie qui est le Service québécois d'authentification. Ce qu'on s'est dit, c'est qu'il ne faut pas avoir 22 systèmes d'authentification, là, il faut faciliter la tâche des citoyens. Ça c'est le premier élément. Et il faut aussi avoir une cohérence au niveau des mesures de sécurité qui vont venir finalement donner la confiance à nos citoyens par rapport à ça.

Donc, on s'est donné, comme stratégie, de mettre en oeuvre un service d'authentification, de le développer et de demander aux ministères et organismes d'utiliser ce service d'authentification plutôt que d'en développer un dans chacun des ministères et organismes. Alors ça, ce sont les grandes stratégies.

En termes de principes, c'est que, sur le plan de l'authentification et du service d'authentification, c'est certain qu'on veut harmoniser les façons de faire, on veut avoir de la cohérence, on veut aussi utiliser des mesures qui font partie des grandes normes internationales et qui sont aussi déjà bien établies et déjà bien contrôlées, si vous voulez.

Une voix: À l'épreuve du temps.

Mme Thiboutot (Louise): Oui, à l'épreuve du temps. On n'utilise pas des technologies, là, qui «pop-up» à tous les jours, là. On ne peut pas, en tant que gouvernement, se donner des outils comme ça. On doit en avoir, là, qui ont fait leurs preuves. Alors, c'est ce sur quoi sera basé le Service québécois d'authentification.

La Présidente (Mme Dionne-Marsolais): Merci. M. le député de Montmorency.

M. Bernier: Vous comprendrez qu'en ce qui regarde cet élément-là au niveau du public, c'est un élément fort important quand on regarde toutes les problématiques qui peuvent arriver dans le cadre des transactions, et c'est toute la confiance à donner. On pense au niveau d'Internet; les gens, quand ils transigent, ça prend une confiance, ça prend des éléments de sécurité.

Et, dans le domaine de la fiscalité, bien vous avez parlé, tout à l'heure, avec le gouvernement: À ce sujet, il est important de noter que ce système sera compatible avec le système du gouvernement du Canada, hein, ce qui permettra aux citoyens d'utiliser les mêmes codes pour les deux gouvernements. Donc, pensons au moment de la préparation de notre rapport d'impôts; comme on en a deux à faire, donc d'avoir des systèmes d'authentification qui seraient identiques, ça faciliterait grandement le travail des gens.

Je veux revenir sur un élément. J'ai encore du temps, madame?

La Présidente (Mme Dionne-Marsolais): Pratiquement pas, non.

Travaux du SCT portant sur les normes de sécurité interne s'adressant aux ministères et organismes

M. Bernier: Pratiquement pas. Bon. J'aurais aimé vous entendre, moi, sur la participation des directions de vérification interne en ce qui regarde la sécurité informatique. Est-ce qu'il y a des normes? Est-ce qu'il y a des choses à venir là-dedans? Parce qu'on sait que la vérification interne va fêter bientôt ses 30 ans. Et est-ce qu'on va utiliser davantage ces gens-là de façon à s'assurer à l'intérieur, parce qu'ils ne sont pas tous homogènes, à l'intérieur des ministères et des organismes? Et la sécurité informatique ne l'est pas non plus.

Donc, est-ce qu'il y a des éléments de réflexion? On parlait de travailler avec les gens de l'extérieur, mais, de l'intérieur, on a quand même ces services-là, là, qui existent depuis plusieurs années, où on a formé du personnel, où on a de la compétence, où on a développé de l'expertise. J'aimerais ça vous entendre sur ça.

La Présidente (Mme Dionne-Marsolais): ...peut-être que le secrétaire du Conseil du trésor qui pourrait peut-être émettre un avis là-dessus. M. le secrétaire.

M. Meunier (Luc): Actuellement, il y a déjà eu, par la présidente du Conseil du trésor, une intention bien, bien claire de réactualiser ou d'ajouter, dans le fond, des préoccupations dans les mandats de vérification interne. Actuellement, le Secrétariat du

Conseil du trésor élabore, dans le fond, des travaux pour élargir, je dirais, les mandats ou élargir les rôles que doit jouer la vérification interne dans chacun des ministères. Et la question de la sécurité informatique fait partie, dans le fond, des discussions, là, dans les travaux, qui seront connus prochainement et que le Secrétariat du Conseil du trésor publiera prochainement, sur les nouvelles balises au niveau de la vérification interne.

