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

Guide de vérification de la sécurité

Mars 2004

Canada

Remerciements

Le Comité de production du Guide de vérification de la sécurité aimerait exprimer ses remerciements, notamment aux ministères et organismes fédéraux suivants, qui ont fourni des documents, de l'information et de l'expertise pour produire ce guide :

- Travaux publics et Services gouvernementaux Canada
- Santé Canada
- Gendarmerie royale du Canada
- Conseils et Vérification Canada
- Centre de la sécurité des télécommunications
- Bureau du vérificateur général du Canada
- Conseil national de recherches du Canada
- Ressources naturelles Canada
- Défense nationale
- Affaires étrangères Canada
- Affaires indiennes et du Nord canadien
- Transports Canada
- Développement social Canada
- Secrétariat du Conseil du Trésor du Canada

Table des matières

Guide de vérification de la sécurité

PRÉFACE

Le présent guide a été préparé par le Centre d'excellence en vérification interne, Bureau du contrôleur général, Secrétariat du Conseil du Trésor du Canada. Il constitue une mise à jour du *Guide de vérification de la sécurité* rédigé par le groupe Évaluation, vérification et examen du Secrétariat du Conseil du Trésor à la suite des modifications apportées à la *Politique du gouvernement sur la sécurité (PGS)* en juin 1994.

Ce nouveau guide tient compte des dernières modifications à la PGS qui sont entrées en vigueur en février 2002.

Le Centre d'excellence en vérification interne (CEVI) a rédigé ce *Guide de vérification de la sécurité* dans le but d'aider la collectivité de la vérification interne à concevoir et à échanger des outils de vérification interne.

Le présent document a été préparé avec l'aide d'un comité consultatif composé de membres des collectivités de la vérification interne et de la gestion fonctionnelle provenant d'un échantillon représentatif de ministères et d'organismes, ainsi que de représentants du Bureau du vérificateur général, de responsables de l'approbation des politiques du Secrétariat du Conseil du Trésor du Canada ainsi que de représentants du CEVI. Il s'agit donc d'un document faisant autorité.

Le CEVI invite les personnes et les organisations à envoyer des commentaires par écrit au sujet du présent guide à l'attention du directeur, Politiques et projets spéciaux, Centre d'excellence en vérification interne.

INTRODUCTION

Contexte

Le précédent *Guide de vérification de la sécurité* (GVS) présentait des directives permettant à la collectivité de la vérification de réaliser des vérifications et des examens de la conformité à la *Politique du gouvernement sur la sécurité* (PGS) et aux normes opérationnelles de sécurité connexes. En février 2002, le Conseil du Trésor a approuvé de nouvelles modifications au Guide afin de tenir compte des récents changements survenus dans la situation politique et économique au Canada et dans le monde. Il fallait également mettre à jour les normes opérationnelles de sécurité. Par suite des modifications apportées à la Politique et aux normes, il est aussi devenu nécessaire de mettre à jour le Guide. La présente version tient compte de ces modifications.

Le Guide ne comprend pas le *Guide de vérification de la sécurité des technologies de l'information* (STI) publié par le Secrétariat du Conseil du Trésor du Canada (le Secrétariat) en septembre 1995, lequel est en cours de révision. À l'origine, le Guide de vérification de la STI avait été conçu comme un document distinct et autonome pouvant être intégré éventuellement au GVS.

But

Le principal objectif du GVS consiste à donner des directives à la collectivité de la vérification interne afin de l'aider à réaliser des vérifications sur l'application de la PGS et sur la conformité à cette politique et aux normes opérationnelles de sécurité. Le GVS a aussi pour objectif d'aider les agents et les gestionnaires de la sécurité à effectuer des autoévaluations et des examens du programme de sécurité de leur ministère.

Le GVS est de nature à faciliter la vérification ou l'examen de certaines parties d'un programme de sécurité en fonction de l'évaluation des risques.

Bien que le GVS vise principalement à faciliter l'évaluation de l'application de la PGS et de la conformité à cette politique et aux normes opérationnelles de sécurité, il peut également être utilisé comme point de départ pour déterminer les possibilités de mieux coordonner le programme de sécurité et de le mettre en œuvre de façon plus efficiente et efficace. Les utilisateurs auraient toutefois avantage à examiner d'autres critères pour ces aspects de l'évaluation des programmes de sécurité.

Avertissement relatif à l'utilisation prévue du GVS

Le présent document n'a pas été conçu pour encadrer de façon rigide la réalisation de vérifications, d'autoévaluations et d'examens du programme de sécurité d'un ministère. Il s'agit

plutôt d'un outil de référence qui doit être utilisé avec discernement et en tenant compte du type d'examen à réaliser. Les procédés de vérification *proposés* dans le présent document ne doivent pas être considérés comme une recette. Ils proposent une démarche permettant de déterminer si un critère de vérification en particulier a été respecté. Ensemble, les conclusions de vérification selon les critères établis devraient permettre au vérificateur de formuler une opinion quant à l'atteinte de l'objectif de gestion visé, tel qu'il est énoncé dans le présent document.

Les normes professionnelles des vérificateurs les obligent à tenir dûment compte des risques que comporte la formulation d'une opinion erronée. Il est donc fortement recommandé de recourir à des spécialistes de la sécurité qui peuvent effectuer des essais ou des évaluations techniques et donner des avis, notamment sur la conception des essais et des procédures, la formulation de questions ou de secteurs d'intérêt, l'interprétation des résultats ou des observations, ou encore, l'encadrement des recommandations.

Un vérificateur peut s'appuyer sur le point de vue d'un spécialiste mais cela ne signifie pas qu'il se décharge de la responsabilité de l'opinion de vérification. Cette opinion demeure la responsabilité du vérificateur. Par ailleurs, celui-ci doit justifier sa décision d'avoir recours à un spécialiste. Pour plus de renseignements, veuillez consulter les normes professionnelles en matière de vérification.

Champ d'application

Le GVS s'adresse à toutes les organisations énumérées à l'annexe I, l'annexe I.1 et l'annexe II de la *Loi sur la gestion des finances publiques* (LGFP).

Le Guide s'applique également :

a) à toute commission instituée en tant que ministère aux fins de la LGFP par décret du gouverneur en conseil, en application de la *Loi sur les enquêtes*;

b) aux Forces canadiennes, à la condition que le terme « employé » utilisé dans le GVS ne s'applique pas aux membres des Forces canadiennes.

Certains organismes et sociétés d'État peuvent conclure des ententes avec le Secrétariat afin d'adopter les exigences du GVS et de les mettre en œuvre dans leurs organisations.

Le GVS traite de la PGS et des normes opérationnelles de sécurité. Il ne donne pas de directives détaillées sur la vérification de la conformité au plan technique. À ce sujet, veuillez consulter l'organisme conseil en matière de sécurité.

Afin d'obtenir de l'aide pour interpréter la PGS, des normes opérationnelles de sécurité ou du GVS, veuillez communiquer avec :

- la Division des politiques de l'information, des communications et de la sécurité du Secrétariat pour l'interprétation de la politique; ou
- le Centre d'excellence en vérification interne, Bureau du contrôleur général du Secrétariat.

Afin d'obtenir de l'aide pour vérifier ou examiner les activités de sécurité relatives aux technologies de l'information (STI) d'un ministère, veuillez consulter le *Guide de vérification de la sécurité des technologies de l'information.*

Organisation du GVS

La matière du GVS est présentée comme suit :

Le *chapitre 1 (Questions de gestion)* donne une vue d'ensemble du rapport entre la PGS et les questions de gestion dans leur ensemble. Essentiellement, ce chapitre décrit le cadre général de contrôle de la sécurité qui doit être mis en œuvre.

Le *chapitre 2* (*Méthode de vérification)* établit les procédés à utiliser pour vérifier la mise en œuvre de la PGS et des normes opérationnelles ainsi que la conformité à celles-ci. Les objectifs, critères et procédés à utiliser dans le cadre des vérifications ou des examens sont présentés dans cette partie du Guide. Les objectifs de gestion décrits dans ce chapitre énoncent les exigences avec plus de précision, de manière à harmoniser le cadre de contrôle de gestion mis en œuvre par la direction avec la PGS et les normes opérationnelles de sécurité connexes.

CHAPITRE 1—QUESTIONS DE GESTION

Le cadre de la sécurité

1.1 Cadre de responsabilisation

L'un des principes fondamentaux de la *Politique du gouvernement sur la sécurité* (PGS) est que les administrateurs généraux ont la responsabilité d'assurer la sécurité des biens du gouvernement et la protection des employés dans leurs ministères. Pour ce faire, ils doivent mettre en œuvre un programme de sécurité ministériel qui énonce clairement les responsabilités de tous les employés. La PGS et les normes opérationnelles de sécurité établissent les mesures de protection obligatoires ou discrétionnaires visant à assurer la continuité des services. Les mesures de protection discrétionnaires doivent être mises en œuvre lorsqu'une évaluation de la menace et des risques le justifie, ce qui constitue une preuve de diligence raisonnable de la part des administrateurs généraux et des agents de sécurité de leur ministère.

Pour que les ministères mettent en œuvre des programmes de sécurité qui soient efficients et efficaces, ils doivent être en mesure de les administrer dans le cadre de leur propre mandat et selon leurs priorités, leur budget, ainsi que leur culture organisationnelle et le contexte où ils évoluent. La politique tient compte de ces facteurs car elle définit les exigences générales visant à assurer un certain niveau de sécurité dans un ministère et dans l'ensemble du gouvernement. Du même coup, elle laisse aux ministères la latitude qui leur est nécessaire pour réagir à leurs contraintes et aux autres conditions qui leur sont propres en permettant d'adopter une approche de gestion du risque lorsque ce niveau de sécurité est atteint.

1.2 Le modèle de sécurité du gouvernement

Dans le contexte de l'administration fédérale, la sécurité s'entend de l'application de mesures de protection visant à réduire les risques de blessures découlant de dangers en milieu de travail ou d'actes de violence; à préserver la confidentialité, l'intégrité et l'accessibilité de l'information; à protéger la valeur et la disponibilité des biens afin d'assurer la permanence des services publics.

Dans la PGS et les normes opérationnelles, on trouve la description d'un modèle de programme de sécurité ministériel qui comporte les exigences suivantes :

- Les ministères doivent nommer un agent de sécurité du ministère (ASM) chargé d'élaborer et de diriger un programme de sécurité. Étant donné l'importance de ce poste, il faudrait que l'agent ait suffisamment d'expérience en matière de sécurité et qu'il occupe un poste stratégique au sein de l'organisation, de manière à pouvoir fournir des conseils et une orientation stratégique à la haute direction (article 10.1 de la PGS).
- Les ministères doivent prendre des mesures appropriées lorsqu'ils échangent des renseignements et d'autres biens du gouvernement du Canada avec d'autres gouvernements

(étrangers, provinciaux, territoriaux et municipaux) et avec des organisations internationales, des établissements d'enseignement et des organismes du secteur privé (article 10.2 de la PGS).

