VÉRIFICATEUR
GÉNÉRAL DU QUÉBEC

RAPPORT À L'ASSEMBLÉE NATIONALE POUR L'ANNÉE 2003-2004 TOME I

Chapitre 4

Gestion de la sécurité informatique

Vérification d'envergure gouvernementale

TABLE DES MATIÈRES

Les commentaires des entités apparaissent à la fin de ce chapitre.

Vérification menée par

Martin Lessard
Directeur de vérification

Yves Denis
Claude Dion
Clarence Kimpton
Anik Michaudville
Caroline Nadeau
Guy Perron

Sigles utilisés dans ce chapitre

AGSIN	Architecture gouvernementale de la sécurité de l'information numérique
CANQ	Conservateur des Archives nationales du Québec
CF	Contrôleur des finances
CT	Conseil du trésor
DGSIG	Direction générale des services informatiques gouvernementaux
DGT	Direction générale des télécommunications
MJQ	Ministère de la Justice du Québec
MRCI	Ministère des Relations avec les citoyens et de l'Immigration
MRQ	Ministère du Revenu du Québec
RAMQ	Régie de l'assurance maladie du Québec
RETEM	Réseau de télécommunication multimédia de l'administration publique québécoise
SAAQ	Société de l'assurance automobile du Québec
SCT	Secrétariat du Conseil du trésor
SQ	Sûreté du Québec

FAITS SAILLANTS

4.1 L'application de mesures de sécurité informatique adéquates est essentielle à la mise en œuvre 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.

4.2 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 leurs actifs informationnels. Pour ce faire, nos travaux ont porté sur celles qui contribuent le plus à l'atteinte des résultats escomptés et dont l'absence ou la défaillance sont susceptibles d'entraîner la multiplication des incidents.

4.3 Nos travaux ont été menés auprès du Secrétariat du Conseil du trésor (SCT) et de cinq autres entités auxquelles des responsabilités particulières ont également 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 (MRQ), la Société de l'assurance automobile du Québec (SAAQ) et la Régie de l'assurance maladie du Québec (RAMQ) ainsi que par deux directions spécialisées du SCT. La présente vérification s'est terminée en mars 2004.

4.4 L'information numérique et les échanges électroniques du MRQ, 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 la technologie que sur des processus bien établis.

4.5 Il appert que l'encadrement offert aux ministères et organismes est plutôt satisfaisant, même si le SCT doit améliorer certains points. Ainsi, le cadre de gestion est incomplet. 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, 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 gouvernementaux se multiplient, sans que la nécessité de chacun d'eux soit démontrée.

4.6 Quant à l'action propre aux entités, nous avons relevé quelques lacunes par rapport à l'encadrement qu'elles doivent assurer, en particulier le manque d'attention à l'égard du suivi de la performance de leur programme de sécurité. En outre, plusieurs processus consacrés à la protection des ressources informationnelles requièrent des améliorations. C'est le cas notamment de ceux qui servent à déterminer la vulnérabilité de l'entité, à planifier l'ensemble des activités en fonction des orientations et des risques, à baliser la sensibilisation et la formation des utilisateurs et des gestionnaires ainsi qu'à gérer adéquatement les mots de passe nécessaires à l'authentification des utilisateurs.

4.7 En ce qui a trait aux services communs d'infrastructure, le SCT n'a pas encore officialisé le cadre de gestion de la sécurité du réseau gouvernemental de télécommunication. Il n'exerce toujours pas les contrôles requis pour garantir la présence et l'efficacité des mesures visant à sécuriser ce réseau. Il n'est pas plus à même de veiller au maintien des services de traitement informatique sur toutes les plates-formes exploitées. Enfin, la planification des services communs que nous avons vérifiés est mal articulée et n'inclut pas l'élaboration d'indicateurs de performance.

4.8 Par ailleurs, nous avons réalisé des tests d'intrusion dans quatre entités pour sonder l'efficacité de leur dispositif 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. Nos travaux révèlent que la protection des actifs informationnels des quatre entités concernées est adéquate par rapport aux flux d'information qui proviennent du réseau Internet. Par contre, elle est moins efficace sur d'autres plans : la résistance des mécanismes de sécurité, la robustesse des mots de passe choisis par les membres de l'effectif, 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. Ainsi, un intrus serait 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.

4.9 Somme toute, notre vérification fait ressortir que les entités vérifiées s'appliquent à assurer la sécurité de leurs ressources informationnelles. 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.

VUE D'ENSEMBLE

4.10 Peu importe leur taille, les entités recueillent, conservent, utilisent et diffusent une quantité de plus en plus grande d'information numérique pour réaliser leur mission. Ces renseignements sont parfois de nature personnelle ou confidentielle et ils ont, dans certains cas, une valeur légale, administrative, économique ou patrimoniale. Par conséquent, ils doivent être protégés, car des atteintes à la sécurité sont possibles. Parmi celles-ci, il convient d'évoquer l'usurpation d'identité, l'intrusion dans les réseaux et les systèmes informatiques, le détournement de communications, l'altération du contenu des banques d'informations ainsi que l'arrêt intempestif d'opérations critiques. L'impact de telles situations peut être considérable. Il suffit de penser au respect de la vie privée, au maintien des services essentiels, à la conduite des activités courantes et à la productivité du personnel. Manifestement, l'application de mesures de sécurité adéquates est essentielle à la mise en œuvre des programmes gouvernementaux.

4.11 La sécurité informatique prend plus d'importance à mesure que le gouvernement en ligne se développe et que les communications électroniques, dont Internet, sont mises à profit. Un autre facteur de risque vient de l'existence d'outils technologiques peu coûteux et relativement accessibles, qui permettent à tout utilisateur quelque peu averti de perpétrer des attaques informatiques, voire de paralyser momentanément un système entier. Des études démontrent que le danger peut provenir tant de l'extérieur (personne étrangère à l'organisation) que de l'intérieur (membre de l'effectif). Enfin, l'utilisation quasi généralisée des technologies de l'information par les entités les rend maintenant dépendantes de ces précieux outils pour mener leurs activités.

4.12 Dans ce contexte, des mesures s'imposent pour maîtriser les risques au regard de la confidentialité[1], de l'intégrité[2] et de la disponibilité[3] de l'information numérique et des échanges électroniques. Afin de dresser un portrait étoffé des éléments visés par les divers moyens de protection, le SCT a circonscrit quatre grandes dimensions – juridique, humaine, organisationnelle et technologique – de la sécurité, dont le détail est présenté à l'annexe 2.

4.13 Par ailleurs, le SCT a élaboré en 1999 la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale*, entrée en vigueur en 2000, et mis à la disposition des ministères et organismes un modèle pour assurer une gestion adéquate en cette matière. Il leur est proposé d'établir d'abord leurs besoins à l'aide d'une classification[4] de l'information et

1. Propriété d'une information de n'être accessible qu'aux personnes autorisées.
2. Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée ni détruite sans autorisation.
3. Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
4. Détermination de la sensibilité d'une information et, conséquemment, de la protection à lui accorder.

d'une analyse de risques qui tiennent compte des valeurs, de la mission et des objectifs de chacun. Ils doivent ensuite évaluer leur dispositif de sécurité par rapport aux besoins établis, dresser un plan d'action global en y intégrant les correctifs requis et mener à bien les activités envisagées, y compris la sensibilisation et la formation de l'effectif. Enfin, on s'attend à ce qu'ils contrôlent l'efficacité des moyens déployés et qu'ils produisent un bilan annuel.

4.14 Le coût de la sécurité informatique est difficile à chiffrer puisqu'elle est l'affaire de tous. On sait toutefois que les dépenses de l'ensemble des ministères et organismes au chapitre des technologies de l'information et des communications électroniques ont totalisé quelque 950 millions de dollars en 2002-2003. Bien entendu, seule une partie de ces fonds a été affectée aux activités liées à la sécurité informatique, qui sont néanmoins essentielles à l'accomplissement de la mission du gouvernement.

Rôles et responsabilités

4.15 La responsabilité première de la sécurité informatique appartient aux ministères et organismes, qui doivent instaurer des mesures internes destinées à gérer les risques de même que les pertes ou dommages éventuels qui peuvent découler des incidents. Le cadre de gestion gouvernemental leur attribue une série d'obligations en matière de planification, d'évaluation des risques, de sensibilisation et de formation, de coordination, de suivi ainsi que de reddition de comptes. Il énonce également certaines exigences par rapport à la structure de gestion, telles la nomination d'un responsable de la sécurité informatique et l'assignation de la responsabilité de toute information numérique ou technologie de l'information à un détenteur dûment désigné.

4.16 Des responsabilités particulières sont aussi conférées en vue de favoriser la synergie à tous les niveaux. Ainsi, le Conseil du trésor (CT) et son secrétariat assument les rôles de gouverne et de coordination de la sécurité. À cette fin, ils sont chargés d'orienter sa mise en œuvre, d'en définir le cadre de gestion et de soutenir les ministères et organismes dans leur action. Ils sont conseillés par le Comité d'orientation stratégique sur la sécurité (COSS), qui est composé des représentants de divers ministères et organismes et dont le mandat est de dégager une vision gouvernementale. Le SCT offre aussi une gamme de services (développement, exploitation et télécommunications) aux entités concernées dans des environnements qui doivent être sécuritaires.

