COMITÉ DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT DE SÉCURITÉ

TRÈS SECRET//RÉSERVÉ AUX CANADIENS

EXAMEN DU COMITÉ DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT DE SÉCURITÉ 2016-05

EXAMEN DES CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

RÉSUMÉ

Un organisme de renseignement de sécurité doit trouver un juste équilibre entre l'impératif de collaboration et d'échange et la limitation de l'accès aux renseignements sensibles. Par conséquent, le Service canadien du renseignement de sécurité (SCRS) a mis en place des contrôles de sécurité avancés visant à remédier aux faiblesses potentielles liées au stockage, à la transmission et à l'échange de renseignements classifiés.

Le Comité de surveillance des activités de renseignement de sécurité (CSARS) a évalué la pertinence des mesures de contrôle de l'accès pour la sécurité relativement à la protection des informations sensibles au sein du Service et a conclu qu'elles répondaient aux exigences établies par le gouvernement du Canada ou les dépassaient.

Le CSARS est d'accord avec les exigences et les recommandations relatives aux contrôles de sécurité

et recommande que le SCRS

applique les constatations dans un délai accéléré et élargisse la portée de l'initiative à l'ensemble de l'organisation.

De même, le CSARS a conclu que le SCRS était pleinement conforme dans la façon dont il gère les risques dans le contexte du contrôle de l'accès à l'information sensible et il recommande que le processus de gestion des risques intègre les renseignements opérationnels sur les menaces afin de renforcer sa position défensive au-delà des niveaux actuels, dans le but d'adopter des pratiques exemplaires en matière de sécurité dans l'ensemble de l'organisation.

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

Table des matières

1	INTRODUCTION	3
2	MÉTHODE.....	5
3	SYSTÈMES ET RENSEIGNEMENTS.....	7
3.1		7
3.2	Renseignements.....	7
4	CONSTATATIONS	9
4.1	Politiques	9
4.2	Systemes.....	9
4.3	Conformité	10
5	CONTRÔLE DE L'ACCÈS	13
5.1		13
5.2		13
5.2.1		14
5.2.2		14
5.2.3		15
6	INTERDÉPENDANCES EN MATIÈRE DE SÉCURITÉ.....	17
6.1	Vérification de la sécurité organisationnelle complète	17
6.2	Dispositifs non sécurisés.....	17
6.3	Contrôle	17
6.4	Continuité des activités	18
7	EFFICACITÉ DE LA GESTION DES RISQUES.....	19
8	CONCLUSION.....	22
	RÉSUMÉ DES CONSTATATIONS	24
	RÉSUMÉ DES RECOMMANDATIONS.....	25

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

1 INTRODUCTION

Dans son plan stratégique 2014-2017, le SCRS s'est engagé à élaborer et à mettre en œuvre des projets de transformation prioritaires au cours des trois prochaines années.

Les objectifs initiaux de ce programme,
ont été atteints.

Dans un examen récent de l'effet de la menace interne sur la gestion de l'information, le CSARS a conclu que

Néanmoins, la menace interne n'est que l'une des nombreuses menaces auxquelles le SCRS est confronté. Puisque l'information est l'instrument du SCRS, l'organisation doit trouver un juste équilibre entre l'impératif de collaboration et d'échange et la limitation de l'accès aux renseignements sensibles.

L'objectif de cet examen était d'évaluer la pertinence des mesures de contrôle de l'accès pour la sécurité dans un contexte de protection des informations sensibles au sein du SCRS. Le principe fondamental de l'évaluation de la suffisance des contrôles de l'accès était de vérifier s'ils étaient conformes aux politiques, aux normes ou aux lignes directrices et de s'assurer qu'ils étaient bien harmonisés en fonction du niveau de risque. Bien que l'examen ait porté principalement sur le contrôle de l'accès, le CSARS s'est également penché sur les mécanismes et les contrôles de sécurité généraux dont dépend l'accès. À cette fin, le CSARS a examiné la conformité des politiques et l'efficacité des mesures de sécurité

Le SCRS est l'un des environnements de sécurité de la technologie de l'information les plus complexes de tous les ministères et organismes. Au cours des dernières années, le SCRS a déployé des mesures de contrôle de sécurité visant à remédier aux faiblesses potentielles liées au stockage, à la transmission et à l'échange de renseignements classifiés. Parallèlement, le SCRS s'est efforcé de s'acquitter de ses obligations

