***Services administratifs des tribunaux judiciaires (SATJ)***

# ***Vérification de la sécurité de la technologie de l'information***

**_____** **_____Septembre 2017___**

**M. DANIEL GOSSELIN** **DATE**
**ADMINISTRATEUR EN CHEF**
**SERVICES ADMINISTRATIF DES TRIBUNAUX JUDICIAIRES**

**TABLE des MATIÈRES**

1. SOMMAIRE ..... 2
1.1 Contexte ..... 3
1.2 Objectifs et portée de la vérification ..... 4
1.3 Constatations et recommandations de la vérification ..... 5
1.4 Points forts observés: ..... 5
1.5 Possibilités d'amélioration: ..... 5
1.6 Résumé de la réponse de la direction ..... 6
1.7 Conclusion ..... 6
1.8 Énoncé de conformité ..... 7
2. INTRODUCTION ..... 8
2.1 Contexte ..... 8
2.2 Objectifs de la vérification ..... 9
2.3 Méthodologie ..... 10
2.4 Attestation ..... 11
3. CONSTATATIONS, RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION ..... 11
3.1 Le cadre de gouvernance et de politiques ..... 11
Structure organisationnelle ..... 11
3.2 Gestion des risques et planification ..... 13
Cadre de gestion des risques ..... 13
Stratégie et plan pour la sécurité de la TI ..... 14
3.3 Mesures et contrôles de la sécurité de la TI ..... 17
Élaboration des systèmes ..... 17
Gestion des correctifs ..... 18
Accès logique ..... 18
Surveillance du réseau ..... 20
Gestion des incidents ..... 21
Gestion des mots de passe ..... 22
3.4 Conformité ..... 22
Politiques et normes ..... 22
ANNEXE A — CRITÈRES DE VÉRIFICATION ..... 24

# 1. SOMMAIRE

## *1.1 Contexte*

Le Service administratif des tribunaux judiciaires (SATJ) a été constitué en 2003 en vertu de la Loi sur le Service administratif des tribunaux judiciaires pour fournir ses services aux quatre Cours: la Cour d'appel fédérale, la Cour fédérale, la Cour d'appel de la cour martiale du Canada et la Cour canadienne de l'impôt (les Cours).

La Loi spécifie que l'Administrateur en chef est responsable de la gestion efficace et efficiente et l'administration de toutes les Cours alors que les juges en chef sont responsables des fonctions judiciaires de leurs Cours. Les Cours auxquelles le SATJ offre ses services sont des Cours itinérantes qui siègent et qui entendent des affaires à travers le Canada. Par conséquent, le SATJ doit être capable de soutenir environ 90 membres de la Cour (juges et protonotaires) dans la préparation de documents, dans la réalisation d'audiences et les décisions écrites, « n'importe où, n'importe quand. »

Le soutien aux quatre Cours est offert par l'entremise de trois programmes: les services judiciaires, les services de greffes et les services internes. Les services judiciaires comme les services juridiques et le soutien administratif judiciaire ont pour but d'aider les membres des quatre Cours à s'acquitter de leurs fonctions judiciaires. Les services de greffe traitent les documents juridiques, offrent de l'information aux plaideurs sur la procédure de la Cour, conservent les dossiers de la Cour, participent aux audiences, soutiennent et assistent lors de l'application des ordres de la Cour et travaillent en étroite collaboration avec les bureaux des quatre juges en chef pour assurer la tenue des audiences et le respect des délais dans la reddition des décisions. Les services internes incluent les services ministériels qui s'appliquent à l'ensemble de l'organisation et sont essentiels au soutien des opérations des Cours. Ceci inclut, mais ne se limite pas à la technologie de l'information (TI), la gestion de l'information (GI) et la sécurité.

Les Cours et le SATJ ont été exemptés de l'application d'un décret du gouverneur en 2011 en regard de l'utilisation des services de courriel, de centre de données et de réseau de Services partagés Canada (SPC), ainsi que d'un décret du gouverneur en 2015 sur l'approvisionnement, le centre de données et le service réseau. Le SATJ conserve son propre centre de données et sa propre infrastructure de la TI.

Le SATJ doit atteindre de haut niveau de sécurité de la TI pour protéger la confidentialité judiciaire, les informations de la Cour, les secrets commerciaux et la vie privée. Le processus d'arbitrage doit être protégé des compromis qui pourraient entraîner un accès non autorisé à l'information. La sécurité doit être assurée pendant que les membres des Cours travaillent à l'intérieur des installations qui appartiennent ou non au SATJ, ainsi que lorsqu'ils voyagent. Les défaillances techniques et les vulnérabilités du système pourraient nuire à l'utilité des systèmes et de l'infrastructure de la TI. Cela compromettrait l'ensemble des efforts de modernisation du système des tribunaux, limiterait sérieusement l'habileté du judiciaire à effectuer le travail des Cours itinérantes et mènerait à des activités du tribunal sans fiabilité et peu sûres. Compte tenu de ce qui précède, les plans de la GI et de la TI du SATJ ont priorisé la sécurité de la TI pour assurer une sécurité adéquate des Cours, de l'information et du réseau du SATJ.

Le service de la sécurité de la technologie et de l'information (SSTI) travaille en collaboration avec d'autres secteurs des services de la GI et de la TI, ainsi qu'avec des programmes et des services pour protéger l'intégrité des Cours et les ressources d'information précieuses et sensibles du SATJ. Le SSTI inclut la promotion de la sécurité de l'information et des technologies de l'information, la gestion des incidents de sécurité et la réponse aux demandes d'informations et d'assistances des clients. Le SSTI est aussi responsable d'une palette d'activités permettant d'assurer des opérations

solides et sécuritaires, ce qui inclut, mais ne se limite pas à: surveiller sur le réseau pour la sécurité de la TI; répondre aux alertes de Services partagés Canada; évaluer les faiblesses de l'infrastructure du SATJ; évaluer les risques et les lignes directrices en termes de sécurité pour les nouveaux logiciels et technologies; et disposer des déchets électroniques. Le SSTI contribue aussi activement à la planification et au compte rendu de la sécurité, comme le plan de la continuité des activités et le plan de sécurité ministériel et il contribue aussi aux analyses, comme les facteurs relatifs à la vie privée et l'évaluation de la menace et des risques.

Le SSTI est aussi responsable des opérations de sécurité quotidienne, ce qui comprend le pare-feu, la protection de la sécurité du bureau et de tous les autres services de sécurité du TI. Ce rapport présente les constatations de la vérification du cadre de contrôle du SATJ et des pratiques associées avec la sécurité de la technologie de l'information. La mission de la vérification fait partie du plan pluriannuel de vérification axé sur les risques (PAAR) adopté par le SATJ pour les périodes 2015-16 à 2019-20.

## *1.2 Objectifs et portée de la vérification*

Les objectifs de la vérification consistent à déterminer la pertinence et l'efficacité:

1) Du cadre de gouvernance en place sur la sécurité de la TI pour protéger la sécurité des informations ministérielles et pour aider à assurer la conformité avec les politiques et directives du gouvernement du Canada; et,
2) Des cadres de contrôle sélectionnés (mesures de sécurité) en place pour mitiger les risques de sécurité du TI du SATJ.

La portée de la vérification inclut l'examen:

- Du cadre de gouvernance et de politiques;
- De la gestion des risques et de la planification;
- Des mesures et contrôles clés de la sécurité de la TI, ce qui inclut la gestion des incidents et la sensibilisation sur la sécurité; et,
- De la conformité.

La portée comprend un examen de la gouvernance, de la gestion des risques, et les contrôles et mesures clé conçus pour protéger la sécurité de l'information et les produits de l'information et pour aider à assurer la conformité avec la Politique sur la sécurité du gouvernement et la norme opérationnelle sur la sécurité matérielle: Gestion de la sécurité des technologies de l'information.