4.17 La directive sur la sécurité fait appel à d'autres acteurs : le ministère de la Justice du Québec (MJQ), pour élaborer le cadre légal assurant la sécurité juridique de la documentation et de l'information ainsi que la valeur juridique des communications et des transactions effectuées au moyen des technologies de l'information ; le ministère des Relations avec les citoyens et de l'Immigration (MRCI), pour mettre en place des règles pertinentes en matière d'accès aux

documents et de protection des renseignements personnels ; la Sûreté du Québec (SQ), pour évaluer les menaces et les risques stratégiques ainsi que pour collaborer aux enquêtes touchant les délits informatiques.

4.18 Deux autres entités complètent le groupe. Le Conservateur des Archives nationales du Québec (CANQ) contribue à l'établissement des normes et des exigences de sécurité en ce qui concerne la protection et la conservation de l'information ayant une valeur patrimoniale ou archivistique. Quant au Contrôleur des finances (CF), il conseille les ministères et les organismes budgétaires dans l'élaboration et la mise en place des mesures de sécurité lors du développement, de modifications importantes ou de refontes majeures des systèmes d'information à caractère financier.

OBJECTIFS ET PORTÉE DE NOTRE VÉRIFICATION

4.19 La présente vérification visait à établir si les cadres de gestion élaborés pour l'ensemble du gouvernement et pour chaque ministère ou organisme ainsi que l'action des entités qui assument des responsabilités particulières soutiennent adéquatement la mise en œuvre de la sécurité informatique au gouvernement. Nous cherchions en outre à évaluer si les ministères et les organismes ont mis en place les composantes majeures de la sécurité informatique. Nos travaux ont porté sur celles qui contribuent le plus à l'atteinte des résultats et dont l'absence ou la défaillance peuvent entraîner la multiplication des incidents. L'annexe 1 présente les objectifs de vérification et les critères d'évaluation retenus.

4.20 Des travaux ont été menés auprès de six entités qui doivent remplir des obligations spéciales, soit le SCT, le MJQ, le MRCI, le CANQ, le CF et la SQ. En ce qui a trait à l'appréciation des composantes, nous avons, d'une part, vérifié trois entités qui dépendent fortement de leurs ressources informationnelles pour réaliser leur mission, fournissent une importante prestation électronique de services et détiennent de l'information critique ou des renseignements personnels. Il s'agit du MRQ, de la SAAQ et de la RAMQ. À titre indicatif, les dépenses affectées aux technologies de l'information et aux communications électroniques de ces trois entités ont totalisé 237 millions de dollars en 2002-2003, soit 25 p. cent des sommes dépensées par les ministères et les organismes en ressources informationnelles. D'autre part, nous avons examiné les activités respectives de la Direction générale des services informatiques gouvernementaux (DGSIG) et de la Direction générale des télécommunications (DGT), toutes deux rattachées au SCT.

4.21 Par ailleurs, nous avons réalisé des tests d'intrusion dans quatre ministères et organismes afin d'éprouver l'efficacité du dispositif de sécurité déployé par ces entités. Pour ne pas accentuer les dangers auxquels celles-ci sont exposées, nous avons choisi de taire leur nom.

4.22 Nos travaux se sont déroulés d'octobre 2003 à mars 2004, mais certains des commentaires formulés portent sur des situations antérieures à cette période.

RÉSULTATS DE NOTRE VÉRIFICATION

4.23 D'entrée de jeu, il faut mentionner que l'information numérique et les échanges électroniques du MRQ, 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. Le niveau de protection obtenu repose beaucoup plus sur l'expertise et l'implication des employés ainsi que la technologie que sur des processus bien établis. Même si la dépendance par rapport aux technologies de l'information s'est accrue et que les dangers se sont multipliés, certains aspects de la gestion de la sécurité ont peu évolué. Nos travaux font ressortir que des activités aussi fondamentales que la classification de l'information et la gestion des risques font particulièrement défaut. L'efficacité des mécanismes d'authentification des utilisateurs devrait aussi être mieux contrôlée et, au besoin, améliorée.

Encadrement central

4.24 La section qui suit porte sur le cadre gouvernemental de gestion de la sécurité informatique ainsi que sur l'action des entités à qui l'on a confié des responsabilités particulières.

Cadre de gestion gouvernemental

4.25 Le cadre de gestion représente l'ensemble des moyens mis en œuvre pour soutenir la prise de décision en vue de l'atteinte des objectifs visés. Il est articulé autour d'une série de constituants – valeurs, objectifs, principes, responsabilités, règles et modalités de fonctionnement – qui conditionnent grandement la gouvernance d'une organisation ou d'un domaine d'activité.

4.26 L'établissement du cadre gouvernemental de gestion de la sécurité est principalement sous la responsabilité du CT. Plusieurs éléments de ce cadre ont été définis dans divers documents : des directives[5], la description d'une vision commune figurant dans l'*Architecture gouvernementale de la sécurité de l'information numérique* (AGSIN) ainsi que des standards divulgués sous forme de guides ou de pratiques recommandées.

4.27 Le cadre actuel respecte la plupart des exigences du modèle de référence que nous avons retenu, notamment une description exhaustive des rôles et des responsabilités des acteurs. Certains aspects pourraient cependant être améliorés de façon à mieux baliser la gestion globale de la sécurité.

5. Quatre directives dont l'une est de portée générale, soit la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale.*

On tarde parfois à élaborer les guides et les outils.

4.28 Comme il se doit, le cadre de gestion gouvernemental aborde plusieurs questions fondamentales telles la classification, la sensibilisation et la formation de l'effectif, la sécurité logique, la sécurité physique de même que la continuité de service. Toutefois, les guides et les outils appelés à soutenir l'application des principes énoncés tardent parfois à venir. Mal synchronisé avec l'entrée en vigueur, en 2000, de la directive sur la sécurité, leur développement s'est accéléré au cours des dernières années. Cela dit, le SCT ne dispose toujours pas d'un portrait d'ensemble du soutien qu'il veut offrir aux ministères et organismes et n'a pas encore fixé le calendrier qu'il entend respecter.

4.29 De plus, la notion de « domaine de confiance[6] », introduite pour mobiliser toutes les parties afin qu'elles répondent aux mêmes exigences de sécurité concernant un système ou un service donné, n'est pas encore intégrée dans la directive sur la sécurité. Cette situation ne favorise pas son appropriation par les ministères et les organismes, car les règles et les responsabilités afférentes n'y sont pas formellement définies. Il est donc possible que la protection des informations soit moindre lors d'échanges avec des entités dont les exigences à cet égard sont inférieures.

4.30 Enfin, les exigences gouvernementales en matière de suivi sont insuffisantes. Dans les faits, le suivi exercé par le SCT ne porte pas sur le respect de l'architecture commune qu'il a adoptée (l'AGSIN). Les activités réalisées en vertu du plan gouvernemental de sécurité ne sont pas non plus évaluées, ce qui ne permet pas de mesurer la performance des entités sur ce point.

4.31 Nous avons recommandé au Secrétariat du Conseil du trésor de s'assurer que le cadre gouvernemental de gestion de la sécurité informatique

- **comprend les guides et les outils nécessaires à l'application des principes généraux qui y sont énoncés;**
- **donne lieu à l'intégration de la notion de « domaine de confiance » dans la directive sur la sécurité;**
- **fixe des exigences plus explicites concernant le suivi.**

Responsabilités particulières

4.32 La directive sur la sécurité présente les responsabilités confiées en propre à quelques entités. Ces responsabilités sont cruciales, leur exercice influant directement sur la gouverne et la coordination des travaux. Nos observations et recommandations à cet égard concernent uniquement le SCT. Les autres entités ont réalisé les activités nécessaires pour assumer leurs obligations.

6. Cadre de gestion, activités et mesures, tous assujettis à une politique de sécurité administrée par une seule autorité.

Conseil du trésor et Secrétariat du Conseil du trésor

Le plan gouvernemental de sécurité ne précise ni les résultats attendus ni les indicateurs de performance afférents.

4.33 Le CT et son secrétariat sont tenus d'élaborer un plan gouvernemental de sécurité, qui fixe les attentes en prenant en compte les risques stratégiques. Pour 2002-2003, un tel plan a effectivement été adopté par le CT en avril 2002, à partir de la situation observée en 2000-2001 ; cependant, le plan pour 2003-2004 n'a été prêt qu'en décembre 2003. En outre, celui-ci ne mentionne que les activités à réaliser par le SCT dans l'année, sans préciser les résultats attendus à court et moyen termes ni inclure des indicateurs afin de mesurer ultérieurement la performance. Enfin, le choix des activités ne résulte pas d'un processus adéquatement structuré et documenté. Ce dernier assurerait leur arrimage non seulement avec la réalité des entités mais aussi avec les exigences de l'AGSIN et les cibles fixées au regard du développement du gouvernement en ligne.

4.34 L'élaboration d'un programme gouvernemental de sensibilisation et de formation de l'effectif n'a pas reçu une attention suffisante de la part du SCT, bien qu'il ait accompli des gestes en ce sens au cours de la dernière année. Des activités ponctuelles ont bien lieu pour répondre aux besoins immédiats et présenter les guides et autres outils destinés aux ministères et aux organismes, mais elles n'ont pas été encadrées par un programme semblable. Les responsables gouvernementaux n'ont donc pas l'assurance que leur action comble les besoins prioritaires communs au moment où ils sont ressentis.

