Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Ligne directrice sur l'élaboration d'un plan de sécurité ministériel

Publié : le 04 déc. 2013

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

N° de catalogue BT39-14/2013F-PDF
ISBN : 978-0-660-09752-7

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Guideline on Developing a Departmental Security Plan

Ligne directrice sur l’élaboration d’un plan de sécurité ministériel

Liste des figures

1. Objet

La présente Ligne directrice a pour objet d'aider les ministères à répondre aux exigences de la Politique sur la sécurité du gouvernement (PSG) et de la Directive sur la gestion de la sécurité ministérielle (DGSM) afin d'élaborer un plan de sécurité ministériel (PSM) qui expose en détail les décisions en matière de gestion des risques en matière de sécurité la sécurité et décrit les stratégies, les buts, les objectifs, les priorités et l'échéancier élaborés en vue d'améliorer la sécurité ministérielle. L'approche concernant l'élaboration du PSM que décrit la Ligne directrice est fondée sur une méthode de gestion des risques en matière de sécurité (GRS) visant à assurer que les décisions prises pour gérer ces risques en matière de sécurité soient étayées au moyen d'analyses approfondies et appuyées de processus rigoureux, reproductibles et documentés. Cette approche tend à appuyer l'élaboration d'un PSM qui fournit aux administrateurs généraux et aux cadres supérieurs un aperçu intégré des besoins en matière de sécurité ministérielle qui concorde avec les priorités stratégiques, les programmes, les plans, les processus et les autres pratiques de chaque ministère.

La Ligne directrice se fonde sur des principes et des pratiques exemplaires bien reconnus en matière de planification, de gestion des risques et d'évaluation du rendement, qui proviennent d'instruments et de lignes directrices du CT, de rapports des administrations, de l'industrie privée et d'autres pays, ainsi que d'organismes de normalisation, comme l'Organisation internationale de normalisation (ISO) et le National Institute of Standards and Technology (NIST). NIST. La Ligne directrice renferme également des commentaires de représentants ministériels qui ont participé à son élaboration.

2. Personnes visées

La Ligne directrice vise les agents de sécurité du ministère (ASM), les professionnels de la sécurité et les gestionnaires de tous les niveaux, dont les rôles et les responsabilités précis en matière de planification de la sécurité ministérielle et de GRS sont stipulés dans la PSG et la DGSM.

La Ligne directrice peut également être utile aux gestionnaires des risques généraux du ministère, aux planificateurs stratégiques, aux coordonnateurs du Cadre de responsabilisation de gestion (CRG), ainsi qu'à d'autres spécialistes, qui jouent un rôle important en aidant à intégrer la sécurité aux pratiques ministérielles de gestion des risques, de planification et de mesure du rendement, et dont les perspectives générales doivent être prises en considération lors de l'élaboration du PSM.

3. Application

Les administrateurs généraux et les ASM de tous les ministères[1] ont des responsabilités stratégiques relativement à la planification de la sécurité et à la GRS. Le mandat, la taille, les programmes, les processus et pratiques de gestion interne, et les ressources affectées aux opérations de sécurité de chaque ministère sont uniques. Compte tenu de ces différences, chaque ministère, y compris les petits ministères et organismes (PMO), doit définir une approche concernant l'élaboration de son PSM, qui tient compte de ses opérations, de ses capacités et de son environnement des risques, en adoptant et en adaptant la présente Ligne directrice, afin de satisfaire de la meilleure façon possible ses besoins opérationnels.

4. Mise en œuvre

La DGSM prévoit une période de transition de trois ans pour la mise en œuvre complète des exigences relatives au PSM[2], celle-ci ayant débuté le 1er juillet 2009 et se terminant le 30 juin 2012. L'ordre des activités ci-dessous est suggéré pour aider à veiller à ce que chacune des étapes de la méthode de GRS puisse être réalisée et que les résultats servent de fondement à l'élaboration du PSM.

- Analyser et définir le contexte; entamer les consultations.
- Mener ou terminer les évaluations des risques :
  - Consolider les résultats des évaluations existantes des risques liés à la sécurité et recenser les écarts en matière de protection (les activités de programmes qui ne sont pas visées par les évaluations actuelles des risques, afin de toucher à l'ensemble des renseignements, des biens et des autres ressources).
  - Définir les besoins pour des contrôles ou des indicateurs de rendement supplémentaires.
- Définir les priorités en matière de sécurité fondées sur les résultats des évaluations des risques pour la sécurité et de l'analyse des options de traitement; élaborer une stratégie de mise en œuvre.
- Élaborer un PSM et le soumettre à l'approbation de l'administrateur général.
- Amorcer la mise en œuvre et faire le suivi du rendement.
- Au besoin, mener ou terminer les évaluations des risques afin de combler les écarts décelés.
- Présenter un rapport d'étape à l'administrateur général et aux cadres supérieurs.
- Mettre à jour le PSM, au besoin.
- Poursuivre les activités de GRS ainsi que la mise en œuvre et le suivi des contrôles.
- Tenir le PSM à jour et rendre compte à l'administrateur général et aux cadres supérieurs.

5. Une approche intégrée en matière de planification

La gestion de la sécurité est la plus efficace lorsqu'elle fait partie intégrante des activités, des programmes et de la culture d'un ministère et de la fonction publique dans son ensemble [3].

Les concepts de planification et de gestion intégrées des risques ne sont pas nouveaux. Le greffier du Conseil privé, dans son *Dix-septième rapport annuel au Premier ministre sur la fonction publique du Canada*, a réaffirmé l'importance de la planification intégrée en énonçant que « la planification devrait être considérée comme une pratique administrative de base pour tous les fonctionnaires; elle est nécessaire pour que s'harmonisent les objectifs, les ressources et les résultats »[4]. Les Plans d'action pour le renouvellement de la fonction publique antérieurs définissent les plans intégrés comme des « assises de l'évaluation et de la compréhension des besoins actuels et futurs des ministères et de la fonction publique dans son ensemble ». La gestion des risques, en ce qu'elle vise l'incertitude liée aux événements et aux résultats à venir, fait partie intégrante de la bonne planification et du processus décisionnel à tous les niveaux[5]. Le Cadre stratégique de gestion du risque reconnaît qu'il faut gérer les risques à chaque niveau de l'architecture des activités de programmes [AAP] (tous les programmes jusqu'aux sous-sous-activités) et cumuler les résultats au niveau ministériel, afin de faciliter l'établissement des priorités et d'améliorer la prise de décisions.

L'intégration consiste à réunir les plans, les activités et les processus de sorte qu'ils interagissent en harmonie, afin d'atteindre des objectifs opérationnels communs. L'harmonisation est l'action d'établir des liens, entre les objectifs à court et à long termes et les objectifs stratégiques et les activités de programmes du ministère, comme le définit son AAP. L'élaboration d'une approche intégrée concernant la planification peut aider à révéler des interdépendances et des liens horizontaux dans les activités individuelles, des possibilités de rationaliser des processus de travail et des opérations, et des économies d'échelle éventuelles. L'harmonisation des plans aux objectifs opérationnels du ministère peut aider à faire en sorte que les ressources puissent être efficacement affectées pour atteindre les résultats stratégiques prévus.

En examinant les pratiques exemplaires des ministères ayant des programmes de sécurité évolués, on constate que la sécurité est fermement intégrée aux fonctions de gestion interne et est harmonisée aux activités de planification ministérielle et de gestion des risques. Les politiques de sécurité et le processus et les plans de GRS sont bien documentés, adaptés aux activités opérationnelles uniques du ministère et comprennent la mesure du rendement en tant que partie intégrante de la planification. L'intégration et l'harmonisation sont davantage appuyées grâce à une gouvernance solide, qui utilise les éléments du Cadre de responsabilisation de gestion (CRG)[6] pour établir les attentes en matière de bonnes pratiques de gestion interne et l'AAP ministérielle en tant que cadre d'harmonisation des pratiques de gestion interne aux résultats de l'exécution des programmes.

Une méthode intégrée de planification et de gestion des risques requiert la participation active des cadres supérieurs et des intervenants internes du ministère et des secteurs de programme. Elle est réalisée grâce à un dialogue régulier et récurrent, à une compréhension claire des rôles et des responsabilités, et à un engagement envers de meilleures pratiques de planification et de gestion des risques à tous les paliers du ministère.

6. Documentation

La documentation des processus, des politiques et des plans de sécurité est un moyen d'établir une compréhension et un cadre de référence communs pour la terminologie sur la sécurité, d'appuyer les communications internes et externes, de définir les rôles et les responsabilités et de porter à maturité les pratiques de sécurité et de GRS. La documentation de l'analyse et des constatations de la GRS aide à faire en sorte que les résultats soient reproductibles et donnent des preuves de diligence raisonnable, afin que tous les intervenants, y compris les gestionnaires et les vérificateurs, comprennent la réflexion qui a mené aux mesures prises et fassent le lien entre ces mesures et les décisions, les plans et les politiques de la direction.

La documentation doit être préparée tout au long du processus d'évaluation et de gestion des risques pour la sécurité, afin de saisir les analyses, les constatations et les mesures qui en découlent et de fournir le fondement de l'examen, de l'établissement des priorités, de la prise de décisions et de l'évaluation du rendement. Cela aidera à prouver les relations entre les contrôles choisis et les résultats des processus d'évaluation et de gestion des risques pour la sécurité des processus.

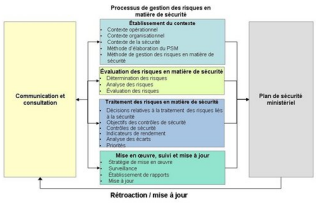
Même si l'étendue et le format de la documentation diffèrent d'un ministère à l'autre, compte tenu de la taille, de la complexité, des opérations et des pratiques de gestion interne de chacun d'entre eux, chaque ministère doit prendre des mesures pour établir et maintenir des preuves du processus et des constatations de GRS lisibles, facilement identifiables et accessibles [7]. Une telle documentation doit également être disponible aux personnes qui en ont besoin, tout en respectant toute exigence stratégique, juridique ou réglementaire, ainsi que toute obligation contractuelle afin de la protéger et de la contrôler. (On trouvera de plus amples détails sur la documentation à la section 8.3 - Plan de sécurité ministériel.)

7. Processus d'élaboration d'un plan de sécurité ministériel

La Ligne directrice sur l'élaboration d'un PSM est organisée selon le processus décrit à la figure 1 - *Processus d'élaboration d'un plan de sécurité ministériel*. Le processus est un mélange de divers modèles de planification et de gestion des risques décrits dans les documents de référence utilisés pour rédiger la présente Ligne directrice (annexe B - Références). Chaque étape du processus de GRS est calquée sur les exigences obligatoires relatives au PSM décrites dans la PSG et la DGSM, ce qui permet d'assurer leur respect.