La vérification inclut aussi des mises à l'essai précises des contrôles de sécurité de la TI mis en œuvre pour protéger l'information, les applications et les dossiers du réseau. Afin que les observations et les recommandations possibles soient actuelles et significatives, la vérification des activités de gestion et d'essai des contrôles de sécurité de la TI en place s'est étendue sur la période de janvier 2016 à janvier 2017, en mettant l'accent sur les activités les plus récentes.

Les activités de la vérification ont été entreprises dans la région de la capitale nationale (RCN) seulement. Les constatations et les conclusions s'appliquent seulement à l'entité examinée ainsi qu'à l'étendue de la vérification et la période visée.

## *1.3 Constatations et recommandations de la vérification*

En général, la vérification a constaté qu'il y avait un cadre de contrôle de la TI en place qui avait besoin de quelques améliorations. Les points forts observés et les secteurs où il y a des possibilités d'amélioration ont été identifiés, y compris les recommandations connexes présentées ci-dessous. Un exposé plus détaillé des constatations de la vérification est présenté dans la section 3 de ce rapport.

## *1.4 Points forts observés:*

Les points forts suivants ont été observés dans le cadre de gestion de contrôles pour la sécurité de la TI:

- Il y existe une structure organisationnelle pour la sécurité de la TI qui consiste en quatre postes, 3 sont actuellement comblés et relèvent directement du dirigeant principal de l'information (DPI). La sécurité de la TI a un rapport hiérarchique fonctionnel avec l'agent ministériel de la sécurité.
- Il y existe des mécanismes d'établissement de rapports permettant de fournir à la gestion l'information appropriée pour la supervision et la prise de décisions. Par exemple, le comité national des juges sur la gestion de l'information et la technologie de l'information est responsable de la collaboration en vue des décisions sur la GI et la TI, y compris la sécurité de la TI.
- Le SATJ utilise un outil de gestion des correctifs pour les postes de travail de table et les serveurs conformes aux normes de l'industrie.
- Des politiques ont été mises en œuvre pour prévenir, détecter et supprimer les logiciels malveillants.
- Des évaluations sur la vulnérabilité ont été conduites dans l'infrastructure du SATJ.
- La sécurité de la TI travaille actuellement à des initiatives d'améliorations.
- Il y existe un processus documenté sur la gestion des incidents en place, qui comprend les rôles et responsabilités des différentes sections à l'intérieur du SATJ.

## *1.5 Possibilités d'amélioration:*

*Cadre de gouvernance et de politiques*

La vérification a constaté que la TI avait besoin d'identifier les relations de hiérarchie et d'autorité de la sécurité de la TI. Cela entraîne le risque que les questions de sécurité de la TI ne soient pas acheminées à l'autorité du SATJ appropriée et, par conséquent, qu'elles ne soient pas résolues. La vérification recommande que le DPI modifie et approuve la charte de l'équipe de sécurité de la TI pour identifier les relations hiérarchiques et l'autorité de la sécurité de la TI. (Référez-vous à la section 3 du rapport.)

La vérification a constaté que le mandat pour le comité directeur de la sécurité de l'information avait besoin d'être élaboré. Sans mandat, il y existe le risque que le comité puisse dévier de son but et de sa structure et, par conséquent, qu'il puisse ne pas accomplir ses objectifs. La vérification recommande que le DPI élabore, documente et communique un mandat approuvé pour le comité directeur de la sécurité de l'information.

*Gestion des risques et planification*

La vérification a déterminé que SATJ avait besoin d'identifier, dans le processus d'élaboration du système, des points précis pour lesquels la sécurité de la TI est responsable d'examiner la conception du système. Sans cela, les nouvelles applications risquent de ne pas inclure les spécifications efficaces de la sécurité de la TI comme prévu. La vérification recommande que le DPI pose dans l'élaboration du système du SATJ des jalons pour lesquels la sécurité de la TI est responsable d'examiner la conception du système et d'identifier des contrôles de base requis.

La vérification a déterminé que le DPI devait documenter une stratégie de sécurité pour la TI et un plan de mise en œuvre. Sans une stratégie et un plan documentés, les risques pourraient ne pas être atténués, les ressources requises pour atténuer les faiblesses pourraient ne pas être identifiées et les options pour atténuer les risques pourraient ne pas être identifiées. La vérification recommande aux DPI de documenter une stratégie de sécurité pour la TI et un plan de mise en œuvre pour permettre au minimum de rapporter les progrès contre la stratégie et la surveillance sur l'accomplissement des objectifs du plan.

*Mesures et contrôle de sécurité de la TI.*
La vérification constate que même si la sécurité du TI a des procédures spécifiques pour répondre à des cas de sécurité de la TI en lien avec les logiciels de sécurité de postes de travail, il n'y a toutefois pas de cadre général (y compris les politiques et procédures) de surveillance. La vérification recommande de développer un tel cadre.

*Conformité*
La vérification a déterminé que le TI n'avait pas une politique définissant certaines règles pare-feu, les exigences pour réviser les registres de vérification et les exigences pour réviser les règles de privilèges administratifs. Cela crée le risque qu'un accès inapproprié à l'infrastructure du SATJ par des employés puisse passer inaperçu. La vérification recommande que le DPI élabore une politique qui définit les exigences pour réviser les registres de vérification et les règles du personnel sur les privilèges administratifs.

## 1.6 Résumé de la réponse de la direction

La direction est en accord avec les observations de la vérification et les recommandations faites dans ce rapport. Des plans d'action appropriés et détaillés seront élaborés et mis en place.

## 1.7 Conclusion

La vérification constate que le cadre de contrôle en place pour la sécurité de la TI en ce qui concerne:

- Le cadre de gouvernance et de politiques;
- La gestion des risques et de la planification;
- Les mesures et contrôles clés de la sécurité de la TI ce qui inclut la gestion des incidents et la sensibilisation sur la sécurité; et.
- La conformité

fonctionne avec des contrôles-clés alors que des améliorations sont nécessaires tel qu'identifié dans ce rapport.

La vérification constate qu'il y a des possibilités d'amélioration en ce qui concerne la conception et la mise en place d'un cadre de contrôle de sécurité de la TI en lien avec la structure organisationnelle, la planification, les applications en développement et quelques activités de surveillance.

Les constatations et les conclusions s'appliquent seulement à l'entité examinée ainsi qu'à l'étendue de la vérification et la période visée.

## *1.8 Énoncé de conformité*

Selon le jugement professionnel du dirigeant principal de la vérification, des procédures suffisantes et adéquates pour la vérification ont été suivies et les éléments probants ont été recueillis en vue de soutenir l'exactitude de la conclusion fournie et contenue dans ce rapport. La conclusion de la vérification sur une comparaison entre, d'une part, les conditions telles qu'elles existaient au moment de la vérification et, d'autre part, les critères de vérification préétablis qui ont fait l'objet d'un consentement auprès de la direction. La conclusion s'applique seulement à l'entité examinée. Les éléments ont été recueillis conformément aux politiques, aux directives et aux normes du Conseil du Trésor sur la vérification interne et se conforment aux Normes relatives à la vérification interne au sein du gouvernement du Canada.

Les éléments recueillis sont suffisants pour fournir à la haute direction des preuves de la conclusion dérivée de la vérification interne.

*André Bolduc CIA*
*Dirigeant principal de la vérification*

# 2. INTRODUCTION

## *2.1 Contexte*

Le SATJ a été créé en 2003 en vertu de la Loi sur le Service administratif des tribunaux judiciaires pour offrir ses services à la Cour d'appel fédérale, à la Cour fédérale, à la Cour d'appel de la cour martiale du Canada et à la Cour canadienne de l'impôt (les Cours).