4.35 Une seule indication concernant la sécurité a été donnée aux ministères et organismes sur le contenu obligatoire des contrats et ententes conclus avec les fournisseurs de services, les partenaires, les mandataires et les autres gouvernements. Elle renvoie au guide relatif aux ententes de sécurité suggérées lors des échanges électroniques entre les organisations ou des prestations électroniques de services. Or, il conviendrait de baliser la conduite à adopter en toutes circonstances. En effet, les diverses parties doivent être bien au fait des exigences de sécurité applicables, des conditions qu'elles ont à respecter et des sanctions prescrites, le cas échéant. Le peu de soutien offert aux entités accroît le risque que les obligations en matière de sécurité soient insuffisantes.

4.36 Par ailleurs, un « état de situation gouvernemental de la sécurité » est produit par le SCT à partir de données fournies par les ministères et organismes. Les deux derniers états couvraient les exercices 2000-2001 et 2001-2002 ; ils ont été soumis au CT avec un décalage de plus d'un an par rapport à la période visée. Même si ces documents étaient assez complets, leur utilité était néanmoins réduite, étant donné que le CT a été saisi tardivement de l'état des choses. Il faut voir aussi que pareil délai ne favorise pas la solution rapide des problèmes, d'autant plus que la divulgation aux entités des résultats globaux et des cibles gouvernementales qui en découlent n'était pas synchronisée avec le calendrier du cycle budgétaire.

L'évaluation de l'application de la directive sur la sécurité est en retard d'un an.

4.37 En 1999, le CT a confié à son secrétariat la responsabilité d'évaluer l'application de la nouvelle directive sur la sécurité au plus tard trois ans après son adoption. Aucune action à cet effet n'a pourtant été entreprise. Le SCT a décidé de surseoir à cette exigence, considérant que l'information présentée dans les états de situation qu'il prépare était suffisante. Or, les renseignements qu'on y trouve ne donnent pas un portrait exhaustif et fidèle quant à l'application de la directive. Seule une évaluation basée sur une réflexion formelle et approfondie permettrait d'accomplir la volonté du CT.

4.38 Le CT et le SCT sont également chargés de déterminer les services communs d'infrastructure à mettre en place. D'importants efforts ont été déployés concernant l'authentification[7] de ceux qui utilisent les systèmes informatiques, une fonction capitale lorsque les services sont personnalisés. Il convient alors de vérifier avec rigueur l'identité déclarée par les utilisateurs et de protéger convenablement les données sensibles qui sont échangées.

La nécessité de maintenir tous les services de certification actuellement offerts n'est pas démontrée.

4.39 Cinq ans après l'instauration des premiers services de certification[8], les orientations gouvernementales demeurent imprécises au regard de l'authentification à effectuer par les ministères et les organismes ainsi que des services de certification à offrir pour satisfaire leurs besoins immédiats et futurs. Cette lacune a conduit notamment à la multiplication des services. Tout d'abord, dans le cadre d'une phase intérimaire, deux services de certification ont été créés pour répondre aux besoins urgents des ministères et des organismes. En octobre 2001, un service externe a été accrédité afin de combler des besoins particuliers. On a également emprunté une autre voie en enclenchant, à partir de novembre 2001, le développement du Service québécois d'authentification gouvernementale. Ce service, qui s'adresse plus spécialement aux citoyens et aux entreprises désireux de transiger en ligne avec le gouvernement, expérimente de nouvelles façons de faire pour délivrer des certificats. Parallèlement à l'émergence de ces services, une réflexion a été menée pour définir des mesures plus complètes et stables ; aucune décision officielle n'a encore été prise à la suite du rapport qui a été produit en décembre 2002. Entre-temps, sans que soient remis en question les besoins des ministères et des organismes, la nécessité de maintenir tous ces services de certification n'est pas démontrée.

7. Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.

8. Selon la *Loi concernant le cadre juridique des technologies de l'information*, les services de certification comprennent la vérification de l'identité des personnes et la délivrance de certificats confirmant leur identité, l'identification d'une association, d'une société ou de l'État ou l'exactitude de l'identifiant d'un objet.

4.40 **Nous avons recommandé au Secrétariat du Conseil du trésor**

- **de veiller à ce que le plan gouvernemental de sécurité précise les résultats attendus et les indicateurs de performance afférents, prenne en compte tous les éléments pertinents et soit approuvé au moment opportun;**
- **de poursuivre l'élaboration d'un programme gouvernemental de sensibilisation et de formation en matière de sécurité et de voir à sa mise en œuvre;**
- **de fournir plus d'indications aux ministères et organismes sur les clauses de sécurité devant figurer dans les contrats et les ententes qu'ils concluent avec les fournisseurs de services, les partenaires, les mandataires et les autres gouvernements;**
- **de réduire les délais de production de l'état gouvernemental de la sécurité;**
- **d'évaluer l'application de la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale*;**
- **d'actualiser les orientations en matière d'authentification des personnes et de déterminer les services de certification à offrir pour satisfaire les besoins actuels et futurs.**

Action propre aux entités

4.41 À titre de premiers responsables de la sécurité informatique, il revient aux ministères et aux organismes de mettre en place leur dispositif de sécurité. Les pages suivantes présentent le fruit des travaux que nous avons réalisés auprès de trois d'entre eux. Elles traitent de tous les critères d'évaluation, à l'exception de celui qui porte sur la gestion des incidents. À ce sujet, nous avons en effet observé que les entités vérifiées disposent dans l'ensemble d'une bonne capacité d'intervention.

Cadre de gestion organisationnel

4.42 En sus du cadre gouvernemental préalablement abordé mais en concordance avec lui, les ministères et les organismes ont à établir leurs propres orientations et objectifs relativement à la protection de leurs actifs informationnels, à déterminer les composantes de leur dispositif de sécurité, à définir puis à assigner les responsabilités à cet égard et à instaurer les processus de gestion requis, incluant le suivi des activités et la reddition de comptes. Ces actions constituent les assises de tout programme de sécurité.

4.43 Les trois entités vérifiées ont accompli une bonne partie des gestes attendus, ce qui dénote qu'elles s'occupent activement de la question. Nous avons néanmoins relevé quelques lacunes.

Le registre d'autorité : un outil à utiliser pour spécifier les devoirs de chacun.

4.44 D'abord, la RAMQ ne dispose pas d'architecture de sécurité ; pareille situation ne favorise pas le déploiement cohérent des moyens de sécurisation. Ensuite, à la SAAQ et au MRQ, les devoirs de chacun ne sont pas dûment spécifiés dans un registre d'autorité, l'outil privilégié pour faire état des responsabilités générales et particulières de toutes les personnes concernées. Signalons que la SAAQ est à élaborer un tel registre tandis que celui du MRQ est incomplet.

4.45 La coordination des activités en matière de sécurité fait également défaut parce que le comité de sécurité informatique, un important mécanisme de concertation, ne rend pas des comptes à la bonne autorité ou ne joue pas pleinement son rôle stratégique. À la RAMQ, bien que remplissant correctement son mandat, il relève d'un comité dont le champ d'action est plus restreint. À la SAAQ, il assume aussi de nombreuses fonctions opérationnelles, ce qui peut l'empêcher d'avoir le recul nécessaire à la réalisation de son rôle stratégique. Pour ce qui est du MRQ, il est peu actif, mais son rôle est assumé, en partie, par d'autres comités qui n'ont toutefois pas le même rayonnement.

4.46 Enfin, même si leur cadre de gestion traite souvent du suivi, les trois entités vérifiées n'exercent pas cette fonction avec la rigueur voulue. En effet, le suivi s'avère insuffisant, notamment au regard de la performance de leur programme de sécurité. De plus, les entités font peu pour évaluer le respect des politiques, des directives et des normes internes relatives à la sécurité informatique ainsi que pour s'assurer de la cohérence entre le dispositif en place et l'architecture visée.

4.47 **Nous avons recommandé à la Régie de l'assurance maladie du Québec de se doter d'une architecture de sécurité informatique.**

4.48 **Nous avons recommandé à la Société de l'assurance automobile du Québec et au ministère du Revenu du Québec de préciser et d'assigner formellement les responsabilités en matière de sécurité informatique.**

4.49 **Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec**

- **de veiller à ce que le comité de sécurité informatique relève de la bonne autorité et joue pleinement son rôle ;**
- **de spécifier les modalités relatives au suivi et de s'assurer que cette fonction est adéquatement exercée.**

Évaluation de la vulnérabilité et de l'efficacité du dispositif de sécurité

4.50 L'état de la sécurité dépend en grande partie de la connaissance qu'une organisation acquiert et maintient concernant la vulnérabilité[9] de ses systèmes informatiques et l'efficacité de son dispositif de sécurité. Outre la mise en place de mécanismes continus de surveillance, de détection d'intrusion et de gestion des incidents, il importe que, de façon périodique, l'entité évalue son niveau de protection et éprouve l'efficacité des moyens employés pour contrer les menaces informatiques[10].

4.51 Les trois entités vérifiées ont réalisé au fil des ans différentes évaluations de portée variable ; la RAMQ a aussi mené quelques tests d'intrusion. Aucune ne dispose cependant d'une stratégie assurant l'évaluation périodique, complète et indépendante[11] de sa vulnérabilité et du comportement de son dispositif de sécurité. Cette méconnaissance de l'état de la sécurité s'observe davantage à la RAMQ, dont les activités courantes en matière de surveillance et de détection sont mal encadrées, ainsi qu'au MRQ, dont les activités à ces égards ne portent pas sur les menaces internes.