À cet égard, le CSARS a conclu que le SCRS était pleinement conforme aux normes gouvernementales en matière de contrôle de l'accès aux informations sensibles et de l'accès aux systèmes, et les a souvent dépassées. L'accès aux installations, aux applications, aux systèmes et au contenu est contrôlé,

Le CSARS a encouragé le SCRS à
tenir compte des constatations

et à accélérer
à l'avenir. À cette fin, le CSARS a formulé des recommandations visant à appuyer et à faire avancer les efforts et les initiatives du SCRS en matière de sécurité interne. Enfin, le CSARS a recommandé que le processus de gestion des risques du SCRS intègre les renseignements opérationnels sur les menaces

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

, l'objectif étant d'adopter des pratiques exemplaires
en matière de sécurité dans l'ensemble de l'organisation.

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

2 MÉTHODE

Cet examen a porté sur l'accès du SCRS à des renseignements et à des systèmes sensibles afin d'assurer la conformité aux lois, aux politiques et aux normes, ainsi que l'efficacité des pratiques exemplaires et du profil de risque du Service. Bien que l'examen ait porté principalement sur le contrôle de l'accès, le CSARS a également examiné les mécanismes et les contrôles de sécurité généraux dont dépend l'accès. Le CSARS a examiné la documentation relative à la sécurité de la technologie de l'information (TI) et aux listes d'accès, notamment : les politiques et procédures internes du SCRS, la planification technologique et organisationnelle, les vérifications internes, les présentations et les preuves de certification. De plus, le CSARS a rencontré des membres du personnel du SCRS afin de fournir un contexte relativement aux questions à l'étude.

La portée de l'examen du CSARS est harmonisée avec celle de l'initiative d'évaluation de sécurité et d'autorisation du SCRS.

Le CSARS a utilisé le cadre d'évaluation suivant :

- L'examen des politiques a servi à vérifier si les politiques et les procédures existantes étaient complètes par rapport aux politiques gouvernementales et ministérielles, aux normes internationales et aux pratiques exemplaires;
- L'analyse des systèmes a permis de dresser la liste des systèmes en place et d'examiner dans quelle mesure les contrôles de l'accès avaient été mis en œuvre. Le CSARS a examiné les dessins, les schémas, les flux d'information et les contrôles de sécurité de l'architecture de conception des systèmes;
- La vérification de la conformité aux politiques a servi à déterminer dans quelle mesure l'organisation respectait les lois, les politiques, les orientations, les normes et les pratiques exemplaires. Il s'agissait notamment d'examiner les vérifications existantes et la preuve de certification au titre du processus d'évaluation de sécurité et d'autorisation;
- L'analyse des interdépendances a servi à examiner les interdépendances critiques en matière de sécurité qui avaient une incidence sur l'accès à des informations sensibles;

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**

ÉTUDE 2016-05

**TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

- L'analyse fondée sur les risques a permis de déterminer si le niveau de sécurité était approprié pour une menace ou un risque donné, et d'évaluer l'efficacité des contrôles de sécurité et de protection des renseignements personnels. Le CSARS a examiné le profil de risque de l'organisation, l'évaluation des menaces et des risques liés aux systèmes, les évaluations du renseignement sur la cybermenace du SCRS, les renseignements issus de sources ouvertes ainsi que d'autres éléments de preuve contemporains.

La principale période visée par cet examen s'échelonnait de novembre 2016 à janvier 2017. Cependant, le CSARS a demandé d'obtenir des renseignements qui ne faisaient pas partie de cette période afin de fournir une évaluation complète.

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ**
AUX CANADIENS

3 SYSTÈMES ET RENSEIGNEMENTS

Le SCRS compte trois unités principales chargées d'assurer l'accès aux systèmes et aux renseignements organisationnels :

L'accès aux applications organisationnelles et aux bases de données opérationnelles est géré par

3.1

est le plus grand réseau du SCRS et le principal réseau utilisé par la majorité du personnel du Service. Ce réseau, qui fournit les capacités quotidiennes générales,

Au cours de l'examen, le CSARS a reçu de la documentation et des séances d'information techniques qui lui ont permis d'avoir une vue d'ensemble des systèmes et des renseignements visés.

3.2

Renseignements

L'accès aux installations, aux applications, aux systèmes et au contenu est contrôlé.