Figure 1 - Processus d'élaboration d'un plan de sécurité ministériel

Processus d'élaboration du PSM



[Version textuelle : Figure 1 - Processus d'élaboration d'un plan de sécurité ministériel]

7.1 Communication et consultation

Un échange uniforme de renseignements pertinents doit avoir lieu à toutes les étapes de l'élaboration du PSM. La communication et la consultation montrent que les intervenants participent et que leurs rétroactions et leurs préoccupations sont prises en compte. Elles montrent également que des sources faisant autorité ont été citées en référence et consultées.

Il importe que les employés chargés de gérer les risques pour la sécurité participent au processus de GRS, car cela aidera à obtenir l'approbation et le soutien du PSM lorsqu'on cherchera à le faire approuver. Des employés de tous les secteurs du ministère peuvent apporter une importante contribution aux différentes étapes, notamment :

- les gestionnaires de programmes et d'activités, les services ministériels, les services juridiques ainsi que les bureaux régionaux, qui sont en mesure de donner des conseils et des points de vue sur le contexte opérationnel, les questions d'importance stratégique, les obligations juridiques, les protocoles de gestion interne, ainsi que la planification stratégique et la mesure du rendement. Ils peuvent contribuer à la définition des critères à utiliser pour évaluer l'importance des risques pour la sécurité et des conséquences en cas de compromission;
- les experts en la matière, qui peuvent aider à cerner et à définir les vulnérabilités et les menaces à la sécurité des renseignements, des biens, des services et des personnes et contribuer à l'analyse, à l'évaluation et à la gestion des risques pour la sécurité. Ces experts peuvent comprendre des personnes œuvrant dans les domaines de l'accès à l'information, de la protection des renseignements personnels, de la gestion des risques ministériels, de la gestion des urgences et de la continuité des activités, de la gestion des ressources humaines, de la santé et de la sécurité au travail, des biens immobiliers et du matériel, de la gestion de l'information (GI), de la technologie de l'information (TI) et des finances;
- l'ASM et les spécialistes de la sécurité ministérielle sont les mieux placés pour donner des conseils et des directives sur le contexte des menaces, l'ensemble du processus de gestion des risques pour la sécurité et les options de traitement des risques pour la sécurité. Ils peuvent également aider à déterminer les outils les plus appropriés à utiliser pour évaluer les risques (évaluations des menaces et des risques, autoévaluations, etc.), interpréter les résultats de ces évaluations des risques et donner des directives sur les priorités que devrait présenter le PSM. L'ASM est également chargé d'élaborer, de mettre en œuvre, de surveiller et de tenir à jour le PSM, ainsi que de gérer le programme de sécurité ministérielle. À ce titre, l'ASM est vraisemblablement le point central de la coordination de la planification de la sécurité et de la gestion des risques pour la sécurité au sein d'un ministère. Les responsabilités de l'ASM et des spécialistes de la sécurité ministérielle peuvent comprendre ce qui suit :
    - déterminer l'approche, les ressources et les capacités nécessaires pour élaborer le PSM;
    - effectuer la coordination avec les intervenants, y compris les gestionnaires de programmes, les agents ministériels de planification, les spécialistes en la matière et les autres personnes participant à l'élaboration du plan;
    - élaborer le plan, y compris l'intégration des résultats des consultations, des évaluations des risques, etc.;
    - faire appel aux conseils du SMA champion et appuyer les comités exécutifs.

La gouvernance est un élément clé des consultations, puisqu'elle établit une structure et un processus permettant la participation des cadres supérieurs, officialise la prise de décisions et appuie l'élan engendré durant le cycle de planification. Il peut s'avérer utile de trouver un champion au niveau de la direction pour amorcer l'élaboration du PSM et agir en tant qu'intermédiaire pour l'échange d'informations et la prise de décisions auprès de la structure de gouvernance ministérielle (au sein des principaux comités ministériels permanents). L'inclusion du PSM au programme de gestion est également une façon de veiller à ce qu'il se fonde sur les résultats et qu'il s'harmonise aux activités et aux priorités opérationnelles du ministère.

Tous les participants à l'élaboration du PSM ou à l'exécution de la GRS doivent connaître les principaux documents ministériels, qui en établissent le mandat, la structure de programmes, les priorités et les engagements. Ensemble, ces documents donnent un aperçu intégré de l'environnement opérationnel, et aident à orienter et à harmoniser l'élaboration et la mise en œuvre d'un PSM. Ceux-ci sont les suivants :

- Consignes aux ministères sur la préparation d'une structure de gestion, des ressources et des résultats
- Rapport sur les plans et les priorités du ministère (RPP)
- Rapport ministériel sur le rendement (RMR)
- Plans intégrés des activités et des ressources humaines (RH)
- Plans d'investissement
- Politique sur la vérification interne
- Rapports du Bureau du vérificateur général du Canada et rapports de vérification interne

7.2 Gestion des risques pour la sécurité

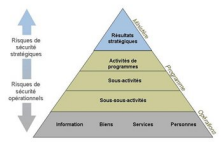
La gestion des risques fait partie intégrante d'une bonne gestion, d'une bonne planification et du processus décisionnel à tous les niveaux. C'est ce qui est observé dans presque toutes les organisations des secteurs public et privé. La GRS est une composante d'une pratique globale de gestion des risques. C'est un processus permanent et itératif d'analyse et de coordination des activités visant à contrôler les risques pour la sécurité. Celles-ci comprennent la détermination et l'évaluation des risques pour la sécurité des ressources essentielles (les renseignements, les biens, les personnes et les services) dont un ministère dépend pour réaliser les programmes et atteindre ses objectifs opérationnels, et la mise en œuvre de mesures pour réduire à un niveau acceptable les risques pour la sécurité. La GRS est importante, puisqu'elle établit un lien entre la sécurité du ministère et les activités de gestion, de planification des opérations et de gestion des risques ministériels plus vastes, et qu'elle aide à bâtir une culture de sécurité plus forte, et permet au ministère de cerner les problèmes de sécurité, puis de les régler de façon proactive.

Les risques pour la sécurité qui ne sont pas atténués peuvent avoir une incidence sur un ministère à tous les niveaux. Au niveau du ministère, ils peuvent empêcher le ministère d'atteindre ses résultats stratégiques. Au niveau d'un programme, ils peuvent influer sur l'obtention des résultats escomptés et des conditions nécessaires pour veiller à la réalisation des services. Au niveau opérationnel, ils peuvent compromettre la confidentialité, la disponibilité ou l'intégrité des renseignements et des biens du ministère, ou exposer des personnes à la violence en milieu de travail. Un lien logique et pratique doit être établi entre la GRS et tous les niveaux des activités de programmes dans le but d'élaborer une perspective holistique de la sécurité ministérielle, et ce, tant sur le plan de la façon dont elle permet l'atteinte des objectifs opérationnels que de celle dont elle peut l'entraver. La figure 2 - *Gestion intégrée des risques pour la sécurité* illustre les relations entre les activités du ministère, du programme et des opérations, et les risques pour la sécurité, afin d'élaborer le processus de GRS.

Le processus de GRS décrit dans la suite de la Ligne directrice traite du risque initial, soit du risque avant qu'il ait été atténué. Cette approche a été adoptée afin de veiller à ce que tous les risques, y compris le risque résiduel (le risque après traitement), soient déterminés et documentés. De cette façon, les ministères seront en mesure d'élaborer avec succès une perspective intégrée de tous les risques pour la sécurité du ministère et de déterminer les options de traitement en tenant compte des obligations opérationnelles et juridiques générales.

Figure 2 - Gestion intégrée des risques pour la sécurité[5]

Gestion intégrée des risques pour la sécurité



[Version textuelle : Figure 2 - Gestion intégrée des risques pour la sécurité]

7.2.1 Établissement du contexte

L'ASM [...] assume la responsabilité de ce qui suit : [...] élaborer, mettre en œuvre, surveiller et actualiser un plan de sécurité ministériel (PSM) qui renferme une vision commune des exigences de sécurité ministérielle [...].

Section 6.1.1.1 de la Directive sur la gestion de la sécurité ministérielle

La première activité du cycle de la planification consiste à établir le contexte. C'est un aspect important de la planification, puisqu'il permet au ministère de mieux comprendre ses forces et ses faiblesses, de même que les possibilités et les menaces découlant de l'environnement dans lequel celui-ci évolue. L'analyse du contexte est principalement axée sur l'environnement global interne et externe de l'organisation. Elle aidera à déterminer la façon dont la sécurité interagit avec les activités internes du ministère afin d'articuler le rôle que joue la sécurité dans l'atteinte des objectifs du ministère et de contribuer à définir les paramètres et les contraintes qui doivent être pris en compte dans le cadre de la gestion des risques pour la sécurité.

Les objectifs opérationnels du ministère sont le facteur déterminant le plus important du PSM et des étapes subséquentes du processus de GRS. Ils constituent le fondement des arguments susceptibles d'être utilisés pour élaborer toute analyse de rentabilisation en vue du changement, aident à établir la priorité des initiatives en se fondant sur les besoins opérationnels et jettent les bases communes des consultations et de la gestion des attentes des partenaires et des intervenants.

Contexte opérationnel

Pour définir le contexte opérationnel, un examen du mandat, des priorités, des résultats stratégiques, des activités de programmes (AP) et des sous-activités de programmes (SAP) du ministère doit d'abord être effectué. L'AAP, le RPP et le RMR du ministère sont des instruments utiles pour colliger ces renseignements et contribuent à orienter et à harmoniser l'élaboration et la mise en œuvre d'un PSM. Plus particulièrement, l'AAP est un inventaire structuré de tous les programmes ministériels[6], ces derniers étant présentés suivant une hiérarchie visant à indiquer la relation logique entre chaque programme et les résultats stratégiques auxquels ils contribuent. Le RPP est utile pour définir le cadre et les obligations juridiques et stratégiques. Les possibilités d'utiliser les renseignements disponibles et de créer des liens avec des spécialistes en matière de gestion des risques et de planification ministériels doivent également être envisagées, ce type d'analyse étant habituellement effectuée dans ces domaines.

Le contexte opérationnel peut aussi servir de fondement pour déterminer les renseignements, les biens, les personnes et les services qui se rapportent aux activités de programmes et aux sous-activités, et pour décrire comment leur protection permet au ministère de réaliser sa mission. Ceci aidera à établir la structure et la portée des évaluations des risques afin de veiller à ce que celles-ci soient liées au contexte du mandat primordial du ministère et, plus tard durant le processus, cela pourra contribuer à définir les priorités en matière de gestion des risques pour la sécurité.