Les failles détectées ne sont pas forcément prises en charge.

4.52 Par ailleurs, on n'accorde pas suffisamment d'attention aux situations qui accentuent la vulnérabilité. En effet, même si nos travaux montrent que de nombreux correctifs sont régulièrement apportés par les entités, celles-ci n'ont pas l'assurance que toutes les failles détectées sont rapidement prises en charge et corrigées, s'il y a lieu, étant donné que les mécanismes nécessaires n'ont pas été instaurés ou ne fonctionnent pas correctement. Plus précisément, la SAAQ ne possède pas de registre regroupant l'ensemble des déficiences. Les deux autres entités ont bien un tel outil, mais le MRQ ne consigne pas l'information avec diligence dans le registre prévu à cette fin alors que la RAMQ n'effectue pas un suivi rigoureux de celle-ci.

4.53 Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec

- **de se doter d'une stratégie pour évaluer, de façon périodique et indépendante, la vulnérabilité de leurs systèmes et l'efficacité de leur dispositif de sécurité ;**
- **de s'assurer que toutes les déficiences détectées sont prises en charge rapidement et corrigées, s'il y a lieu.**

9. Faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent.
10. Événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique.
11. L'évaluation doit être réalisée par des personnes, faisant ou non partie de l'effectif, autres que celles qui ont à gérer la sécurité.

Planification de la sécurité informatique

4.54 La planification de la sécurité sert à déterminer les actions juridiques, humaines, organisationnelles et technologiques qu'il faut accomplir sur un horizon donné pour atteindre le niveau de protection désiré. Elle nécessite de connaître l'état de la sécurité (menaces, vulnérabilité et mesures en vigueur), l'architecture visée ainsi que les travaux de développement des technologies de l'information en cours et à venir. Le plan qui en découle détaille les objectifs poursuivis, les indicateurs de performance retenus, les activités à réaliser et les risques résiduels[12].

Planification inadéquate dans deux entités : elles doivent davantage tenir compte des orientations et des risques.

4.55 Nos travaux montrent que le MRQ a dressé un Plan triennal de gestion de la sécurité informatique (PTGSI), issu d'une démarche bien organisée. Cependant, le processus mis en œuvre par la RAMQ et la SAAQ n'est pas assez structuré. Ainsi, le lien entre les actions planifiées et les besoins (menaces et failles détectées, architecture de sécurité, orientations du plan de gestion des ressources informationnelles, etc.) n'est pas toujours bien documenté ; la SAAQ est d'ailleurs à élaborer un nouveau processus. De plus, la hiérarchisation des activités n'est pas faite. Par conséquent, ces deux entités n'ont pas l'assurance d'instaurer, de façon ordonnée, les mesures les plus pertinentes, tout en tenant compte du coût et de la valeur ajoutée.

4.56 D'autre part, le plan de sécurité des trois entités vérifiées porte essentiellement sur les activités de développement de la sécurité informatique tandis que les travaux récurrents qui ont trait, par exemple, à la coordination et à l'essai des mesures de reprise des opérations sont souvent planifiés distinctement. Dans le plan de la SAAQ, plusieurs projets sont aussi absents parce que leur financement provient de sources différentes. Pareil fractionnement peut nuire à la cohésion des interventions, laquelle est nécessaire à la mise en place d'un dispositif de sécurité intégré. En outre, aucune des trois entités ne fait état des risques résiduels, même si cette information facilite grandement la prise de décision de la part de la direction.

4.57 Ajoutons que les entités vérifiées ont défini peu d'indicateurs pour mesurer l'atteinte des objectifs poursuivis. Sans le recours à de tels indicateurs, l'appréciation de la performance est plus subjective.

4.58 Ces lacunes ne favorisent pas l'équilibre qu'il faut maintenir entre les différentes dimensions de la sécurité, équilibre difficile à réaliser en raison de la propension des organisations à intervenir surtout au regard de la dimension technologique. Il s'ensuit que des éléments d'ordre organisationnel aussi fondamentaux que la classification de l'information et la gestion des risques sont encore peu développés.

12. Portion du risque informatique qui demeure, une fois que les mesures visant à le réduire ont été mises en application.

4.59 **Nous avons recommandé à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec de s'assurer que, lors de la planification, le choix des activités repose sur l'analyse de tous les éléments pertinents et que les activités à réaliser sont hiérarchisées.**

4.60 **Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec de s'assurer que**

- **les activités de sécurité sont considérées comme un ensemble cohérent;**
- **les risques résiduels sont connus et acceptés par la direction;**
- **des indicateurs de performance sont élaborés.**

Risques et mesures de sécurité liés aux systèmes et aux infrastructures critiques

4.61 La classification des actifs informationnels est un exercice de base. Sans qu'il faille s'y limiter, il permet néanmoins de déterminer les systèmes et les ressources qui soutiennent les activités essentielles d'une organisation, c'est-à-dire celles dont elle dépend pour réaliser sa mission. Compte tenu du rôle prépondérant de ces systèmes et de ces ressources, veiller à leur sécurité, en termes de disponibilité, d'intégrité et de confidentialité, est un impératif. Pour ce faire, les entités doivent bien connaître les risques y afférents et instaurer les mesures appropriées.

4.62 Même si les entités vérifiées ont mis en place diverses mesures en ce sens, principalement en ce qui a trait à la reprise des activités après un incident, elles n'ont pas de vue d'ensemble des risques associés aux éléments à sécuriser ni des précautions qui ont été prises. Elles ignorent donc si les principaux risques ont été recensés et si les mesures adoptées sont cohérentes avec la menace réelle.

4.63 **Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec de s'assurer que les mesures de sécurité relatives aux systèmes et aux infrastructures critiques prennent en compte les principaux risques informatiques auxquels ils sont exposés.**

Habilitation des personnes

4.64 Des précautions doivent être prises au regard des personnes à qui des codes d'identification ainsi que des droits et des privilèges d'accès sont attribués. Il faut notamment s'assurer de l'intégrité des personnes concernées, de leur engagement à respecter les règles de sécurité, de la séparation des tâches incompatibles et de l'application de procédures pour la délivrance et le retrait des autorisations. La révision périodique des droits et privilèges accordés est également nécessaire. Il importe en effet d'obtenir l'assurance qu'ils demeurent justifiés.

4.65 Différentes mesures gouvernementales et organisationnelles ont été adoptées en vue d'encadrer l'habilitation. Par exemple, l'obligation de discrétion est enchâssée comme telle dans la *Loi sur la fonction publique*. Signalons aussi que les entités vérifiées se sont toutes dotées d'une procédure d'attribution des droits d'accès. Trois points peuvent cependant être améliorés.

4.66 D'abord, la SAAQ et la RAMQ ne font pas preuve d'assez de prudence relativement à l'intégrité des employés qu'ils embauchent. La *Loi sur la fonction publique* n'impose aucune exigence particulière à ce propos, mais il est souhaitable que les organisations instaurent, dans les limites permises et selon les risques encourus, leur propre système de contrôle pour les employés qui jouent un rôle important en matière de sécurité. Qui plus est, ces deux mêmes entités n'effectuent pas de suivi concernant l'utilisation des privilèges spéciaux conférés à ces utilisateurs afin de vérifier qu'elle est appropriée. Pour sa part, le MRQ contrôle de façon satisfaisante l'intégrité de son personnel.

La classification de l'information est incomplète.

4.67 Ensuite, l'attribution des droits d'accès ne s'appuie pas sur une classification adéquate de l'ensemble des informations exploitées au quotidien à l'aide des divers systèmes. Jusqu'à maintenant, les travaux effectués par la SAAQ et la RAMQ sont trop sommaires tandis que ceux réalisés par le MRQ portent essentiellement sur le caractère confidentiel de l'information. Un exercice d'envergure est cependant en cours à la RAMQ.

4.68 Enfin, seul le MRQ a mis en place un processus afin de réviser, sur une base périodique, les autorisations en vigueur. Nous avons néanmoins constaté que la SAAQ et la RAMQ avaient fait récemment des travaux pour valider, en tout ou en partie, les droits contrôlant l'accès aux ressources informatiques et que la SAAQ avaient entrepris des démarches pour que de tels exercices soient effectués de façon régulière.

4.69 Nous avons recommandé à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec

- **de contrôler, en fonction des risques encourus, l'intégrité des employés qui jouent un rôle important en matière de sécurité et d'exercer un suivi rigoureux quant à l'utilisation des privilèges spéciaux;**
- **d'instaurer un processus afin de réviser périodiquement les droits et les privilèges d'accès.**

4.70 Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec de s'assurer que l'attribution des droits d'accès s'appuie sur une classification appropriée de l'information.

Sensibilisation et formation

4.71 La sensibilisation et la formation de l'effectif demandent une attention toute spéciale en raison du rôle déterminant joué par le facteur humain sur l'état de la sécurité. La sensibilisation fait prendre conscience aux personnes concernées du caractère critique de certaines données, des risques en présence ainsi que de leur responsabilité en la matière. Quant à la formation, elle contribue à parfaire les connaissances des employés et à développer leurs aptitudes pour qu'ils s'acquittent au mieux de leurs tâches. Pour maximiser les retombées, il est nécessaire de s'adresser tant aux utilisateurs qu'aux gestionnaires et au personnel spécialisé. En outre, le choix et le calendrier des activités doivent être le fruit d'un processus adéquat.

Pas de perspective globale concernant la sensibilisation et la formation des utilisateurs et des gestionnaires.

