Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Conseils en matière de sécurité des technologies de l'information

La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie

Aperçu

ITSG-33

Novembre 2012

(modifications rédactionnelles en date du 1er avril 2013)

Canada

Avant-propos

L'*Aperçu* de *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) est un document non classifié publié avec l'autorisation du chef du Centre de la sécurité des télécommunications Canada (CSTC). L'Aperçu et les annexes ont préséance et remplacent les publications suivantes du CSTC :

- Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information (MG-2);
- Guide de certification et d'accréditation des technologies de l'information (MG-4),

Les propositions de modification devraient être envoyées au représentant des Services à la clientèle de la Sécurité des TI du CSTC par l'intermédiaire des responsables de la sécurité des TI du ministère.

Les demandes de copies supplémentaires ou de modification de la distribution devraient être soumises au représentant des Services à la clientèle de la Sécurité des TI du CSTC.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CSTC, par courriel à l'adresse itsclientservices@cse-cst.gc.ca, ou par téléphone au 613-991-7654.

Date d'entrée en vigueur

Cette publication entre en vigueur le 1er novembre 2012.

Signé initialement par

_____

Toni Moffa

Chef adjointe, Sécurité des TI

Résumé

Compte tenu du caractère dynamique de l'environnement de menace d'aujourd'hui et des contraintes financières du gouvernement du Canada (GC), la sécurité des technologies de l'information (TI) ne peut plus être reléguée au second plan et doit désormais être une composante essentielle des plans de projet TI et du ministère. Dans cette optique, nous avons élaboré le guide ITSG-33 dans le but d'aider les ministères du gouvernement à envisager dès le début les enjeux liés à la sécurité. En appliquant les principes énoncés dans ce document, non seulement vous vous assurez de la prévisibilité et de la rentabilité de vos interventions, mais vous contribuez également à éviter les mauvaises surprises qui pourraient vous empêcher d'obtenir l'autorisation d'exploiter vos systèmes et de maintenir cette autorisation.

Le guide décrit d'abord les rôles, responsabilités et activités qui aident les ministères du GC à gérer les risques liés à la sécurité des TI. Le guide décrit les activités à la fois au niveau des programmes (pour aider les agents de sécurité et les coordonnateurs de la sécurité des TI (CSTI) des ministères à harmoniser leurs activités avec la Gestion de la sécurité des TI (GSTI) du GC et les autres politiques et directives du Secrétariat du Conseil du Trésor [SCT]) et au niveau des projets TI (pour les propriétaires et les gestionnaires des projets, et les praticiens de la sécurité). Le processus axé sur les projets décrit dans le guide est conçu pour s'intégrer à un processus ministériel existant. La capacité d'amélioration continue des activités est un aspect clé du processus recommandé et permet de s'assurer que les contrôles mis en place évoluent au même rythme que l'environnement de menace.

Pour appuyer ces activités, le guide contient un catalogue de contrôles de sécurité divisé en trois classes de familles de contrôles : contrôles de sécurité techniques, contrôles de sécurité opérationnels et contrôles de sécurité de gestion. La mise en œuvre des contrôles de sécurité techniques est basée sur la technologie, tels les pare-feu, et celle des contrôles opérationnels, sur des processus humains, telles les procédures manuelles. Les contrôles de sécurité de gestion mettent l'accent sur la gestion de la sécurité des TI et des risques liés à la sécurité des TI. Collectivement, ces trois classes de contrôles constituent un ensemble standardisé d'exigences de sécurité dont vous devez tenir compte et vous inspirer lors de la création et de l'exploitation de vos environnements de TI.

Comme aide supplémentaire pour le développement d'un ensemble de contrôles de sécurité ministériels de référence, le guide propose plusieurs profils de contrôle de sécurité. Un profil est un ensemble de contrôles de sécurité tirés de chaque classe du catalogue qui ont été présélectionnés pour un environnement opérationnel particulier. Plus précisément, le guide propose des profils qui répondent aux besoins en matière de confidentialité, d'intégrité et de disponibilité propres aux environnements cotés PROTÉGÉ A, B et SECRET du GC. Les responsables doivent utiliser ces profils comme point de départ et les adapter aux besoins opérationnels spécifiques de leur ministère.

Les ministères qui appliquent les lignes directrices du guide en tireront des avantages significatifs, dont la conformité à la stratégie et aux objectifs de la gestion globale des risques établis par le SCT, l'assurance que tous les aspects liés à la sécurité des TI sont pris en compte de manière efficace, et la prévisibilité et la rentabilité des activités de gestion des risques liés à la sécurité des TI.