Exigences de vérification interne pour chaque ministère

La Présidente (Mme Dionne-Marsolais): Merci. Sur ce point-là, est-ce que le Conseil du trésor a, dans ses exigences par rapport à l'ensemble des ministères, cette exigence de vérification interne dans tous les ministères, au moment où on se parle? Et sinon, est-ce qu'elle l'a déjà eue, parce que ce que vous nous dites, c'est qu'elle va établir des balises?

M. Meunier (Luc): Il existe déjà des exigences de vérification interne. Chaque ministère doit, je dirais, s'approprier une direction, un service de vérification interne et doit procéder à des vérifications au sein de la gestion de ses ressources. L'étendue de ça est balisée déjà par des normes, des directives du Conseil du trésor. C'est la portée, je dirais, de cette vérification interne là qui fait partie de travaux actuellement au Secrétariat du Conseil du trésor que Mme la présidente du Conseil du trésor avait annoncés dans son plan de modernisation qu'elle a publié au printemps dernier.

La Présidente (Mme Dionne-Marsolais): Mais, dans les faits, est-ce que vous avez un moyen de vous assurer qu'il y a des équipes de vérification interne en place?

M. Meunier (Luc): Je ne sais pas si... Il y a peut-être Marc Laurin, qui est en charge de la sécurité et anciennement vérificateur interne...

Une voix: ...

La Présidente (Mme Dionne-Marsolais): M. Laurin.

M. Laurin (Marc): ...comité des responsables de vérification interne, là, ça me fait plaisir d'entendre parler de ça. Alors, moi, comme réflexe, là, autant pour des qualifications que pour des bilans de sécurité, j'ai eu le réflexe, dans les exigences, de demander au sous-ministre qu'ils associent, par exemple, la vérification interne pour s'assurer de la fiabilité de l'information qu'ils communiquaient au Conseil du trésor, parce que c'est beau de demander des déclarations volontaires, mais il faut s'assurer que l'information, elle est fiable.

Maintenant, des directions de vérification interne, il y en a présentement, justement suite à l'appui du Conseil du trésor, dans à peu près tous les ministères et organismes, même les petits. Il y a tout le temps, à tout le moins, un responsable, et donc c'est positif. Et aussi je dirais que, dans les dernières années, le Secrétariat du Conseil du trésor est souvent allé rencontrer le comité des responsables de vérification interne, a rencontré des ministères et s'associe avec eux surtout pour développer la vérification interne dans le domaine des TI, parce que ce n'est pas facile d'avoir des spécialistes de vérification non seulement de vérification générale, mais spécialisés dans le domaine des TI. Et ce phénomène-là est mondial. On a eu la chance de participer à un groupe qui est reconnu comme consultant mondial, qui est le groupe Gartner, Gartner Group, et c'est aussi une préoccupation des grandes entreprises, des grands gouvernements de ce monde, d'avoir des gens de vérification mais spécialisés dans le domaine des TI.

Alors, nous, on collabore beaucoup à former les ministères et organismes. On organise des séminaires ou des activités de formation, et tout ça. On s'associe avec des groupements, aussi, professionnels, comme l'Association des professionnels de vérification interne, qui est un chapitre d'une association internationale qui est l'ISACA. Donc, oui, on s'associe, les gens de VI, par rapport à la vérification de la sécurité.

Dépenses assumées par les différents ministères et le SCT pour des services de certification

La Présidente (Mme Dionne-Marsolais): Merci. Avant de passer la parole à ma collègue de Marie-Victorin, j'ai une question pour compléter l'information que le député de Montmorency vous a demandée. À 4.39, là, on a • c'est-à-dire la députée de Chauveau, je crois • on a parlé des services de certification et on dit: «Cinq ans après l'instauration des premiers services de certification, les orientations gouvernementales demeurent imprécises au regard de l'authentification...» Vous avez répondu à tout ça.