- Lorsque certaines exigences de la PGS se révèlent difficiles à appliquer dans des endroits particuliers à l'extérieur du Canada, des dispositions spéciales peuvent être formulées de concert avec le ministère des Affaires étrangères et du Commerce international (article 10.3 de la PGS).
- L'autorité contractante doit confirmer le contrôle de sécurité des entrepreneurs et la protection des biens du gouvernement, y compris les systèmes de TI, et énoncer les exigences en matière de sécurité dans les modalités de tout dossier contractuel (article 10.4 de la PGS).
- Les ministères doivent confirmer que les responsables de la sécurité reçoivent une formation appropriée, qu'un programme de sensibilisation à la sécurité est en place et que les personnes sont informées des privilèges d'accès et des interdictions avant d'entrer en fonction (article 10.5 de la PGS).
- Les ministères doivent protéger les renseignements en tenant compte des intérêts de confidentialité définis dans la *Loi sur l'accès à l'information* et dans la *Loi sur la protection des renseignements personnels.* Ils doivent également protéger les autres biens au regard de leur disponibilité, de leur intégrité et de leur valeur (article 10.6 de la PGS).
- Les ministères doivent évaluer régulièrement les menaces et les risques afin de déterminer les mesures de protection requises. Ils doivent surveiller continuellement l'évolution du contexte de la menace et faire les ajustements nécessaires au maintien d'un niveau de risque acceptable (article 10.7 de la PGS).
- Les ministères doivent limiter l'accès aux renseignements classifiés et protégés aux seules personnes qui ont besoin de les connaître et qui ont la cote de sécurité appropriée. L'accès aux autres biens ne doit pas nuire aux mesures de protection visant à assurer la disponibilité, l'intégrité et la valeur de ces biens (article 10.8 de la PGS).
- Les vérifications de sécurité doivent confirmer que les personnes ayant accès aux renseignements et aux autres biens du gouvernement sont fiables et dignes de confiance (article 10.9 de la PGS).
- Les ministères sont responsables de la santé et de la sécurité au travail des employés en vertu de la partie II du *Code canadien du travail* et des politiques du Conseil du Trésor (article 10.10 de la PGS).
- Les ministères doivent confirmer que la sécurité matérielle est pleinement intégrée à l'aménagement et à la conception des installations, et ils doivent prendre des mesures afin de retarder et d'éviter l'accès non autorisé aux biens du gouvernement et afin de protéger les employés de la violence (article 10.11 de la PGS).

- Les systèmes d'information doivent être protégés contre l'évolution rapide des menaces pouvant nuire à la confidentialité, à l'intégrité, à la disponibilité, à l'utilisation prévue et à la valeur de ces systèmes (article 10.12 de la PGS).[1]
- Les ministères doivent concevoir des plans et des procédures en vue de resserrer les mesures de sécurité en cas d'urgence ou de menace accrue (article 10.13 de la PGS).
- Les ministères doivent établir un programme de planification de la poursuite des activités dans le but d'assurer en permanence la disponibilité des services et des biens essentiels (article 10.14 de la PGS).
- Les ministères doivent élaborer des procédures en vue de signaler les incidents de sécurité, de faire enquête et de prendre des mesures correctives (article 10.15 de la PGS).
- Les ministères sont tenus d'imposer des sanctions à la suite d'incidents de sécurité lorsque, de l'avis de l'administrateur général, il y a eu inconduite ou négligence (article 10.16 de la PGS).
- Les ministères sont tenus d'effectuer une surveillance active et des vérifications internes de leur programme de sécurité (article 11 de la PGS).

Puisque l'efficacité du programme de sécurité dépend de la mise en œuvre intégrée de tous ces éléments, un ministère doit coordonner la planification, la gestion et l'administration de son programme de sécurité lorsque les éléments de ce programme relèvent de différentes unités organisationnelles.

1.3 Rôles et responsabilités

Administrateur général

Les administrateurs généraux sont tenus de protéger les employés et les biens qui relèvent de leur secteur de responsabilité et de mettre en œuvre la PGS.[2]

Agent de sécurité du ministère (ASM)

Les ministères doivent nommer un agent de sécurité du ministère (ASM) chargé d'élaborer et de diriger un programme de sécurité afin d'assurer la coordination des fonctions de la politique et la mise en œuvre de ses exigences.[3] Ces fonctions consistent notamment à garantir que les exigences de sécurité mentionnées dans le modèle de programme de sécurité ministériel décrit à la section 1.2 ci-dessus sont effectivement appliquées et respectées.

---

1 La sécurité des technologies de l'information (TI) comprend la prévention, la détection, l'intervention, ainsi que les contrôles et les stratégies de récupération. Comme il a été mentionné précédemment, la sécurité des TI fait l'objet d'un guide de vérification distinct.

2 Article 6 de la PGS.

3 Article 10.2 de la PGS.

Ministères et organismes ayant des responsabilités en matière de sécurité

Les ministères et organismes gouvernementaux ci-après sont chargés d'un ou plusieurs aspects de la sécurité :[4]

- Conseil du Trésor du Canada
- Secrétariat du Conseil du Trésor du Canada (le Secrétariat)
- Comités chargés de fournir des conseils et de l'orientation au Secrétariat
- Service canadien du renseignement de sécurité
- Centre de la sécurité des télécommunications
- Ministère des Affaires étrangères et du Commerce international
- Archives nationales du Canada
- Ministère de la Défense nationale
- Protection des infrastructures essentielles et protection civile (relevant de Sécurité publique et protection civile Canada)
- Bureau du Conseil privé
- Travaux publics et Services gouvernementaux Canada
- Gendarmerie royale du Canada
- Transports Canada

1.4 Le rôle essentiel de la vérification interne

En matière de sécurité, le gouvernement du Canada préconise une approche fondée sur la gestion des risques plutôt que sur les règles. Autrefois, on estimait généralement que l'observance stricte de la PGS était suffisante en soi pour assurer un niveau de sécurité adéquat. Aujourd'hui, on insiste sur le fait que les responsables de la sécurité doivent vérifier l'efficacité des mesures de sécurité en tenant compte des risques particuliers auxquels leur ministère est exposé.

À cette fin, diverses activités de supervision sont menées afin de vérifier l'efficacité des pratiques de sécurité d'un ministère, par exemple :

- évaluations de la menace et des risques (EMR);
- détection des intrusions;
- évaluations de la vulnérabilité technique;
- supervision des gestionnaires à tous les échelons;
- vérification ponctuelle et inspection par des spécialistes de la sécurité;

[4] Des renseignements supplémentaires sont disponibles à l'annexe A (Responsabilités) de la PGS.

- enquêtes sur les incidents de sécurité présumés;
- surveillance active des activités des utilisateurs;
- vérifications techniques des activités des utilisateurs.

Chacune de ces activités contribue à faire en sorte que le personnel, les installations et les autres biens d'un ministère sont bien protégés, compte tenu des risques de sécurité particuliers correspondant à ses activités.

Outre la gestion des risques effectuée par les personnes directement responsables de la supervision de la sécurité, la direction, par l'entremise d'un régime intégré de gestion des risques, et la vérification interne, dans le cadre de ses activités de planification fondées sur les risques, surveillent et évaluent constamment l'exposition aux risques, y compris les risques pour la sécurité du ministère.

Aux termes de la PGS, les ministères sont tenus d'effectuer des vérifications internes de la sécurité (article 11 de la PGS). Les risques et les besoins du ministère détermineront les aspects particuliers à examiner (cycle de vie complet ou aspect d'un domaine de sécurité, menace ou vulnérabilité).

Les coûts liés aux vérifications ou à toute forme d'examen indépendant s'ajoutent aux ressources consacrées à la sécurité par la direction. La collectivité de la vérification interne doit prendre en compte les avantages de ces activités par rapport aux coûts, y compris les coûts de renonciation liés aux activités de sécurité et aux activités permanentes de supervision.

1.5 Interprétation des résultats de la vérification interne

Il faut se rendre compte que les solutions aux problèmes de sécurité ne sont pas toujours simples. La sécurité est une discipline complexe et l'interprétation adéquate des résultats des essais et des procédés de vérification exige souvent des connaissances et une expérience considérables. Par ailleurs, la pertinence d'un programme de sécurité dans un ministère à un moment particulier doit être évaluée dans le contexte des programmes et des activités de ce ministère et des conditions dans lesquelles il évolue. C'est pourquoi il est fortement recommandé de consulter un spécialiste de la sécurité. Dans les meilleurs cas, la vérification de sécurité est une activité de collaboration entre un spécialiste de la sécurité et un spécialiste de la vérification, ce dernier assumant l'entière responsabilité de la vérification.

1.6 Rapports de vérification et dossiers de travail

La matière du GVS n'est pas classifiée. Par contre, les rapports de vérification, les dossiers de travail connexes et la documentation fournie par la direction contiennent vraisemblablement des renseignements de nature délicate sur les pratiques et les arrangements de sécurité, les lacunes

afférentes, les risques que comporte la protection des biens ministériels de valeur, ou d'autres exemples de non-conformité à la PGS. Les vérificateurs doivent prendre des précautions afin de s'assurer que leurs courriels, leurs documents de travail et leurs rapports sont protégés et classifiés comme il se doit. L'ASM et le coordonnateur de l'AIPRP peuvent être consultés à cet égard.

CHAPITRE 2—MÉTHODES DE VÉRIFICATION

Introduction

On trouve dans le présent chapitre les objectifs, critères et procédures que les vérificateurs doivent utiliser pour faire des vérifications de sécurité. Ces éléments prennent en compte les exigences de la nouvelle PGS et les normes opérationnelles de sécurité qui s'appliquent à la mise en œuvre et au maintien d'un programme de sécurité efficace, et ils intègrent des pratiques exemplaires tirées de vérifications antérieures. Les vérificateurs peuvent ajouter, modifier ou éliminer des objectifs, critères et procédés de vérification afin d'adapter le processus aux besoins de leur organisation, compte tenu des particularités du contexte de la menace et des risques ou des vulnérabilités propres aux activités.

Objectifs

Les objectifs de vérification suivants sont regroupés en fonction de la nouvelle PGS et des normes opérationnelles connexes. Tout comme les critères, les objectifs établis doivent être atteints pour que le programme de sécurité soit efficace.

Tous les objectifs ont été élaborés à partir des exigences de la PGS. Certains grands titres, comme « Organisation de la sécurité » et « Administration de la sécurité » contiennent des objectifs qui figurent à plusieurs reprises dans la PGS. D'autres, tels que « Accès restreint » et « Sécurité des employés », se concentrent sur un domaine particulier de la PGS. Nous avons ajouté entre parenthèses l'article de la PGS correspondant à chaque objectif pour aider les vérificateurs à s'y référer.

Programme de sécurité

1. Le ministère a adopté une conception de programme de sécurité qui assure la coordination de toutes les fonctions de la politique et qui respecte les exigences de sécurité de base énoncées dans la PGS (article 10.1 de la PGS).
2. Des évaluations de la menace et des risques (EMR) sont réalisées et les recommandations sont mises en application conformément à la PGS (article 10.7 de la PGS).
3. Le programme de sécurité est de nature à soutenir la gestion des situations d'urgence (p. ex. incendies, alertes à la bombe, matières dangereuses, pannes d'électricité, évacuations, urgences civiles) (article 10.13 de la PGS).
4. L'application du programme de sécurité à l'extérieur du Canada tient dûment compte des risques déterminés et revus par le ministère des Affaires étrangères et du Commerce international (article 10.3 de la PGS).

5. Le ministère effectue la surveillance active de son programme de sécurité (article 11 de la PGS).

Organisation de la sécurité

6. Le mandat et l'expérience de l'ASM correspondent à l'ampleur et à la complexité des activités du ministère (article 10.1 de la PGS).
7. Le ministère a établi une structure de gestion de la sécurité qui englobe la responsabilité générale de la gestion de son programme de sécurité, y compris la sécurité administrative et matérielle, la sécurité des technologies de l'information et la sécurité du personnel, de même que la sécurité de la gestion des mesures d'urgence et des marchés. La structure établie répond aux besoins du ministère (articles 10.1, 10.7 et 11 de la PGS).