Contexte organisationnel

L'analyse du contexte organisationnel consiste à examiner les mécanismes internes du ministère afin de déterminer la façon dont les personnes et les groupes fonctionnent pour atteindre les résultats opérationnels. Elle tient compte de facteurs tels que le nombre d'employés, l'emplacement des installations, les pratiques et les pouvoirs de la direction, les compétences essentielles (connaissances théoriques et pratiques), les technologies et les processus administratifs. Cette analyse aidera à définir les politiques, les activités et les stratégies ministérielles mises en place pour atteindre les objectifs opérationnels et permettra de comprendre les capacités, les limites, les perceptions et les valeurs des intervenants internes.

Le contexte organisationnel est sensiblement différent d'un ministère à l'autre, selon la taille et la complexité des activités. Certains ministères n'ont que quelques secteurs d'activités qui ne nécessitent qu'un seul bureau et sont appuyés de processus rationalisés. D'autres ministères comprennent plutôt de nombreuses activités et sous-activités de programmes auxquelles prennent part des milliers de personnes situées partout dans le monde; ces activités sont appuyés de processus complexes et des pouvoirs décisionnels et font appel à une vaste gamme d'aptitudes et de compétences.

Contexte de la sécurité

Le contexte de la sécurité donne un aperçu de la fonction de sécurité ministériel et de ses activités, y compris les contraintes et les exigences découlant des obligations juridiques, réglementaires, stratégiques et contractuelles, et d'autres obligations. Il permet également d'expliquer la nature des menaces dans le cadre desquelles les activités en matière de sécurité sont menées.

L'analyse du contexte de la sécurité doit prendre en considération les relations qui existent entre la sécurité ministérielle et les autres pratiques de gestion interne, comme elles sont décrites dans le contexte organisationnel, afin d'expliquer la façon dont ces activités fonctionnent de concert pour protéger les ressources ministérielles[10] et appuyer les activités du ministère. Tous les ministères sont exposés à un certain niveau de menace pour la sécurité. Par exemple, la menace que représentent les attaques malveillantes sur les systèmes informatiques est pertinente pour l'ensemble des ministères. Cependant, un nombre limité de ministères sont davantage exposés à l'espionnage ou au sabotage internes. Les caractéristiques de ces menaces définissent la fonction de sécurité ministérielle et influent sur cette dernière.

Approche concernant l'élaboration du PSM

L'approche concernant l'élaboration du PSM varie en fonction des contextes opérationnel, organisationnel et de la sécurité de chaque ministère. Certains ministères choisiront d'élaborer un seul PSM décrivant en détail l'ensemble des principaux éléments exposés dans la présente Ligne directrice. Les ministères plus grands ou plus complexes sont plus susceptibles d'élaborer un PSM appuyé de plans et d'évaluations des risques détaillés pour les régions, les programmes, les services, les activités ou les systèmes déterminés.

L'approche définie par chaque ministère contribuera à établir un cadre pour organiser le PSM et à en déterminer la portée. Elle doit prendre en considération le processus d'élaboration du plan, l'échéancier requis pour élaborer le PSM, les liens qui existent entre le PSM et les autres plans et évaluations des risques et la façon dont le PSM consolide ces autres plans et évaluations des risques, afin de présenter une perspective complète et cohérente des exigences en matière de sécurité ministérielle. La définition de ces liens permettra également de faire en sorte que les constatations et les priorités proposées dans le PSM soient tirées de conclusions plus détaillées d'une évaluation ou d'un plan particulier dans lequel l'analyse des évaluations de risques et les options de traitement sont documentées.

Méthode de gestion des risques pour la sécurité

La GRS est présente dans les contextes opérationnel, organisationnel et de la sécurité du ministère et à l'échelle du gouvernement en général. La détermination de la méthode de GRS du ministère constitue le fondement de la communication de la philosophie, des valeurs et des pratiques en matière de gestion de la sécurité, ainsi que de la définition des critères d'évaluation des risques pour la sécurité et de la prise de décisions pour les atténuer. Chaque ministère a probablement une méthode quelque peu différente, fondée sur les pratiques de gestion des risques ministériels, l'évolution du programme de sécurité, l'exposition aux risques pour la sécurité et la tolérance des risques. La méthode de GRS doit également préciser les autorités chargées de la sélection des options de traitement des risques et de l'acceptation des risques résiduels. Le gestionnaire chargé du programme, de l'activité liée au service ou du système est habituellement l'autorité responsable.

En décrivant la méthode de GRS du ministère, il peut être utile de poser les questions suivantes :

- Comment les liens entre la GRS et les objectifs et les politiques opérationnels des ministères sont-ils déterminés?
- Comment les décisions relatives à la manière dont sont menées les évaluations des risques sont-elles prises en ce qui a trait aux méthodes utilisées, aux processus suivis et à la période pour réaliser ou examiner les évaluations des risques?
- Quel est le critère de risque selon lequel l'importance d'un risque est définie et évaluée pour déterminer s'il est acceptable ou inacceptable?
- Qui sont les autorités chargées de prendre les décisions concernant la traitement des risques pour la sécurité (la sécurité ministérielle, les responsables des risques et des activités, les cadres supérieurs, etc.)?
- Comment les résultats des évaluations et de l'atténuation des risques sont-ils documentés aux fins de preuve?
- Comment les résultats des évaluations et des décisions visant l'atténuation des risques sont-ils combinés et résumés dans le PSM?
- Comment les activités de GRS sont-elles suivies, évaluées et communiquées?

La définition de critères d'évaluation de l'importance des risques pour la sécurité est un élément essentiel du processus de GRS. Les critères doivent tenir compte des valeurs, du contexte et des objectifs opérationnels ainsi que des ressources du ministère. Certains critères peuvent être imposés par des exigences juridiques ou politiques, ou en découler. Le processus décisionnel ayant trait à la traitement des risques pour la sécurité nécessite souvent la pondération de multiples critères afin de décider d'une ligne de conduite fondée sur la mesure dans laquelle les risques pour la sécurité peuvent entraver l'atteinte des objectifs opérationnels. Comme cela peut s'avérer complexe, aucun critère de décision précis ne doit être utilisé ou n'est utilisé. Plusieurs critères de décision reviennent à une certaine fréquence, notamment la rentabilité, le rapport coût-efficacité, le niveau de tolérance des risques, les opinions des intervenants et l'étude des risques multiples. L'utilisation des facteurs de risque sera importante à l'étape de l'évaluation des risques pour décider si les risques sont acceptables ou inacceptables, et comment ils doivent être gérés.

7.2.2 Évaluation des risques pour la sécurité

... un plan de sécurité ministériel (PSM) qui... définit les menaces à la sécurité, les risques et les vulnérabilités afin de fixer un ensemble approprié d'objectifs de contrôle.

Section 6.1.1.2 de la Directive sur la gestion de la sécurité ministérielle

L'évaluation des risques pour la sécurité est le processus qui permet de déterminer, d'analyser et d'évaluer les risques pour la sécurité, afin d'établir l'importance de ceux-ci et de déterminer s'ils sont acceptables ou non et la nécessité de les traiter. Les évaluations des risques pour la sécurité doivent être effectuées de façon méthodique et systématique et peuvent avoir lieu à tout moment, indépendamment du processus général de GRS. Elles doivent être faites périodiquement de manière à traiter tout changement important dans l'environnement de sécurité ou lorsqu'un nouveau service ou une nouvelle pratique opérationnelle est introduit(e).

Les évaluations des risques pour la sécurité visent habituellement les systèmes informatiques, les biens essentiels et les installations. Afin de présenter une perspective consolidée des risques pour la sécurité, les évaluations des risques doivent également être réalisées au niveau des activités de programmes et tenir compte d'autres facteurs, tels que les processus opérationnels. Chaque ministère doit décider comment organiser les évaluations des risques pour la sécurité et l'approche à adopter à cet égard en se fondant sur les opérations et les activités de programmes qui leur sont propres. Ce qui doit rester primordial, c'est l'harmonisation de la portée et de l'objet des évaluations des risques avec les objectifs opérationnels du ministère de façon à ce que les résultats de chaque évaluation des risques puissent être combinés, afin de fournir au ministère un aperçu intégré des risques pour la sécurité et d'appuyer un processus décisionnel éclairé au niveau ministériel.

Il faut tenir compte de la portée de chaque évaluation des risques afin de voir à ce qu'elle documente à un degré de détail suffisant ce qui est à risque (les renseignements, les biens, les services, les personnes, les programmes) et de la façon dont elle cadre avec l'AAP du ministère. L'analyse qui mène à des conclusions doit également être documentée de sorte qu'elle puisse être mentionnée et réévaluée, au besoin. Comme il est probable que de multiples évaluations des risques soient effectuées et regroupées afin de donner un aperçu à l'échelle du ministère, il faut également envisager de décrire les liens entre les évaluations des risques et la façon dont les résultats peuvent être documentés de façon à permettre d'élaborer davantage les détails connexes, et de les comparer.

Les évaluations des risques pour la sécurité n'ont pas toujours besoin d'être une activité de grande envergure, et il n'existe pas d'approche « universelle ». Chaque évaluation des risques doit être effectuée en tenant pleinement compte de la nécessité de justifier les ressources utilisées pour les réaliser. Divers outils et méthodes sont couramment utilisés. Leur complexité, leur objectivité et leur subjectivité, la qualité des résultats qu'ils produisent, ainsi que le niveau relatif de savoir-faire requis pour les utiliser ou les réaliser, varient considérablement. Les méthodes ordinairement utilisées sont notamment les évaluations des menaces et des risques (EMR), les vérifications, l'analyse des répercussions sur les activités (ARA), les évaluations des facteurs relatifs à la vie privée (EFVP), les autoévaluations, la surveillance, les enquêtes de sécurité et les évaluations de la vulnérabilité. Comme certains d'entre eux produisent des renseignements identiques ou semblables sur les risques, les ministères doivent s'efforcer d'éviter le chevauchement en exigeant que ces activités soient coordonnées et que les renseignements qu'elles permettent de recueillir soient partagés (conformément aux lois et aux politiques sur la collecte, l'utilisation, la divulgation et la conservation de renseignements). Les possibilités de collaborer avec d'autres secteurs (les services d'infotechnologie, la gestion des risques ministériels, etc.) ou d'utiliser les évaluations des risques qu'ils produisent doivent également être envisagées.

De manière générale, les évaluations des risques pour la sécurité dans les ministères ont une très vaste portée et se concentrent sur les risques stratégiques relatifs aux activités de programmes et leurs ressources et services connexes. Bien qu'elles ne soient pas aussi détaillées qu'une évaluation des risques plus ciblée, qui peut porter sur une seule installation, un seul réseau ou un seul système, les évaluations ministérielles établissent un cadre contextuel général et un fondement solide pour le programme de sécurité et aident à cerner le besoin d'effectuer des évaluations des risques supplémentaires au niveau des programmes et des systèmes ou d'établir la priorité des projets d'évaluation des risques individuellement.