Ce que je voudrais vous poser comme question: À votre connaissance • et, si vous ne pouvez pas me répondre aujourd'hui, vous pourriez nous répondre plus tard • quel a été le coût, disons, assumé par les différents ministères, que ce soit Justice, l'organisme de la SAAQ ou même la Chambre des notaires, pour se doter des services de certification afin de répondre aux besoins urgents de leurs organismes et de leurs ministères? Combien ça leur a coûté? Et combien, autrement dit, combien vous-mêmes ensuite avez investi pour vous doter de services de certification? Parce que ce que je comprends de ce paragraphe-là, c'est que vous n'avez pas réagi avec suffisamment de rapidité pour assumer, si vous voulez, le leadership qui vous revenait en fonction • c'est l'interprétation que j'en fais, là • en fonction des services de certification au niveau de l'ensemble du gouvernement? Est-ce que je me trompe? Et est-ce que vous pouvez nous fournir cette information-là?

n *(11 h 30)* n

M. Meunier (Luc): Au niveau du coût du service d'authentification développé chez la direction générale de M. Brulotte, peut-être on a les données.

M. Brulotte (Raynald): Oui. Les services de certification proprement dite, qu'on a mis en place à compter de 1999, c'est autour de 2 millions de dollars que ça a coûté. Évidemment, c'est cumulatif, là.

La Présidente (Mme Dionne-Marsolais): Comme investissement initial?

M. Brulotte (Raynald): Non, non, non.

La Présidente (Mme Dionne-Marsolais): Au total?

M. Brulotte (Raynald): J'inclus là-dedans, là, les salaires, là, les coûts de développement, et puis ensuite l'opération comme telle, c'est environ...

M. Meunier (Luc): ...

M. Brulotte (Raynald): Le service de certification du Secrétariat du Conseil du trésor qui va être fusionné avec les services de certification du ministère de la Justice.

Fusion des autres services de certification et du service de certification du Secrétariat du Conseil du trésor

La Présidente (Mme Dionne-Marsolais): Bon. Ces autres services là, à ce moment-là, le travail qu'eux ont fait • parce qu'il dit bien, dans ce paragraphe-là, que deux services avaient été créés pour répondre aux besoins urgents des ministères • les services qu'ils ont créés, eux, et les efforts qu'ils ont investis, est-ce que vous allez pouvoir vous en servir?

M. Brulotte (Raynald): Ah, tout à fait.

La Présidente (Mme Dionne-Marsolais): Oui?

M. Brulotte (Raynald): Oui, oui.

La Présidente (Mme Dionne-Marsolais): Oui.

M. Brulotte (Raynald): Oui, oui, c'est complètement récupéré.

La Présidente (Mme Dionne-Marsolais): Donc, ce n'est pas perdu.

M. Brulotte (Raynald): Non, non, pas du tout, pas du tout, pas du tout. Il y a même un transfert d'actif parce que ce sont des licences, hein? Le service de certification, c'est d'abord et avant tout des licences qu'on achète auprès d'un fournisseur, dans ce cas-ci, Entrust, et ce transfert d'actif là est en cours actuellement vers le ministère de la Justice.

Délais concernant la mise en place

de l'infrastructure à clé publique

La Présidente (Mme Dionne-Marsolais): Est-ce que vous pouvez nous dire pourquoi ça a pris tant de temps, parce que d'après ça on peut estimer à peu près à cinq ans, là, les délais, là, avant d'avoir établi les orientations gouvernementales et puis avoir pris le leadership? Pourquoi ça a pris tant de temps au Conseil du trésor?

Mme Thiboutot (Louise): ...

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot, peut-être.

Mme Thiboutot (Louise): Je vais répondre en partie, et peut-être, Raynald, tu compléteras.

La Présidente (Mme Dionne-Marsolais): Parce que, dans l'ensemble du rapport, là, vraiment on ressent, on a l'impression • on se trompe peut-être • mais on a l'impression qu'il y a une grosse faiblesse au niveau de la planification, au Trésor, au niveau des systèmes informatiques, là, je parle.

Mme Thiboutot (Louise): Bon. Alors, pour répondre à ce volet-là, bien, premièrement, c'est complexe, l'infrastructure à clé publique. Et, d'année en année, c'est certain qu'en 1998, quand on a déterminé la mise en place, là, de l'infrastructure à clé publique gouvernementale, on s'était donné des grandes balises, dont une était officiellement d'avoir l'infrastructure, une infrastructure commune gouvernementale. Alors, déjà là, c'était la meilleure proposition, là, qui a été faite et la meilleure recommandation. Sans ça, ça se serait multiplié.

