Public Health Agency of Canada | Agence de la santé publique du Canada

RAPPORT D'EXAMEN

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

Division des services de vérification

Novembre 2010

Approuvé par l'administrateur en chef de la sécurité publique
le 12 janvier 2011

Canada

Table des matières

Objectifs et portée de l'examen **2**

Contexte **2**

Constatations et recommandations découlant de l'examen **3**

Gouvernance de la sécurité de la TI 3

Exploitation des réseaux 5

Gestion des incidents liés à la TI 7

Conclusion 7

Annexe A : Critères d'examen **9**

Annexe B : Plan d'action de la direction **10**

Annexe C : Description des réseaux utilisés par l'ASPC **16**

Annexe D : Liste des acronymes **18**

HP5-104/2010F-PDF
ISBN: 978-1-100-96297-9

Objectifs et portée

1. L'examen avait pour objectif global d'informer la haute direction de l'ASPC sur la mesure dans laquelle l'infrastructure de sécurité de la technologie de l'information respecte les pratiques exemplaires mondiales mentionnées dans le *Control Objectives for Information and Related Technology (COBIT) Security Baseline Guide* et la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Conseil du Trésor (CT). Un examen ne constitue pas une vérification, puisque son degré d'exactitude (modéré) est moins élevé que celui d'une vérification. L'examen a été effectué en conformité avec la Politique du CT sur la vérification interne.

2. Le projet d'examen de la sécurité de la TI faisait partie du Plan de vérification axé sur les risques pour 2010-2015. L'examen a eu lieu d'avril à novembre 2010.

3. La portée de l'examen comprend un examen de la gouvernance de la TI, de l'exploitation des réseaux et de la gestion d'incidents liés au TI. L'examen ne s'est pas intéressé aux mesures de sécurité et de protection liées à la TI qui ont trait à la planification de la continuité des opérations, au contexte du cycle chronologique de l'élaboration des systèmes et à la passation de marchés.

4. Les critères d'examen présentés à l'Annexe A ont été adoptés du guide de COBIT Security Baseline de l'Association des professionnels de la vérification et du contrôle des systèmes d'information (APVCSI) et des normes GSTI du CT.

Contexte

5. L'ASPC a grandement besoin d'avoir accès à ses systèmes de TI et à une infrastructure technique en bon état qui soutiennent ses quatre services de réseau (voir la description des quatre réseaux qu'utilise actuellement l'ASPC à l'Annexe C). La gestion de la sécurité est plus efficace lorsqu'elle est systématiquement intégrée aux activités, aux programmes et à la culture d'un organisme. Comme pour l'ensemble des ministères et des organismes du gouvernement, l'ASPC fait face à des défis continus de maintenir la fiabilité de l'infrastructure de sécurité de la TI pour être en mesure de cerner de nouvelles menaces et de répondre rapidement à tous les incidents de sécurité.

6. À l'ASPC, le dirigeant principal de l'information (DPI), l'agent de sécurité ministériel (ASM) et le coordonnateur de la sécurité des technologies de l'information (CSTI) participent à la gestion de la sécurité de la TI. Les Services de sécurité de la gestion et de la technologie de l'information (GI/TI) et de la gestion de l'information, qui relèvent de la Direction de la GI/TI (DGITI), sont responsables du programme de sécurité en matière de GI/TI de l'Agence de la santé publique du Canada (ASPC ou l'Agence). Le programme de sécurité en matière de GI/TI vise à protéger les renseignements et les systèmes de renseignements de l'Agence.

7. De plus, les services de périmètre du réseau de l'ASPC comprennent de nombreux joueurs externes : Santé Canada, Travaux publics et Services gouvernementaux Canada (qui a conclu un contrat avec Santé Canada) et des tiers. Dans le cadre d'un protocole d'entente (PE) conclu en 2005, Santé Canada offre à l'ASPC des services directs de GI/TI, des services conjoints et une infrastructure ministérielle en matière de GI/TI.

8. En septembre 2010, les dépenses liées à la direction de la GI/TI pour l'exercice 2009-2010 s'élevaient à 26 millions de dollars et, selon les estimations, elles s'élèveront à 29,7 millions de dollars pour 2010-2011. La direction a indiqué que les dépenses affectées à la sécurité de la TI pour les mêmes périodes étaient de, respectivement, 1,3 million de dollars et 1,4 million de dollars.