Historique des révisions

Document n°	Titre	Date de publication
ITSG-33 Aperçu	La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Aperçu	1er novembre 2012
ITSG-33 Aperçu	De légères modifications rédactionnelles ont été apportées au texte	1er avril 2013

Table des matières

Avant-propos ..... **ii**

Date d'entrée en vigueur ..... **ii**

Résumé ..... **iii**

Historique des révisions ..... **iv**

Liste des figures ..... **v**

Liste des abréviations et des sigles ..... **vi**

1 Introduction **1**
1.1 Contexte 1
1.2 Objet 1
1.3 Auditoire cible 1
1.4 Définitions et utilisation des termes 1
1.5 Structure de la publication 1

2 Gestion des risques liés à la sécurité des TI **2**
2.1 Gestion des risques 2
2.2 Gestion des risques liés à la sécurité 2
2.3 Gestion des risques liés à la sécurité des TI 2
2.4 Objet et champ d'application du guide ITSG-33 3

3 Processus de gestion des risques liés à la sécurité des TI **4**
3.1 Activités de gestion des risques liés à la sécurité des TI 5
3.2 Activités de gestion des risques liés à la sécurité des systèmes d'information 6
3.3 Catalogue des contrôles de sécurité 7
3.4 Profils de contrôle de sécurité 8

4 Valeur pour les ministères **9**

5 Références **10**

Liste des figures

Figure 1 : Processus de gestion des risques liés à la sécurité des TI 4

Liste des abréviations et des sigles

ASM	Agent de sécurité du ministère
C et A	Certification et accréditation
CDS	Cycle de développement des systèmes
CSTC	Centre de la sécurité des télécommunications Canada
CSTI	Coordonnateurs de la sécurité des technologies de l'information
EMR	Évaluation des menaces et des risques
GC	Gouvernement du Canada
GSTI	Gestion de la sécurité des technologies de l'information
ITSG	Conseils en matière de sécurité des technologies de l'information
PASSI	Processus d'application de la sécurité dans les systèmes d'information
PSG	Politique sur la sécurité du gouvernement
PSM	Plan de sécurité ministérielle
SCT	Secrétariat du Conseil du Trésor du Canada
TI	Technologie de l'information

1 Introduction

1.1 Contexte

Les ministères du gouvernement du Canada (GC) recourent à des systèmes d'information pour soutenir leurs activités opérationnelles. Ces systèmes interconnectés font souvent l'objet de sérieuses menaces susceptibles d'influer négativement sur ces activités en compromettant la confidentialité, l'intégrité ou la disponibilité des systèmes d'information et de leurs biens de technologie de l'information (TI). La gestion des risques liés à la sécurité des TI est un des nombreux composants de la gestion des risques que les ministères doivent mettre en œuvre dans le cadre de leurs activités courantes.

1.2 Objet

Cet aperçu donne un résumé de haut niveau de la suite de documents qui composent le guide ITSG-33. Il énonce les principales caractéristiques des activités de gestion des risques liés à la sécurité des TI qui doivent être entreprises tant au niveau des ministères que des systèmes d'information au sein des organisations du GC. Ces activités s'appuient sur un catalogue complet de contrôles de sécurité que les ministères doivent utiliser pour être en mesure de définir les contrôles de sécurité communs et qui permet aux équipes de projet TI de sélectionner des contrôles de sécurité adaptés à leurs besoins.

1.3 Auditoire cible

Cet aperçu vise à faire en sorte que les cadres supérieurs et les gestionnaires de tous les niveaux des ministères du GC comprennent les avantages de l'ITSG-33. Il est également un outil utile pour les coordonnateurs de la sécurité des TI (CSTI) et autres agents de la sécurité ministérielle, les praticiens des systèmes d'information et de la sécurité, les autorités de certification et d'accréditation, et les gestionnaires collectivement responsables de la gestion des risques liés à la sécurité des TI des ministères et des projets TI.

1.4 Définitions et utilisation des termes

Pour connaître les définitions des principaux termes utilisés dans le présent document, consultez l'Annexe 5 du guide ITSG-33 [Référence 2].