Administration de la sécurité

8. Le programme de sécurité a été intégré au processus général de planification du ministère (article 10.1 de la PGS).
9. Les spécialistes de la sécurité reçoivent la formation dont ils ont besoin : des séances de sensibilisation sont données régulièrement afin de renseigner les employés et de leur rappeler leurs responsabilités, les enjeux et les préoccupations en matière de sécurité; des séances d'information sont données au sujet des responsabilités rattachées aux différentes cotes de sécurité (article 10.5 de la PGS).
10. Les renseignements et les biens de nature délicate reçoivent la cote CLASSIFIÉ ou PROTÉGÉ, conformément à la PGS et aux normes opérationnelles de sécurité (au regard de leur confidentialité, de leur intégrité, de leur disponibilité et de leur valeur) et les mentions de sensibilité sont déclassées ou éliminées lorsque la nature des renseignements ou des biens devient moins délicate ou cesse de l'être (article 10.6 de la PGS).
11. Les atteintes et infractions à la sécurité et les autres incidents de sécurité font l'objet d'une enquête. Des mesures visant à réduire les pertes et des mesures administratives, correctives ou disciplinaires sont prises (articles 10.15 et 10.16 de la PGS).

Accès restreint

12. L'accès aux renseignements et aux biens de nature délicate est restreint aux personnes qui ont besoin de les connaître et qui détiennent une approbation officielle et l'autorisation de sécurité requise (article 10.8 de la PGS).
13. Aucune personne ne détient le contrôle unique de tous les aspects d'un processus ou d'un système (en particulier une mesure de protection) (article 10.8 de la PGS).

Échange de renseignements et d'autres biens

14. Des mesures de protection adéquates sont appliquées aux renseignements de nature délicate qui sont échangés avec des sources officielles de l'extérieur du ministère, notamment les gouvernements étrangers, provinciaux, territoriaux et municipaux, les établissements d'enseignement et les organismes du secteur privé (article 10.2 de la PGS).
15. Des processus et des ententes sont en vigueur afin d'assurer la protection des renseignements échangés avec d'autres sources officielles, conformément aux politiques et aux normes de sécurité des parties concernées (article 10.2 de la PGS).

Sécurité matérielle

16. Une évaluation de sécurité adéquate est menée avant de choisir et d'aménager des installations, dans le but de réduire ou d'éliminer les menaces et les risques pour les renseignements et les biens de nature délicate et pour les employés dans ces installations (article 10.11 de la PGS).
17. Des mesures de sécurité matérielle ont été prises afin d'assurer la protection des renseignements et des biens de nature délicate ainsi que la sûreté et la sécurité des employés dans les installations (article 10.11 de la PGS).
18. Des zones de sécurité matérielle de plus en plus restrictives sont établies et maintenues, ainsi que des mécanismes permettant de contrôler l'accès aux renseignements et aux biens de nature délicate (article 10.11 de la PGS).
19. Les mesures de protection matérielles sont constamment examinées afin de tenir compte de l'évolution du contexte de la menace et de tirer avantage des économies qui peuvent être réalisées grâce aux nouvelles technologies (article 10.11 de la PGS).

Sécurité du personnel

20. Toutes les personnes qui ont accès aux biens du gouvernement (à l'exception des personnes nommées par le gouverneur en conseil) doivent avoir à tout le moins une cote de fiabilité (article 10.9 de la PGS).
21. Les enquêtes de sécurité sur les personnes sont menées conformément à la PGS et à la Norme sur la sécurité du personnel (article 10.9 de la PGS).
22. Lorsqu'une personne quitte son emploi, des mesures doivent être prises afin de réduire ou d'éliminer tout risque pour les renseignements, les systèmes et les biens de nature délicate ou pour le personnel du ministère (implicite dans l'article 10.9 de la PGS).

Protection des employés

23. Une évaluation de la menace et des risques (EMR) a été menée afin de déterminer les situations où les employés sont menacés de violence en raison de leurs fonctions ou à cause des situations auxquelles ils sont exposés (article 10.10 de la PGS).
24. Des mécanismes sont en vigueur afin d'identifier, de protéger et d'appuyer les employés (et leurs familles, le cas échéant) menacés de violence ou travaillant dans des secteurs à risque élevé (article 10.10 de la PGS).

Sécurité et gestion des cas d'urgence

25. Les gestionnaires des installations du ministère ont pris les mesures nécessaires pour assurer la protection des renseignements et des biens de nature délicate et celle des employés dans tous les cas d'urgence et de menace accrue (article 10.14 de la PGS).
26. Des plans à l'échelle du ministère sont élaborés afin d'assurer la poursuite des activités, des services et des biens essentiels après une interruption imprévue (article 10.14 de la PGS).

Sécurité et gestion des marchés

27. Les exigences de sécurité relatives à la protection des renseignements, des biens et du personnel sont respectées dans le processus de passation des marchés (article 10.4 de la PGS).

PROGRAMME DE SÉCURITÉ

Objectif n° 1

Le ministère a adopté un programme de sécurité qui assure la coordination de toutes les fonctions de la politique et qui est conforme aux exigences de sécurité de base énoncées dans la PGS (article 10.1 de la PGS).

Critère n° 1.1 Un programme de sécurité ministériel et des documents connexes (normes, directives, lignes directrices et procédures) ont été élaborés et diffusés et ils sont gardés à jour.

Procédés de vérification

1.1.1 Vérifier la pertinence et l'exactitude de la documentation.

1.1.2 Confirmer la conformité du programme de sécurité ministériel et des normes connexes à la PGS en vigueur.

1.1.3 Confirmer que le programme et les normes de sécurité sont regroupés dans un manuel sur la sécurité ou qu'ils sont répartis dans d'autres manuels ou dossiers. Recenser ces manuels ou dossiers.

1.1.4 Confirmer que l'information est facile à obtenir (en direct ou sur papier) dans tout le ministère.

1.1.5 Confirmer que les mises à jour sont annoncées et distribuées et que tous les employés peuvent les obtenir en temps voulu.

1.1.6 Demander aux gestionnaires de vérifier s'ils ont un exemplaire du programme et des procédures et déterminer s'ils en connaissent bien le contenu.

1.1.7 Demander à des employés pris au hasard de vous donner accès au programme et aux normes de sécurité du ministère.

Critère n° 1.2 Les directives de sécurité sont adaptées à la situation du ministère.

Procédés de vérification

1.2.1 Confirmer que les objectifs énoncés dans le programme de sécurité du ministère et dans les documents connexes sont conformes aux objectifs, au mandat, à la mission et au profil de risque du ministère.

Critère n^{o} 1.3 Les directives de sécurité sont conformes à la PGS et aux documents connexes.

Procédés de vérification

1.3.1 Analyser le programme de sécurité du ministère en le comparant directement à la PGS et aux normes opérationnelles de sécurité.

1.3.2 Confirmer que les normes, les directives, les ordonnances et les procédures de sécurité sont conformes aux exigences obligatoires de la PGS.

Critère n^{o} 1.4 Les documents gouvernementaux et ministériels pertinents sont mis à la disposition des spécialistes de la sécurité.

Procédés de vérification

1.4.1 Demander aux principaux agents de sécurité (l'agent de sécurité ministériel, ou ASM, et les responsables de la sécurité ministérielle, de la sécurité des TI, du plan de poursuite des activités et du programme de santé et de sécurité au travail) de vérifier s'ils ont à leur disposition des exemplaires des normes opérationnelles de sécurité du gouvernement et de la documentation technique disponible auprès du Secrétariat et des autres ministères qui jouent un rôle prépondérant en matière de sécurité, y compris les normes de sécurité technique, les spécifications, les pratiques exemplaires et les lignes directrices conçues par ces ministères.

Critère n^{o} 1.5 Les personnes employées par le ministère ou faisant affaire avec lui sont assujetties à la politique ministérielle en matière de sécurité et aux documents connexes.

Procédés de vérification

1.5.1 Confirmer que les personnes employées par le ministère ou faisant affaire avec lui sont désignées dans la politique de sécurité du ministère comme étant tenues de suivre les directives de cette politique pour avoir accès aux renseignements de nature délicate ou aux biens de valeur.

1.5.2 Confirmer que ces personnes ont accès à la politique en matière de sécurité et qu'elles ont reçu l'information dont elles ont besoin pour s'acquitter de leurs responsabilités.

1.5.3 Confirmer que ces personnes ont reconnu avoir compris et accepté leurs obligations en matière de sécurité en signant une déclaration, au besoin.

1.5.4 Confirmer que ces personnes ont suivi les cours de sécurité obligatoires.

Critère n^{o} 1.6 La responsabilité générale de la sécurité relève de l'administrateur général

Procédés de vérification

1.6.1 Confirmer qu'il est clairement établi que l'administrateur général (ou l'équivalent) a la responsabilité générale de protéger les employés et les biens qui relèvent de son domaine de responsabilité et de mettre en œuvre un programme de sécurité ministériel.

1.6.2 Confirmer que les responsabilités en matière de sécurité qui sont déléguées par l'administrateur général sont documentées et attribuées à un poste en particulier pour une période déterminée.

Objectif n° 2

Des évaluations de la menace et des risques (EMR) sont réalisées et les recommandations sont mises en application conformément à la PGS (article 10.7 de la PGS).

Critère n° 2.1 Les employés connaissent bien le processus d'évaluation de la menace et des risques et le rôle qu'il joue dans le choix des mesures de protection ayant le meilleur rapport coût-efficacité.

Procédés de vérification

2.1.1 Vérifier si la politique et les procédures ministérielles en matière de sécurité donnent suffisamment d'explications sur la gestion des risques et le processus d'évaluation de la menace et des risques. (La politique indique-t-elle la portée de chacune des évaluations par secteur d'activité, par fonction, par installation, par direction générale, par direction, ou selon une combinaison de ces éléments ou selon une autre structure organisationnelle répondant aux besoins du ministère?)

2.1.2 Déterminer si les procédures expliquent clairement la façon d'évaluer la menace et les risques et si elles recommandent un format pour les rapports d'évaluation.

2.1.3 Examiner les documents de planification afin de vérifier si la gestion des risques fait partie intégrante de la stratégie de sensibilisation à la sécurité de l'ASM.

2.1.4 Interroger un échantillon de cadres et d'employés subalternes afin d'évaluer leur connaissance et leur compréhension du processus d'évaluation de la menace et des risques.

Critère n° 2.2 Les gestionnaires à qui cette responsabilité incombe font l'évaluation de la menace et des risques.

Procédés de vérification

2.2.1 Confirmer que les rapports d'évaluation de la menace et des risques ont été préparés par les gestionnaires qui sont tenus de le faire selon la PGS. Si tous les gestionnaires n'ont pas produit des rapports d'évaluation, demander une explication à l'ASM.

2.2.2 Confirmer que les cadres supérieurs prennent des décisions en vue de modifier les exigences de base à partir des recommandations faites dans les rapports d'évaluation, après avoir consulté l'ASM.

Critère n^{o} 2.3 Les évaluations de la menace et des risques sont utilisées pour concevoir des mesures de protection.