Les évaluations des risques de programmes ou de ressources qui ne posent aucun risque précis pour l'organisme peuvent être combinées, effectuées sans nécessiter de ressources importantes ou spécialisées, et documentées avec concision. Dans plusieurs cas, les évaluations des risques de programmes ou de ressources dont l'environnement opérationnel et les préoccupations en matière de sécurité sont semblables peuvent être menées au moyen d'évaluations des risques « génériques » susceptibles d'être réutilisées. Les programmes ou les ressources qui sont considéré(e)s à risque plus élevé ou de plus grande valeur justifient une analyse plus rigoureuse et approfondie, étayée par des méthodologies de pointe. Inversement, moins d'effort doit être consacré à l'examen de biens de moindre valeur, de menaces moins importantes et de vulnérabilités plus obscures[11].

Détermination des risques

La détermination des risques pour la sécurité est un exercice à facettes multiples. Elle comprend la détermination des sources de risques (en fonction des menaces et des vulnérabilités) et de leurs conséquences éventuelles. La détermination des risques a pour objet de produire une liste complète des risques pour la sécurité ayant une incidence sur les ressources du ministère[12] qui influent ainsi sur l'atteinte des objectifs opérationnels. Il importe de dresser un inventaire complet des risques (risques initiaux), car ceux qui ne sont pas identifiés ne feront pas l'objet d'une analyse approfondie. Il faut déterminer les risques, que l'organisme contrôle leur source ou non, même lorsque leur source ou leur cause n'est peut-être pas évidente ou que les risques sont atténués adéquatement à l'heure actuelle. Les attaques malveillantes contre les systèmes d'information causant l'incapacité d'offrir des services sont un exemple de risques que l'organisation ne contrôle pas.

Les risques pour la sécurité tombent généralement dans trois catégories : délibérés, accidentels ou naturels. Ils peuvent être génériques ou spécifiques et nécessiter une analyse au cas par cas. Il importe de disposer de renseignements pertinents et à jour pour déterminer les sources de risques. Parmi les méthodes à envisager pour déterminer les sources de risques, il y a le remue-méninges, l'obtention de renseignements sur les menaces et les vulnérabilités auprès des principaux organismes chargés de la sécurité (POS) ou d'autres sources et la consultation de personnes qui possèdent des connaissances pertinentes, comme les gestionnaires de risques ministériels, les responsables de programmes et de systèmes et les autres intervenants.

Voici des exemples de risques pour la sécurité communs à la plupart des ministères :

- pertes financières et non financières, attribuables au vol, à la destruction ou au vandalisme de biens matériels;
- fraude, dommages causés au réseau, divulgation et usage abusif attribuables aux menaces internes;
- dommages causés aux employés ou à leur famille et dont l'emploi les expose à un risque accru de violence en milieu de travail (interactions avec le public, contact avec des personnes instables, garde de biens de grande valeur, etc.);
- interruption de la prestation de services en raison d'un manque ou de la non-disponibilité de ressources humaines (p. ex., les employés souffrant de la grippe, les conditions météorologiques extrêmes, les catastrophes naturelles);
- compromission des renseignements ou des biens sensibles transmis aux partenaires ou aux fournisseurs de services, attribuable à la mise en œuvre inadéquate des contrôles de sécurité;
- pertes financières et atteinte à la réputation attribuables à une atteinte à la protection des données ou à une perte d'intégrité de l'information;
- interruption de la prestation des services de première importance en raison de catastrophes naturelles ou de cyberattaques entraînant des incidences sur l'infrastructure ou les communications essentielles.

Compte tenu du fait que cette liste n'est pas exhaustive, chaque ministère doit faire le nécessaire pour déterminer les risques qui sont propres à ses activités et à son environnement opérationnel.

Analyse des risques

L'analyse des risques a pour objet d'évaluer la probabilité et l'incidence des risques pour la sécurité qui peuvent avoir des incidences sur l'atteinte des résultats stratégiques et opérationnels. Elle comporte la compréhension de la nature et de la gravité des risques, et elle fournit les renseignements et l'analyse nécessaires pour décider s'il faut traiter les risques et de la méthode de traitement des risques qui convient le mieux. Le processus d'analyse est généralement appuyé par l'utilisation de divers modèles et outils et il peut être effectué à divers degrés de détail, en fonction des risques et des renseignements disponibles. Les outils peuvent utiliser des méthodes qualitatives ou quantitatives, ou une combinaison des deux.

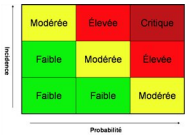
Ci-dessous sont présentés des exemples de matrices qualitatives que les ministères peuvent adapter pour appuyer le processus d'analyse. Ces exemples illustrent une méthode simple d'évaluation de l'incidence et de la probabilité visant à aider l'évaluation de la gravité du risque. Ces matrices peuvent être élargies en ajoutant des lignes ou des colonnes et en adaptant les descriptions aux critères de prise de décisions du ministère. Ces exemples ne mettent pas de l'avant un élément particulier, et les ministères sont invités à adapter ces matrices de façon à ce qu'elles soient conformes aux autres pratiques internes en matière d'analyse des risques (comme celles utilisées par la gestion des risques ministériels). Cela aidera à comparer et à évaluer les risques au moyen d'outils et de cadres de référence communs.

Exemples de matrices d'analyse qualitative des risques

Incidence	
Niveau	**Description**
Élevée	Pertes majeures, perturbation permanente de la prestation des services, grande incidence sur la réputation du gouvernement ou la santé et le bien-être des Canadiens, perte temporaire ou permanente d'infrastructure essentielle
Modérée	Légère perturbation permanente de la prestation des services, incidence modérée sur le bien-être des Canadiens
Faible	Perturbation mineure de la prestation des services, faible incidence sur le bien-être des Canadiens

Probabilité	
Niveau	**Description**
Élevée	Se produit probablement dans la plupart des circonstances
Modérée	Peut se produire à un moment ou à un autre
Faible	Peut se produire seulement lorsque les circonstances sont exceptionnelles

Figure 3 - Exemple de matrice des risques



Version textuelle : Figure 3 - Exemple de matrice des risques

Évaluation des risques

L'évaluation des risques est le processus permettant de déterminer si les risques sont acceptables ou non. Ces décisions doivent être guidées par les critères de risques établis, et prises par les personnes ayant les pouvoirs appropriés. Elles doivent également tenir compte du contexte des risques, de la tolérance du ministère, ses responsables de risques et d'autres intervenants sur lesquels les risques peuvent avoir des incidences.

Si le niveau de risque est jugé acceptable, il peut être accepté sans devoir être géré. Les risques jugés acceptables doivent tout de même être documentés, surveillés et examinés régulièrement pour veiller à ce qu'ils restent acceptables.

Si le niveau de risque est jugé inacceptable, les options de gestion du risque doivent être recensées. Celles-ci peuvent comprendre la réduction du risque, l'évitement du risque ou le transfert de ce dernier.

Il est possible de réduire le risque en mettant en œuvre des contrôles permettant de réduire ou d'éliminer efficacement le risque. Les contrôles qui réduisent le risque avec le plus d'efficacité et pour un coût raisonnable pour le ministère sont les contrôles dont la mise en œuvre est la plus susceptible d'être recommandée.

Il est possible d'éviter le risque en n'entreprenant aucune activité susceptible d'entraîner la matérialisation du risque. Ce n'est peut-être pas toujours une option pratique, mais elle peut tout de même constituer une partie importante de l'examen de l'ensemble des moyens utilisés pour gérer le risque et peut faire partie de l'option de traitement.

Il est possible de transférer le risque en imputant la responsabilité à une autre partie ou en partageant le risque au moyen d'un contrat, d'un partenariat ou d'une coentreprise. Il convient de souligner que de nouveaux risques peuvent se présenter lors du transfert du risque s'il n'est pas géré de façon adéquate par la partie à qui le risque est transféré.

Il est possible de décider, après certaines évaluations des risques, de mener d'autres analyses. L'évaluation, ainsi que les raisons ou la justification permettant d'arriver à la décision, doit être documentée afin de fournir un dossier de la réflexion qui y a mené, car elle fournit un contexte utile aux évaluations des risques futurs.

7.2.3 Traitement des risques pour la sécurité

... définit et établit, au besoin, des mesures de contrôle minimales supplémentaires en vue d'atteindre les objectifs en matière de contrôle et d'en arriver à un niveau acceptable de risque résiduel.

Section 6.1.1.3 de la Directive sur la gestion de la sécurité ministérielle

Il revient à la direction de décider de la méthode de gestion des risques pour la sécurité. Les critères définis dans le cadre de l'approche en matière de GRS du ministère, ainsi que les obligations juridiques, stratégiques ou réglementaires liant le ministère, servent à guider la prise de décisions. La volonté du ministère d'accepter ou de gérer les risques sera également un facteur de la prise de décisions. Le risque qui demeure après la mise en œuvre des contrôles de sécurité ou la prise d'une décision visant à accepter le risque représente le risque résiduel.

Décision concernant la traitement des risques pour la sécurité

Pour chaque risque pour la sécurité, le PSM doit consigner la décision prise en ce qui a trait à la sélection de l'option de traitement du risque (le réduire, l'éviter, le transférer). Les décisions relatives aux risques pour la sécurité dans le cadre desquelles l'option de traitement choisie est l'évitement ou le transfert doivent décrire en détail les mécanismes qui seront utilisés pour gérer les risques adéquatement et assurer un suivi continu.

Objectifs de contrôle de sécurité

Les objectifs de contrôle de sécurité sont les résultats ou le but à atteindre grâce à la gestion des risques pour la sécurité. Ils servent à orienter le choix des contrôles visant à gérer les risques et la détermination des indicateurs de rendement permettant d'évaluer l'atteinte des objectifs.

Les objectifs de contrôle de sécurité doivent être définis pour chaque risque pour la sécurité jugé inacceptable et pour lequel l'option de traitement choisie est de réduire le risque. Ils constituent le fondement de la mesure de l'efficacité des contrôles à gérer les risques pour la sécurité.

Contrôles de sécurité

Les mesures de contrôle de sécurité sont les mesures administratives, opérationnelles, techniques, physiques ou juridiques prises en vue de gérer les risques pour la sécurité et de réduire ceux-ci à un niveau acceptable. Il faut les choisir et les mettre en œuvre pour chaque risque pour lequel un objectif de contrôle a été établi. Il existe deux catégories de contrôles : les contrôles communs à l'échelle du gouvernement et les contrôles propres aux ministères.

Les contrôles communs à l'échelle du gouvernement sont définis à l'annexe C de la DGSM et s'appliquent à tous les aspects de la sécurité ministérielle. Ces contrôles sont liés aux activités comprenant notamment :

- l'assurance des renseignements;
- le filtrage de sécurité des personnes;
- la sécurité matérielle;
- la sécurité de la TI;
- la sécurité en matière de passation des marchés;
- le partage de renseignements et de biens avec d'autres organismes ou ministères;
- l'obtention de services de sécurité auprès d'autres organismes;
- la sensibilisation aux questions de sécurité;
- la formation sur la sécurité;
- la gestion des incidents de sécurité;
- la protection des employés contre la violence en milieu de travail;
- les inspections de sécurité;
- les enquêtes administratives liées aux incidents de sécurité;
- la sécurité dans les situations d'urgence et de menace accrue;
- la planification de la continuité des activités.