1.5 Structure de la publication

Les lignes directrices du guide ITSG-33 sont énoncées dans la suite de documents suivants :

ITSG-33, Aperçu – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*;

ITSG-33, Annexe 1 – *Activités de gestion des risques liés à la sécurité des TI*;

ITSG-33, Annexe 2 – *Activités de gestion des risques liés à la sécurité des systèmes d'information*;

ITSG-33, Annexe 3 – *Catalogue des contrôles de sécurité*;

ITSG-33, Annexe 4 – *Profils de contrôle de sécurité*;

ITSG-33, Annexe 5 – *Glossaire*.

2 Gestion des risques liés à la sécurité des TI

2.1 Gestion des risques

En août 2010, le Secrétariat du Conseil du Trésor du Canada (SCT) a promulgué le *Cadre stratégique de gestion du risque* [Référence 4] pour le GC. Ce cadre reconnaît que de ne pas gérer efficacement les risques peut faire augmenter le coût des programmes et faire rater des occasions, ce qui peut mettre en péril les résultats des programmes et, au bout du compte, miner la confiance du public.

Un des principes clés de la gestion efficace des risques est son intégration aux différents processus concernés. Dans le *Cadre stratégique de gestion du risque*, le SCT définit la gestion intégrée du risque comme suit :

> *« … une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'organisation. Elle favorise la prise de décisions stratégiques qui contribuent à l'atteinte des objectifs globaux de toute l'organisation. »*

Une approche intégrée de la gestion des risques doit tenir compte des différents types de risque auxquels sont confrontées les organisations et peut inclure les risques liés aux politiques, les risques opérationnels, les risques liés aux ressources humaines, les risques financiers, les risques juridiques, les risques liés à la santé et la sécurité au travail, les risques environnementaux, les risques d'atteinte à la réputation, les risques reliés à la gestion des informations personnelles, et les ***risques liés à la sécurité***.

2.2 Gestion des risques liés à la sécurité

Les risques liés à la sécurité découlent de l'exposition des ***activités opérationnelles et des biens connexes d'une organisation*** à des menaces accidentelles ou délibérées et à des risques naturels susceptibles de compromettre leur confidentialité, leur intégrité, leur disponibilité, leur utilisation prévue et leur valeur monétaire. La gestion des risques liés à la sécurité est le processus par lequel les organisations gèrent ces risques. Les biens dont la sécurité doit être protégée incluent les personnes, les renseignements, les activités opérationnelles, les installations, l'équipement de bureau et les ***systèmes d'information***.

Conformément aux exigences de la *Politique sur la sécurité du gouvernement* [Référence 3] et de la *Directive sur la gestion de la sécurité ministérielle* [Référence 8] du SCT, l'administrateur général doit documenter dans le Plan de sécurité ministérielle (PSM) la façon doit il prévoit gérer les risques auxquels sont exposés les biens du ministère.

2.3 Gestion des risques liés à la sécurité des TI

Les risques liés à la sécurité des TI découlent de l'exposition des biens de TI, qui appuient les activités opérationnelles du ministère, à des menaces accidentelles ou délibérées et à des risques naturels susceptibles de compromettre leur confidentialité, leur intégrité, leur disponibilité et leur utilisation prévue. Ces risques sont un sous-ensemble des risques mentionnés ci-dessus et qui sont susceptibles de compromettre les biens de TI. La gestion des risques liés à la sécurité des TI est le processus par lequel les organisations gèrent ces risques et qui fait appel à la gestion et à l'application de contrôles, de solutions, d'outils et de techniques de sécurité conçus pour protéger les biens de TI contre ces compromissions.

Les ministères qui appliquent ce processus de gestion des risques liés à la sécurité des TI doivent, tout en respectant leur mission, leurs objectifs et leurs priorités, viser un juste équilibre entre la mise en œuvre des contrôles et leurs niveaux acceptables de risque résiduel.

Conformément aux exigences de la *Directive sur la gestion de la sécurité ministérielle* [Référence 8] du SCT, l'administrateur général doit également documenter dans le Plan de sécurité ministérielle (PSM) la façon doit il prévoit gérer les risques liés à la sécurité des TI auxquels sont exposés les biens de TI du ministère.

2.4 Objet et champ d'application du guide ITSG-33

La gestion des risques liés à la sécurité des TI est une activité multidimensionnelle qui exige la participation de tout un ministère, des cadres supérieurs qui établissent les objectifs organisationnels aux employés qui développent et exploitent les systèmes d'information qui appuient ces objectifs. Dans cette optique, le processus de gestion des risques liés à la sécurité des TI documenté dans le guide ITSG-33 propose un ensemble d'activités qui peuvent être entièrement intégrées à un programme de sécurité ministérielle existant et à un cycle de développement de système d'un projet TI. Ces activités, clairement définies, visent à s'assurer que les étapes clés sont exécutées régulièrement au cours de la vie des systèmes d'information et que les activités de gestion des risques sont menées à l'échelle de l'organisation. Le processus défini dans le guide ITSG-33 remplace le processus de gestion des risques liés à la sécurité des TI du GC ainsi que le processus de certification et d'accréditation (C et A) promulgués dans le *Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information* (MG-2) et le *Guide de certification et d'accréditation des technologies de l'information* (MG-4).