Procédés de vérification

2.3.1 Confirmer qu'il existe un répertoire des exigences de sécurité de base (sécurité du personnel et sécurité matérielle, technique et administrative).

2.3.2 Confirmer que l'application de mesures de protection additionnelles ou modifiées s'appuie sur une décision éclairée de la haute direction du ministère découlant d'une EMR à jour.

- Définir de nouvelles mesures de protection à partir des comptes rendus ou des entrevues menées avec des spécialistes de la sécurité et faire correspondre les mesures de protection aux EMR disponibles.
- Lorsque les mesures de protection ne correspondent pas à une EMR, confirmer les raisons pour lesquelles il a été décidé de modifier les exigences de sécurité de base.

2.3.3 Confirmer que le ministère évalue officiellement et officieusement la menace et les risques afin de déterminer s'il est nécessaire d'adopter de nouvelles mesures de protection (en plus des mesures de base).

2.3.4 Confirmer que le ministère emploie des méthodes établies (p. ex. utilisées par le CST, la GRC, le MDN, COBITS) ou qu'il a conçu un modèle ministériel pour l'évaluation de la menace et des risques. Le cas échéant, confirmer que le modèle tient compte des éléments de ces méthodes relatifs à l'intention et aux risques.

2.3.5 Déterminer si les évaluations de la menace et des risques sont réalisées à l'interne ou si elles sont confiées à des consultants. Confirmer que les évaluateurs internes et les consultants ont reçu la formation nécessaire pour s'acquitter de cette fonction.

2.3.6 Examiner un échantillon de rapports d'évaluation et demander aux gestionnaires responsables de confirmer que les évaluateurs ont suivi le processus établi dans la PGS et les procédures et que les rapports sont complets et exhaustifs. Dans le cadre de cet examen, déterminer la provenance des renseignements sur les menaces et les solutions envisagées pour réduire les risques au moment de choisir les mesures de protection appropriées.

2.3.7 Passer en revue les incidents de sécurité qui se sont produits aux installations et choisir les incidents les plus graves. Obtenir les rapports sur les incidents et les évaluations de la menace et des risques pour les mêmes installations. Examiner les deux documents et vérifier s'il y a des lacunes dans le processus d'évaluation.

2.3.8 Confirmer le processus qu'utilise l'ASM pour contrôler les rapports d'évaluation afin de vérifier :

- s'ils sont complets, exhaustifs et conformes à la PGS et aux procédures;
- si des mesures ont été prises à la suite des recommandations des rapports;
- s'il existe des lacunes dans le programme de sécurité du ministère.

2.3.9 Confirmer qu'il existe une politique régissant la mise à jour des évaluations de la menace et des risques et si cette politique est à jour. Par exemple, déterminer si la politique est mise à jour lorsqu'il se produit :

- une atteinte à la sécurité ou un autre incident de sécurité grave;
- un changement dans la mission opérationnelle du ministère ou l'ajout de nouveaux mandats;
- un changement important dans les renseignements et les biens de nature délicate, les systèmes d'information, l'infrastructure ou les employés;
- un changement dans les menaces pour la sécurité des renseignements ou biens de nature délicate ou la sécurité des employés, ou encore, un changement dans la probabilité que de telles menaces se concrétisent;
- des travaux de construction ou de rénovation importants à l'installation.

Critère n^{o} 2.4 Le ministère a conservé les évaluations antérieures de la menace et des risques et il a donné suite aux recommandations.

Procédés de vérification

2.4.1 Obtenir une liste des EMR disponibles et vérifier auprès de l'ASM si la liste est complète.

2.4.2 Confirmer que les spécialistes fonctionnels ou régionaux de la sécurité peuvent obtenir les EMR au besoin.

2.4.3 Examiner les documents relatifs aux incidents de sécurité récents (c.-à-d. depuis la dernière évaluation de la menace et des risques) et les mesures prises afin d'assurer la tenue appropriée de dossiers.

2.4.4 Procéder à des essais afin de confirmer que les recommandations ont été mises en application ou qu'il existe un document (compte rendu de réunion, courriel, note de service, etc.) établissant que la haute direction a décidé de ne pas donner suite à une recommandation.

Objectif n° 3

Le programme de sécurité est de nature à soutenir la gestion des situations d'urgence (p. ex. incendies, alertes à la bombe, matières dangereuses, pannes d'électricité, évacuations, urgences civiles) (article 10.13 de la PGS).

Critère n° 3.1 La gestion des risques pour la sécurité tient dûment compte des situations d'urgence et des mesures d'intervention en cas d'urgence.

Procédés de vérification

3.1.1 Demander à l'ASM de décrire brièvement la façon dont le programme de sécurité traite les situations d'urgence et complète les activités de gestion des situations d'urgence.

3.1.2 Confirmer que les affirmations de l'ASM en examinant les politiques, les plans ou les procédures de gestion des situations d'urgence.

3.1.3 En comparant un certain nombre de plans et de procédures de sécurité, analyser le programme de sécurité ministériel, les documents connexes et les autres plans et procédures obligatoires afin de confirmer qu'ils sont complémentaires.

Critère n° 3.2 Le ministère coordonne adéquatement son programme de sécurité avec les autres organismes ministériels, notamment les organismes interministériels de services d'urgence.

Procédés de vérification

3.2.1 Obtenir une liste des bureaux de première responsabilité (BPR) chargés de l'application des plans d'urgence qui ne se situent pas dans le cadre proprement dit du programme de sécurité ministériel. Confirmer que leurs rôles et responsabilités sont clairement définis.

3.2.2 Obtenir une vue d'ensemble du mandat de chaque organisation, les rôles et responsabilités qui lui incombent et l'approche employée pour garder les BPR dûment informés, notamment l'utilisation de comités.

3.2.3 Confirmer que des rapports hiérarchiques ont été établis entre l'ASM et les autres BPR dans le but d'harmoniser les rôles, politiques, procédures et programmes respectifs.

3.2.4 Interroger certains BPR afin de vérifier s'ils sont suffisamment consultés au moment de prendre des décisions d'intérêt commun et si l'information leur est donnée en temps voulu pour leur permettre de s'acquitter de leurs fonctions respectives.

Objectif n° 4

L'application du programme de sécurité à l'extérieur du Canada tient dûment compte des risques déterminés et revus par le ministère des Affaires étrangères et du Commerce international (article 10.3 de la PGS).

Critère n° 4.1 L'ASM connaît les risques reliés aux activités internationales et les arrangements en matière de sécurité. Toutes les normes de sécurité spéciales ont été examinées par le ministère des Affaires étrangères et du Commerce international et élaborées en collaboration avec ce ministère.

Procédés de vérification

4.1.1 Examiner les énoncés de mission ministériels et les documents connexes et vérifier si l'ASM comprend toutes les activités menées à l'extérieur du Canada.

4.1.2 Confirmer que les ententes et les normes de sécurité (sécurité du personnel et sécurité matérielle, technique, administrative, etc.) s'appliquant aux activités à l'étranger ont été examinées par le ministère des Affaires étrangères et du Commerce international et si elles ont été adaptées en collaboration avec ce ministère.

4.1.3 Examiner les documents ou les activités de planification de l'ASM afin de confirmer qu'ils tiennent dûment compte des activités à l'étranger.

Critère n° 4.2 Les employés qui travaillent à l'extérieur du Canada ont été informés des exigences spéciales au plan de la sécurité et de toute restriction imposée à leurs activités personnelles.

Procédés de vérification

4.2.1 Confirmer que l'ASM a pris les mesures nécessaires pour que le personnel qui travaille à l'extérieur du Canada soit avisé des exigences de sécurité spéciales en temps voulu, au moyen de mécanismes tels que :

- des séances d'information structurées sur la sécurité;
- des bulletins de sécurité;
- des fiches documentaires sur les pays;
- des rapports des services de renseignements.

4.2.2 Interroger un échantillon d'employés afin de confirmer qu'ils sont informés des conditions locales et des pratiques de sécurité visant à assurer leur sécurité personnelle.

Objectif n° 5

Le ministère effectue la surveillance active de son programme de sécurité (article 11 de la PGS).

Critère n° 5.1 Des processus efficaces de surveillance de la sécurité sont mis en œuvre.

Procédés de vérification

5.1.1 Obtenir une vue d'ensemble de l'approche et de l'information que l'ASM utilise pour surveiller les pratiques ministérielles et déceler les anomalies.

5.1.2 Vérifier l'existence et la raison d'être des processus automatisés ou manuels de surveillance de la sécurité (systèmes de détection des intrusions, outils d'évaluation de la vulnérabilité technique, etc.).

5.1.3 Lorsque des mécanismes de surveillance sont en vigueur, confirmer que leur utilisation (p. ex. détection d'utilisation malveillante ou détection des anomalies, détection active ou passive, détection fondée sur l'hôte ou sur le réseau, etc.) est régie ou justifiée par les résultats d'une évaluation de la menace et des risques.

5.1.4 Confirmer que les anomalies sont signalées à l'ASM.

5.1.5 Confirmer que l'ASM examine régulièrement les rapports de surveillance de la sécurité.

Critère n° 5.2 Un processus de surveillance de la sécurité est en vigueur.

Procédés de vérification

5.2.1 Décrire le cadre de gouvernance utilisé par l'administrateur général pour assurer la supervision de la gestion du programme de sécurité ministériel.

5.2.2 Obtenir des exemples des rapports sur les activités du programme préparés par l'ASM, y compris les contrôles ponctuels faits par le personnel de sécurité, les mécanismes de surveillance active des systèmes de TI, les examens annuels, les enquêtes sur les anomalies, etc., afin de démontrer la diligence raisonnable

5.2.3 Confirmer l'intégrité des rapports établissant la portée des interventions de l'ASM et des spécialistes de la sécurité (sécurité ministérielle, sécurité des technologies de l'information, plans de poursuite des activités, santé et sécurité au travail).

Critère n^{o} 5.3 Des vérifications internes de la sécurité sont réalisées au besoin.

Procédés de vérification

5.3.1 Confirmer que la fonction de vérification emploie des méthodes de planification fondées sur les risques qui tiennent dûment compte des risques pour la sécurité.

5.3.2 Obtenir un exemplaire des vérifications récentes portant sur des questions de sécurité et comparer leur portée et leurs objectifs à la PGS afin de déterminer l'envergure des vérifications internes.

5.3.3 Examiner les résultats de la vérification afin de déterminer dans quelle mesure l'administrateur général et l'ASM ont approuvé les conclusions de la vérification.

5.3.4 Confirmer que les rapports de vérification et les plans d'action correspondants sont disponibles sur le site Web du ministère (selon leur niveau de sensibilité), qu'ils ont été distribués aux responsables de la sécurité du Secrétariat et qu'il y a eu un suivi approprié.

Remarque : Étant donné que la fonction de vérification interne ne peut vérifier elle-même son rendement et l'efficacité de ses pratiques de façon indépendante et objective, le critère no 5.3 doit être évalué directement par le Secrétariat.

ORGANISATION DE LA SÉCURITÉ

Objectif n° 6

Le mandat et l'expérience de l'ASM correspondent à l'ampleur et à la complexité des activités du ministère (article 10.1 de la PGS).

Critère n° 6.1 Le ministère a nommé un ASM ayant le pouvoir d'établir et de diriger un programme de sécurité ministériel.