L'utilisation de
et de contrôle de la conformité

facilite l'application des mesures de sécurité

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

Date : _____
FÉV. 2019

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

5 avril 2017

8

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

4 CONSTATATIONS

4.1 Politiques

Les politiques gouvernementales⁹ exigent que le SCRS tienne à jour ses politiques et procédures en matière de sécurité. La feuille de route ministérielle sur la sécurité de la TI s'appuie sur les normes et lignes directrices établies du gouvernement du Canada, comme la norme ITSG-33 *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie* et la norme Gestion de la sécurité des technologies de l'information. La norme Gestion de la sécurité des technologies de l'information prévoit que les ministères doivent adopter une stratégie de défense active qui inclut la prévention, la détection, la réaction et la reprise¹⁰. La prévention est le premier mécanisme de défense, mais les mesures de prévention peuvent être vaines. Le SCRS doit être en mesure de détecter rapidement les incidents, de réagir rapidement pour contenir les dommages et de restaurer les systèmes et les données rapidement pour poursuivre ses opérations¹¹. **Le CSARS a examiné les politiques, les procédures et les directives du SCRS en matière de sécurité pour s'assurer qu'elles étaient complètes par rapport aux politiques et aux normes du gouvernement et du Ministère, et il a conclu qu'elles répondaient aux exigences établies par le gouvernement du Canada ou les dépassaient.**

4.2 Systèmes

suit une méthode officielle pour évaluer et recommander des contrôles de sécurité pour les systèmes de TI en s'appuyant sur l'Architecture de sécurité intégrée du Secrétariat du Conseil du Trésor.

⁹ Politique sur la gestion de l'information du gouvernement (1^{er} juillet 2007) et Politique sur la sécurité du gouvernement (1^{er} juillet 2009).

¹⁰ PDRR (Prévention, Détection, Réponse et Reprise) n'est généralement pas considéré comme une stratégie de défense active, mais plutôt comme une stratégie réactive au sein de l'industrie.

¹¹

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

Le CSARS est parvenu à déterminer tous les composants des systèmes et les contrôles de l'accès pour la sécurité. Les documents qui ont été examinés faisaient souvent référence au réseau du SCRS comme

Le CSARS estime qu'il est utile de mettre en œuvre les initiatives décrites dans la feuille de route sur la sécurité de la TI.

Les constatations du CSARS sont étayées par des documents procéduraux et techniques, des séances d'information et des entrevues avec des experts de la Direction de la vérification interne, Le CSARS a mentionné que le SCRS avait une feuille de route claire sur la sécurité de la TI et que la haute direction s'était engagée à considérer la sécurité de la TI comme une priorité stratégique organisationnelle. **Le CSARS a conclu que le SCRS avait fait preuve d'une grande maturité en matière de gestion de l'information, de sécurité et de protection des renseignements personnels, et que le personnel avait démontré une compréhension exemplaire de la sécurité, des renseignements, de la technologie et des systèmes organisationnels.**

4.3 Conformité

Le processus d'évaluation de sécurité et d'autorisation du réseau de production classifié d'entreprise a été mis en œuvre après la méthodologie harmonisée d'évaluation des menaces et des risques (EMR). La méthodologie harmonisée d'EMR a servi à évaluer les menaces et les risques physiques et informatiques, et le cadre d'analyse s'appuyait sur les Lignes directrices sur la sécurité de la technologie de l'information (ITSG-33 et ITSG-22). La Ligne directrice ITSG-33 et la méthodologie harmonisée d'EMR sont les outils dont le SCRS se sert pour mesurer le respect des contrôles de sécurité normalisés discrets et, par déduction, le risque résiduel. **Le CSARS souscrit aux exigences et aux recommandations relatives aux contrôles de sécurité déposées dans le cadre de l'évaluation de sécurité et d'autorisation (ESA) de l'organisation et recommande que le SCRS mette en œuvre ses conclusions dans un délai accéléré et étende la portée de l'initiative à l'ensemble de l'organisation.**

En ce qui concerne les lois et les politiques gouvernementales, seule la Ligne directrice ITSG-33 porte sur le contrôle de l'accès de manière suffisamment précise, mais elle n'est pas normative en soi, et renvoie plutôt aux « pratiques exemplaires ». La Ligne directrice ITSG-33 est dérivée de la norme ISO 17099, qui est en vigueur depuis plus de vingt ans et qui n'a jamais été conçue pour s'appliquer à des environnements litigieux.