Au fur et à mesure, c'est qu'effectivement d'un côté les ministères et organismes n'étaient pas prêts, dans leur démarche, à évaluer le niveau de sécurité nécessaire. Donc, ils n'avaient pas vraiment besoin, en 1998, de ce niveau de sécurité là. C'était progressivement, là, que le besoin s'est fait ressentir. Et donc, au fur et à mesure, on a délivré des certificats pour certains ministères et organismes qui en ont vraiment eu besoin. On pense à la SAAQ, on pense au ministère de la Justice, on pense également à la Sûreté du Québec. Alors, c'est vraiment des volets très précis. C'est un très haut niveau de sécurité quand on embarque dans les certificats. Alors, la majorité des autres ministères utilise encore l'authentification avec identification mot de passe, et ça demande des études assez, je dirais, importantes, pour décider qu'on va vers un service de certification, parce que les impacts sont grands. Donc, ça, c'est un volet.

L'autre volet, c'est qu'en 2001-2002 on a évalué d'élargir la portée de la directive. Donc, la première portée était pour les employés, les mandataires et les partenaires. Donc, ça, ça existe toujours; on appelle ça la phase intérimaire des services de certification. Actuellement, c'est ce qu'on utilise et c'est uniquement pour ces clientèles-là. En 2002, donc 2001-2002, on a évalué d'élargir aux citoyens et entreprises. Alors, ça a été une étude qui nous a confrontés à une réalité, là, qui est encore présente aujourd'hui • Gartner en parlait encore récemment • ce sont les coûts élevés de la mise en place d'une telle infrastructure pour élargir à la communauté et aux citoyens. Alors, à l'époque, c'étaient des chiffres de 30 millions d'investissement. Alors, ce pourquoi on s'est ravisés, c'est pour ça: c'est qu'on n'était pas en mesure d'investir 30 millions il y a deux ans, là, mais pas du tout. Alors, on s'est...

La Présidente (Mme Dionne-Marsolais): Par rapport aux coûts-bénéfices, là?

Mme Thiboutot (Louise): Par rapport aux coûts-bénéfices. Parce que, pour le citoyen, il faut comprendre qu'on ne leur fera pas payer leur certificat, hein? Bon. Alors donc, c'est sous l'épaule du gouvernement, là, qu'on doit investir tous ces argents-là. Alors, on a évalué, on s'est retournés, on a dit: O.K., on a cette évaluation-là; maintenant, on va regarder autre chose.

Entre temps, le gouvernement fédéral a travaillé le même processus. Il était un peu plus en avance au niveau du volet d'authentification et de certification auprès des entreprises et des citoyens. Et ils ont créé ce qu'ils appellent le «e-pass». Alors, le «e-pass», c'est un certificat numérique mais qui est beaucoup plus facile. On appelle ça un certificat itinérant. Donc, pour le citoyen, c'est beaucoup plus intéressant de pouvoir se situer partout, aller n'importe où, là, et avoir accès à son certificat. Donc, on a fait l'évaluation de ça, et c'est dans cette démarche-là qu'on a amené notre stratégie du SQAG, qui est le Service d'authentification québécois.

Alors, c'est certain qu'on n'a pas pris ces décisions-là, mais je crois que présentement on est contents de ne pas les avoir prises, là, ces décisions-là. C'était beaucoup d'investissement. Et encore aujourd'hui les grands groupes comme Gartner, Metagroup évoquent les mêmes choses: si vous voulez aller vers des services de certification, allez vers une autorité externe, là, pour aller chercher ces services-là, ne montez pas une autorité de certification.

La Présidente (Mme Dionne-Marsolais): Merci. Mme la députée de Marie-Victorin.

Travaux du SCT sur les normes de sécurité interne s'adressant aux ministères et organismes (suite)

Mme Vermette: Oui. Alors, moi, ce qui m'importe beaucoup, c'est la protection des renseignements personnels. Moi, j'ai été sur la commission en fait là-dessus, la Commission de la culture, puis on a travaillé beaucoup sur cette commission-là. Et en fait ce qu'on voit par rapport à ce que le Vérificateur a écrit à la page 98 en fait, «la protection des actifs informationnels des quatre entités soumises aux tests d'intrusion est [tout à fait] incomplète». Et il nous démontrait aussi l'importance de recourir périodiquement à une approche pour évaluer les limites du dispositif de sécurité.