Procédés de vérification

6.1.1 Confirmer qu'un ASM à plein temps a été nommé.

6.1.2 Obtenir un énoncé de mandat expliquant les responsabilités de l'ASM dans la direction du programme de sécurité ministériel. Vérifier si des responsabilités importantes ont été déléguées à d'autres entités (p. ex. si la sécurité des TI a été déléguée au dirigeant principal de l'information) et confirmer qu'il existe un rapport hiérarchique fonctionnel, à tout le moins, entre l'ASM et ces entités (p. ex. la sécurité ministérielle, la sécurité des TI, la santé et la sécurité au travail, les affaires internes, la poursuite des activités, etc.).

6.1.3 Confirmer que l'ASM est le point de contact unique pour les demandes de renseignements sur le programme de sécurité ministériel et les documents correspondants. Si ce n'est pas l'ASM, identifier les points de contact et confirmer que l'ASM a la responsabilité fonctionnelle de les appuyer.

6.1.4 Confirmer que les responsabilités en matière de sécurité sont prises en charge lorsque l'ASM et les principaux spécialistes de la sécurité ne sont pas disponibles. Confirmer que l'ASM et les principaux spécialistes de la sécurité donnent régulièrement des conseils, de la formation et de l'orientation à leurs subalternes afin de les préparer à prendre de plus grandes responsabilités. Confirmer que les subalternes ont l'occasion de prendre des responsabilités additionnelles en temps normal et lorsque les mesures de sécurité sont resserrées.

Critère n° 6.2 L'expérience de l'ASM correspond à l'ampleur et à la complexité des activités du ministère.

Procédés de vérification

Déterminer le niveau d'expertise et d'expérience de l'ASM compte tenu des compétences requises ainsi que de l'ampleur et de la complexité des activités du ministère.

6.2.1 Tenir compte d'indicateurs tels que :

- les années d'expérience dans des postes de sécurité;
- les certifications professionnelles;
- les études;
- les conférences auxquelles l'ASM a assisté;
- l'appartenance et la participation à des associations professionnelles.

6.2.2 Confirmer que l'ASM dispose d'un budget de perfectionnement professionnel pour les principaux spécialistes de la sécurité. Déterminer si ce budget est suffisant, compte tenu de l'ampleur des activités de sécurité du ministère.

Objectif n° 7

Le ministère a établi une structure de gestion de la sécurité qui englobe la responsabilité générale de la gestion de son programme de sécurité, y compris la sécurité administrative et matérielle, la sécurité des technologies de l'information et la sécurité du personnel, de même que la sécurité de la gestion des mesures d'urgence et des marchés. La structure établie répond aux besoins du ministère (articles 10.1, 10.7 et 11 de la PGS).

Critère n° 7.1 L'ASM occupe une position stratégique dans l'organisation afin de pouvoir fournir des conseils et une orientation stratégique à la haute direction.

Procédés de vérification

7.1.1 Confirmer que l'ASM est considéré comme un cadre supérieur du ministère selon le système de classification du gouvernement.

7.1.2 Évaluer la pertinence de la situation de l'ASM dans l'organisation et du rapport hiérarchique entre l'ASM et l'administrateur général (en consultant l'organigramme, dans la mesure du possible) en temps normal et en cas d'urgence.

7.1.3 Confirmer que l'ASM peut communiquer directement avec l'administrateur général pour un motif valable.

Critère n° 7.2 Le ministère a nommé un représentant de la fonction de la sécurité dans toutes les fonctions ou régions et il gère efficacement les éléments du programme de sécurité ministériel s'appliquant à son secteur.

Procédés de vérification

7.2.1 Confirmer qu'une personne a été désignée pour représenter l'ASM dans les fonctions ou les régions.

7.2.2 Confirmer que ce représentant a reçu une formation appropriée au moment de sa nomination. Relever les cours, les séminaires et les séances de sensibilisation auxquels il a assisté depuis un an.

Critère n^{o} 7.3 Le ministère a une structure hiérarchique claire et bien documentée qui favorise l'échange d'information entre l'ASM et le représentant fonctionnel ou régional de la fonction de la sécurité.

7.3.1 Confirmer qu'il existe un processus pour les rapports courants ou les rapports exceptionnels préparés pour l'ASM. Confirmer que ce processus est documenté et qu'il est compris par le représentant fonctionnel ou régional de la fonction de la sécurité.

Critère n^{o} 7.4 Les responsabilités en matière de sécurité sont établies, définies et attribuées.

Procédés de vérification

7.4.1 Confirmer que le ministère a nommé un agent de sécurité ministériel (ASM) chargé d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de contrôler le programme de sécurité ministériel.

7.4.2 Confirmer que le ministère a établi des postes clés responsables de la sécurité ministérielle (p. ex. sécurité matérielle, sécurité du personnel et sécurité administrative), de la sécurité des TI, des enquêtes réalisées dans le cadre du plan de poursuite des activités et du programme de santé et de sécurité au travail.

7.4.3 Confirmer qu'il existe un rapport fonctionnel ou hiérarchique entre l'ASM et les postes clés responsables de la sécurité et que l'ASM rencontre régulièrement les titulaires de ces postes; en interrogeant l'ASM et les titulaires de ces postes, déterminer si les rapports fonctionnels sont de nature à favoriser l'efficience et l'efficacité du programme de sécurité.

7.4.4 Vérifier si tous les rapports hiérarchiques fonctionnels de la structure de la sécurité figurent dans les organigrammes les plus récents ou s'ils sont documentés dans le programme de sécurité ministériel.

7.4.5 Vérifier si les descriptions de travail des postes clés relatifs à la sécurité font état des fonctions et des responsabilités requises. Lorsque le poste comporte des responsabilités dans d'autres domaines, la priorité des fonctions de sécurité et le pourcentage du temps qui leur est attribué sont-ils indiqués? La priorité et le pourcentage du temps sont-ils suffisants pour le titulaire d'un poste clé relatif à la sécurité?

7.4.6 Interroger les principaux responsables de la sécurité afin de confirmer qu'ils connaissent bien leurs tâches et leurs responsabilités en matière de sécurité.

7.4.7 Confirmer que la politique ministérielle prévoit l'attribution de la responsabilité et de l'obligation de rendre compte pour la sécurité aux échelons de la région, de la direction et de l'unité, et que les fonctions figurent dans la description de poste. Confirmer les rapports fonctionnels et hiérarchiques entre ces postes et l'ASM.

Critère n^{o} 7.5 Les liens nécessaires existent avec les fonctions administratives.

Procédés de vérification

7.5.1 Obtenir une vue d'ensemble des liens internes et de la relation de travail constante entre l'ASM et les principaux spécialistes de la sécurité, d'une part, et les secteurs ci-dessous, d'autre part; déterminer la fréquence des contacts et des réunions et en évaluer la pertinence :

- Accès à l'information et protection des renseignements personnels;
- Vérification interne;
- Santé et sécurité au travail;
- Informatique (y compris les télécommunications);
- Services juridiques;
- Cabinet du ministre;
- Ressources humaines;
- Gestion du matériel;
- Gestion des biens immobiliers;
- Gestion des documents.

7.5.2 Interroger les gestionnaires de ces secteurs afin de vérifier si leurs relations de travail avec les principaux spécialistes de la sécurité sont harmonieuses et si elles sont de nature à favoriser l'efficience et l'efficacité du programme de sécurité.

7.5.3 Confirmer la participation de l'ASM et des principaux spécialistes de la sécurité à des comités de sécurité interministériels, groupes de travail et projets. Dresser une liste des comités.

7.5.4 Obtenir une vue d'ensemble des liens du ministère avec des organismes extérieurs et des relations de travail permanentes de l'ASM et des principaux spécialistes de la sécurité avec les secteurs des organismes extérieurs suivants (déterminer la fréquence des contacts et des réunions et en évaluer la pertinence) :

- Secrétariat du Conseil du Trésor —organisme central responsable des questions relatives à la sécurité et à la prestation des services, y compris la PGS, pour le gouvernement du Canada;
- Comités qui appuient le Secrétariat—conseils et orientation sur la mise en œuvre de la PGS, examen et recommandation des normes opérationnelles de sécurité;
- Service canadien du renseignement de sécurité—renseignements sur l'évaluation de la menace et enquêtes de sécurité sur le personnel;
- Centre de la sécurité des télécommunications—autorité technique en matière de cryptologie et de sécurité des TI, inspections, essais et évaluation des systèmes et procédures visés par la COMSEC;
- Ministère des Affaires étrangères et du Commerce international—ministère responsable de la conduite des relations extérieures;
- Archives nationales du Canada—organisme responsable de la gestion des documents gouvernementaux;
- Défense nationale—responsable de conseiller les ministères sur le renseignement militaire et d'assurer la sauvegarde du renseignement atomique de l'OTAN;
- Bureau de la protection des infrastructures essentielles et de la protection civile—entité responsable de la gestion efficace des situations d'urgence et des menaces qui touchent la disponibilité des biens et des services essentiels;
- Bureau du Conseil privé—responsable de l'orientation stratégique générale en matière de sécurité et de renseignement dans l'administration fédérale ainsi que des incidents pouvant porter atteinte à l'intégrité des documents confidentiels du Cabinet;
- Travaux publics et Services gouvernementaux Canada—fournit des services communs pour la gestion des marchés et des biens immobiliers, ainsi que pour les technologies de l'information et les télécommunications;
- Gendarmerie royale du Canada—organisme responsable de la sécurité matérielle et de la sécurité des technologies de l'information; participe aux enquêtes de sécurité;
- Transports Canada—ministère chargé de la sécurité maritime, terrestre et aérienne;

- Agents de santé et de sécurité nommés en vertu du *Code canadien du travail*—pour tout incident pouvant être considéré comme dangereux ou susceptible de causer des blessures aux employés;
- Services de police et d'incendie locaux—pour les renseignements relatifs à l'évaluation de la menace.

7.5.5 Demander à l'ASM et aux principaux responsables de la sécurité s'ils ont eu des contacts ou des réunions récemment avec les ministères et organismes ci-dessus.

ADMINISTRATION DE LA SÉCURITÉ

Objectif n° 8

Le programme de sécurité a été intégré au processus général de planification du ministère (article 10.1 de la PGS).

Procédés de vérification

8.1.1 Obtenir une vue d'ensemble des activités de planification en matière de sécurité et de leur interaction avec la planification ministérielle.

8.1.2 Confirmer que le programme de sécurité ministériel comprend des plans et des objectifs à court et à long terme, les examiner et confirmer qu'ils sont complets, raisonnables au plan des échéanciers et des ressources disponibles, conformes aux plans stratégiques du ministère et approuvés par la haute direction.

8.1.3 Confirmer que le financement du programme de sécurité est un poste de dépense distinct dans le budget du ministère.

8.1.4 Examiner le financement du programme de sécurité et déterminer, en collaboration avec l'ASM, si les fonds sont suffisants et quelles seraient les conséquences de toute réduction importante des sommes qui y sont consacrées.

Objectif n° 9

Les spécialistes de la sécurité reçoivent la formation dont ils ont besoin : des séances de sensibilisation sont données régulièrement afin de renseigner les employés et de leur rappeler leurs responsabilités, les enjeux et les préoccupations en matière de sécurité; des séances d'information sont données au sujet des responsabilités rattachées aux différentes cotes de sécurité (article 10.5 de la PGS).

Critère n° 9.1 Les spécialistes de la sécurité, qu'ils exercent leurs fonctions à plein temps ou à temps partiel, reçoivent en temps voulu la formation et le perfectionnement professionnel dont ils ont besoin.