Il convient de souligner que les lignes directrices énoncées dans le guide ITSG-33 ne s'appliquent à aucune autre activité d'un programme organisationnel de gestion des risques que celles directement associées à la sécurité des TI. Les lecteurs qui désirent de l'information sur les autres aspects de la gestion des risques d'une organisation devraient consulter le *Cadre stratégique de gestion du risque* [Référence 4] du SCT.

3 Processus de gestion des risques liés à la sécurité des TI

Les lignes directrices du guide ITSG-33 proposent un ensemble d'activités qui doivent être menées à deux niveaux au sein de l'organisation, soit le niveau ministériel et le niveau des systèmes d'information.

- Niveau ministériel – Activités qui doivent être intégrées au programme de sécurité de l'organisation pour planifier, gérer, évaluer et améliorer la gestion des risques liés à la sécurité des TI. Ces activités sont décrites en détail à l'Annexe 1 du guide ITSG-33 [Référence 5].
- Niveau des systèmes d'information – Activités qui doivent être intégrées au cycle de vie des systèmes d'information pour s'assurer de répondre aux besoins en matière de sécurité des TI des activités opérationnelles prises en charge et pour veiller à ce que les contrôles de sécurité appropriés soient mis en œuvre et exploités comme prévu et à ce que le rendement des contrôles existants soit évalué en permanence, qu'il fasse l'objet de rapports et que des mesures appropriées soient prises pour corriger toute lacune relevée. Ces activités sont décrites en détail à l'Annexe 2 du guide ITSG-33 [Référence 6].