Constatations et recommandations

Gouvernance de la sécurité de la TI

Critère : L'ASPC utilise des principes adéquats en matière de gouvernance pour organiser et gérer son programme de sécurité en TI.

9. La Politique sur la sécurité de la TI a été approuvée en 2006 et, avec le temps, des politiques, des directives et des lignes directrices complémentaires ont été élaborées. Toutefois, l'ensemble des politiques en matière de sécurité qui ont été élaborées ne sont pas complètes. Les rôles et les responsabilités du DPI, du CSTI et de l'ASM sont bien documentés dans la Politique sur la sécurité de la TI, sous réserve des commentaires formulés dans le paragraphe suivant. Des procédures opératoires normalisées bien documentées sont en place pour s'assurer que les employés et les entrepreneurs font l'objet d'un contrôle ou d'une attestation de sécurité au niveau de sécurité qui s'impose avant la nomination.

10. Même si le CSTI a été nommé responsable de la sécurité de la TI pour l'ensemble de l'Agence, en réalité, il n'est pas habilité à agir à ce titre dans le Laboratoire national de microbiologie (LNM). En fait, c'est le directeur, Soutien informatique, Laboratoires et régions, qui est responsable de la sécurité de la TI dans le LNM. Vu cette fragmentation de la responsabilité, il est possible que la gestion de la sécurité ne soit pas uniforme et efficace au sein de l'ASPC. De plus, les responsabilisations à l'égard de la sécurité de la TI au sein de l'Agence ne sont pas clairement définies.

11. Le comité de gestion de la GI/TI, qui est responsable de l'examen et des décisions touchant les questions de GI/TI importantes et significatives, se rapporte depuis juillet 2010 à un sous comité du Comité exécutif. Le DPI a présenté à ce comité de surveillance une analyse de rentabilisation qui décrivait la situation de la sécurité de la TI au sein de l'Agence et des investissements prioritaires à faire dans les années futures. Nous n'avons pas décelé des rapports fréquents et complets à ce comité de surveillance sur la situation de la sécurité de la TI. Par conséquent, la haute direction n'est pas bien renseignée sur la situation de la sécurité des

programmes de la TI, des pratiques et contrôles, de la conformité à la politique et des risques en matière de sécurité de la TI.

12. GI/TI a mis en place un plan opérationnel qui supporte le plan stratégique de la GI/TI. Cependant, le plan opérationel devrait fournir plus d'information quant au support à la stratégie de sécurité de la TI, à savoir comment améliorer les évaluations du cadre d'imputabilité de la gestion du CT et l'efficacité de la sécurité intégrée.

13. Certains systèmes et certaines applications n'ont pas fait l'objet d'une évaluation des menaces et des risques. De plus, l'Agence ne dispose pas d'un processus de certification et d'accréditation rigoureux et systématique permettant de veiller à ce que les nouveaux systèmes et les principales applications respectent les exigences officielles établies en matière de sécurité avant d'être mis en place au sein du contexte opérationnel. En l'absence d'un rigoureux programme de gestion du risque, l'Agence ne connaît pas bien les risques qui ont trait à ses renseignements et à son infrastructure de TI. Toutefois, un cadre préliminaire de certification et d'accréditation décrivant un nouveau processus proposé est en train d'être élaboré.

14. Le PE et la convention sur les niveaux de service (CNS) conclus entre l'ASPC et Santé Canada ne comprennent pas les indicateurs de niveau de service relatif à la TI. En l'absence de mesures de la gestion du service, y compris des indicateurs de niveau de service relatif à la TI adéquats, le DPI ne peut assurer une gestion efficace du rendement des services relatifs à l'infrastructure de la TI offerts par Santé Canada, notamment sur le plan de la sécurité.

15. Il n'existe aucune stratégie complète ou de programme en place qui explique l'importance de la sécurité de la TI et décrit les responsabilités reliées du personnel de l'ASPC. Un manque de sensibilisation expose l'ASPC à des risques de rupture en sécurité. Nous avons observé que l'Agence a embauché en juillet 2010 un nouvel agent de sensibilisation et de formation en sécurité dont les premières tâches furent de définir les exigences d'un programme et d'une stratégie complète de sensibilisation de la sécurité. Nous avons aussi observé que des personnes qui avaient des tâches spécifiques en sécurité de la TI avaient reçu une formation adéquate en sécurité et suivaient leur plan à-jour annuel de formation professionnelle.