La Loi spécifie que l'Administrateur en chef est responsable de la gestion efficace et efficiente, ainsi que l'administration de toutes les Cours, alors que les juges en chef sont responsables des fonctions judiciaires de leurs Cours. Les Cours auxquelles le SATJ offre ses services sont des Cours itinérantes qui siègent et qui entendent des affaires partout au Canada. Par conséquent, le SATJ doit être capable de soutenir environ 90 membres de la Cour (juges et protonotaires) dans la préparation de documents, dans la réalisation d'audiences et dans la rédaction de décisions « n'importe où, n'importe quand. »

Le soutien aux quatre Cours est offert par l'entremise de trois programmes: les services judiciaires, les services de greffe et les services internes. Les services judiciaires, comme les services juridiques et le soutien administratif judiciaire, sont offerts pour aider les membres des quatre Cours à s'acquitter de leurs fonctions judiciaires. Les services de greffe traitent les documents juridiques, offrent de l'information aux plaideurs sur la procédure de la Cour, conservent les dossiers de la Cour, participent aux audiences, soutiennent et assistent dans l'application des ordres de la Cour et travaillent en étroite collaboration avec les bureaux des quatre juges en chef pour assurer la tenue des audiences et le respect des délais dans la réédition des décisions. Les services internes incluent les services ministériels qui s'appliquent à l'ensemble de l'organisation et sont essentiels au soutien des opérations des Cours. Ceci inclut, mais ne se limite pas à la technologie de l'information, la gestion de l'information et la sécurité.

Les Cours et le SATJ ont été exemptés d'un décret du gouverneur en 2011 concernant l'utilisation du courriel, du centre de données et du réseau de Services partagés Canada (SPC), ainsi que d'un décret du gouverneur en 2015 sur l'approvisionnement, le centre de données et le service réseau. Le SATJ conserve son propre centre de données et sa propre infrastructure de la TI.

Le SATJ doit atteindre de hauts niveaux de sécurité de la TI pour protéger la confidentialité judiciaire, les informations de la Cour, les secrets commerciaux et la vie privée. Le processus d'arbitrage doit être protégé des compromis qui pourraient entraîner un accès non autorisé à l'information. La sécurité doit être assurée pendant que les membres des Cours travaillent à l'intérieur des installations qui appartiennent ou non au SATJ, ainsi que lorsqu'ils voyagent. Les défaillances techniques et les vulnérabilités du système pourraient nuire à l'utilité des systèmes et de l'infrastructure de la TI. Cela compromettrait l'ensemble des efforts de modernisation du système des tribunaux, limiterait sérieusement l'habileté du judiciaire à effectuer le travail des Cours itinérantes et mènerait à des activités du tribunal sans fiabilité et peu sûres. Compte tenu de ce qui précède, les plans de la GI et de la TI du SATJ a priorisé la sécurité de la TI pour assurer une sécurité adéquate des Cours, de l'information et du réseau du SATJ.

Le service de la sécurité de la technologie et de l'information (SSTI) travaille en collaboration avec d'autres secteurs de services de la GI et de la TI, ainsi qu'avec des programmes et des services pour protéger l'intégrité des Cours et les ressources d'information précieuses et sensibles du SATJ. Le

SSTI inclut la promotion de l'information et de la sécurité technologiques, la gestion des incidents de sécurité et la réponse aux demandes d'informations et d'assistances des clients. Le SSTI est aussi responsable d'une palette d'activités permettant d'assurer des opérations solides et sécuritaires, ce qui inclut, mais ne se limite pas à: surveiller sur le réseau pour la sécurité de la TI; répondre aux alertes du centre de la sécurité des télécommunications (CST) et services partagés Canada; évaluer les faiblesses de l'infrastructure du SATJ; évaluer les risques et les lignes directrices en termes de sécurité pour les nouveaux logiciels et technologies; et disposer des déchets électroniques. Le SSTI contribue aussi activement à la planification et au compte rendu de la sécurité, comme le plan de la continuité des activités et le plan de sécurité ministériel de discussions, mais il contribue aussi à l'analyse, comme les facteurs relatifs à la vie privée et l'évaluation de la menace et des risques.

Le SSTI est aussi responsable des opérations de sécurité quotidienne, ce qui comprend le pare-feu, la protection de la sécurité du bureau et de tous les autres services de sécurité du TI. Ce rapport présente les constatations de la vérification et du cadre de contrôle du SATJ et des pratiques associées avec la sécurité de la technologie de l'information. La mission de la vérification fait partie du plan pluriannuel de vérification axé sur les risques (PAAR) adopté par le SATJ pour les périodes 2015-16 à 2019-20.

## *2.2 Objectifs de la vérification*

Les objectifs de la vérification consistent à déterminer la pertinence et l'efficacité:

- Du cadre de gouvernance en place sur la sécurité de la TI pour protéger la sécurité de l'information ministérielle et pour s'assurer de la conformité aux politiques et aux directives du gouvernement du Canada; et,
- Des cadres de contrôle sélectionnés (mesures de sécurité) en place pour atténuer les risques de sécurité de la TI.

La portée de la vérification inclut l'examen:

- Du cadre de gouvernance et de politiques
- De la gestion des risques et de la planification
- Des mesures et contrôles clés de la sécurité de la TI ce qui inclut la gestion des incidents et la sensibilisation sur la sécurité.
- De la conformité

La portée comprend un examen de la gouvernance, de la gestion des risques et des mesures, et les contrôles conçus pour protéger la sécurité de l'information et les produits de l'information et pour aider à assurer la conformité avec la Politique sur la sécurité du gouvernement et la norme opérationnelle sur la sécurité matérielle: Gestion de la sécurité des technologies de l'information.

La vérification inclut aussi des mises à l'essai précises des contrôles de sécurité de la TI mis en œuvre pour protéger l'information, les applications et les dossiers du réseau. Afin que les observations et les recommandations possibles soient actuelles et significatives; la vérification des activités de gestion et d'essai des contrôles de sécurité de la TI en place s'est étendue la période de janvier 2016 à janvier 2017 en mettant l'accent sur les activités les plus récentes; le travail sur le terrain de la vérification s'est effectué au siège.

Les activités de la vérification ont été entreprises dans la région de la capitale nationale (RCN) seulement.

## *2.3 Méthodologie*

La mission de vérification a été menée conformément aux *Normes relatives à la vérification interne au sein du gouvernement du Canada*, qui intègre *les normes internationales pour la pratique professionnelle de la vérification interne de l'institut des vérificateurs internes.* Ces normes professionnelles exigent que la vérification interne soit planifiée et menée de façon à garantir que les objectifs de la vérification sont atteints.

L'équipe de vérification a conduit une évaluation du risque lors de phase de planification de la vérification. Les risques principaux ont été identifiés et évalués en utilisant un jugement professionnel et après la considération des faits/facteurs connus par l'équipe de vérification et/ou identifiés lors de la phase de planification de la vérification. La vérification détermine si un risque sera traité par cette vérification en se fondant sur l'évaluation du risque après avoir considéré les mesures d'atténuation, conformément aux discussions avec le personnel du SATJ.

Dans le but de réaliser l'objectif défini par la vérification, des critères de vérification ont été élaborés, d'une part, et des observations, des évaluations et des conclusions ont été tirées, d'autre part. Ces critères de vérification viennent principalement de l'exercice du jugement professionnel, après avoir examiné les résultats des évaluations de risques entrepris dans la phase de planification de la vérification. L'Annexe A de ce rapport présente une liste de critères pour la vérification et la conclusion atteinte pour chaque critère.