4.72 Plusieurs activités de sensibilisation et de formation ont été tenues dans les trois organisations faisant l'objet de notre vérification. Or, ces activités ne sont pas encadrées par un programme formel qui vise à répondre aux besoins de l'ensemble de l'effectif. La RAMQ fait exception : un tel programme existe, mais il n'est pas soutenu par un plan favorisant sa mise en œuvre. Les besoins du personnel spécialisé sont tout de même pris en compte par les trois entités dans leur planification usuelle du développement des ressources humaines et de la formation pertinente est donnée à cet effectif. Pour ce qui est des utilisateurs et des gestionnaires, les interventions sont souvent organisées à la pièce. Force est de reconnaître les efforts marqués du MRQ pour sensibiliser son personnel à la nécessité de préserver la confidentialité de l'information.

4.73 De façon générale, on ignore donc dans quelle mesure les besoins sont comblés, notamment ceux des gestionnaires, à qui sont confiées de nombreuses responsabilités au chapitre de la sécurité informatique. Il est également difficile d'assurer la cohérence, la complémentarité et la continuité des activités et d'obtenir une rétroaction valable.

4.74 **Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec de mettre en œuvre un programme de sensibilisation et de formation répondant aux besoins de l'ensemble de leur effectif et d'évaluer son efficacité.**

Continuité de service

4.75 Le maintien des fonctions vitales devient la priorité lorsque survient un sinistre informatique[13]. Pour ce faire, il faut avoir préalablement mis au point une stratégie recouvrant l'ensemble des risques. Il faut aussi pouvoir se référer aux procédures se rapportant à chaque volet de cette stratégie, lesquelles sont habituellement regroupées dans des plans qui indiquent les mesures d'urgence à enclencher jusqu'au retour à la normale.

4.76 Certaines organisations n'auront d'autre choix que de faire appel à un centre de secours[14] tandis que d'autres pourront se tirer d'affaire grâce à une simple intervention manuelle. Dans tous les cas, il importe d'organiser le retour à la normale, qui comprend le rattrapage des activités ayant été suspendues pendant l'indisponibilité des ressources.

Une entité devra se doter d'une stratégie de continuité de service.

4.77 Or, la RAMQ n'a pas conçu de stratégie de continuité – incluant les mesures d'urgence, la reprise hors site et les interventions assurant le retour à la normale –, même si des besoins à cet égard ont été recensés. Cette entité a tout de même pris quelques mesures en vue de maintenir certaines fonctions essentielles. Les deux derniers essais relatifs à l'une de ces mesures ont toutefois démontré que la solution prévue ne produisait pas les résultats attendus depuis mai 2003.

4.78 La situation des deux autres entités est meilleure, sans être totalement exempte de problèmes. En effet, les moyens déployés par la SAAQ pour assurer la continuité de service ne s'appliquent pas aux systèmes d'information exploités sur une plate-forme[15] donnée. Par ailleurs, la documentation des procédures est incomplète, tant à la SAAQ qu'au MRQ. Enfin, la portée des tests qui visent à éprouver l'efficacité de leurs plans respectifs est trop restreinte.

4.79 Nous avons recommandé à la Régie de l'assurance maladie du Québec de concevoir une stratégie en vue d'assurer la continuité de service lors d'un sinistre informatique ainsi que d'élaborer et d'éprouver les plans nécessaires à sa mise en œuvre.

4.80 Nous avons recommandé au ministère du Revenu du Québec et à la Société de l'assurance automobile du Québec de parfaire leur stratégie en matière de continuité de service. Ils doivent notamment documenter adéquatement les mesures retenues et tester celles-ci de manière à s'assurer de leur efficacité. La Société de l'assurance automobile du Québec doit également veiller à ce que les mesures qu'elle a adoptées s'appliquent à l'ensemble de ses systèmes d'information.

13. Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants à un système ou à un centre informatique.

14. Centre informatique prenant temporairement le relais d'un centre principal rendu indisponible en raison d'un sinistre informatique majeur, afin que soit maintenue la continuité de service.

15. Structure matérielle d'un système informatique, principalement basée sur le type de système d'exploitation utilisé.

Contrôle d'accès aux systèmes et aux données

4.81 La sécurité logique est définie comme la mise en vigueur de mesures de sécurité dans le but de protéger les biens informatiques immatériels (logiciels, programmes, données et réseaux) ainsi que les opérations informatiques. Parmi ces mesures, l'authentification sert, dans un premier temps, à vérifier l'identité de l'utilisateur. Cette étape réalisée avec succès, celui-ci peut alors exploiter les ressources de l'entité dans la limite de ses droits d'accès. Ce type de contrôle, de nature technique, contribue à empêcher toute action non autorisée.

4.82 L'authentification constitue donc la première ligne de défense de l'entité ; par ricochet, elle aide à responsabiliser les personnes qui ont accès à ses ressources informationnelles. De façon générale, les entités retiennent la forme la plus courante de ce moyen de contrôle, c'est-à-dire le couplage d'un nom d'utilisateur à un mot de passe. On obtient ainsi des niveaux de sécurité très satisfaisants, à condition de bien gérer les mots de passe. Une telle approche comporte cependant des inconvénients. Notamment, les mots de passe peuvent être facilement devinés ou découverts s'ils ne sont pas judicieusement choisis ni régulièrement renouvelés. Enfin, l'utilisateur doit veiller à les garder secrets.

La gestion des mots de passe réclame plus de rigueur.

4.83 Nos travaux révèlent que la gestion des mots de passe appelle plus de rigueur. Les lacunes observées varient selon l'environnement propre à chaque entité, mais les plus répandues sont les suivantes :

- Au MRQ et à la RAMQ, les règles en vigueur donnent lieu à des mots de passe trop simples ; par surcroît, en ce qui a trait au MRQ, la longueur exigée n'est pas toujours suffisante. Mentionnons que la SAAQ s'est dotée d'un outil spécialisé conçu pour favoriser ce qu'il est convenu d'appeler la « robustesse » des mots de passe.
- Au MRQ et à la RAMQ, il est parfois possible que les utilisateurs ne soient pas soumis au changement périodique qui a été programmé.
- Dans les trois entités, le nombre de tentatives d'authentification infructueuses entraînant un refus d'accès n'est pas toujours limité ; qui plus est, à la SAAQ, le nombre d'essais toléré est, dans certains cas, supérieur aux exigences de la norme interne.

4.84 Le contrôle d'accès protège aussi les biens informatiques immatériels contre les modifications, les manipulations ou les divulgations indues. En effet, autant les utilisateurs doivent avoir accès aux ressources nécessaires à leur travail, autant il faut les tenir éloignés de celles qui ne les concernent pas. À cet égard, nous avons constaté que les efforts du MRQ au chapitre de la sécurité logique devraient être accentués : il lui arrive d'accorder des droits d'accès trop permissifs, eu égard aux besoins réels des utilisateurs. En outre, certaines voies d'accès à l'un de ses environnements de traitement ne sont pas protégées.

4.85 **Nous avons recommandé au ministère du Revenu du Québec, à la Société de l'assurance automobile du Québec et à la Régie de l'assurance maladie du Québec de veiller à ce que la gestion des mots de passe soit appropriée.**

4.86 **Nous avons recommandé au ministère du Revenu du Québec de prendre les mesures nécessaires pour que les accès accordés correspondent aux besoins réels des utilisateurs et se limitent aux ressources visées.**

Suivi de l'activité des systèmes

4.87 L'activité des systèmes informatiques est aussi variée que considérable, d'où la nécessité de surveiller étroitement les multiples opérations qui s'y déroulent. Nous avons vu que l'attribution des droits d'accès constitue un premier contrôle. Néanmoins, selon le niveau de sensibilité associé à chaque situation, l'entité doit mettre en œuvre d'autres moyens pour s'assurer que les interventions sont justifiées. Il convient aussi d'investiguer lorsque des anomalies surviennent. Pour effectuer les analyses permettant de suivre l'activité des systèmes, on scrute habituellement des journaux où sont enregistrés des événements prédéterminés.

Deux entités se limitent à surveiller la confidentialité.

4.88 Nos travaux montrent que le suivi des événements exercé par la SAAQ est adéquat, mais qu'il laisse à désirer dans les deux autres entités vérifiées. En effet, le MRQ et la RAMQ n'ont pas établi tous leurs besoins à ce propos. Ceux-ci s'emploient surtout à surveiller la consultation des renseignements personnels pour voir si leur confidentialité est protégée. Dès lors, les interventions susceptibles d'influer sur l'intégrité et la disponibilité de l'information critique ou sur le système de sécurité ne reçoivent pas toute l'attention voulue.

4.89 **Nous avons recommandé au ministère du Revenu du Québec et à la Régie de l'assurance maladie du Québec de contrôler adéquatement l'activité de leurs systèmes informatiques.**

Services communs d'infrastructure

4.90 Cette section traite des mesures instaurées par la DGSIG et la DGT, qui relèvent du SCT, pour sécuriser les services communs d'infrastructure qu'elles fournissent à bon nombre de ministères et organismes. Nous en avons sélectionné trois, en fonction de leur impact global sur la sécurité de l'information : le Réseau de télécommunication multimédia de l'administration publique québécoise (RETEM) ainsi que deux services de traitement informatique multiplate-forme offerts respectivement à l'aide d'ordinateurs de moyenne et de grande puissance (tableau 1).