Moi, j'aimerais bien savoir où est-ce que vous en êtes rendus par rapport à ça, faire périodiquement, en fin de compte, sur ces entités-là, comme le MRQ, la SAAQ, la RAMQ? Parce que dans le fond, si un de ceux-là ne fonctionne pas, c'est votre réseau aussi qui est mis en péril aussi parce qu'on peut finalement s'introduire. S'il y a une faille à une place, on diminue finalement sa puissance et sa sécurité finalement et puis on peut s'introduire et aller plus loin. Alors, moi, je pense que ça, c'est un des aspects très importants parce que ça touche à la sécurité aussi de l'information.

Alors, où est-ce que vous en êtes rendus par rapport à ça? Est-ce que vous travaillez en collaboration, à silos. Comment on fait?

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot.

Mme Thiboutot (Louise): Oui. Alors, comme je le mentionnais tout à l'heure, nous avons recommandé de suivre les entités à partir de l'an prochain. Alors, ce qui veut dire que les plans d'action... On leur demande de faire une analyse de risques formelle. Le ministère du Revenu en a fait plusieurs, la SAAQ aussi. Il en avait fait une parcelle et il proposait, là, d'en faire une également prochainement. Et enfin les entités vérifiées et les autres ministères et organismes devront faire leur analyse de risques et nous présenter un plan d'action. Ce n'est qu'à partir de ce moment-là qu'on pourra faire des suivis par rapport à leur plan d'action. Présentement, on n'a pas les mesures nécessaires ni l'équipe nécessaire pour pouvoir répondre à ce volet-là. Et c'est ce qu'on va mettre en place progressivement, là, au cours de l'année.

Mme Vermette: C'est-à-dire que ça, vers quand serait prêt finalement...

Mme Thiboutot (Louise): L'an prochain.

Tests d'intrusion

Mme Vermette: L'an prochain, déjà là. Pourrez-vous vérifier, faire régulièrement, allez-vous être capables de faire • comment on appelle ça? Il y a un terme particulier • des tests d'intrusion?

Une voix: Des tests d'intrusion.

La Présidente (Mme Dionne-Marsolais): M. Brulotte.

M. Brulotte (Raynald): Oui, effectivement. Effectivement, tout à l'heure, j'évoquais l'existence de la cellule de sécurité, là, le CERT. Et effectivement c'est le mandat de cette petite équipe là, de réaliser, de temps à autre, des tests d'intrusion ainsi que des analyses de vulnérabilité et puis de voir comment se comportent, j'allais dire nos réseaux, nos infrastructures quand on simule des attaques de l'intérieur. Mais Dieu sait que ces attaques-là sont bien réelles. Et puis, quotidiennement, cette cellule-là encore une fois réussit à endiguer, si je peux dire, ce problème-là.

Et puis peut-être un complément d'information, Mme la députée de Marie-Victorin, par rapport à l'inquiétude que vous formuliez tout à l'heure à l'effet que, si, à un moment donné, l'infrastructure d'un ministère est...

Mme Vermette: Pas solide, vulnérable.

n *(11 h 40)* n

M. Brulotte (Raynald): ...victime d'une intrusion • je tiens à rassurer les membres de la commission • le réseau de

télécommunications, tel qu'on l'a bâti avec le partenaire privé, offre un cloisonnement extrêmement étanche. C'est un cloisonnement virtuel, logique, un cloisonnement extrêmement étanche. Chaque ministère, au fond chaque organisme qui utilise l'infrastructure commune a au fond son propre réseau privé logique ou virtuel. Et, si jamais, par exemple, un ministère, par une faiblesse quelconque face à la zone hostile, est victime d'une intrusion, les dégâts n'iront pas au-delà de ce ministère-là.

Une voix: Ah non?

M. Brulotte (Raynald): Non.

Cas d'intrusion dans les systèmes informatiques du SCT

La Présidente (Mme Dionne-Marsolais): M. Brulotte, est-ce qu'à votre connaissance il y a eu des cas d'intrusion au Conseil du trésor dans les systèmes informatiques?

M. Brulotte (Raynald): C'est-à-dire, des cas d'intrusion, non; des tentatives d'intrusion, ça, il y en a...

La Présidente (Mme Dionne-Marsolais): À tous les jours.

M. Brulotte (Raynald): ...des centaines par mois.

La Présidente (Mme Dionne-Marsolais): D'accord. M. le député de Verdun. On va terminer là-dessus.