Procédés de vérification

9.1.1 Vérifier si des cours et des séminaires sur la sécurité ont été offerts aux principaux spécialistes de la sécurité au cours des deux années précédentes. L'information doit prendre en compte les compétences requises et devrait être disponible auprès des organisations suivantes :

- Division de la politique de l'information, des communications et de la sécurité du Secrétariat;
- Association fédérale des responsables de la sécurité;
- Direction générale des programmes de formation de la Commission de la fonction publique (Formation et Perfectionnement Canada);
- Principaux organismes de sécurité;
- Autres organismes de professionnels de la sécurité;
- Direction générale de la formation de la Gendarmerie royale du Canada;
- Collèges et universités;
- Autres organismes de professionnels de la sécurité tels que l'American Society for Industrial Security, la Société canadienne de la sûreté industrielle, la High Tech Crime Investigation Association, la Information System Security Association, le Disaster Recovery Institute, etc.

9.1.2 Déterminer comment l'ASM :

- se renseigne sur les cours et les séminaires offerts au personnel de sécurité;
- s'assure que les spécialistes de la sécurité et les autres employés sont informés des séances d'information qui leur sont offertes;

- contrôle la formation reçue et les séances d'orientation offertes aux autres employés et au personnel à contrat.

9.1.3 Vérifier si des cours ont été donnés aux principaux spécialistes de la sécurité au cours des deux dernières années afin de les aider à s'acquitter de leurs fonctions.

9.1.4 Vérifier si les spécialistes de la sécurité reçoivent de la formation et du perfectionnement professionnel de niveau avancé à l'extérieur du ministère. Déterminer si des mesures ont été prises afin que les spécialistes de la sécurité obtiennent une certification professionnelle et qu'ils participent aux séminaires et aux activités des associations de professionnels de la sécurité.

9.1.5 Obtenir une vue d'ensemble de la façon de déterminer les besoins de formation des autres employés qui assument à temps plein ou à temps partiel des fonctions liées à la sécurité (déterminer si l'ASM est le principal point de contact en ce qui concerne la formation sur la sécurité. Sinon, identifier le point de contact).

9.1.6 Déterminer la formation sur la sécurité qui a été donnée au cours des 12 derniers mois aux autres employés qui assument à temps plein ou à temps partiel des fonctions liées à la sécurité.

9.1.7 Vérifier si le personnel de l'ASM reçoit des périodiques sur la sécurité et assiste aux présentations des entrepreneurs, aux séminaires sur les produits et à d'autres présentations professionnelles afin de se tenir au courant des nouvelles technologies.

Critère n^{o} 9.2 L'ASM a une stratégie adéquate de sensibilisation à la sécurité et le financement nécessaire pour la mettre en œuvre

Procédés de vérification

9.2.1 Obtenir une vue d'ensemble des activités de l'ASM dans le cadre de la stratégie de sensibilisation à la sécurité ainsi que des méthodes utilisées pour déterminer les problèmes qui nécessitent des mesures correctives.

9.2.2 Vérifier si l'ASM a adopté un processus permettant de contrôler l'efficacité du programme de formation et de la stratégie en matière de sécurité. Examiner des éléments comme :

- les statistiques sur les incidents de sécurité (atteintes et infractions);
- le volume de correspondance sur la sensibilisation à la sécurité;

- le nombre de séances de sensibilisation à la sécurité;
- les sujets abordés dans la correspondance sur la sensibilisation à la sécurité et pendant les séances de sensibilisation (afin d'en vérifier la pertinence et l'opportunité).

9.2.3 Examiner les incidents de sécurité (atteintes et infractions) qui se sont produits au cours des 12 derniers mois afin de vérifier l'efficacité de la stratégie de sensibilisation à la sécurité.

9.2.4 Vérifier, de concert avec l'ASM, si le budget attribué au programme de sensibilisation à la sécurité est suffisant.

Objectif n° 10

Les renseignements et les biens de nature délicate reçoivent la cote CLASSIFIÉ ou PROTÉGÉ, conformément à la PGS et aux normes opérationnelles de sécurité (au regard de leur confidentialité, de leur intégrité, de leur disponibilité et de leur valeur) et les mentions de sensibilité sont déclassées ou éliminées lorsque la nature des renseignements ou des biens devient moins délicate ou cesse de l'être (article 10.6 de la PGS).

Critère n° 10.1 Les renseignements et les biens de nature délicate sont classifiés et désignés au moyen d'un *Guide de classification de l'information* ministériel ou par les agents autorisés à le faire par l'administrateur général, ou les deux.

Procédés de vérification

10.1.1 Obtenir une vue d'ensemble des pratiques permettant de recenser les renseignements de nature délicate et d'en déterminer la classification.

10.1.2 Vérifier si les procédures et les pratiques ministérielles répondent aux exigences suivantes :

- Les renseignements de nature délicate et les autres biens qui doivent être protégés contre toute communication non autorisée sont recensés et catégorisés comme étant ou non d'intérêt national (mais assujettis aux dispositions de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*), afin de répondre aux exigences relatives à la confidentialité.
- Les renseignements et les biens de valeur sont recensés et catégorisés en fonction de la gravité du préjudice qu'entraînerait leur modification, afin de répondre aux exigences relatives à l'intégrité.
- Les renseignements et les biens de valeur sont recensés et catégorisés en fonction de la gravité du préjudice qu'entraînerait leur perte, afin de répondre aux exigences relatives à la disponibilité.
- Le ministère attribue aux renseignements et aux autres biens une valeur monétaire ou culturelle, une survaleur ou une autre valeur dans l'éventualité où ils seraient modifiés ou perdus, afin de répondre aux exigences relatives à la valeur des actifs.
- Le ministère a préparé un *Guide de classification de l'information* pour l'attribution de mentions de sensibilité aux renseignements et aux biens de valeur.

10.1.3 Si le ministère utilise un guide, l'examiner et vérifier :

- si le manuel décrit bien le type de renseignements de nature délicate qui sont produits par le ministère, aux plans de la confidentialité, de l'intégrité, de la disponibilité et de la valeur.
- si le guide est conforme à la PGS et aux normes opérationnelles de sécurité; s'il établit clairement la façon d'attribuer des classifications de sécurité aux documents.
- si le guide a été mis à jour à la suite des modifications apportées à la PGS en février 2002; déterminer qui est responsable de la mise à jour du guide et le processus utilisé pour confirmer qu'il est gardé à jour.
- si les employés dont les fonctions comprennent la création et la collecte de renseignements de nature délicate disposent déjà d'un exemplaire du guide.

10.1.4 Interroger les employés dont les fonctions comprennent la création et la collecte de renseignements de nature délicate afin de vérifier s'ils connaissent bien le processus à suivre pour classifier des renseignements de nature délicate.

10.1.5 Si certains postes et titulaires ont l'autorisation de classifier des renseignements de nature délicate, examiner la liste des postes et vérifier :

- si l'ASM conserve une liste à jour de ces postes et des employés qui les occupent;
- si les postes occupent une position stratégique dans le ministère afin que tous les employés puissent joindre facilement les titulaires;
- si l'ASM examine la liste périodiquement afin de s'assurer que les postes ont manifestement besoin d'avoir et de conserver cette autorisation et que les titulaires ont reçu la formation nécessaire pour s'acquitter de cette tâche.

10.1.6 Interroger les fonctionnaires qui occupent des postes où ils sont autorisés à classifier des renseignements de nature délicate et vérifier s'ils connaissent bien leurs responsabilités à cet égard. Déterminer s'ils ont un rapport fonctionnel avec l'ASM à titre de conseillers spécialisés.

Critère n^{o} 10.2 Les mentions de sécurité attribuées aux renseignements classifiés et protégés indiquent les mesures de protection minimales qui doivent être appliquées à ces renseignements.

Procédés de vérification

10.2.1 Vérifier s'il existe des procédures expliquant la façon d'attribuer des mentions de sécurité aux dossiers, documents, manuels, microformats et autres biens de valeur qui contiennent des renseignements de nature délicate. Déterminer si ces procédures sont mises à la

disposition des employés dont les fonctions comprennent la création et la collecte de renseignements de nature délicate. Il est fortement recommandé d'inclure ces directives dans un *Guide de classification de l'information*.

10.2.2 Vérifier s'il existe des procédures pour attribuer des mentions aux biens de nature délicate et de valeur en fonction de leur disponibilité, de leur intégrité ou de leur valeur, même en l'absence de considérations touchant la confidentialité.

10.2.3 Examiner plusieurs types de documents de nature délicate afin de vérifier s'ils portent les mentions nécessaires, conformément aux directives écrites et aux normes opérationnelles sur l'identification des biens. En cas de non-conformité, déterminer, si possible, qui a attribué les mentions et vérifier si ces personnes connaissent les directives sur les mentions à attribuer aux renseignements de nature délicate et aux biens de valeur.

Critère n^{o} 10.3 Les mentions de sensibilité (CLASSIFIÉ ou PROTÉGÉ) attribuées aux renseignements de nature délicate sont éliminées ou modifiées lorsque la nature des renseignements devient moins délicate ou cesse de l'être et lorsqu'il n'est plus nécessaire de leur appliquer des mesures de protection de niveau supérieur.

Procédés de vérification

10.3.1 Vérifier si le ministère a mis en vigueur des procédures (qui figurent généralement dans un *Guide de classification de l'information*) expliquant la déclassification et le déclassement des renseignements et des biens de nature délicate. Vérifier si les directives sur la classification incitent les auteurs à ajouter des limites de temps et d'autres mises en garde afin de permettre le déclassement ou la déclassification automatique.

10.3.2 Vérifier si les procédures relatives à la déclassification et au déclassement sont claires et si elles donnent suffisamment de précisions sur le processus à suivre. Déterminer si les directives sur la classification expliquent clairement le bien-fondé de la déclassification et du déclassement des renseignements et des biens de nature délicate et le processus à suivre.

10.3.3 Déterminer les postes autorisés à déclassifier et à déclasser des renseignements de nature délicate et vérifier si ces postes figurent dans le programme et les procédures de sécurité. Confirmer que les procédures sont facilement mises à la disposition des titulaires de ces postes.

10.3.4 Déterminer les procédures à suivre pour la mise à jour des cotes de sensibilité ainsi que la fréquence des mises à jour.

10.3.5 Vérifier si le programme de sécurité établit que les renseignements de nature délicate provenant de sources extérieures ne doivent pas être déclassifiés ou déclassés sans l'approbation préalable[5] des propriétaires ou des auteurs[6].

10.3.6 Demander aux titulaires des postes ayant l'autorisation de déclassifier et de déclasser des renseignements de nature délicate quels sont les renseignements qu'ils ont déclassifiés ou déclassés au cours de l'année précédente.

10.3.7 Déterminer si les renseignements qui ont été déclassifiés et déclassés portent une mention indiquant clairement qu'ils ne sont plus classifiés ou désignés ou qu'ils ont une classification ou une désignation inférieure, ainsi que la date ou la mise en garde qui a donné lieu au déclassement.

Remarque : Il est important de déclassifier et de déclasser les renseignements de nature délicate parce que la surclassification d'une grande quantité de renseignements se traduit par l'obligation de maintenir les mesures de protection longtemps après que cette protection a cessé d'être nécessaire. La déclassification et le déclassement de renseignements de nature délicate répartis dans un grand nombre de dossiers a peut-être une plus grande incidence sur les ressources que le fait de laisser les renseignements classifiés ou désignés à leur niveau initial. Les objectifs de la politique sur la sécurité pourraient être atteints au moyen de mesures de substitution, comme la destruction régulière des dossiers selon le calendrier de conservation et de retrait des Archives nationales du Canada.