Par conséquent, **le CSARS recommande que le processus de**

Date: _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**

ÉTUDE 2016-05

**TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

gestion des risques du SCRS intègre des renseignements opérationnels sur les menaces pour renforcer sa position défensive au-delà des niveaux actuels, dans le but d'adopter des pratiques exemplaires en matière de sécurité dans l'ensemble de l'organisation.

participe en tant que membre à part entière de l'équipe à tous les nouveaux projets de systèmes de TI afin d'aider et de conseiller les concepteurs et les développeurs en matière de conception, de mise à l'essai et d'exécution des systèmes de sécurité.

Les Lignes directrices sur la sécurité de la technologie de l'information sont les normes minimales qu'un ministère ordinaire doit appliquer. Bien que, de façon générale, le SCRS dépasse ces normes, il doit continuer de chercher à appliquer les pratiques exemplaires dans l'ensemble de l'organisation.

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

5 CONTRÔLE DE L'ACCÈS

Le SCRS est l'un des environnements de sécurité de la TI les plus complexes de tous les ministères et organismes du gouvernement du Canada. Au cours des dernières années, le SCRS a déployé des contrôles de sécurité supplémentaires visant à remédier aux faiblesses potentielles liées au stockage, à la transmission et à l'échange de renseignements classifiés.

Au sens le plus simple, le contrôle de l'accès est le moyen par lequel l'utilisateur légitime d'un ordinateur obtient l'autorisation, ou se voit refuser l'autorisation, d'effectuer des activités sur des objets informatiques. De manière générale, l'objectif d'un système de contrôle de l'accès est de protéger les ressources du système informatique contre l'accès inapproprié par un utilisateur. Les activités visées sont notamment la lecture, l'écriture, l'exécution et l'impression. Les objets¹⁷ protégés peuvent inclure des fichiers (comme un document Word ou une feuille de calcul Excel), des dossiers, des applications, des bases de données, etc. Les contrôles de l'accès, qui sont généralement classés comme discrétionnaires ou non discrétionnaires, font l'objet d'un examen dans cette section.

5.1

5.2

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

5.2.1

5.2.2

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

5.2.3

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

6 INTERDÉPENDANCES EN MATIÈRE DE SÉCURITÉ

Le CSARS a effectué une analyse des interdépendances afin d'étudier les interdépendances critiques, les propriétés en matière de sécurité, les composantes et les contrôles qui ont une incidence sur l'accès à l'information sensible. Bien que le principal objet de l'examen ait été le contrôle de l'accès au sein de celui-ci ne peut être examiné de façon isolée. Le CSARS a donc examiné les caractéristiques globales en matière de sécurité des réseaux qui ont une incidence sur le contrôle de l'accès²⁴.

6.1 Vérification de la sécurité organisationnelle complète

L'initiative d'évaluation de sécurité et d'autorisation du SCRS a établi une norme élevée en matière d'assurance de la sécurité. Le SCRS aurait avantage à déployer la même rigueur dans toute l'organisation,

Une analyse de la surface d'attaque et une vérification externe de la sécurité opérationnelle de l'organisation sont également des pratiques exemplaires²⁵.

6.2 Dispositifs non sécurisés

Le SCRS contrôle étroitement et restreint l'utilisation des dispositifs sans fil.

Comme le SCRS reconnaît le risque résiduel il devrait continuer à élaborer une politique régissant les conditions et les lieux dans lesquels peuvent mener leurs activités dans les installations du Service. Le CSARS encourage le SCRS à élaborer une solution

6.3 Contrôle

Dans le cadre de l'initiative sur la protection des renseignements personnels, le SCRS a cherché à contrôler l'utilisation de

²⁴ Vous trouverez des mesures de sécurité supplémentaires à l'annexe C.

²⁵ Une analyse de la surface d'attaque est une évaluation externe de l'organisation du point de vue d'un adversaire. L'analyse mesure la présence humaine, informatique et physique de l'organisation et établit des modèles à partir de celle-ci, afin de vérifier le ciblage des vecteurs d'attaque et des expositions possibles et probables en fonction du facteur lié au travail. Il s'agit d'une analyse fondée sur des données probantes et qui tient compte des menaces.

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**

ÉTUDE 2016-05

**TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

**Le CSARS approuve la recommandation visant à étendre le contrôle de
à d'autres réseaux et systèmes**

L'efficacité des contrôles de _____ déployés dans tous les environnements de l'organisation devrait être vérifiée régulièrement.