Les contrôles propres aux ministères sont définis par ces derniers en fonction de leurs objectifs opérationnels. Par conséquent, ils sont probablement uniques pour chaque ministère. Même s'ils peuvent être décrits à un très haut niveau dans le PSM, ils fournissent un cadre permettant de déterminer des contrôles plus précis propres au ministère. C'est ce qui est généralement nécessaire lorsqu'un ministère doit atteindre un niveau supérieur en matière de sécurité en raison des activités qui lui sont propres ou d'autres contraintes. Un exemple de contrôle propre au ministère pourrait être les mesures de protection visant à protéger les employés à l'extérieur du milieu de travail en raison des risques accrus pour la sécurité auxquels ils sont exposés. Lorsqu'un ministère définit les contrôles qui lui sont propres, il doit absolument garder à l'esprit l'incidence que pourrait avoir la mise en œuvre des contrôles sur les autres ministères.

Le choix des mesures de contrôle doit permettre d'atteindre les objectifs de contrôle établis au cours de l'étape précédente. Il doit tenir compte de l'équilibre à réaliser entre les coûts et les efforts déployés pour gérer les risques et les avantages de ces mesures et les exigences en matière de conformité. La possibilité de faire plus avec moins au ministère doit être prise en considération.

La PSG, la DGSM et les normes afférentes établissent les mesures de contrôle de sécurité ayant pour but de maintenir un environnement opérationnel adapté à la plupart des programmes, des services, des activités ou des systèmes. En fonction de la nature et du niveau des risques à gérer, les ministères peuvent choisir de mettre en application des contrôles supplémentaires afin de satisfaire leurs exigences uniques ou élevées. Il est également possible de trouver des contrôles de sécurité dans diverses lignes directrices produites par les principaux organismes chargés de la sécurité (POS) et fondées sur leur domaine de compétence, notamment la Gendarmerie royale du Canada (GRC) pour la sécurité matérielle, le Centre de la sécurité des télécommunications Canada (CSTC) pour la sécurité de la technologie de l'information, Travaux publics et Services gouvernementaux Canada (TPSGC) pour la sécurité des marchés, Sécurité publique Canada pour la gestion des urgences et la planification de la continuité des activités, et le Secrétariat du Conseil du Trésor (SCT) et le Service canadien du renseignement de sécurité (SCRS) pour le filtrage de sécurité des personnes.

Indicateurs de rendement

Les indicateurs de rendement sont le fondement de l'évaluation de la mesure dans laquelle les contrôles atteignent les objectifs de contrôle. Grâce au processus systématique et permanent de collecte et d'analyse de ces indicateurs de rendement, les ministères peuvent évaluer la mesure dans laquelle les contrôles permettent d'atteindre les résultats escomptés et établir des rapports en la matière.

Un indicateur de rendement peut être quantitatif ou qualitatif. Les indicateurs quantitatifs se composent d'un nombre et d'une unité. Le nombre fournit la magnitude (combien) et l'unité fournit au nombre sa signification (quoi), p. ex., le nombre de cas de vol documentés. Par contre, les indicateurs qualitatifs sont plus subjectifs ou relatifs, p. ex., une évaluation de la qualité d'une enquête. Dans la mesure du possible, les indicateurs qualitatifs doivent être résumés à l'aide d'une échelle de notation (la qualité de la recherche est notée « excellente », « moyenne » ou « inférieure à la moyenne »[13].

Il faut définir entre un et trois indicateurs de rendement pour chaque contrôle de sorte que la masse de renseignements à suivre, à recueillir et à tenir à jour peut être gérée. En choisissant ou en élaborant des indicateurs de rendement, il importe de poser les questions suivantes :

- L'indicateur de rendement prouve-t-il clairement et reflète-t-il pertinemment l'atteinte des objectifs de contrôle?
- Les indicateurs de rendement sont-ils simples et faciles à mesurer?

- Est-il possible d'utiliser des renseignements déjà disponibles dans le ministère, d'autres ministères, des organismes de statistiques, des organisations internationales, etc.?
- Les indicateurs de rendement peuvent-ils être suivis et comparés avec le temps afin de permettre des comparaisons d'une année à l'autre?
- Sera-t-il difficile ou onéreux de saisir les renseignements?

Pour chaque indicateur de rendement, il importe de déterminer ce qui suit :

- les sources des données ou de renseignements à recueillir ou à créer ou celles qui sont régulièrement disponibles;
- la fréquence de la collecte et de l'évaluation des données (une ou deux fois par an, mensuellement);
- les cibles (ou le degré de réussite) à atteindre au cours d'une période précise.

Le document du SCT intitulé *Consignes aux ministères sur la préparation d'une structure de gestion, des ressources et des résultats* donne des indications précieuses sur l'élaboration d'indicateurs de rendement, et il est possible de s'y reporter pour obtenir de plus amples renseignements. Bien qu'il soit peu probable que les indicateurs de rendement en matière de sécurité soient ajoutés au Cadre de mesure du rendement (CMR) du ministère, ce niveau de détail n'étant habituellement pas présenté dans le cadre de l'AAP, il pourrait être utile de le faire pour obtenir la cohérence.

Analyse des écarts

L'évaluation des écarts a pour objet de déterminer les objectifs de contrôle de sécurité qui ne sont pas atteints, pour lesquels des contrôles doivent être mis en œuvre, améliorés ou autrement ajustés ou pour lesquels des indicateurs de rendement ne sont pas encore établis. Elle aide à confirmer les risques qui sont déjà gérés à un niveau acceptable. Pour chaque risque déterminé qui a été jugé inacceptable et pour lequel des objectifs de contrôle ont été déterminés, une analyse des écarts doit chercher à déterminer ce qui suit :

- Existe-t-il actuellement des contrôles pour atteindre l'objectif de contrôle et pour gérer les risques pour la sécurité?
- Les contrôles gèrent-ils efficacement les risques et permettent-ils d'atteindre les objectifs de contrôle (comme le démontrent les indicateurs de rendement)?
- Les indicateurs de rendement sont-ils suffisants et pertinents pour mesurer l'efficacité du contrôle?

Les résultats d'une analyse des écarts servent de point de départ à l'établissement d'une liste des priorités relatives en matière de mise en œuvre des contrôles supplémentaires et à l'établissement d'indicateurs de rendement. Les résultats peuvent également indiquer les endroits où les contrôles peuvent être excessifs et doivent être réduits, éliminés ou autrement remplacés.

Priorités

Les priorités doivent porter sur les éléments généraux qui sont cruciaux pour la réalisation de la mission du ministère ou pour assurer la conformité aux obligations législatives et politiques. La détermination des priorités doit être confirmée avec les priorités ministérielles connues et énoncées; il peut également être utile de consulter les autres intervenants internes afin de déterminer les possibilités d'harmonisation ou de collaboration. Puisqu'il y a toujours plus de problèmes qui requièrent l'attention qu'il n'y a de ressources pour les examiner, il peut être utile de poser les questions suivantes :

- Un lien est-il établi entre les priorités en matière de sécurité, les priorités ministérielles et les résultats stratégiques?
- Cette priorité traite-t-elle des exigences de conformité définies par les obligations stratégiques, législatives, contractuelles ou d'autres obligations?
- Quels liens y a-t-il entre cette priorité et les priorités gouvernementales?
- Quelles sont la disponibilité ou les limites des ressources ministérielles ou gouvernementales?
- Cette priorité traite-t-elle des attentes des intervenants ou des conséquences négatives éventuelles pour la réputation?
- Les possibilités de collaborer avec d'autres intervenants ministériels ou de combiner les priorités avec d'autres plans et initiatives ont-elles été prises en considération?
- Quel risque résiduel demeure si les risques ne sont pas gérés et comment sera-t-il géré?

7.2.4 Mise en œuvre, suivi et mise à jour

... énonce des stratégies, des objectifs, des priorités et des délais de sécurité pour améliorer la posture de sécurité du ministère.

Section 6.1.1.4 de la Directive sur la gestion de la sécurité ministérielle

La dernière étape du processus de GRS comprend la formulation d'une stratégie pour mettre en œuvre les contrôles de sécurité et les indicateurs de rendement, pour effectuer le suivi des progrès et pour rendre compte des résultats atteints. La stratégie de mise en œuvre constitue un moyen de gérer le processus et les ressources, de se concentrer sur l'atteinte des résultats escomptés, de renforcer les partenariats avec les intervenants ministériels et de mettre l'accent sur l'évaluation de l'obtention des résultats. Les détails concernant la mise en œuvre sont ce qui figure généralement dans les plans de travail et les plans de projet.

Stratégie de mise en œuvre

Une stratégie de mise en œuvre expose en détail les activités et confère à des personnes précises la responsabilité de les mener. Elle établit également l'échéancier et les estimations des besoins en ressources et décrit la manière dont les progrès seront évalués et suivis. Il importe de tenir des consultations lors de l'élaboration d'une stratégie de mise en œuvre, car elles fournissent un moyen d'harmoniser les objectifs, l'échéancier et les besoins en ressources avec d'autres plans ministériels.

Une stratégie de mise en œuvre typique établira ce qui suit :

- les buts à court terme (un à deux ans) et à long terme (trois à cinq ans) en vue de mettre en œuvre les contrôles de sécurité et les indicateurs de rendement, conformément aux priorités établies;
- les activités, les rôles et les responsabilités nécessaires à la mise en œuvre de contrôles supplémentaires et à l'établissement d'indicateurs de rendement (chaque activité peut à son tour être traduite en un certain nombre de plans de travail précis);
- l'échéancier et les jalons qui déterminent l'ordre des activités;
- les ressources nécessaires pour mettre en œuvre les contrôles et surveiller leur efficacité[14];
- les risques et les contrôles qui continuent d'exister pendant la période de transition.

Surveillance

La surveillance s'entend de la collecte et de l'analyse de renseignements visant à mesurer les progrès dans la mise en œuvre des contrôles et dans l'établissement des indicateurs de rendement, ce qui permet de faire en sorte que les activités prévues et la mise en œuvre des contrôles respectent l'échéancier et les ressources affectées. Elle s'entend également du suivi de l'efficacité des contrôles dans l'atteinte des objectifs de contrôle (à l'aide des indicateurs de rendement). Les gestionnaires de tous les niveaux et les spécialistes de la sécurité sont chargés de surveiller la mise en œuvre et l'efficacité des contrôles de sécurité et, en conséquence, d'en rendre compte à l'ASM[15].