Notion du domaine de confiance

M. Gautrin: Merci, Mme la Présidente. Je vais rentrer sur un autre domaine que vous avez abordé dans votre rapport, M. le secrétaire général, qui est celui des domaines de confiance. Vous avez introduit, dans votre rapport, vous signalez que vous êtes en train de faire l'éducation actuellement au concept du domaine de confiance, c'est-à-dire un domaine dans lequel l'information peut circuler pour être protégée d'une manière absolument, avec le même degré de protection. Vous n'êtes pas sans savoir certainement que le MRCI est en train de penser à réviser la Loi sur la protection des renseignements personnels et à voir un concept en quelque sorte de faciliter, disons, tout en protégeant les renseignements personnels, de faciliter le circulation de l'information, les échanges d'information, d'où l'importance du concept de domaine de confiance et de la protection du domaine de confiance.

Alors, je ne sais pas si vous êtes en rapport avec cette démarche qui est faite actuellement et comment votre concept de domaine de confiance... être réenforcé si, disons, on facilite les échanges à l'intérieur de certains domaines gouvernementaux.

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot.

Mme Thiboutot (Louise): Alors, effectivement, depuis toujours, là, depuis l'entrée en vigueur de la directive et même avant, on travaille de très près avec le ministère des Relations avec les citoyens et l'Immigration. Alors, l'ensemble de nos travaux sont faits conjointement avec le MRCI, particulièrement avec le groupe, là, de M. Marc Lafrance avec lequel nous avons travaillé l'an dernier, dans le cadre d'un projet qui s'appelait administration électronique et les enjeux de la protection des renseignements personnels.

Alors, ce qu'on a fait, c'est qu'on a amené ce qu'on avait développé en termes de domaine de confiance en sécurité et on l'a amené en réflexion pour le volet de la protection des renseignements personnels. Alors, cette démarche-là a permis effectivement, là, d'amener ces concepts-là de périmètre de sécurité, à la fois un périmètre petit quand on parle d'un système ou un périmètre d'un ministère quand il est seul. Le domaine de confiance s'élargit au fur et à mesure qu'on va avec des services intégrés ou au fur et à mesure où c'est l'ensemble du gouvernement qui doit être protégé. Alors, toute cette notion-là a été amenée dans la réflexion du futur projet de loi.

M. Gautrin: Mais vous comprenez bien que • je pense que c'était la Vérificatrice générale qui avait donné cette image-là • dans un domaine de confiance... C'est le maillon le plus faible et si on étend l'échange d'information, d'où l'importance de restructurer et de bien baliser, à ce moment-là, la sécurité dans tout le périmètre du domaine de confiance.

Mme Thiboutot (Louise): Oui. Alors donc, les ministères ont des outils, ils ont déjà l'architecture gouvernementale de sécurité qui leur permet justement d'établir les périmètres et les mesures applicables.

M. Gautrin: Attendez, madame, je m'explique. Je vais terminer là-dessus. Oui, bien sûr chaque ministère a des outils, je sais bien que chaque ministère est responsable de sa sécurité, mais, à partir du moment où on a un domaine de confiance qui est multiorganisme ou multiministère, à ce moment-là, parce vous facilitez la circulation de l'information, il est important qu'il y ait quelqu'un qui s'assure que toute la barrière soit de la même résistance partout. Donc, je voulais m'assurer réellement...

Mme Thiboutot (Louise): Absolument.

M. Gautrin: ...que le Secrétariat du Conseil du trésor en soit conscient et s'assure qu'à l'intérieur tout, si je prends l'image de la barrière pour le champ de moutons, soit aussi rigide ou étanche, quel que soit le ministère qui est concerné.

Mme Thiboutot (Louise): Tout à fait. Alors, quand je disais, tout à l'heure, que les périmètres partaient de petits aux plus grands, à l'ensemble du gouvernement, oui, il y aura ces vérifications-là. Et aussi ce qu'il ne faut pas oublier...

M. Gautrin: Et le Conseil du trésor va les faire.

Mme Thiboutot (Louise): Le Conseil du trésor, oui, sera en mesure de pouvoir les faire.

M. Gautrin: Parfait.

La Présidente (Mme Dionne-Marsolais): M. le député de Montmorency.

M. Bernier: Donc, ça veut dire que, si un ministère décide d'ouvrir par rapport à une consultation de son fichier, de ses banques, O. K., à ce moment-là, vous allez être mis au courant qu'ils rouvrent l'information à un autre ministère ou à un autre organisme, c'est ça? Et vous allez vous assurer de l'homogénéité puis que les barrières sont là pour s'assurer de tout ça.