6.4 Continuité des activités

Le traitement et le contrôle de l'accès pendant la continuité des activités sont également bien contrôlés,

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

7 EFFICACITÉ DE LA GESTION DES RISQUES

Les cybermenaces sont la deuxième priorité du gouvernement du Canada en matière de sécurité nationale. Par conséquent, le profil de risque du SCRS pour 2016-2017 appuie un solide programme national de cybersécurité, et constitue l'un des principaux domaines d'intervention de l'organisation²⁹. Les capacités sophistiquées des acteurs étatiques et non étatiques, pour mener des cyberattaques contre la sécurité et la prospérité du Canada doivent accroître leur production de renseignements en ce qui a trait aux cybermenaces. En outre, à la suite de fuites de documents classifiés de haut niveau, comme ceux attribués à WikiLeaks, à Edward Snowden et au sous-lieutenant Jeffrey Paul Delisle,

Le même profil de risque a permis d'établir l'exigence relative aux mesures de sécurité pour l'accès aux renseignements, étant donné la présence d'une menace crédible.

²⁹ Selon le profil de risque du SCRC, les acteurs de cybermenaces disposent de capacités de plus en plus sophistiquées

Puisque les cybermenaces sont un nouveau secteur de menace à la sécurité nationale,

De plus, les systèmes et réseaux du gouvernement du Canada demeurent vulnérables aux attaques des acteurs étatiques et non étatiques

Date : FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

La Politique sur la sécurité du gouvernement du Secrétariat du Conseil du Trésor exige que chaque administrateur général veille à ce que les renseignements, les biens et les services de son ministère soient adéquatement protégés en suivant le processus d'évaluation de sécurité et d'autorisation³⁰.

Le CSARS a conclu que le SCRS était pleinement conforme dans la façon dont il gérait les risques dans le contexte du contrôle de l'accès à de l'information sensible.

³⁰ Le processus d'évaluation de sécurité et d'autorisation est le processus formel par lequel des éléments de preuve sont recueillis et présentés aux autorités responsables afin d'être utilisés comme système de TI. Les preuves démontrant l'existence de risques sont organisées à l'aide de
dans la norme ITSG-33 afin d'évaluer les mesures de protection contre les
classes de vulnérabilité également appelées contrôles de sécurité.

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**

ÉTUDE 2016-05

**TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

Il est raisonnable de penser que le SCRS est une cible potentielle pour les agents et les initiés spécialisés dans les cybermenaces, et que l'information qu'il détient est sensible et périssable. En même temps, la sophistication croissante des capacités des cyberacteurs

. Il est donc à la fois raisonnable et nécessaire que le SCRS respecte les normes et les pratiques gouvernementales, mais aussi qu'il les dépasse compte tenu de la nature de ses activités. Par conséquent, l'accès aux renseignements sur les menaces pourrait orienter les fonctions de défense et de gestion des risques au-delà des niveaux actuels.

Date : _____
FÉV. 2019

CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

ÉTUDE 2016-05

TRÈS SECRET//RÉSERVÉ
AUX CANADIENS

8 CONCLUSION

Le SCRS est un environnement de sécurité de la technologie de l'information complexe qui fait l'objet de pressions liées au ciblage direct

. Bien que le CSARS ne souhaite pas être trop normatif en ce qui concerne la solution technique pour pallier certaines des lacunes relevées dans le cadre de diverses évaluations internes, les mesures de contrôle de l'accès et de sécurité du SCRS devraient respecter les principes suivants :

- Le SCRS doit dépasser les normes et adopter des pratiques exemplaires à l'échelle de l'organisation;
- L'accès à de l'information et des systèmes sensibles devrait être strictement contrôlé,
- Les mesures et les contrôles de sécurité devraient être classés en ordre de priorité en fonction du rendement de leur capital investi et de leur indice de protection³⁴, et faire l'objet d'une évaluation des risques fondée sur des données probantes;
- La gestion intégrée des risques devrait s'appuyer sur des données crédibles sur les menaces opérationnelles, la vulnérabilité et la probabilité, être fondée sur des données scientifiques et respecter les priorités opérationnelles.

Pour l'avenir, les avantages transformationnels générés par la mise au point de technologies de l'information dans les domaines de la communication, de l'éducation, du divertissement, du commerce et des pouvoirs publics ont également fait naître de nouvelles menaces qui tirent parti de l'omniprésence des réseaux informatiques dans tous les domaines de l'activité humaine et de la dépendance des sociétés modernes à l'égard d'infrastructures critiques interconnectées.