Recommandations

16. Le dirigeant principal de l'information devrait réviser le plan opérationnel visant à soutenir la stratégie de sécurité de la technologie de l'information, élaborer un ensemble complet de politiques couvrant tous les risques importants relatifs à la sécurité de l'information, mettre en œuvre des processus adéquats de surveillance continue et rendre des comptes à la haute direction sur la situation de la sécurité de la technologie de l'information,

17. Le dirigeant principal de l'information devrait mettre en œuvre un processus officiel

de certification et d'accréditation pour les nouveaux systèmes et les applications importantes pour l'Agence.

18. L'agent de sécurité ministériel, en collaboration avec le coordonnateur de la sécurité des technologies de l'information, devrait :

    a) cerner les évaluations des menaces et des risques qui doivent être effectuées;

    b) soutenir les efforts déployés par l'agent de la formation et à la sensibilisation à la sécurité pour élaborer une stratégie et un programme exhaustifs applicables à l'ensemble de l'Agence en vue de sensibiliser les employés aux questions liées à la sécurité à un niveau adéquat.

19. Le sous-ministre adjoint, Affaires organisationnelles et gestion des urgences, devrait chercher à modifier le protocole d'entente et la convention sur les niveaux de service conclus avec Santé Canada en ce qui concerne la sécurité de la technologie de l'information afin que l'ASPC puisse s'assurer qu'elle reçoit le niveau de service dont elle a besoin. Il faudrait notamment inclure des indicateurs de niveau de service pour établir la qualité des services, les coûts, le niveau de rendement escompté et les délais requis. Il faudrait aussi que Santé Canada établisse chaque année la mesure dans laquelle il respecte ses engagements à l'égard des services offerts à l'ASPC au chapitre de la sécurité de la technologie de l'information.

Exploitation des réseaux

Critère : Les réseaux informatiques utilisés par l'ASPC sont protégés par des mesures de contrôle, de sécurité et de protection adéquates.

20. Le processus d'obtention d'un compte de réseau fonctionne bien. Toutefois, il n'existe aucun processus concerté dans l'ensemble des réseaux permettant d'informer les responsables de la GI/TI du départ d'un employé ou d'un entrepreneur. Il est possible que l'identificateur de l'utilisateur et ses droits d'accès restent actifs, même lorsque l'employé ou l'entrepreneur a quitté l'Agence ou occupe de nouvelles fonctions, à la suite d'un changement de ses responsabilités.

21. Les systèmes, les serveurs et les postes de travail de l'Agence ne font pas tous l'objet d'un contrôle régulier en ce qui concerne l'autorisation d'accès et la surveillance des flux d'information vers et depuis les réseaux. Nous avons observé que les pratiques de gestion en place en matière de contrôle des mots de passe sont complètes.

22. L'Agence dispose d'un processus de gestion du changement permettant de gérer les correctifs de sécurité. Toutefois, le système de gestion de la configuration n'est pas robuste, ce qui réduit l'efficacité de la surveillance de l'infrastructure de la TI.

23. Lorsque des parties externes ont accès à de l'information de l'ASPC, il est important qu'elles comprennent leurs responsabilités et s'engagent à la protéger.

Généralement, ces responsabilités sont assurées par des clauses sur la sécurité de l'information, dans les protocoles d'entente ou les conventions sur les niveaux des services. La responsabilité concernant la sécurité de l'information est partagée dans l'ensemble de l'organisme. L'ASPC est exposée à des risques que des normes différentes soient appliquées dans diverses parties de l'ASPC et que des normes ne soient pas suffisamment robustes.

24. Les processus régissant les mesures de sécurité physique sont généralement bien établis, puisque les parties responsables respectives sont concernées et que les mesures de sécurité physique constituent des mesures de protection adéquate.

25. Les fichiers de données sont sauvegardés systématiquement, toutefois, seuls les fichiers de sauvegarde mensuels sont stockés dans un endroit externe. Si un incident physique se produit et détruit ou rend inutilisables les bandes de sauvegarde sur place, l'ASPC s'expose à un risque de perte de données, et les utilisateurs pourraient avoir à suivre un long processus pour récupérer les données perdues.