La Présidente (Mme Dionne-Marsolais): Mme Thiboutot.

Mme Thiboutot (Louise): Oui. En fait, c'est la CAI présentement qui joue ce rôle, effectivement. Et tous les ministères doivent présenter leurs projets...

M. Bernier: Oui, oui, effectivement, mais la CAI ne connaît pas nécessairement l'état de sécurité de chacun des ministères et des organismes. C'est pour ça que je vous pose la question.

Mme Thiboutot (Louise): Alors, oui, effectivement, il y a ce suivi-là, là, qui sera assuré par le Secrétariat du Conseil du trésor, mais il y a aussi des ententes qui seront signées. Donc, quand les ministères vont vouloir ouvrir, ça sera encadré par une entente qui sera disponible et qui précisera l'ensemble des mesures qui doivent être mises en place pour la sécurité.

M. Bernier: Parce que vous comprenez qu'actuellement il y a quand même des organismes qui sont davantage suivis • je pense à la Régie de l'assurance maladie du Québec • et où on a l'information de base en ce qui regarde les changements d'adresse, l'inscription, et tout ça. Donc, on connaît quand même les ministères et les organismes où les fichiers puis les banques de données sont intéressantes pour d'autres ministères et organismes aussi.

La Présidente (Mme Dionne-Marsolais): Alors, je vous remercie beaucoup. Je note que vous avez déposé le plan d'action du Secrétariat du Conseil du trésor concernant la gestion de la sécurité informatique. Aimeriez-vous faire quelques remarques en terminant?

M. Meunier (Luc): Bien, peut-être laisser la parole à notre responsable des technologies de l'information.

M. Desbiens (Robert): Bien, il est évident qu'on est préoccupés, tout comme vous, de la sécurité et qu'on va faire plus d'efforts, on va mettre tous les efforts en place pour répondre aux attentes des ministères, des citoyens et des entreprises. Et c'est également une préoccupation de tous les gouvernements, et on en est fiers, là, de pouvoir échanger avec les différents responsables de la sécurité à travers le Canada, pas juste au niveau international, mais on a une plateforme canadienne qui nous permet d'échanger.

Mme Thiboutot et son équipe siègent sur le comité. Donc, ça nous permet d'évaluer les bonnes pratiques et s'assurer que notre mise à jour est permanente, là, à ce niveau-là. Et on est très fiers de voir que notre guide a été retenu, à l'échelle canadienne, pour les évaluations, donc c'est dire qu'on prend notre place à ce niveau-là et on est sûrs de battre la mesure au niveau de la sécurité.

La Présidente (Mme Dionne-Marsolais): Iriez-vous jusqu'à dire que vous êtes parmi les deux, trois premiers si on interprète bien ce que vous nous dites, là? Puisqu'on se sert de certains de vos outils, ça doit être que vous êtes bons?

M. Meunier (Luc): À l'échelle canadienne... dans les comités, là, auxquels Robert et Mme Thiboutot participent, on est un peu leaders à ce niveau-là.

La Présidente (Mme Dionne-Marsolais): Alors, on vous félicite. M. le Vérificateur général, peut-être quelques commentaires avant de lever la séance.

M. Lachance (Renaud): Oui, seulement dire que le dépôt d'un plan d'action par le Secrétariat du Conseil du trésor, nous, on aime beaucoup ce genre de plan d'action parce qu'il prouve le sérieux de notre travail de vérification et la pertinence de nos recommandations. Et surtout ça dit que l'entité vérifiée montre un grand sérieux dans l'atteinte d'une meilleure gestion publique. Donc, on est bien heureux de ce dépôt.

La Présidente (Mme Dionne-Marsolais): Nous aussi. Et ça nous permet aussi de vous dire que nous allons vous réinviter dans le cadre de certains points de référence • je ne sais pas comment on dit ça en français, là • des checks points, là, mais en tout cas...

Une voix: Des vérifications ponctuelles.

La Présidente (Mme Dionne-Marsolais): Des vérifications; non, des rencontres ponctuelles pour un suivi. Alors, je vous remercie beaucoup. Et nous allons donc ajourner quelques minutes et continuer après, entre nous, si vous le permettez. Merci infiniment de votre disponibilité et de votre rigueur.

(Fin de la séance à 11 h 49)