Un programme de vérification a été élaboré pour traiter des critères de vérification avec les approches suivantes:

i. Des entrevues et discussions ont été réalisées avec le personnel directement en rapport avec la sécurité de la TI et la sécurité. Une liste des personnes interrogées est présentée dans l'annexe B de ce rapport;

ii. Un examen de la documentation pertinente qui inclut, mais ne se limite pas aux: politiques, procédures, procès-verbaux du CNM, plans et rapports de surveillance; et

iii. Des essais détaillés des contrôles clés et des assertions de la direction.

Dans le but de mener à bien des essais détaillés, un échantillon des documents a été judicieusement choisi pour faire l'essai de la gestion des correctifs et des contrôles d'accès logiques.

### *2.4 Attestation*

L'équipe de vérification atteste la collaboration et le support reçu des personnes interrogées au sein de la gestion de l'information et de la gestion de la technologie de l'information et des services de sécurité.

## 3. CONSTATATIONS, RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION

### *3.1 Le cadre de gouvernance et de politiques*

Il était attendu qu'un cadre de gouvernance de sécurité de la TI soit fixé, afin de définir et communiquer les rôles et les responsabilités, et afin de permettre une gestion efficace des prises de décisions et de la supervision de la sécurité de la TI.

Nous avons conduit des entrevues avec les deux responsables faisant partie des services de sécurité de la TI, le Chef de l'information et agent de sécurité du ministère (ASM). Nous avons révisé plusieurs documents qui comprennent, mais ne se limitent pas au cadre de gestion de la sécurité de l'information.

*Le cadre de gestion de la sécurité de l'information* décrit la gouvernance de la sécurité de l'information du SATJ. La structure de gouvernance inclut un Comité de régie des systèmes informatiques (CRSI) qui est composé d'un dirigeant principal de la gestion de l'information (DPGI), d'un agent de sécurité des systèmes d'information (ASSI), d'un coordonnateur à la sécurité de la TI (CSTI) et d'un architecte d'entreprise technique (AET). La vérification n'a pas trouvé de mandat ou de description de la responsabilité du comité de direction sur la sécurité de l'information. Sans un mandat, il y a un risque que le CRSI dévie de son but et de sa structure et, par conséquent, ne puisse pas accomplir ses objectifs. En plus de du CRSI, le comité national des juges sur la gestion de l'information et technologie de l'information (CNJ GI/TI) est tenu de collaborer en ce qui concerne les décisions en lien avec la GI et la TI. Notre examen des procès-verbaux du CNJ GI/TI montre que les éléments de la sécurité de la TI sont discutés par des intervenants clés. La gouvernance inclut aussi le comité de direction des juges en chef du SATJ et le comité exécutif du SATJ qui établissent l'orientation des stratégies de sécurité du TI et sont tenus au courant des progrès sur les plans de sécurité de la TI.

#### Structure organisationnelle

*Le plan de gestion de la TI* s'identifie à une organisation de la sécurité de la TI avec 4 postes approuvés dédiés à la sécurité de TI. La présente structure organisationnelle de la TI[1] montre que le directeur de la sécurité de la TI se rapporte directement au DPI sans aucune relation officielle et formelle à l'agent de sécurité du ministère (ASM). Le poste de directeur du SSTI est actuellement libre.

La sécurité de la TI est responsable de surveiller l'application de la conformité selon les exigences de la sécurité du gouvernement du Canada, de répondre aux incidents en lien avec la sécurité de la

TI, de surveiller toutes les alertes de sécurité, de recueillir les rapports de performance et de réviser ces rapports pour déceler une tendance et d'offrir une formation sur la sécurité de la TI. La principale responsabilité de la sécurité de la TI est de protéger l'intégrité des Cours et les atouts des renseignements sensibles et précieux du SATJ.

Un projet de *charte de l'équipe de sécurité des technologies de l'information*[2] mentionne que l'équipe de sécurité de la TI est responsable de tous les aspects de la sécurité de l'information et de la technologie du Service des tribunaux judiciaires. La fonction coordonne et promeut l'utilisation responsable des systèmes en accord avec les politiques, les directives et les meilleures pratiques de sécurités du gouvernement du Canada. La charte indique aussi qu'il y a un responsable des services de la sécurité de la TI. Par contre, la charte ne décrit aucune relation hiérarchique ou d'autorité. Cela entraîne le risque que les questions de sécurité de la TI ne soient pas acheminées vers l'autorité du SATJ approprié et, par conséquent, qu'elles ne soient pas résolues. En plus de la charte de l'équipe de sécurité des technologies de l'information, il y existe une *charte de l'équipe des opérations de sécurité des technologies de l'information* qui mentionne que l'équipe est responsable de:

- Coordonner, promouvoir l'utilisation responsable de, et d'offrir un paramètre de sécurité et une stratégie de défense active pour le SATJ;
- Superviser et détecter les problèmes de sécurité au niveau de l'hôte.
- Répondre aux problèmes de sécurité; et
- Offrir le soutien en service, et la gestion du cycle de vie des solutions de sécurité du réseau.

Selon la charte de l'équipe des opérations de sécurité des technologies de l'information en matière de sécurité, l'équipe de sécurité de la TI est censée être composée d'un directeur et de deux analystes de la sécurité. Ce projet de charte d'équipe a été élaboré en janvier 2016 et modifié en novembre 2016.

La sécurité de la TI se rapporte directement au DPI et est responsable de la surveillance des alertes, du recueil des rapports et de l'examen de ces rapports pour déceler une tendance[3]. En plus de la sécurité de la TI, la recommandation 3b du *Plan d'action en matière de sécurité des renseignements judiciaires* mentionne que chaque juridiction est censée s'assurer qu'un agent de la sécurité informatique du système judiciaire est sélectionné. L'agent de la sécurité informatique du système judiciaire rend compte au judiciaire et il est sélectionné pour superviser la gestion des opérations de sécurité de la technologie de l'information de la cour. Le rôle de l'agent de la sécurité informatique du système judiciaire est actuellement occupé par le DPI, qui offre des conseils en matière de sécurité de la TI aux judiciaires rattachés aux informations du judiciaire, à savoir les juges en chef, le CNJ GI/TI où les problèmes de sécurité de la TI sont discutés régulièrement, et plusieurs comités judiciaires, et les membres individuels des Cours. Il y a des réunions trimestrielles de tous les agents de la sécurité informatique du système judiciaire à travers les territoires des Cours canadiennes qui sont assistées par les DPI. Les DPI travaillent actuellement sur l'élaboration de fonctions précises au SATJ pour les agents de la sécurité informatique du système judiciaire. On s'attend à ce que les responsabilités des agents de la sécurité informatique du système judiciaire proposé soient assignées au directeur du SSTI avec des responsabilités quotidiennes de la TI pour la sécurité de la TI avec les Cours et le SATJ. On s'attend à ce que les agents de la sécurité informatique du système judiciaire se rapportent aussi bien au SATJ qu'au judiciaire. Ce n'est pas encore clair quels autres rôles et responsabilités feront partie des tâches des agents de la sécurité informatique du système judiciaire du SATJ.

La structure hiérarchique des services de sécurité de la technologie montre que SSTI rend compte directement au DPI sans rapport hiérarchique formel à l'ASM. En revanche, la vérification a appris

de la part du DPI, aussi bien que de l'ASM, que les services de sécurité de la TI ont un rapport hiérarchique avec l'ASM. Les cas importants de sécurité de la TI sont rapportés à l'ASM.