La surveillance peut également comprendre le maintien d'une sensibilisation aux menaces et à l'environnement opérationnel afin de pouvoir déterminer, évaluer et gérer en permanence les risques. La consultation régulière des intervenants et des responsables des risques devrait aider à rester au fait de l'évolution des activités ministérielles tandis qu'une analyse périodique de l'environnement devrait aider à surveiller les menaces. De plus, la consultation présente une occasion d'informer les responsables des risques des progrès et de prendre une décision si des modifications sont essentielles. Comme c'est le cas des étapes précédentes, les résultats de la surveillance devraient être documentés aux fins de preuves et être utilisés pour rendre compte des progrès à la haute direction.

L'utilité d'effectuer un examen indépendant (une vérification) pour évaluer l'efficacité du processus et des activités de GRS ainsi que les progrès réalisés dans le cadre de la mise en œuvre du PSM peut être prise en considération. Un tel plan doit faire l'objet de consultations internes, être entrepris en connaissant les coûts connexes, et être fait en fonction des autres priorités relatives aux vérifications et aux évaluations ministérielles.

Établissement de rapports

L'établissement périodique de rapports, qui est utile pour demander à la direction de formuler des commentaires ou de prendre des décisions, afin de s'attaquer aux problèmes émergents, représente une occasion de prouver les progrès réalisés vers l'obtention des résultats escomptés. L'établissement de rapports améliore la prise de décisions en évaluant les réussites et les échecs, en surveillant l'utilisation des ressources et en diffusant l'information sur les pratiques exemplaires et les leçons apprises. Les ministères doivent évaluer périodiquement l'efficacité de leurs processus de GRS[16] afin de favoriser l'apprentissage et l'amélioration permanente.

L'établissement de rapports doit se fonder sur des renseignements fiables et exacts afin de prouver que les activités prévues permettent d'obtenir les résultats escomptés avec efficacité et efficience. Si les constatations et les décisions sont documentées tout au long du processus de GRS et que les renseignements concernant les progrès réalisés, recueillis grâce aux activités de surveillance, sont consignés, l'établissement de rapports ne sera pas une tâche ardue.

Mise à jour

Le PSM et les évaluations des risques à l'appui doivent être mises à jour et révisées de façon périodique ou lorsque les circonstances changent de façon importante.

7.3 Grille du plan de sécurité ministériel

Les administrateurs généraux sont responsables [...] d'approuver le programme de sécurité ministérielle qui détaille les décisions en matière de gestion de risques liés à la sécurité et qui expose les stratégies, les buts, les objectifs et les échéanciers élaborés en vue d'améliorer la sécurité ministérielle et de favoriser sa mise en œuvre

Section 6.1.3 de la Politique sur la sécurité du gouvernement

Un plan bien préparé démontre que les gestionnaires ont bien réfléchi aux activités de l'organisation et comprennent ce qu'ils doivent faire pour appuyer ces activités et la façon de le faire. Le PSM officialise le lien entre les objectifs opérationnels et la gestion des risques pour la sécurité, afin d'atteindre ces objectifs. Il aide l'administrateur général et les cadres supérieurs à atteindre l'excellence en gestion en leur donnant un moyen de déterminer et de gérer proactivement les risques pour la sécurité que posent les opérations.

Le PSM expose en détail les décisions en matière de gestion des risques pour la sécurité, selon leur priorité relative, l'échéancier de mise en œuvre des contrôles supplémentaires pour améliorer la sécurité ministérielle, et les indicateurs de rendement utilisés pour mesurer l'atteinte des résultats. Bien que la gestion de l'ensemble des risques pour la sécurité entre dans le cadre de la GRS, le PSM devrait mettre l'accent sur les risques les plus susceptibles d'avoir une incidence sur la capacité du ministère à remplir son mandat, qui influent considérablement sur les ressources humaines ou financières, qui peuvent empêcher la conformité aux exigences de sécurité définies dans les politiques ou la réglementation ou qui peuvent entraîner une interruption des services essentiels.

Le PSM est un document stratégique qui fournit à l'administrateur général et aux cadres supérieurs un « aperçu intégré des risques pour la sécurité pour le compte du ministère ». Même s'il est entendu que le format et la structure du document, ainsi que de tout document probant, peuvent varier d'un ministère à l'autre, l'utilisation de la grille ci-dessous est recommandée pour veiller à ce que les éléments du PSM soient relativement cohérents d'un ministère à l'autre et qu'ils reflètent les résultats de la GRS.

Le PSM peut également servir de fondement à l'élaboration de plans de travail et de plans de projet annuels qui appuient la mise en œuvre des buts et des objectifs de sécurité approuvés par le PSM à l'échelle du ministère.

Les trois premières sections visent à fournir au lecteur une introduction et une orientation sur le PSM lui-même. Les autres sections servent à décrire le processus de GRS de même que les exigences de la PSG et la DGSM.

Élément du PSM	Description
Approbation	• Un énoncé de l'administrateur général (ou d'une autorité équivalente) qui vise à appuyer les décisions concernant la traitement des risques, de même que la mise en œuvre des contrôles et des indicateurs de rendement.
Sommaire	• Un sommaire non technique du PSM qui souligne les principaux points, enjeux et conclusions, et qui contient suffisamment de renseignements pour faire connaître au lecteur les éléments abordés dans le plan complet.
	• Une brève description de la structure et du processus de gouvernance relatifs à l'élaboration du

Communications et consultations	PSM (qui a participé et de quelle façon, les rôles, les responsabilités et les pouvoirs des principaux intervenants). • La désignation des personnes et des organisations qui ont été consultées ou qui ont participé à l'élaboration du PSM. • La liste des documents de référence et des sources faisant autorité qui ont été consultés dans le cadre de l'élaboration du PSM.

Contexte	• Contexte opérationnel
	  ○ Une brève description du mandat, des priorités, des résultats stratégiques, des activités de programmes et des sous-activités de programmes du ministère
	  ○ Un aperçu des ressources et des services ministériels se rapportant à ces activités et ces sous-activités de programmes.
	• Contexte organisationnel
	  ○ Une brève description de la structure organisationnelle, géographique et de gouvernance du ministère.
	  ○ Une brève description des politiques, des processus et des activités internes mis en place pour aider le ministère à atteindre ses objectifs opérationnels.
	• Contexte de la sécurité
	  ○ Une description générale du rôle que joue la sécurité pour permettre au ministère de réaliser sa mission et d'appuyer les priorités gouvernementales.
	  ○ Une brève description des contraintes et des exigences en matière de sécurité découlant des obligations juridiques, réglementaires, stratégiques, contractuelles ou d'autres obligations.
	  ○ Un aperçu des menaces de sécurité propres aux contextes opérationnel et organisationnel de l'organisme.
	  ○ Peut comprendre une description d'autres facteurs ou contraintes qui peuvent avoir une incidence sur les décisions concernant les risques pour la sécurité.
	  ○ Peut comprendre une description des liens qui existent entre la sécurité ministérielle et les autres pratiques de gestion et activités de programmes internes.
	• Approche concernant l'élaboration du PSM
	  ○ Une description de la portée du PSM (concerne l'ensemble du ministère ou seulement un sous-ensemble du ministère ou des programmes).
	  ○ Une description de la structure et de l'organisation des plans et des évaluations des risques pour la sécurité fournissant, dans l'ensemble, un aperçu intégré des risques pour la sécurité du ministère (dans le cas des ministères importants pour lesquels le PSM peut en fait être constitué d'un ensemble de plans).
	• Méthode de GRS
	  ○ Une brève description de l'approche du ministère en ce qui concerne la GRS (comprend une description de l'harmonisation entre le processus de GRS et les activités de programmes du ministère).
	  ○ Les critères permettant d'évaluer l'importance des risques pour la sécurité.
	  ○ Une description de la manière dont les résultats des évaluations des risques et les facteurs de traitement des risques sont documentés afin d'assurer la traçabilité.

	Nota : Certaines parties de la présente section et de la section suivante peuvent être mieux résumées dans une matrice.

Évaluation des risques pour la sécurité	• Détermination des risques
	  ○ Une liste des principaux risques pour la sécurité visant les ressources et les services du ministère (établie selon les évaluations des risques réalisées).
	  ○ Doit comprendre la désignation des responsables des risques et des intervenants.
	• Analyse des risques
	  ○ La détermination de la probabilité et de l'incidence des risques pour la sécurité
	• Évaluation des risques
	  ○ La détermination des risques qui ont été jugés inacceptables (avec une explication).
	  ○ La détermination des risques qui ont été jugés acceptables et l'approche qui sera adoptée pour effectuer le suivi et l'examen périodique.

Traitement des risques pour la sécurité	• Décision concernant la traitement des risques pour la sécurité
	  ○ La détermination de l'option de traitement du risque choisie pour chaque risque.
	• Objectifs de contrôle de sécurité
	  ○ Une description des objectifs de contrôle concernant les risques pour lesquels l'option de traitement choisie consiste à mettre en application des mesures de contrôle.
	• Contrôles de sécurité
	  ○ Une description des contrôles de sécurité permettant d'atteindre les objectifs de contrôle.
	  ○ Il existe plusieurs catégories de contrôles. Ceux-ci peuvent être administratifs, techniques ou physiques, ou alors être communs à tous les ministères ou propres à un ministère.
	• Indicateurs de rendement
	  ○ Une description des indicateurs de rendement permettant de surveiller l'efficacité des contrôles de sécurité.
	  ○ Pour chaque indicateur de rendement, indiquer les sources de données, la fréquence et les cibles.
	• Analyse des écarts
	  ○ Un recensement des objectifs de contrôle de sécurité qui ne sont pas encore atteints et pour lesquels des contrôles doivent être mis en œuvre, améliorés ou autrement ajustés, ou pour lesquels des indicateurs de rendement ne sont pas encore établis.
	  ○ Peut indiquer les contrôles qui sont jugés excessifs et qui seront éliminés.
	• Priorités
	  ○ Une liste des priorités recommandées afin de mettre en œuvre des contrôles supplémentaires et d'établir des indicateurs de rendement.

Mise en œuvre	• Stratégie de mise en œuvre
	  ○ Un résumé des objectifs à court et à long termes visant à mettre en œuvre les contrôles de sécurité et les indicateurs de rendement.
	  ○ Les activités, les rôles et les responsabilités
	  ○ L'échéancier et les jalons
	  ○ Les ressources
	  ○ Les facteurs à prendre en considération à l'égard de la période de transition.
	• Surveillance et établissement de rapports
	  ○ Une description de l'approche adoptée pour surveiller les éléments qui suivent et pour établir des rapports à cet égard :
	  ▪ les progrès réalisés relativement à la mise en œuvre des contrôles et des indicateurs de rendement;
	  ▪ l'efficacité des contrôles de sécurité en ce qui a trait à l'atteinte des objectifs de contrôle (à l'aide des indicateurs de rendement);
	  ▪ les changements dans les environnements opérationnel, organisationnel et de la sécurité;
	  ▪ l'efficacité des processus de GRS.
	  ○ Une description de la façon dont seront surveillés les risques résiduels.
	• Mise à jour
	  ○ Une description du processus et de l'échéancier requis pour effectuer la mise à jour du PSM.