Recommandations

26. L'agent de sécurité ministériel, en collaboration avec le directeur général des ressources humaines devrait renforcer le processus en place pour modifier l'accès des utilisateurs afin de veiller à ce que les responsables des activités de gestion de l'information et de la technologie de l'information soient informés rapidement des changements de situation d'employés et d'entrepreneurs.

27. Le dirigeant principal de l'information devrait :

    a) établir des lignes directrices et des normes assurant une surveillance régulière de l'ensemble des systèmes, des serveurs et des postes de travail de l'Agence pour autoriser l'accès et surveiller les flux d'information vers et depuis les réseaux;

    b) compléter les processus de gestion de la configuration de la technologie de l'information à l'échelle de l'Agence pour gérer et surveiller les importants éléments de configuration en place;

    c) revoir les pratiques de stockage concernant les supports de sauvegarde de données électroniques et élaborer un plan visant à réduire le risque de perte de données attribuable à un incident se produisant dans l'une des salles de serveur.

28. L'agent de sécurité ministériel, en collaboration avec le dirigeant principal de l'information, devrait mettre en place un processus rigoureux pour soutenir l'élaboration de protocoles d'entente ou de conventions sur les niveaux de service suffisamment robustes pour protéger les renseignements auxquels ont accès les parties externes par l'intermédiaire de l'ASPC.

Gestion des incidents liés à la TI

Critère : Des mesures en place permettent de gérer les incidents liés à la TI, du moment où ils ont été constatés jusqu'à la mise en œuvre des mesures qui s'imposent.

29. Pour détecter les incidents liés à la TI, Santé Canada et l'ASPC ont recours à une multitude d'outils et de techniques. Nous avons remarqué que l'ASPC ne s'est pas prévalue de certains des systèmes et des logiciels de détection au sein de l'Agence. Les risques de ne pas détecter des incidents liés à la TI sont donc plus élevés.

30. La Base de données sur le signalement d'incidents de sécurité, système par lequel tous les incidents liés à la sécurité doivent être déclarés, ne semble pas faire l'objet d'un usage exhaustif. Par conséquent, la gestion des incidents liés à la TI n'est pas des plus efficaces.

Recommandation

31. L'agent de sécurité ministériel, en collaboration avec le dirigeant principal de l'information, devrait prendre une décision à l'égard de l'utilisation future et des changements requis de la Base de données sur le signalement d'incidents de sécurité.

Conclusion

32. Malgré les efforts déployés pour introduire et opérer les systèmes, les pratiques et les contrôles de sécurité de la GI/TI afin de respecter les normes gouvernementales, il faut renforcer l'infrastructure de la sécurité de la TI au sein de l'ASPC afin de respecter les normes GI/TI et les pratiques exemplaires du COBIT. Les domaines suivants qui méritent le plus l'attention de la direction sont : le plan opérationnel et le cadre stratégique exhaustifs liés à la sécurité de la TI, la gestion, le contrôle et la sensibilisation à l'égard des risques et la certification et l'accréditation des nouveaux systèmes et des applications importantes.

33. La mise en œuvre des recommandations mentionnées dans ce rapport permettra de renforcer le programme de sécurité de la TI de l'Agence et d'atténuer les risques de sécurité dans la mesure du possible.

Déclaration de certification

34. Selon mon jugement professionnel en qualité de dirigeant principal de la vérification par intérim, nous avons appliqué des procédures d'examen suffisantes et adéquates, et des éléments probants recueillis soutenant l'exactitude de la conclusion de l'examen sont énoncés dans le rapport. La conclusion de l'examen s'appuie sur une comparaison des conditions, qui prévalaient à l'époque, aux critères d'examen préétablis (voir Annexe A) tel qu'énoncés dans la portée de l'

examen. De plus, les éléments probants ont été recueillis en conformité avec les Normes relatives à la vérification interne au sein du gouvernement du Canada .

Daniel Surprenant, B. Comm., CA
Dirigeant principal de la vérification par intérim

Réponse de la direction

35. La direction de l'Agence souscrit à nos constatations et à nos recommandations, et un plan d'action de la direction est présenté à l'Annexe B.

Remerciements

36. Nous tenons à témoigner notre appréciation à l'égard de la coopération et de l'aide apportées par la direction et les employés à l'équipe d'examen au cours de l'exercice.