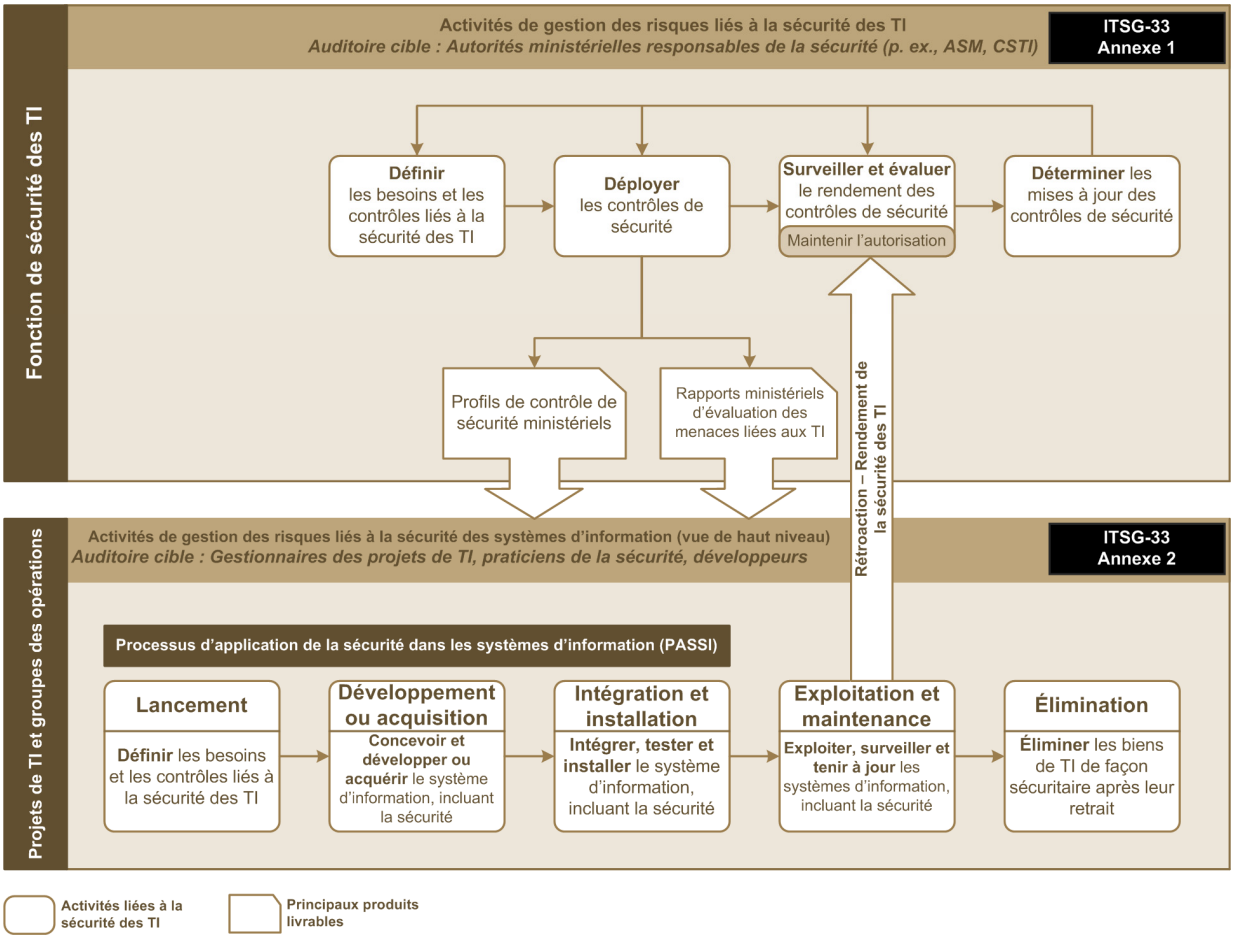

Figure 1 : Processus de gestion des risques liés à la sécurité des TI

La figure 1 illustre les activités de gestion des risques liés à la sécurité des TI de haut niveau ainsi que les activités de gestion des risques liés à la sécurité des systèmes d'information qui seront décrites plus loin dans le document. Elle met également en évidence la façon dont les activités de gestion des risques aux deux niveaux interagissent dans un processus continu pour maintenir et améliorer efficacement la posture de sécurité des systèmes d'information ministériels.

Nota : Le guide ITSG-33 ne prévoit aucune ligne directrice relativement à l'établissement d'une fonction de sécurité des TI dans le cadre d'un programme de sécurité ministérielle, ni aucune directive sur la façon d'intégrer les activités proposées ici dans une telle fonction. Les ministères qui désirent mettre en place cette fonction peuvent s'en remettre aux directives habituelles de leur ministère ou du SCT concernant les programmes du GC. Avant d'intégrer les activités du guide ITSG-33 à leur programme de sécurité ministérielle, les ministères doivent s'assurer d'harmoniser leur structure de gouvernance (rôles, responsabilités et pouvoirs décisionnels) à celle définie dans les plus récents instruments de politique du SCT. Les lignes directrices du présent guide s'harmonisent avec la plus récente structure de gouvernance.

3.1 Activités de gestion des risques liés à la sécurité des TI

Après avoir défini l'ensemble des rôles et responsabilités, les lignes directrices à l'Annexe 1 du guide ITSG-33 [Référence 5] proposent et décrivent des activités de gestion des risques liés à la sécurité des TI qui permettent de définir, de déployer, de surveiller, d'évaluer et de mettre à jour les contrôles de sécurité à l'échelle du ministère. La mise en œuvre de ces activités suit un processus de cycle de vie standard qui doit être intégré au programme global de sécurité ministérielle.

La première étape de ce processus consiste à **définir** les besoins opérationnels en matière de sécurité[1] et les contrôles de sécurité obligatoires correspondants (voir la section 3.3) nécessaires à la protection des activités opérationnelles et de l'information connexe prises en charge par les systèmes d'information. Cette activité inclut l'identification des contrôles de sécurité communs et des secteurs opérationnels responsables de leur mise en œuvre et de leur exécution. La nature des besoins opérationnels en matière de sécurité et des contrôles de sécurité d'un ministère est intimement liée au type d'activités opérationnelles, à leur sensibilité et criticité et à l'environnement de menace du ministère.

Une fois définis, les contrôles de sécurité doivent être **déployés**. Certains contrôles peuvent être assignés à différents groupes au sein du ministère, par exemple, les contrôles de sécurité matérielle et du personnel. D'autres peuvent tirer avantage des infrastructures existantes, par exemple, un système d'authentification commun. Dans certains cas, les ministères peuvent être tenus de mettre en œuvre des contrôles de sécurité communs en recourant à des projets TI (p. ex., un nouveau système ministériel d'authentification des utilisateurs ou une infrastructure centralisée de journalisation et de surveillance). Dans le cas des contrôles de sécurité qui doivent être intégrés aux systèmes d'information, les responsables de la sécurité des TI recommandent aux équipes de projet TI d'utiliser des profils de contrôle de sécurité ministériels (voir la section 3.4). Ensuite, les équipes de projet TI intègrent les contrôles de sécurité nécessaires aux systèmes d'information et les groupes responsables des opérations de TI se chargent de les exploiter et de les tenir à jour en menant les activités de gestion des risques prévues pour les systèmes d'information.