7.3.1 Documents probants

Tous les risques pour la sécurité doivent être documentés dans des documents probants servant à consigner l'analyse et les constatations de chaque étape du processus de GRS. Conjointement avec des politiques et des processus adéquatement documentés, ils consignent les activités de GRS aux fins de référence, d'examen et de prise de décisions permanents et peuvent servir à orienter les activités quotidiennes de GRS. Les documents probants peuvent comprendre ce qui suit :

Le processus de gestion des risques pour la sécurité

- Établit l'approche concernant la GRS du ministère et peut comprendre des descriptions de politiques, de procédures et de pratiques permettant d'évaluer, de gérer et de surveiller les risques pour la sécurité.
- Établit les critères définis par le ministère pour décider si les risques pour la sécurité sont acceptables ou inacceptables (outils, méthodes, etc.).
- Explique les relations entre le PSM et les documents probants.

L'analyse du contexte de la sécurité

- Analyse les menaces internes et externes et évalue l'exposition actuelle aux risques du ministère.

Le rapport de communication et de consultation

- Documente la méthode de consultation des intervenants internes et externes ou les résultats de celles-ci, ou les deux.

Les documents et les politiques sur le programme de sécurité ministérielle

- Décrivent les activités de programmes de la sécurité du ministère et les pratiques de gestion ayant trait à l'ensemble des aspects de la sécurité ministérielle.
- Décrivent les mécanismes de gouvernance, de délégation, de coordination et d'établissement de rapports au sein du programme de sécurité et entre celui-ci et d'autres groupes ayant des responsabilités en matière de sécurité (p. ex., planification d'urgence, santé et sécurité au travail, GI, TI, régions, etc.) et les services de sécurité fournis par une autre partie ou à celle-ci, comme un ministère de portefeuille ou un fournisseur de services partagés.

Les rapports d'évaluation des risques pour la sécurité

- Exposent en détail les résultats des évaluations des risques pour la sécurité, ainsi que leur analyse et leurs décisions quant à la façon de gérer ces risques en se fondant sur les critères de GRS établis.
- Ces renseignements peuvent également être consignés dans un registre des risques pour la sécurité (voir ci-dessous).

Les rapports de traitement des risques pour la sécurité

- Les analyses et les décisions détaillées concernant le choix des options de traitement des risques, la détermination des objectifs de contrôle, le choix des contrôles et des indicateurs de rendement, la réalisation des analyses des écarts et l'établissement des priorités.
- Ces renseignements peuvent également être consignés dans un registre des risques pour la sécurité (voir ci-dessous).

Le Cadre de mesure du rendement en matière de sécurité

- Décrit les rôles et les responsabilités, les outils, les méthodes, les processus et la fréquence d'évaluation du rendement du programme de sécurité, l'évaluation de l'efficacité des pratiques de GRS, l'évaluation de la mesure dans laquelle les contrôles atteignent les objectifs de contrôle, et l'établissement de rapports à l'intention de la haute direction.

Les plans de travail et les plans de projet annuels

- Décrivent les activités et les affectations ciblées, qui appuient la mise en œuvre des priorités approuvées dans le PSM à l'échelle du ministère, ainsi que les activités relatives à l'administration du programme de sécurité ministérielle.

7.3.2 Registre des risques pour la sécurité

Un registre des risques est un outil couramment utilisé par de nombreux gestionnaires des risques ministériels et certains organismes de sécurité pour documenter les résultats de la gestion des risques. Un RRS sert à consigner les résultats de la GRS. Ce genre d'outil peut être désigné comme un registre des risques ministériels (RRM), une fiche d'évaluation des risques pour la sécurité ou un journal des risques pour la sécurité. Un RRS peut servir à consigner les mêmes renseignements qui seraient autrement documentés dans certains des documents probants décrits ci-dessus (sauf les documents relatifs aux politiques). Un RRS complet comprend les détails des risques déterminés, ainsi que leur analyse et les plans exposant la façon de les gérer. Un des avantages du RRS est qu'il fournit un moyen de consolider et de faire la synthèse d'une grande quantité d'information de façon pertinente, uniforme et concise, en plus de permettre des comparaisons entre plusieurs programmes afin de faciliter le processus décisionnel.

Un RRS peut être tenu comme un simple document avec un logiciel de traitement de texte ou un tableur, ou il peut prendre la forme d'une base de données. Un exemple de RRS sous forme de tableau figure à l'annexe C - Exemple de registre des risques pour la sécurité.

Les documents probants et le RRS doivent être mis à jour régulièrement, y compris dans les cas où de nouveaux renseignements ou enjeux rendent cette mise à jour appropriée, lorsqu'il y a des changements ou des ajustements de l'exposition du ministère aux plans des opérations ou de la sécurité ou lorsque l'AAP du ministère est mise à jour.

8. Demandes de renseignements

Pour toute demande de renseignements au sujet du présent instrument de politique, veuillez communiquer avec la Division de la sécurité et gestion de l'identité.

Annexe A — Définitions

Architecture des activités de programmes (AAP) (*Program Activity Architecture*)
Inventaire de tous les programmes et de toutes les activités dressé par un ministère ou un organisme. Les activités et les programmes sont présentés d'après le lien logique qui les unit à la fois entre eux et aux résultats stratégiques auxquels ils contribuent. L'AAP est le document initial permettant d'établir la structure de gestion, des ressources et des résultats (SGRR).

Cadre supérieur (*executive*)
Fonctionnaire nommé au groupe de la direction (niveaux EX-01 à EX-05), c.-à-d. un directeur, un directeur général, un sous-ministre adjoint ou l'équivalent.

Compromission (*compromise*)
Accès ou interruption d'accès à des biens ou à des renseignements sans autorisation et divulgation, destruction, suppression, modification ou utilisation non autorisée de biens ou de renseignements.

Confidentialité (*confidentiality*)
Qualité conférée à des renseignements pour signifier qu'ils ne peuvent être divulgués qu'à des personnes autorisées afin de prévenir tout préjudice à l'intérêt national ou à d'autres intérêts.

Contrôle de sécurité (*security control*)
Mesure administrative, opérationnelle, technique, physique ou légale de gestion des risques liés à la sécurité. Ce terme est synonyme de protection.

Critères de risque (*risk criteria*)
Cadre de référence grâce auquel un ministère définit et évalue l'importance des risques pour déterminer s'ils sont acceptables ou inacceptables (NOUVEAU).

Disponibilité (*availability*)
État de ce qui est accessible et utilisable de manière fiable et en temps opportun.

Évaluation des facteurs relatifs à la vie privée (EFVP) (*privacy impact assessment*)
Processus stratégique permettant de déterminer, d'évaluer et d'atténuer les risques liés à la protection des renseignements personnels. Les institutions gouvernementales doivent élaborer et tenir à jour des évaluations des facteurs relatifs à la vie privée pour tous les programmes nouveaux ou modifiés et toutes les activités nouvelles et modifiées, qui utilisent des renseignements personnels à des fins administratives (tiré de la Politique sur la protection de la vie privée).

Gestion des risques (*risk management*)
Méthode systématique servant à déterminer la meilleure façon de procéder lorsqu'il existe une certaine incertitude en déterminant, en évaluant et en comprenant les risques qui se posent, en prenant des mesures pour y donner suite et en communiquant l'information à ce sujet (tiré du Cadre de gestion intégrée du risque (CGIR)

Gestion des risques pour la sécurité (*security risk management*)
Composante d'un processus général de gestion des risques comprenant l'organisation et la coordination d'activités et de processus afin de maîtriser les risques pour la sécurité (GSTI).

Gestion intégrée des risques (*integrated risk management*)
Démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques dans la perspective de l'ensemble de l'organisation afin d'appuyer la prise de décisions stratégiques qui contribuent à l'atteinte des objectifs généraux d'un organisme (adapté du CIFR).

Gestionnaires à tous les niveaux (*managers at all levels*)
Comprend les superviseurs, les gestionnaires et les cadres supérieurs.

Intégrité (*integrity*)
État de ce qui est précis, complet, authentique et intact.

Interopérabilité (*interoperability*)
Capacité des ministères fédéraux de fonctionner en synergie au moyen de pratiques cohérentes de gestion de la sécurité et de l'identité.

Menace (*threat*)
Événement ou acte délibéré ou accidentel qui, s'il se produisait, pourrait porter préjudice aux renseignements, aux biens ou aux personnes.

Ministère (*department*)
Tous les ministères mentionnés à l'annexe I de la *Loi sur la gestion des finances publiques*, les divisions ou directions de l'administration publique fédérale mentionnées à la colonne I de l'annexe I.1, personnes morales mentionnées à l'annexe II et secteurs de l'administration publique fédérale mentionnés aux annexes IV et V de la *Loi sur la gestion des finances publiques* (LGFP), sauf si des lois, des règlements ou des décrets les en excluent.

Objectif de contrôle (*control objective*)
Énoncé des résultats escomptés ou des objectifs à atteindre en mettant en œuvre des contrôles de sécurité (adapté des *Objectifs de contrôle de l'Information et des Technologies Associées* (COBIT)).

Programme de sécurité (*security program*)
Ensemble de moyens mis en œuvre et d'activités apparentés qui sont gérés dans le but de répondre à des besoins particuliers et pour obtenir les résultats prévus.

Registre des risques pour la sécurité (*Security risk register*)
Dossier consolidé des risques pour la sécurité déterminés à partir d'une évaluation des risques qui fournit un résumé de leur analyse et des décisions en matière de traitement. La consolidation peut s'effectuer à l'échelle du ministère, de la direction générale, de la région ou du programme. Ce terme est synonyme de « journal des risques pour la sécurité », de « fiche d'évaluation des risques pour la sécurité » et d'« inventaire des risques pour la sécurité » comme les définissent les pratiques ministérielles de gestion des risques(NOUVEAU).

Risque (*risque*)
Incertitude que peut engendrer une exposition à des situations, des événements ou des résultats futurs non désirés. C'est l'expression de la probabilité et de l'incidence d'un événement ou d'une situation susceptible de nuire à la réalisation des objectifs d'une organisation.

Risque pour la sécurité (*security risk*)
Expression de la probabilité et de l'incidence d'événements susceptibles de porter préjudice aux renseignements, aux biens, aux personnes ou aux services (NOUVEAU).

Risque résiduel (*residual risk*)
Risque qui continue d'exister après la mise en œuvre des mesures (contrôles) de sécurité.

Résultat stratégique (*strategic outcome*)
Avantage durable à long terme pour les Canadiens, qui découle du mandat et de la vision d'un ministère ou d'un organisme. Il s'agit d'un résultat qu'un ministère ou un organisme entend obtenir au profit de la population canadienne, qui devrait être mesurable et s'inscrire dans la sphère d'influence du ministère (SGRR).