*Recommandation (Moyenne – amélioration moyenne des présents processus et contrôles)*

1. *Le DPI devrait modifier et approuver la charte de l'équipe de sécurité de la TI pour identifier les relations hiérarchiques et l'autorité de la sécurité de la TI. En plus, le DPI devrait élaborer, documenter et communiquer un mandat approuvé pour le CRSI.*

| *Réponse de la direction et le plan d'action — Recommandation #1*<br><br>Acceptée/adoptée. Alors que les services de sécurité de la TI sont une petite organisation et que les membres de l'équipe en son sein connaissent les rôles, les responsabilités et relations de tous, il est plus prudent de documenter son rapport hiérarchique et d'autorité ainsi que de documenter et communiquer la gouvernance pour la sécurité de l'information et de la technologie. | | |
|---|---|---|
| Plan d'action de la direction<br><br>Réviser et adopter la charte de l'équipe de la sécurité de la TI pour les services de sécurité de la TI. Documenter et communiquer la structure de gouvernance pour la sécurité de l'information et de la technologie. | Agent responsable<br><br>DPI | Échéance pour la finalisation<br><br>Septembre 2017 |

## *3.2 Gestion des risques et planification*

### Cadre de gestion des risques

Il était prévu qu'un cadre de gestion des risques documentés existe, permettant l'évaluation constante des risques de sécurité de la TI et la certification des biens de la TI, ce qui signifie que la direction a autorisé l'utilisation de ces biens et a accepté tous les risques résiduels.

Afin de déterminer si un cadre de gestion des risques existe, la vérification a révisé plusieurs documents y compris le *rapport des contrôles généraux de la technologie de l'information (CGTI) du ministère des Finances*, le *cadre de politique sur la gestion de la TI*, procès-verbaux du CNJ GI/TI et le *PSM*. La vérification constate que le cadre de gestion de risques de la TI existe. Le SATJ utilise les services de surveillance et de cyberdéfense du gouvernement ainsi que ses propres outils pour surveiller la sécurité de la TI. Le PSM mentionne qu'un ensemble d'indicateurs d'usage général est nécessaire pour surveiller quotidiennement l'ensemble des changements dans l'environnement de sécurité et que ces indicateurs seront rapportés sur une base mensuelle. Même si les chartes de l'équipe de la sécurité de la TI n'ont pas encore été mises en place, elles mentionnent toutes les deux que les équipes utiliseront un processus de gestion des risques pour documenter, suivre et surveiller les risques.

La vérification constate que les évaluations des risques effectuées identifient clairement les risques et les activités d'atténuation, mais les activités de surveillance ne sont pas encore efficacement

mises en œuvre. Les plans d'action de la direction ont été documentés pour réduire les risques trouvés.

L'évaluation et l'autorisation de sécurité (EAS) sont le processus par lequel les ministères fédéraux examinent leur infrastructure de la technologie de l'information et élaborent les données probantes nécessaires à l'accréditation d'assurance sécurité. Même s'il n'existe pas de certificats d'accréditation pour les applications d'entreprise existantes, le SATJ a effectué des évaluations de risques sur un nouveau logiciel. Par contre, la vérification ne peut pas déterminer si les risques des biens de la TI des entreprises existantes tombent sous la tolérance au risque du SATJ.

*Recommandation (Élevée – amélioration importante des présents contrôles et processus)*

*2. Le DPI devrait mettre en place un processus complet d'EAS sur les applications clés pour s'assurer que ces applications tombent sous la tolérance au risque de le SATJ.*

| *Réponse de la direction et plan d'action — Recommandation #2*<br><br>Acceptée/adoptée. Un tel exercice assurera que les risques sont évalués de façon appropriée en fonction du niveau de risque du SATJ. | | |
|---|---|---|
| Plan d'action de la direction<br><br>Élaborer un plan global pour mettre en place l'EAS pour les principaux éléments de l'infrastructure et pour les principales applications. | Agent responsable<br><br>DPI | Échéance pour la finalisation<br><br>Novembre 2017 |

## Stratégie et plan pour la sécurité de la TI

Une stratégie de la sécurité de la TI est un plan ou une idée utilisée pour accomplir les buts/objectifs de la sécurité de la TI du SATJ. En revanche, un plan de sécurité de la TI est une liste précise de projets/activités pour atteindre les buts/objectifs de la sécurité de la TI soulignée dans les stratégies de sécurité de la TI.

La vérification s'attend à qu'une stratégie de sécurité de la TI globale et un plan de sécurité de la TI soient documentées et alignées avec le PSM et le plan de la TI, et offrent aussi l'intégration des exigences de la technologie de l'information dans les autres processus. La stratégie de la sécurité de la TI et le plan de sécurité de la TI devraient souligner plus particulièrement les ressources exigées pour la réussite de la stratégie.

Le DPI a souligné les défis opérationnels généraux de la GITI en lien avec le roulement du personnel et l'équilibrage des projets et des opérations quotidiennes[4]. Quelques-uns de ces défis sont réduits par le recours à des experts en sous-traitance pour répondre à des besoins précis. Le *plan de sécurité ministériel* (PSM) pour 2015-2019 identifie un manque de personnel dans l'équipe de sécurité de la GI/TI et indique des mesures ont été prises pour y remédier d'ici mars 2016.

En 2015, le SATJ a reçu des fonds du gouvernement pour améliorer la sécurité physique et de la TI pour les Cours fédérales, y compris les deux nouveaux employés de la sécurité de la TI qui ont été engagés. En plus, le *plan de gestion de l'infrastructure de la TI pour 2016-17 à 2020-21,* soutenu par des fonds reçus en 2016, inclut quatre ETP en TI. Un de ces quatre ETP est pour le groupe des services de sécurité de la TI.

Il y existe un *sommaire/résumé des projets et tâches de la sécurité de l'information* qui identifie les activités de sécurité et les opérations quotidiennes. Il y existe aussi une *liste maîtresse de tâches des STI* qui identifie les différentes tâches de sécurité de la TI. La vérification n'a pas vu de stratégie de la sécurité de la TI, qui inclut les besoins en ressources et les échéanciers ainsi que les rapports réguliers sur une stratégie pour surveiller si la stratégie touche sa cible.

Avoir de multiples listes de projets/tâches crée le risque de chevauchement des projets/tâches, de n'avoir aucune source d'autorité pour les projets/tâches officiels et d'avoir des besoins en ressources imprécis.

*Recommandation (Moyenne – amélioration des processus actuels)*

3. *Le DPI devrait élaborer une liste reconnue pour les projets de sécurité de la TI identifiant les dates estimatives de début et de fin, le financement requis et le besoin en ressources. Une fois cette liste élaborée, le DPI fournira des rapports d'étape sur la liste des projets à la haute direction sur une base régulière.*

*Réponse et plan d'action de la direction — Recommandation #3*

Acceptée/adoptée. Combiner tous les projets et les initiatives de la sécurité de la TI en une liste reconnue sera plus efficace pour suivre le progrès et affecter les ressources.

| Plan d'action de la direction | Agent responsable | Échéance pour la finalisation |
|---|---|---|
| Consolider toutes les listes de projets de sécurité de la TI en une seule liste avec les dates et les ressources nécessaires et s'assurer qu'un processus pour la remise de rapports réguliers sur les progrès à la haute direction du DPI et aux comités de gouvernance appropriés. | DPI | Septembre 2017 |

*Recommandation (Moyenne – amélioration des processus actuels)*

4. *Le DPI élabora un plan de ressources de la sécurité de la TI pour identifier les compétences requises et les processus pour identifier et choisir les ressources requises en sécurité de la TI. Ce plan devra aussi fixer un échéancier raisonnable pour l'embauche de ressources pour la sécurité de la TI.*

*Réponse et plan d'action de la direction — Recommandation #4*

Acceptée/adoptée. Ce plan assurera que les compétences requises sont proprement identifiées et que

| | | |
|---|---|---|
| l'échéancier pour l'embauche de nouvelles ressources pour la sécurité de la TI soit raisonnable. | | |
| Plan d'action de la direction<br><br>Le plan des services de la sécurité de l'information et de la technologie identifiera les compétences requises pour offrir les services ciblés et les ressources nécessaires à l'offre de ces services y compris l'échéancier prévu pour l'embauche du personnel requis. | Agent responsable<br><br>DPI | Échéance pour la finalisation<br><br>Mai 2017 |

Le gouvernement du Canada a identifié les contrôles de base qui représentent les meilleures pratiques pour protéger les réseaux du gouvernement du Canada et pour s'adresser aux cyber menaces actuelles et potentielles. Le SATJ a entièrement mis en œuvre quelques-uns des contrôles alors que d'autres sont à des stades variables de mise en œuvre.