Critère n^{o} 10.4 Les renseignements qui ont été déclassifiés et déclassés portent une mention indiquant clairement qu'ils ne sont plus classifiés ou désignés ou qu'ils ont une classification ou une désignation inférieure.

Procédés de vérification

10.4.1 Vérifier si le ministère a mis en vigueur des procédures expliquant la façon de modifier les mentions de sécurité sur les documents qui contiennent des renseignements déclassifiés ou déclassés. Confirmer que les procédures sont facilement mises à la disposition de tous les postes ayant l'autorisation de déclassifier ou de déclasser des renseignements de nature délicate.

---

5 L'approbation peut être obtenue au cas par cas ou en concluant des ententes écrites ou des protocoles d'entente avec les parties concernées.

6 Le ministère doit aussi émettre des procédures sur les mesures à prendre lorsqu'il est impossible de consulter les propriétaires ou les auteurs.

10.4.2 Examiner plusieurs types de documents de nature délicate qui ont été déclassifiés ou déclassés et vérifier s'ils ont reçu la mention appropriée au moment de leur déclassification ou de leur déclassement.

Objectif n° 11

Les atteintes et infractions à la sécurité et les autres incidents de sécurité font l'objet d'une enquête. Des mesures visant à réduire les pertes et des mesures administratives, correctives ou disciplinaires (articles 10.15 et 10.16 de la PGS) sont prises.

Critère n° 11.1 Un organisme d'enquête effectue des enquêtes sur la sécurité.

Procédés de vérification

11.1.1 Obtenir une vue d'ensemble des arrangements organisationnels concernant les enquêtes sur les atteintes et les infractions à la sécurité et sur les autres incidents de sécurité.

11.1.2 Vérifier si la politique et les procédures sont conformes à la PGS et aux normes opérationnelles de sécurité et si elles font état des infractions mentionnées dans la *Politique sur les pertes de deniers et infractions et autres actes illégaux commis contre la Couronne.*

11.1.3 Vérifier si les descriptions de travail des spécialistes de la sécurité (ASM, sécurité ministérielle, plans de poursuite des activités, santé et sécurité au travail, etc.), ainsi que les politiques et procédures connexes, présentent les caractéristiques suivantes :

- les responsabilités des enquêtes sont clairement définies;
- la portée des enquêtes est clairement délimitée;
- le champ d'intervention et les pouvoirs des enquêteurs sont clairement énoncés par écrit;
- les enquêteurs doivent rendre compte à l'administrateur général de l'efficacité et de la légalité de toute enquête;
- la responsabilité de l'ASM de formuler des commentaires sur toute enquête ayant trait à la sécurité est clairement établie.

Critère n° 11.2 Un processus est en vigueur pour signaler les atteintes, les infractions et les autres incidents de sécurité éventuels.

Procédés de vérification

11.2.1 Obtenir une vue d'ensemble des pratiques et procédures utilisées pour signaler les atteintes, les infractions et les autres incidents de sécurité éventuels.

- Examiner les rapports concernant les atteintes éventuelles à la sécurité qui ont été signalées depuis la dernière vérification interne et vérifier si elles ont été rapportées immédiatement à l'ASM, puis à l'administrateur général.

- Vérifier si une politique et des procédures ont été mises en vigueur au sujet de la communication des incidents mentionnés dans la *Politique sur les pertes de deniers et infractions et autres actes illégaux commis contre la Couronne*).

11.2.2 Vérifier si des rapports hiérarchiques officiels ou officieux ont été établis entre les organismes suivants et l'ASM pour :

- Les actes criminels
- Les atteintes à l'intégrité des documents confidentiels du Cabinet
- Les menaces contre les intérêts nationaux
- La disponibilité des biens et services essentiels
- Situations dangereuses et blessures
- Modifications aux normes de sécurité
- Organismes d'application de la loi
- Bureau du Conseil privé
- Service canadien du renseignement de sécurité
- Protection des infrastructures essentielles et protection civile
- Agent de santé et de sécurité
- Secrétariat du Conseil du Trésor

11.2.3 Examiner les rapports concernant les éventuelles atteintes à la sécurité qui ont été signalées et déterminer si ces atteintes ont été rapportées aux organismes ci-dessus comme il se doit. Déterminer également si les cas suivants s'appliquent et s'ils nécessitent d'autres rapports :

- Le ministère qui a communiqué les renseignements qui ont fait l'objet d'une atteinte à la sécurité a été informé de l'incident, le cas échéant;
- Les autres ministères dont les renseignements ou les biens ont fait l'objet d'une atteinte à la sécurité ont été informés de la situation et des conclusions qui les concernaient, le cas échéant.

11.2.4 Vérifier si l'ASM exerce une surveillance sur les atteintes à la sécurité et sur les autres incidents de sécurité. Évaluer la pertinence de la surveillance qu'exerce l'ASM dans le but de s'acquitter pleinement de ses responsabilités envers l'administrateur général dans le cadre du programme de sécurité ministériel.

11.2.5 Examiner les documents sur les incidents de sécurité pour les deux dernières années. Vérifier si les rapports nécessaires ont été transmis à la GRC à des fins de production de statistiques. Si les rapports n'ont pas été transmis, demander s'il y a une explication raisonnable à ce sujet.

Critère n^{o} 11.3 Un processus est en vigueur afin de réduire les pertes découlant d'une atteinte ou d'une infraction à la sécurité ou d'un autre incident de sécurité.

Procédés de vérification

11.3.1 Obtenir une vue d'ensemble des pratiques et procédures en vigueur relativement aux blessures et à la mise en œuvre de contre-mesures et de mesures correctives dans le but de réduire les pertes découlant d'une atteinte ou d'une infraction à la sécurité ou d'un autre incident de sécurité.

11.3.2 Vérifier si les atteintes ou les infractions à la sécurité et les autres incidents de sécurité sont analysés afin de déceler les problèmes communs qui devraient être abordés dans le cadre de la stratégie de sensibilisation à la sécurité de l'ASM.

11.3.3 Vérifier si les pratiques en vigueur exigent que les spécialistes de la sécurité recommandent des mesures correctives à la suite d'une enquête sur un incident de sécurité.

11.3.4 Vérifier si les pratiques en vigueur exigent qu'une EMR dirigée soit réalisée afin de confirmer le changement dans le risque résiduel à la suite d'une enquête sur un incident de sécurité.

Critère n^{o} 11.4 Le ministère est en mesure d'intervenir efficacement en cas d'incident de sécurité.

Procédés de vérification

11.4.1 Vérifier si les pratiques en vigueur exigent :

- que la surveillance des capteurs électroniques soit centralisée;
- que l'installation soit en mesure de réagir en cas d'accès non autorisé.

11.4.2 Vérifier si le personnel d'intervention dispose du matériel nécessaire.

11.4.3 Vérifier si le personnel de surveillance et d'intervention a reçu une formation adéquate. Examiner les descriptions de travail, les documents de formation, les consignes de poste et les marchés, le cas échéant.

Critère n^{o} 11.5 Des sanctions administratives ou disciplinaires sont appliquées, au besoin, en cas d'atteinte à la sécurité, d'infraction à la sécurité ou d'autre incident de sécurité.

Procédés de vérification

11.5.1 Obtenir une vue d'ensemble des pratiques et procédures en vigueur concernant le processus d'imposition de sanctions administratives et disciplinaires, y compris les responsabilités de l'ASM.

11.5.2 Vérifier si les critères régissant l'attribution de récompenses et l'imposition de sanctions sont clairement énoncés. Vérifier si les gestionnaires à tous les échelons savent qu'il est possible de recommander des récompenses et des sanctions. Vérifier si les gestes qui constituent de l'inconduite ou de la négligence sont clairement définis.

11.5.3 Examiner les cas où les récompenses et les sanctions étaient méritées et déterminer si la mesure qui a été prise était conforme à la politique et aux procédures.

ACCÈS RESTREINT

Objectif n° 12

L'accès aux renseignements et aux biens de nature délicate est restreint aux personnes qui ont besoin de les connaître et qui détiennent une approbation officielle et l'autorisation de sécurité requise (article 10.8 de la PGS).

Critère n° 12.1 Toute personne ayant besoin d'accéder à des renseignements ou à des biens de nature délicate a reçu une autorisation officielle d'un gestionnaire bien renseigné et responsable en vertu du principe du « privilège minimal ».

Procédés de vérification

12.1.1 Obtenir une vue d'ensemble du processus utilisé pour accorder l'accès et faire des essais sur un échantillon afin de vérifier si le processus permet de garantir que les employés ayant accès à des renseignements de nature délicate ont obtenu une autorisation officielle de leur gestionnaire (habituellement donnée par écrit ou au moyen d'une séance d'information).

12.1.2 Vérifier si le principe du privilège minimal[7] est mis en application, s'il est expliqué dans la politique sur la sécurité et s'il est compris par le personnel.

12.1.3 Interroger un groupe d'employés afin de confirmer qu'ils comprennent la façon d'appliquer le principe du privilège minimal.

Critère n° 12.2 L'accès aux renseignements de nature délicate est accordé uniquement aux personnes qui ont la cote de fiabilité ou l'autorisation de sécurité appropriée et qui sont autorisées à prendre connaissance des renseignements.

Procédés de vérification

12.2.1 Vérifier si des procédures adéquates ont été mises en vigueur pour la communication de renseignements de nature délicate d'un employé à un autre employé ou à une autre personne.

12.2.2 Vérifier si les procédures qui ont été mises en vigueur pour les contrôles à effectuer dans les installations de gestion des documents portent sur les aspects suivants :

[7] Le personnel a accès uniquement aux renseignements et aux biens dont il a besoin pour faire son travail.

- le prêt de dossiers contenant des renseignements de nature délicate;
- les documents à remplir lors du prêt et du retour de ces dossiers;
- la vérification périodique de l'ASM.

12.2.3 Vérifier si une surveillance est exercée pour s'assurer que les services de gestion des documents respectent la politique et les procédures relatives à la protection, au contrôle, au prêt et au retour des dossiers contenant des renseignements de nature délicate.

12.2.4 Examiner un service de gestion des documents et :

- observer le processus suivi lors du prêt de dossiers contenant des renseignements de nature délicate;
- vérifier les documents gardés lors du prêt de dossiers contenant des renseignements de nature délicate et s'assurer qu'ils sont bien tenus;
- choisir des dossiers contenant des renseignements de nature délicate qui ont été prêtés pour une période anormalement longue et obtenir des explications;
- choisir des dossiers contenant des renseignements de nature délicate[8] qui sont prêtés; s'assurer que les employés à qui les dossiers sont prêtés les ont en leur possession, qu'ils ont la cote de fiabilité approfondie ou la cote de sécurité nécessaire et que les dossiers sont en lieu sûr dans un coffre de sécurité lorsqu'ils ne sont pas utilisés.

12.2.5 À partir d'un échantillon, vérifier si les employés savent qu'ils doivent vérifier l'autorisation de sécurité et le besoin de savoir du destinataire avant de prêter des dossiers contenant des renseignements de nature délicate.

[8] Choisir uniquement des dossiers classifiés **TRÈS SECRET** et **SECRET** et des dossiers désignés extrêmement sensibles (**PROTÉGÉ C**).