[1] Les besoins opérationnels en matière de sécurité sont dérivés des lois applicables du GC, des politiques du SCT, des objectifs opérationnels et autres exigences juridiques et opérationnelles du ministère. Ils incluent également les exigences en matière de confidentialité qui requièrent le soutien de la fonction de sécurité des TI aux fins de gestion des risques liés à la protection de la vie privée.

Pour être efficaces, les activités de gestion des risques liés à la sécurité des TI des ministères doivent inclure des étapes qui permettent la **surveillance et l'évaluation continues**[2] du rendement des contrôles de sécurité existants, l'examen de la catégorie de sécurité des activités opérationnelles prises en charge et la réévaluation des environnements techniques et de menace pertinents. Ces activités permettent aux agents de la sécurité ministérielle de connaître en permanence l'état de la posture de sécurité des systèmes d'information. Les activités d'évaluation de la sécurité sont semblables aux activités d'assurance de la qualité de l'industrie. Elles permettent aux ministères de réagir en temps opportun aux différents changements (opérations, sécurité, menaces et environnement technologique).

À partir des résultats des activités de surveillance et d'évaluation et des changements observés dans l'environnement, les ministères seront en mesure déterminer les mises à jour requises pour répondre de manière appropriée et efficiente aux nouveaux besoins en matière de sécurité, à l'apparition et à l'évolution des menaces et des vulnérabilités, et aux incidents de sécurité. Les mises à jour peuvent exiger d'apporter des changements aux besoins opérationnels en matière de sécurité ou aux contrôles de sécurité obligatoires (activité de **définition**), de déployer de nouveaux contrôles de sécurité ou de modifier les contrôles de sécurité existants (activité de **déploiement**), et de modifier les composants de surveillance et d'évaluation de la fonction de sécurité des TI (activité de **surveillance et d'évaluation**). Les activités liées à la sécurité des TI interagissent donc en permanence pour maintenir et améliorer efficacement la posture de sécurité des systèmes d'information ministériels.

3.2 Activités de gestion des risques liés à la sécurité des systèmes d'information

Les lignes directrices à l'Annexe 2 du guide ITSG-33 [Référence 6] proposent des activités de gestion des risques liés à la sécurité des TI pour mettre en œuvre, exploiter et maintenir des systèmes d'information fiables. Ces activités s'appliquent au cycle de vie des systèmes d'information, qui inclut les phases de mise en œuvre, d'exploitation et de maintenance et d'élimination. Pour aider les ministères, l'Annexe 2 du guide ITSG-33 [Référence 6] propose un processus de cycle de développement des systèmes (CDS) sécurisé appelé *processus d'application de la sécurité dans les systèmes d'information*, ou PASSI.

Pour appliquer le PASSI de manière efficace et rentable, les équipes de projet TI doivent intégrer ses activités à celles de l'ingénierie des systèmes, des tests système et autres activités de leur propre processus de CDS. Le PASSI établit les correspondances entre les activités liées à la sécurité et les phases d'un processus de CDS de référence.

La première phase du PASSI est la phase de **lancement** du cycle de vie des systèmes. Les premières étapes concernent l'identification et la motivation des intervenants de la sécurité, l'intégration des aspects de la sécurité du projet TI au plan de projet et la **définition** des contrôles de sécurité qui doivent être mis en œuvre pour protéger adéquatement le système d'information. Les contrôles de sécurité propres au système sont dérivés des contrôles de sécurité obligatoires définis au niveau du ministère et basés sur la sensibilité et la criticité des activités opérationnelles prises en charge par le système d'information.

[2] La surveillance et l'évaluation continues ne désignent pas nécessairement une évaluation en temps réel. Certaines activités de surveillance (p. ex., l'examen d'un événement de vérification) peuvent être menées automatiquement en temps réel, tandis que d'autres activités d'évaluation (p. ex., l'examen des procédures de sauvegarde de système) sont habituellement menées manuellement ou selon un calendrier préétabli.