La vérification a déterminé qu'il n'y avait pas de stratégie décrivant comment le SATJ planifie de mettre en œuvre les contrôles restants et les risques pour SATJ de ne pas avoir les contrôles restants.

En 2014/2015, le SATJ a engagé deux entreprises afin de se livrer à des évaluations sur les faiblesses de l'infrastructure de la TI du SATJ. Les entreprises ont cerné des possibilités d'amélioration. Le DPI a fourni à ExCom et au CNJ GI/TI des rapports de situation. Par contre, la vérification n'a pas vu le moindre plan de sécurité de la TI cernant l'échéancier, les ressources requises et une approche en matière de gestion du risque.

*Recommandation (Élevée – amélioration importante des processus actuels)*

5. *Le DPI devrait documenter une stratégie de la sécurité de la TI qui permet:*
   - *établir officiellement l'étendue et les objectifs de la sécurité de la TI,*
   - *prévoir des mesures nécessaires à l'application des objectifs de sécurité de la TI,*
   - *élaborer des rapports sur le progrès de la stratégie,*
   - *superviser pour s'assurer que le plan respecte ses échéanciers,*
   - *assurer le suivi des points en suspens, et*
   - *prévoir les exigences du SATJ*

| | | |
|---|---|---|
| *Réponse et plan d'action de la direction — Recommandation #5*<br><br>Acceptée/adoptée. Une stratégie de la sécurité de la TI va formuler les stratégies et les objectifs déterminants et les plans pour les rencontrer ainsi que l'approche de surveillance et d'établissement des rapports. | | |
| Plan d'action de la direction<br><br>La charte d'équipe révisée (réponse de la direction #1) clarifiera l'étendue et les objectifs des services de sécurité de la TI. Ceci combiné avec le Plan d'activités (réponse de la direction #2) suivra le progrès des projets et des activités de la sécurité de la TI. La remise de rapports réguliers à la haute direction du SATJ et au CNJ GI/TI sera mise en place. | Agent responsable<br><br>DPI | Échéance pour la finalisation<br><br>Septembre 2017 |

## *3.3 Mesures et contrôles de la sécurité de la TI*

La vérification s'attendait à constater que les contrôles de la sécurité de la TI actuellement mise en place sont raisonnablement efficaces en matiere de prévention et de détection des brèches de contrôle.

### Élaboration des systèmes

La vérification n'a pas trouvé de documentation faisant état d'un cycle de gestion et de contrôle des projets d'informatique (CGCPI) du SATJ et, par conséquent, la vérification ne peut pas conclure s'il y existe ou non des exigences de sécurité de la TI définies et communiquées pour les nouveaux projets. La technologie de l'information du SATJ n'a pas son propre cycle de gestion et de contrôle des projets d'informatique (CGCPI), mais possède un cadre de gestion de projet conforme aux directives sur la gestion des projets du Conseil du Trésor et au cadre de gestion de projet de l'Agence.

La vérification s'est fait dire que la sécurité de la TI approuve les modifications des applications ainsi que les nouvelles, avant qu'elles soient installées. La vérification a appris que la sécurité de la TI participait à la réunion hebdomadaire (mercredi) sur la gestion du changement, qui comprend les solutions opérationnelles pour discuter de la liste de demandes de changement en suspens.

La vérification a testé l'un des projets afin de déterminer si la sécurité de la TI est impliquée dans le processus d'élaboration des systèmes. La vérification a constaté que les exigences et les opportunités valides de la sécurité de la TI étaient identifiées.

Toutefois, la documentation n'identifie pas qui a l'autorité pour exécuter les différentes fonctions clés comme faire des examens de la sécurité de la TI.

*Recommandation (Moyenne – améliorations des processus et contrôles actuels)*

6. *Le DPI devrait insérer dans l'élaboration des systèmes du SATJ des points précis auxquels la sécurité de la TI est responsable pour faire l'examen des conceptions des systèmes et permettre à la sécurité de la TI d'identifier les contrôles de base requis pour les nouveaux systèmes.*

| *Réponse et plan d'action de la direction — Recommandation #6*<br><br>Acceptée/adoptée. Les examens de la sécurité de la TI seront officiellement incorporés dans le processus d'élaboration des systèmes. | | |
|---|---|---|
| Plan d'action de la direction | Agent responsable | Échéance pour la finalisation |
| Incorporé dans le CMR et le CGCPI, des points de contrôle précis qui s'adresse aux activités recommandées de la sécurité de la TI tel que spécifié par le processus de mise en place des systèmes de sécurité mentionnée dans le ITSG33. | DPI | Septembre 2017 |

## Gestion des correctifs

Les correctifs sont des pièces additionnelles de code élaborées pour traiter des problèmes (communément appelés « bogues ») dans les logiciels. Les correctifs permettent une fonction supplémentaire ou s'adressent aux faiblesses de la sécurité à l'intérieur d'un programme. Les correctifs et la gestion des faiblesses sont une pratique de sécurité conçue pour prévenir de façon proactive l'exploitation des faiblesses qui existent au sein du SATJ.

L'évaluation des risques précédemment effectuée recommande de renforcer le processus de gestion des correctifs, mais n'indique pas s'il y existe un cadre de gestion des risques efficaces pour les systèmes d'exploitation et des applications opérationnelles.

Le SATJ a révisé son processus de gestion des correctifs. Le PSM de 2015-2019 DSP[5] mentionne que, au cours des trois prochaines années il y aura l'élaboration d'une feuille de route pour continuer à améliorer les correctifs. Le PSM mentionne aussi qu'en 2016 l'application rapide de correctifs de routine aux logiciels sera en place. Les priorités incluent le déploiement de logiciels de correctifs d'ici mars 2016.

La vérification constate que le SATJ a maintenant documenté une *Stratégie de gestion des correctifs pour les ordinateurs d'utilisateurs finaux*, qui décrit le processus à suivre pour distribuer des mises à jour aux ordinateurs de bureau et portables (ordinateurs d'utilisateurs finaux). La vérification constate que le SATJ a pris des mesures pour appliquer des correctifs aux serveurs du réseau du SATJ.

Le SATJ utilise un outil de gestion des correctifs qui correspond aux standards de l'industrie pour offrir une gestion des correctifs. Par contre, les licences sont insuffisantes pour pouvoir utiliser ce logiciel sur tous les serveurs et par conséquent quelques serveurs doivent recevoir l'application de correctifs selon un processus manuel plutôt qu'un processus automatique.

Le SATJ utilise aussi des services pour permettre aux administrateurs de systèmes de gérer la distribution des mises à jour et des « HotFix ». En plus, le SATJ a récemment acquis un ensemble d'outils web interactifs visant les logiciels et les matériels informatiques de gestion ce qui inclut l'application de correctifs automatisés pour quelques-uns des logiciels basés sur le serveur.

Il y existe quelques correctifs en suspens basés sur le serveur qui ne sont pas encore installés, compte tenu de tests approfondis à compléter pour déterminer l'impact sur les nombreuses applications utilisées du SATJ.