Annexe A : Critères d'examen

Gouvernance de la sécurité de la TI
L'ASPC utilise des principes adéquats en matière de gouvernance pour organiser et gérer son programme de sécurité en TI.

Exploitation des réseaux
Les réseaux informatiques utilisés par l'ASPC sont protégés par des mesures de contrôle, de sécurité et de protection adéquates.

Gestion des incidents liés à la TI
Des mesures en place permettent de gérer les incidents liés à la TI, du moment où ils ont été constatés jusqu'à la mise en œuvre des mesures qui s'imposent.

Annexe B : Plan d'action de la direction

Recommandation	Plan d'action de la direction	Cadre de première responsabilité	Date cible
Gouvernance de la sécurité de la TI			
16. Le dirigeant principal de l'information devrait réviser le plan opérationnel visant à soutenir la stratégie de sécurité de la technologie de l'information, élaborer un ensemble complet de politiques couvrant tous les risques importants relatifs à la sécurité de l'information, mettre en œuvre des processus adéquats de surveillance continue et rendre des comptes à la haute direction sur la situation de la sécurité de la technologie de l'information,	D'accord.		
	i) La stratégie de sécurité de la TI mentionnée dans le plan stratégique de la DGITI pour 2010-2013 a été récemment approuvée par le CGITI. Le DPI examinera et intégrera le plan d'action sur la conformité avec la GSTI dans un plan opérationnel exhaustif visant à soutenir la stratégie de sécurité de la TI et cherchera à obtenir l'appui du CGITI. Le plan opérationnel exposera en détail les diverses initiatives, y compris le niveau d'effort, les coûts et les délais, et mentionnera les ressources qu'il faut investir pour répondre aux questions liées à la sécurité de la TI, notamment la conformité avec la GSTI et l'efficacité de la sécurité intégrée.	DPI	Mars 2011 Mise en oeuvre avril 2011
	ii) D'accord. Le bureau du DPI élaborera un ensemble de politiques liées à la sécurité de la TI pour régler les questions prioritaires relatives aux risques, aux incidents de sécurité, les systèmes de détection et d'enquêtes.	DPI	Mars 2011

Recommandation	Plan d'action de la direction	Cadre de première responsabilité	Date cible
	iii) D'accord. Des mesures ont été prises pour améliorer la sécurité globale du processus de reddition de comptes (p. ex. mesures mensuelles). Nous prêterons davantage attention à l'uniformité des politiques et des procédures. Les mesures de contrôle évoluent, et un financement supplémentaire reçu en juillet 2010 a été attribué à l'amélioration de la capacité de surveillance dans la RCN et au LNM. Les améliorations apportées aux mesures de contrôle au sein de la DGITI s'ajouteront aux initiatives d'intervention proactive de la DSAC.	DPI DPI	Mars 2011 Mars 2011
17. Le dirigeant principal de l'information devrait mettre en œuvre un processus officiel de certification et d'accréditation pour les nouveaux systèmes et les applications importantes pour l'Agence.	D'accord. Le DPI cherchera à obtenir l'approbation du processus officiel de certification et d'accréditation auprès du CGITI.	DPI	Mars 2011
18. L'agent de sécurité ministériel, en collaboration avec le coordonnateur de la sécurité des technologies de l'information, devrait :			
a) cerner les évaluations des menaces et des risques qui doivent être effectuées;	D'accord. L'ASM, en collaboration avec le coordonnateur de la sécurité des TI et les	ASM	Mars 2011

Recommandation	Plan d'action de la direction	Cadre de première responsabilité	Date cible
	gestionnaires de programme concernés, établira un plan intégré pour cerner les évaluations des menaces et des risques qui doivent être effectuées, établir l'ordre de priorité quant à l'élaboration des évaluations, prévoir les ressources nécessaires pour effectuer chaque évaluation et établir l'horaire de la mise en œuvre.		
b) soutenir les efforts déployés par l'agent de la formation et à la sensibilisation à la sécurité pour élaborer une stratégie et un programme exhaustifs applicables à l'ensemble de l'Agence en vue de sensibiliser les employés aux questions liées à la sécurité à un niveau adéquat.	D'accord. L'ASM, en collaboration avec le coordonnateur de la sécurité des TI, soutiendra les efforts de l'agent de la sensibilisation à la sécurité et de la formation pour élaborer et mettre en œuvre un programme de formation obligatoire à tous les employés dans l'ensemble de l'Agence.	ASM	Mars 2011
19. Le sous-ministre adjoint, Affaires organisationnelles et gestion des urgences, devrait chercher à modifier le protocole d'entente et la convention sur les niveaux de service conclus avec Santé Canada en ce qui concerne la sécurité de la technologie de l'information afin que l'ASPC puisse s'assurer qu'elle reçoit le niveau de service dont elle a besoin. Il faudrait notamment inclure des indicateurs de niveau de service pour établir la qualité des services, les coûts, le niveau de rendement escompté et les délais requis. Il	D'accord, le SMA AOGU cherchera à apporter des modifications au PE conclu entre l'ASPC et Santé Canada pour inclure des indicateurs de niveau de service relatif à la sécurité de la TI et un rapport d'assurance annuel selon les recommandations.	SMA, AOGU	Mars 2011