Les étapes suivantes sont celles de la phase de **développement** ou d'**acquisition**. L'objectif est de **concevoir et développer** ou d'**acquérir** des systèmes d'information dotés des contrôles de sécurité requis. À cette fin, les responsables doivent intégrer les contrôles de sécurité aux conceptions de système, effectuer une évaluation des menaces et des risques et développer et tester les composants de sécurité. Dans le cas d'une acquisition, les contrôles de sécurité doivent être inclus dans les exigences obligatoires des énoncés de travail.

Après avoir terminé la phase de développement, les équipes de projet TI passent à la phase d'**intégration** et d'**installation** au cours de laquelle elles doivent **intégrer**, **tester** et **installer** les systèmes d'information, incluant les contrôles de sécurité en place. À la fin de cette phase, on autorise l'exploitation des systèmes.

Au cours de la phase d'**exploitation** et de **maintenance** du cycle de vie, les systèmes d'information passent sous le contrôle des groupes responsables des opérations de TI, qui sont chargés d'**exploiter**, de **surveiller** et de **tenir à jour** à la fois les systèmes et leurs contrôles de sécurité. Les activités de surveillance continue ont également lieu au cours de cette phase afin de s'assurer non seulement que les contrôles de sécurité en place fonctionnent comme prévu, mais également, au fur et à mesure qu'évolue l'environnement de menace, que des contrôles sont ajoutés ou modifiés pour répondre aux besoins changeants en matière de sécurité. S'il arrive que les systèmes d'information ne fonctionnent plus à des niveaux acceptables de risque résiduel même après que des changements ont été apportés aux contrôles de sécurité durant la phase d'exploitation et de maintenance, il est possible que les autorisateurs doivent envisager de révoquer l'autorisation d'exploitation jusqu'à ce que des mesures correctives soient prises. La révocation de l'autorisation entraîne dans un premier temps des activités supplémentaires d'analyse de la sécurité, afin de cerner les lacunes spécifiques du contexte opérationnel, puis des mesures correctives ou des améliorations des contrôles en place pour ramener les systèmes à leur état d'autorisation.

Au cours de la phase d'**élimination** du cycle de vie, à la fin de leur vie utile, les systèmes d'information doivent être déclassés et les groupes responsables des opérations de TI doivent **éliminer** de manière sécuritaire les biens de TI sensibles, en conformité avec les politiques, normes et procédures établies.

3.3 Catalogue des contrôles de sécurité

L'Annexe 3 du guide ITSG-33 [Référence 1] inclut un catalogue de contrôles de sécurité dont les ministères doivent se servir pour répondre aux besoins opérationnels et aux priorités de leur ministère en matière de sécurité et se conformer aux instruments de politique du SCT portant sur la sécurité des TI et la gestion des risques liés à la sécurité des TI. Du point de vue du ministère, les praticiens de la sécurité utilisent ce catalogue pour définir les contrôles de sécurité communs qui doivent faire partie du profil global de contrôle de la sécurité du ministère. Du point de vue des projets TI, ces contrôles doivent servir à mieux cibler les contrôles obligatoires imposés par les ministères afin de les adapter aux besoins spécifiques en matière de sécurité des systèmes d'information.

Les contrôles de sécurité du catalogue sont groupés au niveau supérieur en trois classes puis subdivisés en plusieurs familles (ou regroupements) de contrôles reliés. Les trois classes du niveau supérieur sont définies comme suit :

- ***Contrôles de sécurité de gestion*** : Inclut les contrôles de sécurité qui portent principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI;

- ***Contrôles de sécurité techniques*** : Inclut les contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité qu'on retrouve dans les composants matériels, logiciels et micrologiciels;
- ***Contrôles de sécurité opérationnels*** : Inclut les contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies tels les logiciels de soutien.

Grâce à ces contrôles de sécurité, les praticiens de la sécurité sont en mesure de définir les contrôles qui correspondent aux besoins opérationnels en matière de sécurité de leur ministère et de s'assurer de leur mise en œuvre appropriée dans les systèmes d'information.

3.4 Profils de contrôle de sécurité

L'Annexe 4 du guide ITSG-33 [Référence 7] propose, pour plusieurs environnements différents, une série de profils de contrôle de sécurité basés sur le catalogue des contrôles de sécurité. Ces profils incluent des propositions de contrôles de sécurité et d'améliorations aux contrôles que les autorités ministérielles responsables de la sécurité peuvent utiliser comme point de départ pour créer des profils de contrôle de la sécurité propres à leur ministère. Lorsqu'ils sont appliqués de manière appropriée, ces profils sont aptes à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI du ministère contre les menaces susceptibles de causer des préjudices aux activités opérationnelles. Ceci dit, les profils proposés constituent uniquement un point de départ et doivent être adaptés aux contextes opérationnels, techniques et de menace des ministères ainsi qu'à la tolérance au risque de l'organisation.