Tableau 1

SERVICES COMMUNS D'INFRASTRUCTURE :
DESCRIPTION SOMMAIRE DES TROIS SERVICES VÉRIFIÉS

RETEM
Le RETEM repose sur une infrastructure unique, destinée à traiter en temps réel des trafics de toute nature, que ceux-ci contiennent des messages vocaux, des images ou des données. La DGT offre ce service à l'ensemble des ministères et organismes du gouvernement et les dépenses y afférentes sont de l'ordre de 25 millions de dollars par année.
Traitement informatique multiplate-forme
La DGSIG fournit des services de traitement informatique à partir d'ordinateurs de moyenne et de grande puissance. Ces deux types de services, qui regroupent aussi le stockage de données, l'impression centrale, l'accès aux plates-formes de traitement et la gestion des productions, donnent lieu à des dépenses annuelles de quelque 45 millions de dollars.

4.91 Nous avons examiné si ces services répondaient aux principales exigences en matière de sécurité. C'est ainsi que nos constats portent sur l'encadrement, l'évaluation de la vulnérabilité et de l'efficacité des dispositifs déployés, l'élaboration des plans de sécurité et la reprise des opérations.

4.92 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 de 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. De plus, les mécanismes qui permettraient aux ministères et aux organismes d'être consultés pour sa mise au point et sa révision sont insuffisants. Pour sa part, la DGSIG commence tout juste à élaborer son architecture de sécurité. Ces travaux devraient notamment l'amener à déterminer les diverses mesures de sécurité à prendre concernant les services communs, à analyser leurs interrelations et à évaluer la possibilité de partager les ressources.

Peu d'informations sont disponibles sur la vulnérabilité et l'efficacité de la sécurité du RETEM.

4.93 Pour ce qui est des aspects clés de la sécurité, nous avons noté que la DGT 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. En effet, rares sont les évaluations faites à ce propos jusqu'à maintenant. La DGT n'est donc pas en mesure de spécifier à sa clientèle le niveau de sécurité du RETEM ni de s'assurer qu'il sera ajusté au besoin. Ces évaluations sont d'autant plus pertinentes qu'on tarde à réaliser certaines activités jugées nécessaires au moment de la conception du devis du RETEM (détection d'intrusion, conception des outils d'accès aux journaux, analyse des vulnérabilités, etc.).

4.94 Quant à la DGSIG, elle a apprécié globalement, en 2001, la vulnérabilité et l'efficacité de sa stratégie de sécurité en fonction d'une norme reconnue et, depuis, procède à des travaux complémentaires afin de répondre à des besoins ponctuels. Par ailleurs, elle est en train de s'approprier de nouveaux outils pour

poser de meilleurs diagnostics, tels une méthode d'analyse des risques et un processus permettant l'examen systématique des journaux qui enregistrent l'activité des systèmes informatiques. 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.

4.95 En ce qui concerne la planification, la DGT aussi bien que la DGSIG omettent de prendre en considération des éléments pertinents, comme le résultat des évaluations et les incidents ; de plus, leurs plans de sécurité ne comportent aucun indicateur de performance. Ces directions générales n'ont donc pas l'assurance de traiter comme il se doit les priorités et peuvent difficilement mesurer l'effet de leurs interventions.

4.96 Enfin, le plan de reprise du RETEM est confié au fournisseur des services de télécommunication et l'entente contractuelle comporte des dispositions pour que les services soient constamment disponibles. Pour ce qui est de la DGSIG, le plan en vigueur se limite aux services centraux. Par contre, les travaux en cours à cet égard, notamment des essais concernant les ordinateurs de moyenne puissance, montrent que l'organisation est en voie de corriger la situation. Néanmoins, force est de conclure que, pour le moment, la reprise complète des opérations en cas de sinistre n'est pas organisée.

4.97 Nous avons recommandé au Secrétariat du Conseil du trésor

- **de veiller à ce qu'un cadre de gestion de la sécurité soit officialisé concernant le Réseau de télécommunication multimédia de l'administration publique québécoise et, pour ce faire, de consulter les ministères et les organismes visés ;**
- **de s'assurer que le Réseau bénéficie d'un dispositif de sécurité approprié et que les moyens déployés font périodiquement l'objet d'une évaluation rigoureuse et indépendante ;**
- **de poursuivre l'élaboration d'une architecture de la sécurité des infrastructures de traitement informatique multiplate-forme, de mettre au point un processus assurant l'évaluation périodique et indépendante de leur vulnérabilité et de compléter la mise en place des mesures de reprise afférentes ;**
- **de parfaire la planification des activités de sécurité informatique relatives aux services communs d'infrastructure vérifiés ; à cet effet, il doit notamment prendre en compte l'ensemble des éléments pertinents et déterminer des indicateurs de performance.**

Tests d'intrusion réalisés aux fins de notre vérification

4.98 Les ministères et les organismes se doivent de protéger leurs actifs informationnels en adoptant une approche intégrée et structurée, qui offre une couverture proportionnée aux risques encourus. Il leur faut garder à l'esprit qu'il ne serait pas rentable de vouloir contrer tous les risques et que de nouvelles menaces ne cessent d'apparaître. Les tests d'intrusion figurent dans la liste des moyens préconisés pour évaluer la vulnérabilité. À cet effet, l'entité fait appel à un spécialiste qui est chargé d'apprécier dans quelle mesure un intrus – qu'il s'agisse d'un pirate informatique[16], d'un bidouilleur[17], d'un membre de l'effectif ou d'un tiers (mandataire, sous-traitant, etc.) – serait capable de déjouer le dispositif de sécurité et d'accéder indûment aux systèmes et aux données. Simulant des attaques éventuelles, les tests de ce type permettent de trouver et d'éliminer les faiblesses avant qu'elles soient exploitées.

4.99 Il va de soi que cette méthode de contrôle n'est pas une panacée : l'expérience ne saurait s'étendre à toutes les situations possibles. Les tests d'intrusion visent des cibles particulières et sont effectués selon des protocoles prédéterminés, à des moments précis et en fonction d'un environnement technologique donné. Comme la menace revêt parfois différentes formes, les tests sont susceptibles de simuler plus d'un scénario. Des travaux réalisés par des experts montrent que les incidents sont provoqués autant de l'interne que de l'externe. Plusieurs sources tendent également à conclure que les actes de vandalisme, le vol d'information ou le sabotage de données sont au moins la moitié du temps le fruit de personnes proches des organisations lésées.

4.100 Forts de ces considérations, nous avons éprouvé certains aspects relatifs à la sécurité de quatre entités, et ce, sans perturber leurs activités. Les tests ont été menés sous cinq angles, qui ont été adaptés pour tenir compte des environnements sondés et des menaces perçues comme étant les plus plausibles. Les entités ont été mises à contribution en fournissant de l'information sur leurs systèmes et leurs réseaux informatiques, ce qui a facilité nos travaux. Néanmoins, la plupart des renseignements qu'elles nous ont communiqués auraient pu être rassemblés à l'intérieur de six mois par une personne déterminée à les obtenir.

4.101 Nous avons procédé à 19 tests différents, pour un total de 55 évaluations faites la plupart du temps en compagnie de représentants des entités sélectionnées. Ces dernières ont toutes subi 11 de ces tests afin que nous soyons à même de tirer des constats plus généraux. Plus de 70 p. cent des tests simulaient une situation répondant aux critères suivants : les connaissances de l'intrus éventuel concernant l'organisation et en matière informatique sont faibles ou moyennes (le grand

16. Criminel informatique qui exploite les failles dans une procédure d'accès pour casser un système informatique, qui viole l'intégrité de ce système en dérobant, altérant ou détruisant de l'information, ou qui copie frauduleusement des logiciels.

17. Personne passionnée d'informatique qui, par jeu, curiosité, défi personnel ou par souci de notoriété, sonde, au hasard plutôt qu'à l'aide de manuels techniques, les possibilités matérielles et logicielles des systèmes informatiques afin de pouvoir éventuellement s'y immiscer.

public ou un étudiant en informatique, par exemple), le coût de l'opération est inférieur à 1 000 dollars et le tout peut se dérouler en 24 heures ou moins. Les autres tests se rapportaient à des menaces moindres, puisqu'ils requéraient la participation soit d'une personne travaillant dans le domaine de l'informatique, soit d'un membre de l'effectif de l'entité, soit des deux.

4.102 Précisons aussi que les tests d'intrusion ont fait appel à des techniques ou à des outils souvent élémentaires et aisément disponibles, entre autres dans Internet. Nous avons avant tout cherché à simuler des scénarios selon lesquels une personne tentait d'accomplir une action répréhensible. Enfin, presque tous nos tests supposaient une intervention humaine se déroulant à l'intérieur du périmètre de sécurité[18].

4.103 Pour des raisons évidentes, le nom des entités, la nature exacte des tests ainsi que les résultats détaillés ne sont pas présentés dans ce rapport. Il est cependant possible de dresser un bilan sommaire quant au dénouement de nos travaux à cet égard (tableau 2).

Des coupe-feu efficaces contre les menaces liées à Internet.