Recommandation	Plan d'action de la direction	Cadre de première responsabilité	Date cible
faudrait aussi que Santé Canada établisse chaque année la mesure dans laquelle il respecte ses engagements à l'égard des services offerts à l'ASPC au chapitre de la sécurité de la technologie de l'information.			
Exploitation des réseaux			
26.L'agent de sécurité ministériel, en collaboration avec le directeur général des ressources humaines devrait renforcer le processus en place pour modifier l'accès des utilisateurs afin de veiller à ce que les responsables des activités de gestion de l'information et de la technologie de l'information soient informés rapidement des changements de situation d'employés et d'entrepreneurs.	D'accord.		
	i) L'ASM va améliorer et introduire les changements requis aux processus de modification à l'accès des usagers, et fournir une formation appropriée.	ASM	Mars 2011
	ii) Les opération GI/TI seront améliorées et introduiront les changements requis au processus de modification à l'accès des usagers, en temps opportun.	DPI	Mars 2011
27. Le dirigeant principal de l'information devrait :			
a) établir des lignes directrices et des normes assurant une surveillance régulière de l'ensemble des systèmes, des serveurs et des postes de travail de l'Agence pour autoriser l'accès et surveiller les flux d'information vers et	D'accord. Les processus de contrôle en place concernant les postes de travail, les serveurs et les systèmes sous la responsabilité du DPI s'appuient sur les outils acceptés par l'industrie en matière de détection d'incident et d'intervention en cas d'incident, et les	DPI	Commen-çant en avril 2011

Recommandation	Plan d'action de la direction	Cadre de première responsabilité	Date cible
depuis les réseaux;	techniques feront l'objet d'un examen et d'une amélioration systématiques, au besoin. Quant au suivi des équipements informatiques de nos clients ou de ceux qui résident sur des réseaux de services (par exemple, ceux de Santé Canada ou Travaux publics et Services gouvernementaux Canada), des ententes de services et un périmètre de sécurité amélioré seront développés et utilisés afin d'assurer un contrôle et suivi approprié.		
b) compléter les processus de gestion de la configuration de la technologie de l'information à l'échelle de l'Agence pour gérer et surveiller les importants éléments de configuration en place;	D'accord. Le DPI établira un programme complet pour la gestion de l,intégrité de la sécurité ainsi que la configuration des appareils attachés aux réseaux.	DPI	Mars 2011 Mise en œuvre débutant en juin 2011
c) revoir les pratiques de stockage concernant les supports de sauvegarde de données électroniques et élaborer un plan visant à réduire le risque de perte de données attribuable à un incident se produisant dans l'une des salles de serveur.	D'accord. Le DPI effectuera une revue des pratiques de l'Agence concernant le stockage, la récupération, l'archivage et le recouvrement de données électroniques	DPI	Commen-çant en avril 2011
28. L'agent de sécurité ministériel, en collaboration avec le dirigeant principal de l'information, devrait mettre en place un processus rigoureux pour soutenir l'élaboration de protocoles d'entente ou de	D'accord. i) L'ASM, en collaboration avec le DPI, introduira des exigences obligatoires de service en sécurité afin de protéger	ASM	Juin 2011