*SATJ aborde certaines préoccupations concernant la gestion des correctifs.*

## Accès logique

La vérification a déterminé que la fonction de la sécurité de la technologie de l'information avait établi des politiques et des procédures de surveillance qui s'adressaient à la demande, à l'établissement, à l'émission, à la suspension, à la modification et à la fermeture des comptes d'utilisateurs et aux privilèges d'utilisateur qui en découlent. Les rôles et responsabilités pour le contrôle de l'accès sont clairement définis, documentés et communiqués.

L'accès au contrôle est permis aux employés qui ont besoin de travailler avec des applications particulières et d'accéder à de l'information dans des dossiers ou des centres de données particuliers. Le contrôle est exercé par le gérant demandant un compte d'utilisateur pour les nouveaux employés ou ceux qui ont été transférés. Les procédures ont noté dans la *requête pour un compte réseau d'un employé du SATJ ou un transfert*.

Le directeur, le service à la clientèle et l'infrastructure sont responsables de l'établissement des procédures qui permettent l'accès au réseau électronique du SATJ[6]. Selon la *requête pour un compte réseau d'un employé du SATJ ou un transfert*, la division des services de technologie de l'information (DSTI) accepte un formulaire de « requête pour un compte réseau d'un employé du SATJ ou un transfert » pour le traitement d'une requête pour un nouveau compte d'utilisateur. La DSTI envoie une enveloppe scellée au demandeur qui contient les justificatifs de réseau de l'employé et l'*accusé de réception de la Politique d'utilisation acceptable des réseaux électroniques*, qui est signé par l'employé. Le demandeur retourne l'accusé de réception signé à la section des services du réseau. Ce le même processus utilisé lorsque qu'un employé change d'équipe.

La *politique de sortie du SATJ* mentionne que le responsable doit aviser la TI lorsqu'un employé est licencié ou détaché du SATJ, alors que les *procédures des comptes réseau – responsabilités du superviseur* décrivent le processus de gestion quand un employé arrive et part.

La vérification a testé le processus de compte en obtenant la liste de tous les utilisateurs au SATJ et a choisi un échantillon de 10 utilisateurs. La vérification a déterminé que tous les 10 ont eu les autorisations appropriées pour l'obtention de l'accès aux utilisateurs. Par contre, seulement un utilisateur avait signé un formulaire de confirmation qui est requis par la politique du SATJ en TI. Par conséquent, le SATJ court le risque de ne pas avoir de documentation qui indique que les employés reconnaissent les exigences en ce qui concerne leur utilisation du réseau du SATJ.

*Recommandation (Moyenne – amélioration moyenne aux présents processus et contrôles)*

*7. Le DPI devrait s'assurer que tous les employés qui signent le formulaire sur la politique d'utilisation du réseau pour qu'il reconnaisse leurs responsabilités lors de leur utilisation du réseau du SATJ.*

| *Réponse de la direction et plan d'action — Recommandation #7*<br><br>Acceptée/adoptée. Il est important de s'assurer que ce processus est constamment appliqué. | | |
|---|---|---|
| Plan d'action de la direction | Agent responsable | Échéance pour la finalisation |
| La Politique sur l'utilisation acceptable des dispositifs et des réseaux (PUADR) pour les employés du SATJ sera mise à jour et les employés seront requis de signer officiellement leur attestation. Les employés se feront rappelés la politique lorsqu'ils se connectent et un programme de sensibilisation pour les employés sera lancé pour s'assurer qu'ils soient au courant du PUADR révisé. | DPI | Décembre 2017 |

Selon les *CGTI des Finances*, l'accès des employés licenciés au système financier « Free Balance », au système « Performance Budgeting and Human Capital » et au système des comptes en fiducie n'a pas été invalidé ou enlevé en temps opportun. Conséquemment à cette observation, la vérification a établi un test afin de déterminer si les employés licenciés avaient accès au réseau du SATJ une fois qu'ils avaient quitté le SATJ.

À l'exception d'un compte qui est resté actif, la vérification a déterminé que les individus radiés n'ont plus accès au réseau du SATJ. Tous les comptes sont invalidés ou enlevés dans une courte période de temps. Avoir ce seul compte encore actif expose le SATJ au risque que quelqu'un puisse utiliser le compte pour obtenir un accès non autorisé à l'infrastructure du SATJ.

La *Politique sur l'utilisation acceptable des dispositifs et des réseaux* indique qu'une violation de cette politique fera l'objet d'une mesure disciplinaire correspondant à la gravité et aux circonstances de l'incident. Il est aussi mentionné qu'une violation de la politique sera traitée de façon juste et transparente. Les activités suspectes seront communiquées aux autorités chargées de l'application de la loi et pourraient mener en mesures disciplinaires même s'il n'y a pas de poursuite aux pénales ou au civil.

Les employés sont responsables de la protection de leur identité personnelle en ligne et le gestionnaire, la sécurité de l'information est responsable de la clarification de tous les usages questionnables du réseau. Les employés enverront au bureau d'aide le formulaire de demande et d'autorisation des services d'accès à distance pour obtenir l'accès à distance.

Les politiques de gestion des identités sont mises en application dans chaque nouveau compte et comptes transférés suit les *procédures d'un compte réseau* et les *procédures d'un compte pour un nouvel employé*. La sécurité de la TI fait actuellement l'examen du processus et a recommandé la suppression de quelques comptes.

La sécurité de la TI produit un *rapport des événements de la sécurité de la TI* qui identifie le nombre d'alertes différentes générées, les avis sur la vulnérabilité, les détails des événements de la sécurité et les événements en suspens des mois précédents. Ce rapport inclut aussi les mesures prises. Se référer à la recommandation #8 ci-dessous concernant la surveillance des comptes d'utilisateurs.

## Surveillance du réseau

On s'attendait à ce que SATJ surveille régulièrement son réseau pour des événements de sécurité et l'accès des utilisateurs.

On constate que le réseau du SATJ est surveillé régulièrement pour des événements sur la sécurité de la TI[7]. Les pare-feu du SATJ utilisent un produit qui est un outil de gestion centralisé pour tous les pare-feu sur le réseau. Il a un registre central de tous les pare-feu et peut faire un rapport historique. Le SATJ utilise un outil de rapport qui peut identifier les menaces, les problèmes et les tendances principaux à la sécurité du réseau. Il peut surveiller et obtenir des aperçus cruciaux et en temps opportun sur la sécurité du réseau, en temps réel de n'importe où à n'importe quel moment.

Un système de surveillance de réseau sert généralement à faire le suivi de l'entièreté de l'infrastructure de la TI y compris tous les appareils et les systèmes.

*Recommandation (Moyenne – amélioration moyenne aux présents processus et contrôles)*

#8. *Le DPI devrait élaborer une politique et une procédure pour la surveillance régulière des événements de sécurité qui se produisent sur le réseau du SATJ. Ceci devrait inclure la surveillance des dernières dates d'accès pour tous les comptes d'utilisateur et s'assurer aussi que les employés et entrepreneurs licenciés ont leurs comptes invalidés.*

| *Réponse et plan d'action de la direction — Recommandation #8*<br><br>Acceptée/adoptée. Un cadre assurera une approche plus coordonnée pour la surveillance de la sécurité de la TI ce qui inclut l'identification des comptes inactifs. | | |
|---|---|---|
| Plan d'action de la direction | Agent responsable | Échéance pour la finalisation |
| Élaborer une politique soulignant la surveillance régulière des événements de sécurité de la TI et documenter les procédures opérationnelles utilisées pour la surveillance de ces événements de sécurité de la TI. | DPI | Septembre 2017 |
| Élaborer des processus améliorés pour obtenir, en temps opportun, l'information sur le départ des employés et des entrepreneurs, ce qu'incluent les rapports pour identifier les comptes inactifs et les procédures détaillées pour les invalider ou les supprimer. | DPI | Septembre 2017 |

## Gestion des incidents

On s'attendait à constater un processus de gestion des incidents permettant la classification des incidents, l'enregistrement des incidents et l'établissement de rapports sur les incidents au sein du SATJ.