Sous-activité (*sub activity*)
Groupe d'activités connexes sous le niveau de l'activité de programme (deuxième niveau de la structure de l'AAP) (SGRR).

Sous-sous-activité (*sub-sub activity*)
Groupe d'activités connexes sous le niveau de la sous-activité (troisième niveau de la structure de l'AAP) (SGRR).

Violence en milieu de travail (*workplace violence*)
Agissement, conduite, menace ou geste qui pourrait vraisemblablement causer un dommage, des blessures ou une maladie à un employé en milieu de travail.

Vulnérabilité (*vulnerability*)
Lacune liée à la sécurité et pouvant augmenter la susceptibilité à une compromission ou à une blessure.

Annexe B — Références

Gouvernement fédéral

- Rapports annuels au Premier ministre sur la fonction publique du Canada
- Rapports et publications du vérificateur général
- Directive sur la gestion de la sécurité ministérielle (DGSM)
- Rapports ministériels sur le rendement (RMR)
- Méthodologie harmonisée d'évaluation des menaces et des risques
- Guide de la planification intégrée
- Cadre stratégique de gestion de risque
- Consignes aux ministères sur la préparation d'une structure de gestion, des ressources et des résultats
- Cadre de responsabilisation de gestion
- Politique sur la sécurité du gouvernement (PSG)
- Politique sur la structure de gestion, des ressources et des résultats (SGRR)
- *Loi sur la modernisation de la fonction publique (LMFP)*
- Rapports sur les plans et les priorités (RPP)
- Cadres stratégiques du Conseil du Trésor
- Ensemble des politiques du Conseil du Trésor
- Cadre pangouvernemental

Gouvernements provinciaux

- Results Oriented Government - A Guide to Strategic Planning and Performance Measurement in the Alberta Government
- Government of British Columbia - Enterprise Risk Management (ERM) Guideline (PDF 850 KO)

Autres gouvernements

- Australian National Audit Office (ANAO) - Security Risk Management (rapport numéro 44 élaboré en 2008-2009)
- Department of Homeland Security - National Infrastructure Protection Plan - Partnering to Enhance Protection and Resiliency
- UK National Risk Register (PDF 4,53 MO)
- Publication spéciale 800-18 du NIST - *Guide for Developing Security Plans for Federal Information Systems*
- Publication spéciale 800-30 du NIST - *Risk Management Guide for Information Technology Systems*
- Publication spéciale 800-37 du NIST - *Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Lifecycle Approach* (version finale - 2009)
- Publication spéciale 800-39 du NIST - *Managing Risk from Information Systems*

Références internationales

- ISO 31000:2009 (version définitive) - Gestion du risque - Principes et lignes directrices
- ISO/IEC 27001:2005 - Technologies de l'information - Techniques de sécurité - Système de gestion de la sécurité de l'information - Exigences
- ISO/IEC 27002:2005 - Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information

Annexe C - Exemple de registre des risques pour la sécurité

Portée : (au niveau du ministère ou détermination des programmes ou des ressources visés par l'évaluation des risques ou le registre des risques)

		Évaluation des risques		Traitement des risques		Mise en œuvre	Surveillance	
Identificateur	Responsable des risques/ autorité		Décision					Rapport/

Identificateur des risques (unique)	Énoncé des risques	Harmonisation à l'AAP	Autorité d'approbation de la traitement des risques	Intervenants	Détermination des risques	Analyse des risques	Évaluation des risques	Décision concernant la traitement des risques	Objectifs de contrôle	Contrôles	Indicateur de rendement	Analyse des écarts	Priorité	Échéancier/jalons	Affectation des ressources	Transition	Sources de données	Fréquence	Cible	Mise à jour
Un identificateur unique des risques. La référence peut être utile pour faire un renvoi entre le RRS et les autres registres ou journaux portant sur les risques ou le PRM.	Brève description des ressources affectées, de l'importance des ressources pour le ministère et de l'incidence sur les activités, si les risques se matérialisaient. Phrases structurées qui traduisent clairement les deux composantes de risque (probabilité et incidence) relativement aux activités ou aux ressources du ministère dans l'environnement actuel.	Préciser l'AP, la SAP ou la SSAP touchée par les risques.	Nom ou titre des personnes chargées de gérer les risques	Nom et titre des organismes touchés par les risques	Source des risques (p. ex., interne ou externe); conséquence éventuelle (p. ex., compromission de la confidentialité, l'intégrité, la disponibilité, la sécurité des personnes, le manque de conformité); la cause fondamentale (p. ex., condition fondamentale qui cause les risques et la vulnérabilité). Lorsqu'un risque provient uniquement d'une obligation législative, politique ou contractuelle, il est possible d'indiquer qu'il s'agit d'un « risque pour la conformité » en faisant référence à la législation, à la politique, au règlement ou au marché applicable.	Probabilité et incidence des risques (fondé sur une méthodologie d'évaluation des risques et doit comprendre une cotation globale des risques, p. ex., élevée, modérée, faible).	Détermination du caractère acceptable ou inacceptable d'un risque et fondement de la décision.	Décision concernant la traitement des risques inacceptables (éviter, réduire, transférer).	Énoncé d'intention de gérer les risques déterminés. Dans certains cas, plusieurs objectifs de contrôle peuvent être établis pour un risque donné.	Description des contrôles de sécurité choisis pour atteindre les objectifs de contrôle énoncés. Plusieurs contrôles peuvent être nécessaires pour atteindre un objectif de contrôle donné.	Moyens qualitatifs ou quantitatifs de mesurer l'atteinte de l'objectif de contrôle par le contrôle (entre un et trois).	Détermination des contrôles qui n'ont pas encore été mis en œuvre, qui doivent être améliorés ou pour lesquels aucun indicateur de rendement n'a été établi.	Priorité en matière de mise en œuvre de contrôles et d'indicateurs de rendement supplémentaires (fondé sur une analyse des coûts, des avantages, de l'harmonisation aux priorités ministérielles, etc.).	Échéancier d'établissement, de mise en œuvre ou d'amélioration des contrôles existants ou d'établissement d'indicateurs de rendement (y compris l'ordre des activités, les dépendances ou les autres considérations en matière d'harmonisation, le cas échéant, et la date butoir d'atteinte des objectifs précisés).	Ressources de gestion pour mettre en œuvre les contrôles et pour surveiller l'efficacité.	Risques et contrôles qui demeurent pendant la période de transition, notamment des contrôles compensatoires qui doivent être mis en œuvre durant la période précédant la mise en œuvre intégrale des contrôles choisis.	Source de saisie, de création ou de disponibilité régulière de données sur le rendement.	La fréquence de collecte des données sur le rendement pour établir des rapports d'étape (p. ex., annuellement, semestriellement).	Niveau de rendement que vise le ministère dans un délai donné. Les cibles doivent être quantifiables.	Renseignements descriptifs supplémentaires pouvant être utiles, notamment : • des références à d'autres plans ou documents où on peut trouver des renseignements de base ou des détails supplémentaires (p. ex., évaluations des risques détaillées, profil des risques ministériels, etc.); • des engagements « en cascade » dans les ententes de gestion du rendement, les plans de travail, etc.

Notes en bas de page

Note en bas de page ftn1

Les exigences en matière d'élaboration d'un PSM s'appliquent aux administrateurs généraux de tous les ministères au sens des annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques* (LGFP), sauf si des lois, des règlements ou des décrets les en excluent, comme le précise la section 2 de la Politique sur la sécurité du gouvernement.

Renvoi à la référence de la note en bas de page [1]

Note en bas de page ftn2

Directive sur la gestion de la sécurité ministérielle, section 1.2, Secrétariat du Conseil du Trésor.

Renvoi à la référence de la note en bas de page [2]

Note en bas de page ftn3

Politique sur la sécurité du gouvernement, section 3.5, Secrétariat du Conseil du Trésor.

Renvoi à la référence de la note en bas de page [3]

Note en bas de page ftn4

Dix-septième rapport annuel au Premier ministre sur la fonction publique du Canada

Renvoi à la référence de la note en bas de page [4]

Note en bas de page ftn5

Cadre de gestion intégrée des risques, Secrétariat du Conseil du Trésor.

Renvoi à la référence de la note en bas de page [5]

Note en bas de page ftn6

Le Cadre de responsabilisation de gestion est structuré en dix éléments clés qui, collectivement, définissent la « gestion » et établissent les attentes en matière de bonne gestion d'un ministère ou d'un organisme.

Renvoi à la référence de la note en bas de page [6]

Note en bas de page ftn7

ISO/IEC 27001:2005, Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences, section 4.3.

Renvoi à la référence de la note en bas de page [7]

Note en bas de page ftn8

Adapté de la publication spéciale 800-39 du NIST, *Integrated Enterprise-Wide Risk Management: Organization, Mission and Information System View*(publication prévue en 2010).

Renvoi à la référence de la note en bas de page [8]

Note en bas de page ftn9

Politique sur la structure de gestion, des ressources et des résultats.

Renvoi à la référence de la note en bas de page [9]

Note en bas de page ftn10

Les ressources s'entendent des renseignements, des biens, des services et des personnes dont les ministères dépendent pour mener à bien leur mission générale.

Renvoi à la référence de la note en bas de page [10]

Note en bas de page ftn11

Méthodologie harmonisée d'évaluation des menaces et des risques, publiée le 23 octobre 2007 sous l'autorité du chef du Centre de la sécurité des télécommunications Canada (CSTC) et du commissaire de la Gendarmerie royale du Canada (GRC).

Renvoi à la référence de la note en bas de page [11]

Note en bas de page ftn12

Les ressources s'entendent des renseignements, des biens, des services et des personnes dont les ministères dépendent pour mener à bien leur mission générale.

Renvoi à la référence de la note en bas de page [12]

Note en bas de page ftn13

Consignes aux ministères sur la préparation d'une structure de gestion, des ressources et des résultats, section 7.2.3, Secrétariat du Conseil du Trésor.

Renvoi à la référence de la note en bas de page [13]

Note en bas de page ftn14

Le PSM n'établit que les ressources de haut niveau permettant la prise de décisions et la priorisation. Des renseignements plus détaillés concernant les projets, les ressources et l'échéancier requis pour mettre en œuvre les contrôles de sécurité et pour surveiller leur efficacité sont fournis dans les plans de travail.

Renvoi à la référence de la note en bas de page [14]

Note en bas de page ftn15

Directive sur la gestion de la sécurité ministérielle, Secrétariat du Conseil du Trésor.

Renvoi à la référence de la note en bas de page [15]

Note en bas de page ftn16

Cadre de gestion intégrée du risque, Secrétariat du Conseil du Trésor.

Renvoi à la référence de la note en bas de page [16]