La sélection des contrôles de sécurité de chaque profil indiqué à l'Annexe 4 a été articulée, suivant certaines hypothèses de menace, sur les meilleures pratiques de l'industrie et du gouvernement en matière de sécurité, et est dérivée de l'analyse, effectuée par le CSTC, de l'environnement de menace auquel sont confrontés les systèmes d'information dans le contexte opérationnel documenté. Les profils ont été créés comme outil pour soutenir les efforts des praticiens de la sécurité visant à protéger les systèmes d'information en conformité avec les lois applicables du GC et les politiques, directives et normes du SCT. Ils sont utilisés par la fonction de sécurité des TI pour la mise en œuvre et la coordination du déploiement des contrôles de sécurité communs dans l'ensemble de l'organisation. Ils servent également à informer les équipes de projet TI des contrôles de sécurité dont leurs systèmes d'information héritent ou hériteront, et des contrôles qu'elles doivent mettre en œuvre dans le cadre du projet pour assurer la protection des systèmes d'information qu'elles développent ou mettent à jour.

4 Valeur pour les ministères

En adoptant le processus défini dans les différents documents du guide ITSG-33, les ministères pourront tirer de nombreux avantages, dont les suivants :

1. Gestion uniforme et rentable des risques liés à la sécurité des TI;
2. Mise en place uniforme et rentable de systèmes d'information fiables en augmentant la capacité des projets TI à mettre en œuvre des mesures de sécurité dans les systèmes d'information;
3. Capacité de prendre en charge efficacement tous les aspects de la sécurité des TI et de répondre aux besoins opérationnels de sécurité du ministère en appliquant une approche holistique de manière uniforme et reproductible à l'échelle de l'organisation;
4. Capacité de répondre aux besoins des intervenants en s'assurant de tenir compte au niveau ministériel des exigences des propriétaires des programmes (les autorisateurs), et de celles des évaluateurs de la sécurité qui collaborent avec eux, pendant l'élaboration des évaluations des menaces et des exigences des contrôles de sécurité et durant la mise en œuvre des systèmes d'information;
5. Amélioration des communications entre tous les intervenants de la sécurité en utilisant une terminologie normalisée pour toutes les activités liées à la sécurité des TI et les exigences des contrôles de sécurité;
6. Amélioration de la transparence de l'information relative à la sécurité et à la gestion des risques en favorisant l'échange d'information sur les menaces et les exigences des contrôles de sécurité entre les collectivités des TI et de la sécurité des TI des ministères;
7. Amélioration du processus de prise de décisions liées à la gestion des risques en se basant sur des exigences de contrôles et sur des résultats d'évaluation de la sécurité normalisés et facilement comparables pour interconnecter les systèmes d'information des ministères;
8. Conformité à la stratégie et aux objectifs de gestion globale des risques établis par le SCT par la mise en œuvre des principales exigences des instruments de politique du SCT concernant la sécurité des TI et la gestion des risques liés à la sécurité des TI.

5 Références

[Référence 1] Centre de la sécurité des télécommunications Canada. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Catalogue des contrôles de sécurité*. ITSG-33, Annexe 3. 1er novembre 2012.

[Référence 2] Centre de la sécurité des télécommunications Canada. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Glossaire*. ITSG-33, Annexe 5. 1er novembre 2012.

[Référence 3] Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement*. 1er juillet 2009.

[Référence 4] Secrétariat du Conseil du Trésor du Canada. *Cadre stratégique de gestion du risque*. 19 août 2010.

[Référence 5] Centre de la sécurité des télécommunications Canada. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des TI*. ITSG-33, Annexe 1. 1er novembre 2012.

[Référence 6] Centre de la sécurité des télécommunications Canada. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Activités de gestion des risques liés à la sécurité des systèmes d'information*. ITSG-33, Annexe 2. 1er novembre 2012.

[Référence 7] Centre de la sécurité des télécommunications Canada. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Profils de contrôle de sécurité*. ITSG-33, Annexe 4. 1er novembre 2012.

[Référence 8] Secrétariat du Conseil du Trésor du Canada. *Directive sur la gestion de la sécurité ministérielle*. 1er juillet 2009.