Les cybermenaces constituent une méthode peu coûteuse et très profitable. Le risque de pertes économiques et de dommages physiques est donc réel. Non seulement les menaces seront plus complexes à gérer, mais le rythme auquel elles se dérouleront devrait s'accélérer de manière significative. L'omniprésence de l'infonuagique, qui permet l'analyse de données massives grâce à des ressources informatiques distribuées et évolutives, modifie également la position de défense statique : de plus en plus, les attaques se dérouleront sur de multiples fronts³⁵.

Cet examen a permis au CSARS de mieux comprendre les activités du SCRS en ce qui a trait aux défis que pose le contrôle de l'accès dans un environnement complexe,

³⁴ L'indice de protection est une mesure relative ou absolue de l'efficacité d'un contrôle de sécurité.

³⁵ « Une aube nouvelle : Examen de l'évolution des cyberconflits », *série Regards sur le monde : avis d'experts*, publication n° 2015-06-01, SCRS, délibérations de la conférence du Centre de la sécurité des télécommunications.

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**
ÉTUDE 2016-05 **TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

Le futur processus de gestion des risques profitera de l'échange de renseignements opérationnels sur les menaces

, l'objectif étant d'adopter des pratiques exemplaires en matière de sécurité dans l'ensemble de l'organisation. Une meilleure gestion intégrée des risques facilite : la prévision précise des menaces; la réduction proactive des menaces; la création d'une capacité de détection des menaces présentant une acuité et une fidélité accrues; et le renforcement de la capacité d'établir un ordre de priorité des mesures de sécurité susmentionnées et de les appliquer selon les normes et en fonction des risques opérationnels.

Le contrôle de l'accès génère des interdépendances critiques avec les initiatives, les mécanismes et les propriétés de sécurité générale. Le traitement d'un sous-élément de façon isolée est problématique. Pour sécuriser une organisation, il faut appliquer des solutions combinées qui couvrent les domaines humain, informatique et physique, et qui, à leur tour, doivent être validées par un cadre de gestion intégrée des risques. Nous estimons qu'il est utile d'élargir la portée de cet examen pour couvrir les cyberopérations défensives et d'enquête dans l'ensemble du Service au cours de l'année. À l'avenir, la portée des examens du CSARS pourrait être plus large et inclure la sécurité des technologies de l'information et des communications du SCRS de manière à comprendre :

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**

ÉTUDE 2016-05

**TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

RÉSUMÉ DES CONSTATATIONS

Le CSARS a examiné les politiques, les procédures et les directives du SCRS en matière de sécurité pour s'assurer qu'elles étaient complètes par rapport aux politiques et aux normes du gouvernement et du Ministère, et il a conclu qu'elles répondaient aux exigences établies par le gouvernement du Canada ou les dépassaient.

Le CSARS a conclu que le SCRS avait fait preuve d'une grande maturité en matière de gestion de l'information, de sécurité et de protection des renseignements personnels, et que le personnel avait démontré une compréhension exemplaire de la sécurité, de l'information, de la technologie et des systèmes organisationnels.

Le CSARS a conclu que le SCRS était pleinement conforme dans la façon dont il gère les risques dans le contexte du contrôle de l'accès à l'information sensible, mais il a noté que l'évaluation des risques ne semblait pas avoir profité explicitement des renseignements stratégiques ou opérationnels sur les menaces

Date : _____
FÉV. 2019

**CONTRÔLES DE SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION DU SERVICE
CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ**

ÉTUDE 2016-05

**TRÈS SECRET//RÉSERVÉ
AUX CANADIENS**

RÉSUMÉ DES RECOMMANDATIONS

Le CSARS souscrit aux exigences et aux recommandations relatives aux contrôles de sécurité déposées dans le cadre de l'évaluation de sécurité et d'autorisation de l'organisation et recommande que le SCRS mette en œuvre ses conclusions dans un délai accéléré et étende la portée de l'initiative à l'ensemble de l'organisation.

Le CSARS recommande que le processus de gestion des risques du SCRS intègre les renseignements opérationnels et les procédés perfectionnés sur les menaces afin de renforcer sa position défensive au-delà des niveaux actuels, dans le but d'adopter des pratiques exemplaires en matière de sécurité dans l'ensemble de l'organisation.

Le CSARS recommande que le SCRS élabore des politiques, des orientations et des procédures qui définissent la séparation des tâches et leur mise en œuvre dans toutes les directions générales. En se fondant sur les pratiques exemplaires, ces instruments de politique pourraient exiger que l'utilisateur s'authentifie à l'aide de nombreux facteurs.

Date : _____
FÉV. 2019