Recommandation	Plan d'action de la direction	Cadre de première responsabilité	Date cible
conventions sur les niveaux de service suffisamment robustes pour protéger les renseignements auxquels ont accès les parties externes par l'intermédiaire de l'ASPC.	l'information dont les parties externes on accès dans l'Agence. Des énoncés seront fournis à la division des actifs et la gestion du matériel pour être inclus dans les contrats de l'ASPC; ii) L'ASM introduira un processus qui rendra obligatoire à tous les gestionnaires de programmes d'inclure toutes les ententes incluant les PE et les CNS dans les systèmes de la gestion du matériel. L'ASM obtiendra la liste des ententes, fera une revue annuelle et confirmera avec les auteurs ou propriétaires la conformité et la pertinence des ententes en fonction de la méthodologie intégrée de la sécurité.	ASM	Novembre 2011
Gestion des incidents liés à la TI 31. L'agent de sécurité ministériel, en collaboration avec le dirigeant principal de l'information, devrait prendre une décision à l'égard de l'utilisation future et des changements requis de la Base de données sur le signalement d'incidents de sécurité.	D'accord. L'ASM, en collaboration avec le coordonnateur de la sécurité des TI, soutiendra la tenue d'une évaluation des menaces et des risques et d'une évaluation des facteurs relatifs à la vie privée de la Base de données sur le signalement d'incidents de sécurité dans le but de déterminer s'il est possible d'accroître l'utilisation de la Base de données et d'assurer une formation adéquate quant à son utilisation.	ASM	Mars 2011

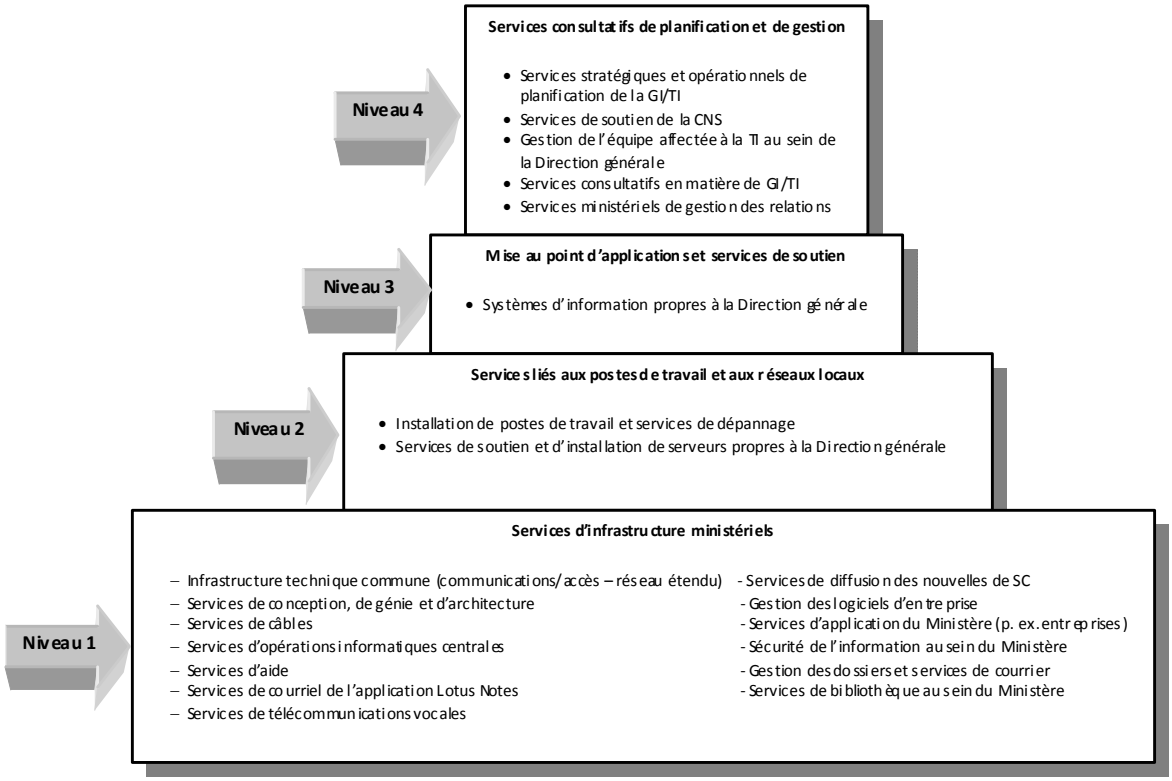
Annexe C : Description des réseaux utilisés par l'ASPC

À l'heure actuelle, l'Agence utilise quatre réseaux : réseau de SC, réseau de l'ASPC, réseau scientifique et réseau de la bioinformatique.