Tableau 2

Bilan sommaire des tests d'intrusion

Angles considérés	Constats
Efficacité des coupe-feu*	Les coupe-feu en place gèrent adéquatement les flux d'information entre les réseaux internes et Internet.
Résistance des mécanismes de sécurité	Certains mécanismes peuvent être contournés à l'aide d'outils plus ou moins sophistiqués.
Robustesse des mots de passe	Des déficiences ont été détectées à plusieurs reprises par rapport à la robustesse des mots de passe ainsi qu'à leur gestion.
Pertinence des droits et privilèges d'accès	Des vulnérabilités ont été décelées concernant les droits d'accès aux ressources et la configuration des postes de travail.
Cloisonnement des zones de sécurité	Des problèmes ont été observés au regard de l'aménagement des lieux et du contrôle d'accès physique.

* Dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public.

18. Aux fins de cette vérification, nous avons considéré que cette notion réfère à la zone où les activités de l'entité font l'objet de mesures de sécurité physique.

Les lacunes détectées pourraient permettre, dans certaines circonstances, de mener diverses activités inappropriées.

4.104 Nous avons remis aux entités concernées toute l'information recueillie au cours des tests d'intrusion pour leur faciliter la mise en œuvre de contre-mesures. En effet, certaines des failles que nous avons mises en lumière affaiblissaient, individuellement et plus encore si elles étaient combinées, la protection relative à la confidentialité, à l'intégrité et à la disponibilité des actifs informationnels. Celles-ci ouvraient également la porte à des interventions pouvant aller à l'encontre des obligations découlant de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Ainsi, les lacunes détectées pourraient permettre, dans certaines circonstances, de mener diverses activités inappropriées, entre autres :

- accéder de façon illégitime à des systèmes informatiques ;
- visualiser et utiliser de façon frauduleuse des données sensibles ;
- modifier ou supprimer des données ou des programmes ;
- installer des programmes malveillants ;
- empêcher le bon fonctionnement de plusieurs équipements.

4.105 Les travaux que nous avons menés illustrent que la protection des actifs informationnels des quatre entités soumises aux tests d'intrusion est somme toute incomplète. Ils démontrent l'importance de recourir périodiquement à cette approche pour évaluer les limites du dispositif de sécurité. Ils confirment également la nécessité de prêter davantage attention à la dimension humaine de la sécurité, trop souvent négligée par rapport à ses dimensions juridique, organisationnelle et technologique.

4.106 Nous avons recommandé aux quatre entités vérifiées de réaliser des tests d'intrusion de façon périodique afin d'évaluer adéquatement la vulnérabilité de leurs actifs informationnels et l'efficacité de leur dispositif de sécurité.

4.107 Commentaires du Secrétariat du Conseil du trésor

« Le Secrétariat du Conseil du trésor accorde une priorité à la gestion de la sécurité informatique gouvernementale. C'est d'ailleurs dans cette optique qu'il a réuni une équipe dédiée à cette fonction depuis quelques années. Toutefois, la mise en place de mécanismes complètement opérationnels nécessite un certain temps.

« **Encadrement central.** Le Secrétariat prévoit revoir sa directive au cours de la prochaine année et il prendra en compte le concept de "domaine de confiance".

« Par ailleurs, concernant les exigences gouvernementales en matière de suivi, le Secrétariat a produit, au cours des dernières années, un bilan de la sécurité donnant une image globale de la situation prévalant dans l'ensemble de l'appareil gouvernemental, une première au Canada. Lors du bilan 2004, il est prévu que les préoccupations du Vérificateur général concernant l'architecture gouvernementale de sécurité de l'information numérique seront ajoutées. De plus, 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 font face pour mieux les suivre ultérieurement. 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, 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. C'est pourquoi, avant d'agir, le Secrétariat désire étudier les impacts d'une telle décision. Cet exercice permettra de déterminer les mesures qui peuvent être mises en place. Il faudra notamment tenir compte de l'imputabilité des ministères et des organismes quant à leur plan d'action et de la reddition de comptes qui s'ensuit.

« En matière de planification, des objectifs stratégiques, tactiques et opérationnels ont été, depuis 2002, élaborés annuellement par le Secrétariat dans le plan gouvernemental de sécurité, et ce, en fonction des cibles prioritaires déterminées par l'examen des bilans réalisés par les ministères et les organismes. Un calendrier de réalisation est également préparé annuellement. Par ailleurs, l'*Architecture gouvernementale de la sécurité de l'information numérique* identifie l'ensemble des éléments pouvant nécessiter une intervention du Secrétariat dans les prochaines années. De plus, pour réduire les délais de production de l'état de situation gouvernemental de la sécurité ainsi que pour permettre aux ministères et aux organismes de s'arrimer au calendrier du cycle budgétaire, le Secrétariat a démarré le processus de reddition de comptes de l'année civile 2003 en décembre 2003 et les ministères et organismes ont pu utiliser leurs propres résultats dans leur budgétisation de 2004-2005. Somme toute, le Secrétariat considère que le mode de fonctionnement était bien adapté aux problématiques auxquelles il faisait face dans les premières étapes de mise en œuvre du plan d'action. En effet, il fallait tenir compte des besoins, de la culture et de la capacité d'intégration des ministères et des organismes. Cependant, le Secrétariat effectuera une analyse de l'ensemble des éléments mentionnés afin de les inscrire au sein d'un cadre pluriannuel.

« Également, le Secrétariat est à compléter le développement d'un programme formel de sensibilisation et de formation amorcé au cours de l'exercice 2003-2004. Il vise à orienter son action à ce chapitre pour les prochaines années, et ce, en collaboration avec les ministères et les organismes. Ce programme vise d'abord à agir sur des cibles prioritaires qui sont définies en fonction des résultats du bilan gouvernemental annuel de sécurité et des demandes exprimées par les ministères et les organismes.

« Quant aux contrats et ententes, le Secrétariat considère que les ministères et les organismes sont les premiers responsables des contrats et des ententes qu'ils concluent. Toutefois, pour les soutenir, il leur fournira un modèle recensant l'ensemble des sujets dont ils devraient tenir compte dans l'élaboration de leurs contrats et ententes.

« En matière d'authentification des personnes et de l'organisation des services de certification, le Secrétariat est d'accord avec la recommandation du Vérificateur général et il entend ajuster ses travaux à cet égard.

« **Services communs d'infrastructure.** Concernant le Réseau de télécommunication multimédia de l'administration publique québécoise (RETEM) et les services de traitement sur plates-formes intermédiaires et centrales, le Secrétariat entend poursuivre ses efforts

d'intégration de tous les éléments pertinents dans la planification de ses activités de sécurité et verra à amorcer une démarche pour se doter d'indicateurs de performance.

« Pour le RETEM, le Secrétariat verra, d'une part, à compléter le cadre de gestion afin que tous les éléments pertinents de la sécurité soient définis, et d'autre part, à s'entendre avec les ministères et les organismes en vue d'augmenter leur niveau de compréhension des exigences de sécurité et des procédures ainsi qu'à leur rappeler leurs responsabilités sur les mesures qu'ils doivent prendre pour la continuité de leurs opérations. Par ailleurs, des efforts seront consacrés à l'intégration de mécanismes de sécurité au RETEM ainsi qu'à un contrôle accru quant à leur fonctionnement.

« Pour les services de traitement sur plates-formes intermédiaires et centrales, le Secrétariat prévoit compléter l'architecture de sécurité lors de la réalisation de l'infrastructure sécurisée de la prestation électronique de services et du projet Service québécois d'authentification gouvernementale. Le Secrétariat réalise des évaluations pour chaque changement d'élément de l'infrastructure qui pourrait avoir un impact sur la sécurité et apporte les corrections requises. Un registre des vulnérabilités et des actions correctives sera mis en place pour faciliter le suivi du programme de sécurité. Pour faire suite au projet pilote réalisé en novembre 2003, concernant la reprise des plates-formes intermédiaires, le Secrétariat a prévu compléter la documentation des mesures de reprise et procéder aux premiers essais à compter d'avril 2004. »

4.108 Résumé des commentaires des entités

Les entités vérifiées acquiescent pleinement aux constats et aux recommandations du Vérificateur général. Les sections suivantes présentent les actions entreprises ou envisagées pour remédier aux situations décrites.

Cadre de gestion organisationnel. « Dans le cadre de la révision de la politique de sécurité informatique, le MRQ en profitera pour préciser, notamment, les rôles et les responsabilités du comité de sécurité informatique et améliorer la coordination de ses activités et aussi celles des autres intervenants en matière de sécurité informatique. Il est prévu d'intégrer à la nouvelle politique des éléments qui permettront un suivi et une reddition de comptes quant à son application. »

Pour sa part, la RAMQ élabore actuellement son architecture d'entreprise, laquelle comporte un cadre de référence de la sécurité de l'information. Par la suite, l'architecture de sécurité de l'organisation sera développée. Elle mentionne aussi qu'une stratégie d'évaluation périodique du respect des politiques sera établie après la révision de son cadre normatif.

Évaluation de la vulnérabilité et de l'efficacité du dispositif de sécurité. La SAAQ et le MRQ réaliseront, au cours des prochains mois, une analyse de risque en s'appuyant notamment sur les outils fournis par le SCT.

Planification de la sécurité informatique. La RAMQ et la SAAQ nous ont fait savoir que le processus d'élaboration du plan de sécurité tiendra compte de l'ensemble des éléments pertinents.

Le MRQ et la RAMQ considèrent que la planification de la sécurité informatique prend en compte les risques résiduels, mais que ceux-ci ne sont pas bien documentés. Ils conviennent qu'il y aurait avantage à intégrer formellement cette information.