On a constaté que SATJ a un processus de gestion des incidents efficace qui inclut le *guide opérationnel de la gestion des incidents de sécurité de la TI et de la cyber sécurité* qui identifie les rôles et les responsabilités des différentes sections au sein du SATJ. Le guide définit et classifie les incidents en impacts faible, moyen ou élevé, souligne les procédures pour la détection des incidents, la réponse aux incidents, l'élaboration de rapports sur les incidents et le rétablissement après des incidents. En plus, un guide du SATJ produit pour décrire le déploiement de logiciel anti-maliciel et anti-exploitation décrit les procédures pour la gestion des incidents quand un maliciel est découvert sur les ordinateurs. SATJ a aussi une procédure pour s'occuper d'un événement qui a été détecté soit par CST ou SPC et décrit comment SATJ réagit en face d'un serveur menacé.

La vérification a fait l'examen d'un rapport d'incident de février 2017 *(rapport d'évènements de sécurité de la TI)* et constate que les incidents sont classifiés, les mesures documentées[8] et les incidents communiqués à la direction à travers ce *rapport d'événements de sécurité de la TI*.

La vérification détermine que le processus de gestion des incidents de sécurité inclut:

- La détection et la classification des événements
- La corrélation des événements et évaluation des menaces/incidents

- La résolution de la menace ou la création et la transmission de l'ordre de travail aux échelons supérieurs
- Les critères pour commencer le processus de réponse à un incident de l'organisme
- Qui a l'autorité pour déclarer un incident
- Les procédures de transmission aux échelons supérieurs
- La vérification et les niveaux requis de documentation de la résolution
- L'analyse de l'après-mise en œuvre
- La clôture de l'ordre de travail/incident

Alors que le traitement des incidents suit le plan de gestion des incidents, il n'y a pas d'échéanciers pour résoudre les faiblesses en suspens de la sécurité de la TI.

*Le SATJ s'occupe des préoccupations autour de la gestion des incidents.*

### Gestion des mots de passe

On s'attend à ce que SATJ ait une politique sur les mots de passe identifiant les exigences pour les mots de passe forts, la protection des mots de passe et le changement de mots de passe.

On constate que la gestion des identités au SATJ inclut une *politique de protection des mots de passe* qui est la norme pour la création des mots de passe forts, la protection de ces mots de passe et l'identification de la fréquence de changement des mots de passe.

Les *meilleures pratiques de sécurité de la TI du SATJ* incluent aussi des instructions sur la création d'un mot de passe fort (diapositive 3).

*Le SATJ aborde les préoccupations autour de la gestion des mots de passe*

## *3.4 Conformité*

Il était prévu qu'un cadre de contrôle de la sécurité de la TI qui inclut les politiques appropriés pour assurer que la sécurité de la technologie de l'information soit adéquatement en place pour réduire les risques de sécurité de la TI du SATJ.

### Politiques et normes

L'examen du *cadre de gestion de la sécurité de l'information* version 6 montre que la politique et les normes de sécurité de l'information reflètent un ensemble pertinent de directives, de règles et de pratiques qui prescrivent comment SATJ gère, protège et distribue l'information. Le cadre de gestion de la sécurité de l'information fait référence à des politiques précises du gouvernement du Canada ce qui inclut, mais ne se limite pas à : *Politique sur la sécurité du gouvernement, Directive sur la gestion de la sécurité ministérielle, Directive sur les rôles et responsabilités en matière de gestion de l'information, Politique sur la gestion de l'information et la protection des renseignements personnels - politiques et publications*. Il fait aussi référence aux politiques ministérielles du SATJ lesquelles incluent: *le cadre de gestion de l'information, le cadre de gestion des documents, l'information et la gestion des documents, et la sécurité de l'information*.

La vérification détermine que le cadre de gestion de la sécurité de la TI du SATJ inclut les politiques et procédures utiles en lien avec le cadre de gestion de la sécurité de l'information comme:

- *Le plan de gestion de la TI du SATJ* qui mentionne que les services réseau et l'infrastructure soutiennent un grand éventail d'applications et plusieurs mesures de sécurité qui inclut le contrôle de l'accès;
- *La politique de sécurité de la TI du SATJ* qui mentionne que le personnel des opérations du DSTI sous la direction du directeur de la DSTI est responsable de la gestion des privilèges et des droits d'accès;
- *La politique du SATJ sur l'accès à distance* qui mentionne que l'un des objectifs de la politique est d'équilibrer la technologie et les contrôles avec le soutien pour gérer l'accès à distance[9] et décrit les exigences pour contrôler l'accès à distance;
- *La politique sur l'utilisation des réseaux électroniques et des dispositifs* mentionne que SATJ va avertir les personnes autorisées de SATJ de ses pratiques de surveillance et que les utilisateurs autorisés sont responsables de la prise de mesures raisonnables pour contrôler l'utilisation, la force et la confidentialité de leur mot de passe;
- *La politique des mots de passe du SATJ* requiert des mots de passe forts qui doivent être changés tous les trois mois.

Des politiques ont été mises en œuvre pour prévenir, détecter et supprimer les logiciels malveillants. Ces politiques incluent une politique de protection contre des logiciels malveillants communiqués à travers SATJ. Ces politiques sont situées sur l'Intranet du SATJ. N'importe quelle violation des politiques et des procédures mentionnées ci-dessus peut être sujette à des actions disciplinaires contre l'employé.

La vérification constate que le cadre de sécurité de la TI du SATJ offre un contrôle des accès logiques efficaces, mais ne décrit pas certaines règles et exigences d'examen. Ceci crée le risque qu'un accès inapproprié à l'infrastructure du SATJ par le personnel puisse passer inaperçu.

*Recommandation (Moyenne – améliorations des processus et contrôles actuels)*

9. *Le DPI devra élaborer une politique qui définit:*
   - *les exigences pour l'examen des journaux de la vérification; et,*
   - *des règles pour les privilèges administratifs.*

| *Réponse et plan d'action de la direction Recommandation #9*<br><br>Acceptée/adoptée. Une politique assurera que les exigences et les responsabilités en lien aux pratiques opérationnelles sont proprement appliquées. | | |
|---|---|---|
| Plan d'action de la direction<br><br>Élaborer une politique de protection périmètre.<br><br>Élaborer une politique en lien avec la gestion et la surveillance des privilèges administratifs. | Agent responsable<br><br>DPI | Échéance pour la finalisation<br><br>Décembre 2017 |

# ANNEXE A — CRITÈRES DE VÉRIFICATION

| | |
|---|---|
| **C1** | Un cadre de gouvernance de sécurité de la TI existante qui permet la prise de décisions efficace et un aperçu de la sécurité de la TI. |
| **C2** | Un plan global de la mise en place de la sécurité de la TI est documenté et s'aligne avec le PSM et le plan de la TI et permet l'intégration des exigences de la sécurité de l'information dans d'autres processus. |
| **C3** | Un cadre documenté de la gestion des risques existants permet l'évaluation continue des risques de sécurité de la TI et l'attestation des biens de la TI ce qui signifie que la direction a autorisé l'utilisation de ces biens et a accepté les risques résiduels. |
| **C4** | Un cadre de contrôle de la sécurité de la TI existant qui inclut les politiques qui sont appropriées pour assurer que la sécurité de la technologie de l'information soit adéquate. |
| **C5** | Les contrôles de sécurité de la TI qui sont actuellement en place sont raisonnablement efficaces dans la prévention et la détection des brèches de contrôle. |