Réseau de SC – Depuis ses débuts, l'ASPC doit gérer la sécurité de ses renseignements électroniques principalement stockés dans le réseau de SC géré par Santé Canada. Un protocole d'entente et une convention sur les niveaux de service ont été ratifiés entre l'ASPC et Santé Canada en ce qui concerne les services de soutien des réseaux fournis par Santé Canada.

La convention sur les niveaux de service précise que les services sont partagés entre Santé Canada et l'ASPC. De façon générale, le DPI-DSGI de Santé Canada offre des services de niveaux 1, 3 et 4 à l'ASPC, tandis que le DPI de l'ASPC offre des services de niveaux 2 et 3 aux utilisateurs de l'ASPC.

Modèle de niveaux de service



L'infrastructure de réseau qu'utilise l'ASPC relève de Santé Canada. Le pouvoir fonctionnel du réseau de SC revient au DPI de Santé Canada, pour autant que l'ASPC et SC mènent leurs activités dans une infrastructure technique commune, qui n'est pas séparée (sur le plan physique ou logique).

À l'ASPC, l'ensemble des employés, des entrepreneurs et des étudiants (environ 2 500) sont liés au réseau de SC et reçoivent les services prévus au niveau 1 mentionnés ci-dessus comme l'accès à l'infrastructure du réseau, aux courriels, aux mesures de protection et de sécurité du réseau, à Internet, aux services d'aide nationaux, aux serveurs et aux systèmes d'exploitation et à la gestion du compte de l'utilisateur.

Réseau de l'ASPC – Les responsables de la GI/TI de l'ASPC ont lancé il y a trois ans le réseau de l'ASPC : un contexte d'infrastructure de réseau plus performant et sécuritaire. Le but principal de ce réseau est d'établir et de mettre en œuvre un réseau qui tolère peu les risques capable de répondre aux exigences en matière de transmission des renseignements et de sécurité énoncées dans la nouvelle *Politique sur la sécurité du gouvernement* du Canada. Le réseau de l'ASPC n'est pas encore pleinement opérationnel.

Réseau scientifique – Le Laboratoire national de microbiologie a créé son propre réseau scientifique et son propre réseau de la bioinformatique pour contourner les limites du réseau de SC. Le réseau a été conçu de façon à offrir aux scientifiques et aux employés du LNM un réseau informatique à haute vitesse ayant une plus grande capacité de stockage et permettant aux scientifiques de recueillir et de transmettre des renseignements et d'établir une base de données d'information accessible par l'ASPC et des scientifiques externes.

Réseau de la bioinformatique – Le réseau local de la bioinformatique constitue une plateforme centrale de la recherche biologique qui doit s'appuyer sur des systèmes informatiques à rendement élevé et des ressources et des connaissances spécialisées en matière d'informatique scientifique. Les principaux utilisateurs de ce système sont les membres de la section de la bioinformatique du LNM, des scientifiques externes à l'ASPC et des collaborateurs invités. Le réseau local vise à améliorer la santé publique en accroissant les connaissances scientifiques, en élaborant des techniques diagnostiques et thérapeutiques de pointe et en facilitant les programmes de surveillance de santé publique. Le réseau offre une base de données traitées à tous les laboratoires qui font partie du LNM. Le réseau est soutenu par le groupe de la bioinformatique.

Annexe D : Liste des acronymes

Agence ou ASPC	Agence de la santé publique du Canada
ASM	Agent de sécurité ministériel
CGITI	Comité de gestion de l'information et de la technologie de l'information
COBIT	*Control Objectives for Information and Related Technology*
CNS	Convention sur les niveaux de service
CSTI	Coordonnateur de la sécurité des technologies de l'information
CT	Conseil du Trésor
EMR	Évaluation des menaces et des risques
DG	Directeur général
DGITI	Direction de la gestion de l'information et de la technologie de l'information
DPI	Dirigeant principal de l'information
DSGI	Direction des services de gestion de l'information
GI/TI	Gestion de l'information/Technologie de l'information
GSTI	Gestion de la sécurité des technologies de l'information
LNM	Laboratoire national de microbiologie
PE	Protocole d'entente
RH	Ressources humaines
SMA	Sous-ministre adjoint
TI	Technologie de l'information