« Au MRQ, des indicateurs de performance ont été définis après le passage du Vérificateur général pour plusieurs processus développés et mis en place dans le cadre du Plan triennal de gestion de la sécurité informatique (PTGSI). »

Risques et mesures de sécurité liés aux systèmes et aux infrastructures critiques. Toutes les entités soulignent que des travaux actuels ou futurs contribueront à améliorer la protection des infrastructures critiques. Ainsi, le MRQ compte sur la mise en œuvre complète du PTGSI tandis que la RAMQ mentionne qu'elle élaborera une architecture de sécurité. La SAAQ, quant à elle, mise sur divers projets prévus pour 2004, notamment la poursuite de la mise en œuvre du registre d'autorité, le projet d'analyse de risque et le projet de reprise de la plate-forme intermédiaire.

Habilitation des personnes. La RAMQ et la SAAQ ont toutes deux choisi de ne pas vérifier systématiquement les antécédents d'une personne avant son embauche ou sa nomination. La SAAQ travaille actuellement au développement d'un processus de vérification avant l'embauche de nouveaux employés. Des décisions seront prises par la suite.

La SAAQ considère aussi que la poursuite du projet de mise en œuvre du registre d'autorité permettra de définir les guides et les processus requis afin de parvenir à une catégorisation suffisamment fine pour appuyer le processus d'habilitation.

« Au MRQ, un dossier spécifique sera réalisé pour raffiner la classification actuelle de l'information qu'il détient. »

Sensibilisation et formation. Depuis la vérification, la RAMQ a déjà fait un pas dans le sens des recommandations formulées par le Vérificateur général. Ainsi, « pour l'exercice 2004-2005, un plan d'action concernant la sensibilisation et la formation des intervenants a été élaboré ».

« La SAAQ se dotera d'un plan pour encadrer les efforts importants qu'elle consacre à la sensibilisation et à la formation de son personnel en matière de sécurité de l'information et elle procédera périodiquement à son évaluation. »

« Dans un souci d'aborder les différents aspects de la sécurité et de la sensibilisation, le MRQ s'appliquera à arrimer les activités de formation et de sensibilisation dans un programme global, tout en s'assurant que les besoins en sécurité de tous les groupes d'employés sont pris en compte. »

Continuité de service. Les entités prévoient, dans un avenir rapproché, aborder les questions commentées par le Vérificateur général à la lumière des recommandations formulées par celui-ci.

La RAMQ mentionne que, depuis la fin des travaux du Vérificateur général, des correctifs ont été apportés aux essais et que les derniers réalisés le 13 mai 2004 sont concluants à cet égard.

Contrôle d'accès aux systèmes et aux données. Le MRQ et la RAMQ entendent améliorer le contrôle d'accès à leurs ressources informationnelles, notamment en resserrant la gestion des mots de passe.

« La SAAQ ramènera le nombre de tentatives d'authentification infructueuses au niveau des exigences de la norme interne. »

« Le MRQ poursuit ses travaux pour réviser son processus d'attribution des droits d'accès en regard des profils de fonction. Il vise également à améliorer son exercice de révision massive périodique des accès à ses ressources informationnelles. »

Suivi de l'activité des systèmes. La RAMQ projette de définir ses besoins à cet égard et d'évaluer les coûts et les impacts des solutions potentielles, et ce, en fonction des risques encourus.

« Le MRQ convient qu'il devra mettre en place des mécanismes permettant d'analyser régulièrement l'ensemble de ses journaux d'évènements afin d'assurer un contrôle adéquat de l'activité des systèmes informatiques. »

Tests d'intrusion réalisés aux fins de notre vérification. Une entité mentionne qu'« un processus régulier de vérification sera défini au cours de l'exercice 2004 et que diverses vérifications ont été ou seront réalisées ».

Une deuxième indique que « la fréquence et la portée des tests d'intrusion seront établies en fonction des risques appréhendés et des coûts inhérents à de telles évaluations par des firmes externes ».

Enfin, les deux autres entités se sont dites en accord avec les commentaires du Vérificateur général à ce chapitre et sa recommandation.

ANNEXE 1 – OBJECTIFS DE VÉRIFICATION ET CRITÈRES D'ÉVALUATION

La responsabilité du Vérificateur général consiste à fournir une conclusion sur les objectifs présentés dans ce mandat de vérification. Pour ce faire, nous avons recueilli les éléments probants suffisants et adéquats pour fonder raisonnablement notre conclusion et pour obtenir un niveau élevé d'assurance. Notre évaluation est basée sur les critères que nous avons jugés valables dans les circonstances et qui sont exposés ci-après.

Les critères d'évaluation émanent, avec les adaptations requises, de modèles préconisés, entre autres, par l'International Federation of Accountants (IFAC), le National Institute of Standards and Technology (NIST), l'International Organization for Standardization (ISO) et l'International Electrotechnical Commission (IEC). Les travaux de vérification dont traite ce rapport ont été menés en vertu de la *Loi sur le vérificateur général* et conformément aux méthodes de travail en vigueur. Ces méthodes de travail respectent les normes des missions de certification émises par l'Institut Canadien des Comptables Agréés.

Objectif

S'assurer que le cadre gouvernemental de gestion de la sécurité informatique et l'action des entités qui doivent assumer des responsabilités particulières à cet égard soutiennent la mise en œuvre des moyens assurant la protection des biens et des données ainsi que la continuité de service.

Critères

- Le cadre gouvernemental de gestion de la sécurité informatique (politiques, directives, architecture, procédures, normes, etc.) doit :
  - énoncer les valeurs gouvernementales, les objectifs, la portée et les principes directeurs ;
  - définir les rôles et les responsabilités ;
  - présenter les assises de la sécurité ;
  - favoriser la mise en place de mesures efficaces, efficientes et cohérentes dans l'Administration ;
  - prévoir des mécanismes de suivi relatifs à la mise en œuvre et à l'état de la sécurité informatique ainsi que de reddition de comptes.
- Les entités qui assument des responsabilités particulières en la matière (CT, SCT, MJQ, MRCI, CANQ, CF, SQ) doivent jouer le rôle qui leur est dévolu.

Objectif

S'assurer que les ministères et organismes respectent le cadre de gestion gouvernemental de la sécurité informatique et soutiennent à l'interne sa mise en œuvre.

Critère

- Le cadre de gestion de la sécurité informatique (politiques, directives, architecture, procédures, normes, etc.) de l'entité doit s'arrimer à celui du gouvernement. Il doit aussi :
  - énoncer les valeurs organisationnelles, les objectifs, la portée et les principes directeurs ;
  - définir les rôles et les responsabilités ;
  - édicter les règles de conduite ;
  - présenter les assises de la sécurité ;
  - favoriser la mise en place de mesures efficaces, efficientes et cohérentes ;
  - prévoir des mécanismes de suivi, d'évaluation et de reddition de comptes.

Objectif

S'assurer que les ministères et les organismes ont mis en place les composantes majeures de la sécurité informatique.

Critères

- Une évaluation périodique de la vulnérabilité de l'entité et de l'efficacité de son dispositif de sécurité doit être réalisée.
- Une analyse des systèmes informatiques et des infrastructures critiques doit être effectuée pour déterminer et appliquer les mesures de sécurité nécessaires à leur protection.
- L'attribution des codes d'identification ainsi que des droits et privilèges d'accès doit être encadrée adéquatement.
- Un plan de sécurité prenant appui sur l'évaluation des risques et du dispositif de sécurité ainsi que sur les standards en vigueur doit être élaboré et maintenu à jour.
- Des activités de sensibilisation et de formation doivent être offertes aux utilisateurs, au personnel spécialisé et aux gestionnaires.
- Des mesures pour faire face aux imprévus et aux sinistres, traiter les incidents et assurer la continuité de service doivent être instaurées.
- Un contrôle efficace de l'accès aux systèmes informatiques et aux données doit être exercé.
- L'enregistrement et l'analyse de l'activité des systèmes informatiques doivent être effectués et des actions doivent être entreprises lorsque des anomalies sont détectées.

ANNEXE 2 – PORTRAIT DE LA SÉCURITÉ INFORMATIQUE (ÉLÉMENTS REGROUPÉS PAR DIMENSIONS)

Dimension juridique	Aspects légaux	• Lois et règlements nationaux • Lois et règlements provinciaux, généraux et particuliers • Conventions internationales • Contrats et ententes • Avis juridiques
Dimension humaine	Sécurité du personnel	• Enquêtes de sécurité • Habilitation des personnes • Sensibilisation • Formation
	Éthique, pratiques professionnelles et imputabilité	• Responsabilités de l'entité • Responsabilités des gestionnaires • Responsabilités du personnel et des utilisateurs
Dimension organisationnelle	Sécurité administrative	• Politiques, normes, directives, guides et procédures • Rôles et responsabilités du personnel chargé de la sécurité • Classification de l'information • Évaluation de la vulnérabilité • Analyse de risques • Registres et dossiers de sécurité • Gestion du consentement • Prévention
	Sécurité physique et sécurité du milieu	• Installations principales et auxiliaires des ressources informationnelles • Contrôle de l'accès physique • Sécurité du matériel
	Sécurité des opérations	• Administration • Contrôle de l'accès logique • Surveillance et audit • Utilisation et gestion des supports • Mesures d'urgence, de relève et de continuité
Dimension technologique	Sécurité des logiciels, du matériel, des communications et des informations de sécurité	• Mise en place des fonctions de sécurité • Développement des applications • Sélection des applications ou des équipements • Installation et configuration des applications ou équipements

Source : Secrétariat du Conseil du trésor.