Objectif n° 13

Aucune personne ne détient le contrôle unique de tous les aspects d'un processus ou d'un système (en particulier une mesure de protection) (article 10.8 de la PGS).

Procédés de vérification

13.1.1 Vérifier si le principe de la « séparation des responsabilités », voulant qu'aucune personne ne puisse détenir le contrôle unique de tous les aspects d'un processus ou d'un système ou contourner les mesures de sécurité, est intégré dans les politiques et procédures relatives à l'accès aux renseignements classifiés et protégés, y compris les renseignements, les systèmes et les autres biens.

13.1.2 Déterminer les pratiques utilisées par l'ASM pour confirmer que le principe de la séparation des responsabilités est expliqué au personnel.

13.1.3 Déterminer les pratiques utilisées par l'ASM pour examiner et contrôler la mise en application du principe.

13.1.4 Lorsque la séparation des responsabilités est impossible, déterminer comment l'ASM est informé de telles situations et si des contrôles ou des arrangements de substitution ont été mis en œuvre[9].

[9] Exiger la présence de deux personnes lors de l'ouverture d'une chambre forte ou deux signatures sur un chèque sont des exemples de contrôles de substitution.

ÉCHANGE DE RENSEIGNEMENTS ET D'AUTRES BIENS

Objectif n° 14

Des mesures de protection adéquates sont appliquées aux renseignements de nature délicate qui sont échangés avec des sources officielles de l'extérieur du ministère, notamment les gouvernements étrangers, provinciaux, territoriaux et municipaux, les établissements d'enseignement et les organismes du secteur privé (article 10.2 de la PGS).

Critère n° 14.1 Des ententes écrites ou des protocoles d'entente sont mis en œuvre dans le but de protéger les renseignements de nature délicate qui sont échangés avec d'autres ministères et d'autres gouvernements et organisations.

Procédés de vérification

14.1.1 Obtenir une vue d'ensemble des pratiques, politiques et procédures mises en œuvre pour l'application des exigences relatives aux ententes et aux accords écrits, ainsi qu'aux éléments à y inclure, avec :

- d'autres gouvernements et organisations au sujet des mesures qu'ils doivent prendre pour protéger les renseignements classifiés qui leur sont communiqués;
- d'autres ministères au sujet des mesures qu'ils doivent prendre pour protéger les renseignements désignés de nature particulièrement délicate[10] ou de nature extrêmement délicate[11] qui leur sont communiqués sur une base régulière.

14.1.2 Vérifier si l'ASM examine les ententes et les protocoles d'entente avant qu'ils soient signés afin de s'assurer qu'ils sont complets et exhaustifs.

Critère n° 14.2 Les renseignements échangés avec d'autres ministères sont inventoriés

Procédés de vérification

14.2.1 Vérifier si le ministère peut déterminer quels gouvernements fédéraux, provinciaux, territoriaux et municipaux au Canada et à l'étranger fournissent et reçoivent des renseignements de nature délicate. Cette information peut être conservée par l'ASM ou décentralisée dans les différents groupes fonctionnels. On peut obtenir des directives à ce sujet dans le *Guide de classification de l'information* du ministère ou auprès des responsables de la gestion de l'information ou des fonds de renseignements.

---

[10] Les renseignements peuvent porter la mention **PROTÉGÉ B** lorsqu'ils sont de nature particulièrement délicate.

[11] Les renseignements peuvent porter la mention **PROTÉGÉ C** lorsqu'ils sont de nature extrêmement délicate.

14.2.2 Vérifier s'il existe un processus suivi par l'ASM pour formuler des observations sur le besoin constant d'échanger des renseignements avec des entités extérieures et sur les risques que cela comporte.

Critère n^{o} 14.3 Des mesures de protection adéquates sont appliquées aux renseignements de nature délicate qui sont échangés avec des sources officielles extérieures

Procédés de vérification

14.3.1 Vérifier si les normes de sécurité et le *Guide de classification de l'information* contiennent des instructions sur la façon de protéger les renseignements de nature délicate qui sont échangés avec des sources officielles extérieures et si ces instructions sont bien suivies.

14.3.2 Vérifier si les directives en matière de sécurité établissent que les renseignements de nature délicate obtenus de sources extérieures ne doivent pas être déclassifiés ou déclassés sans l'approbation préalable des propriétaires ou auteurs.

Objectif n° 15

Le ministère a adopté des processus et conclu des ententes afin de confirmer la protection des renseignements échangés avec d'autres sources officielles, conformément aux politiques et aux normes de sécurité des parties concernées (article 10.2 de la PGS).

Procédés de vérification

15.1.1 Vérifier si des essais sont effectués périodiquement afin de s'assurer que les renseignements communiqués par d'autres sources officielles sont traités suivant les instructions données par ces sources.

15.1.2 Vérifier si les personnes qui traitent des renseignements communiqués par d'autres sources officielles ont en main les instructions données par ces sources.

15.1.3 Vérifier si les instructions spéciales de traitement sont abordées pendant les séances de sensibilisation ou dans la correspondance sur la sécurité.

SÉCURITÉ MATÉRIELLE

Objectif n° 16

Une évaluation de sécurité adéquate est menée avant de choisir et d'aménager des installations, dans le but de réduire ou d'éliminer les menaces et les risques pour les renseignements et les biens de nature délicate et pour les employés dans ces installations (article 10.11 de la PGS).

Critère n° 16.1 Les exigences de sécurité sont prises en compte dans le choix d'un site et dans l'acquisition ou la construction de nouvelles installations

Procédés de vérification

16.1.1 Obtenir une vue d'ensemble des pratiques, politiques et procédures relatives au processus à suivre pour l'évaluation des exigences de sécurité relatives :

- au choix du site de nouvelles installations;
- à l'acquisition ou à la construction de nouvelles installations.

16.1.2 Examiner la politique et les procédures afin de vérifier si elles sont exhaustives et complètes. À l'étape de la planification, vérifier si les mesures de protection de la sécurité matérielle sont conformes aux exigences de sécurité de base énoncées dans la documentation pertinente.

16.1.3 Lorsqu'il est prévu que les mesures de protection de la sécurité matérielle dépasseront les exigences de base, vérifier si l'application de ces mesures est justifiée par une EMR et déterminer :

- si l'incidence des voisins sur la sécurité a été prise en compte dans une EMR et si les mesures de protection ont été renforcées au besoin;
- si le contrôle exercé sur les droits d'usage a été confirmé au moment du choix du site et de la négociation du bail;
- si les risques et les problèmes relatifs à la sécurité des employés dans les parcs de stationnement ont été examinés dans une EMR et si les mesures de protection ont été renforcées au besoin.

16.1.4 Vérifier si le matériel électronique de détection des intrusions, les appareils vidéo en circuit fermé et les autres dispositifs techniques permettant de contrôler l'accès aux installations (préciser) sont utilisés judicieusement. S'assurer que le contrôle n'est pas exercé uniquement par des employés ou des gardes de sécurité.

16.1.5 Vérifier si les spécialistes de la sécurité matérielle utilisent l'approche suivante :

- « protection » (des barrières ont été installées pour retarder ou empêcher l'accès non autorisé)
- « détection » (les cas d'accès non autorisé sont signalés)
- « intervention » (les incidents de sécurité sont signalés aux spécialistes de la sécurité et des mesures correctives sont prises).

16.1.6 Vérifier si les responsabilités respectives du gardien et de l'occupant ont été délimitées et harmonisées de manière à assurer la protection totale. Vérifier s'il existe un processus pour faire en sorte que le gardien avertisse l'occupant (en général, l'ASM) de tout changement dans le fonctionnement des installations afin qu'une évaluation de la sécurité puisse être faite.

Critère n^{o} 16.2 Le ministère prépare des énoncés établissant les exigences de sécurité pour le choix d'un site et l'aménagement d'une installation

Procédés de vérification

16.2.1 Vérifier s'il existe un processus pour informer l'ASM des projets relatifs à l'acquisition ou à la construction de nouvelles installations.

16.2.2 Vérifier si un spécialiste de la sécurité participe officiellement ou officieusement à l'aménagement, à la conception, au choix et à la modification des installations.

16.2.3 Vérifier si l'ASM a établi un processus pour :

- la préparation d'énoncés établissant les exigences de sécurité pour le choix du site et l'aménagement des installations;
- la vérification de la conformité des mesures de sécurité matérielle aux règlements et codes pertinents.

16.2.4 Vérifier si l'ASM approuve toutes les caractéristiques de sécurité qui figurent dans les documents de planification, les demandes de propositions et les documents d'appels d'offres.

Critère n^{o} 16.3 Les exigences de sécurité sont prises en compte à toutes les étapes de la conception, de l'ébauche des plans à la fin du projet

Procédés de vérification

16.3.1 Obtenir une vue d'ensemble des processus utilisés pour :

- confirmer que des guides de sécurité du site et des guides de sécurité de la conception sont inclus dans les documents d'information sur l'architecture;

- concilier les divergences entre les propositions relatives à la conception architecturale et les guides de sécurité de la conception;
- s'assurer de l'application constante des guides de sécurité de la conception à partir de l'étape de la conception par dessin jusqu'à l'achèvement des nouvelles installations et l'approbation des plans à chaque étape;
- confirmer que des inspections de sécurité sont faites dans les installations avant qu'elles ne soient occupées.

16.3.2 Choisir des plans de sites et confirmer qu'ils ont été examinés et approuvés par l'ASM aux étapes critiques de la mise en œuvre.

16.3.3 Vérifier si les coûts relatifs à la sécurité sont séparés des autres coûts liés à la conception, au choix et à la construction des installations. Vérifier si l'ASM a le pouvoir d'affecter des fonds et des ressources à la sécurité dans le cadre des projets. Interroger l'ASM afin de déterminer l'incidence éventuelle du financement consacré à la sécurité.

Objectif n° 17

Des mesures de sécurité matérielle ont été prises afin d'assurer la protection des renseignements et des biens de nature délicate ainsi que la sûreté et la sécurité des employés dans les installations (article 10.11 de la PGS).

Critère n° 17.1 Un programme d'autorisation d'accès aux sites approuvé par le Conseil du Trésor est mis en œuvre

Procédés de vérification

17.1.1 Confirmer que l'accès aux principales installations et aux zones à accès restreint est contrôlé dans le cadre d'un programme d'autorisation d'accès aux sites mis en œuvre par l'ASM et approuvé par le Conseil du Trésor.

17.1.2 Choisir des sites et vérifier s'ils sont inclus dans le programme d'autorisation d'accès aux sites.

Critère n° 17.2 Les employés et les visiteurs sont identifiés et leur entrée dans une installation ou une zone est contrôlée et surveillée au moyen de systèmes de contrôle et de surveillance appropriés, au besoin.

Procédés de vérification

17.2.1 Obtenir une vue d'ensemble des pratiques, politiques et procédures d'identification des employés et des visiteurs aux points de contrôle d'accès. Examiner la politique et les procédures avec l'ASM et vérifier si les systèmes utilisés dans chaque installation répondent aux besoins du ministère.

17.2.2 Au moyen d'un échantillon, vérifier :

- si des procédures ont été mises en vigueur pour le contrôle et l'utilisation des cartes d'identité, des cartes de proximité, des clés ou des jetons dans toutes les installations et pour les mesures à prendre en cas de perte ou de vol des cartes;
- si chaque employé est tenu responsable de ces articles de sécurité et si des sanctions ou des amendes sont prévues lorsque les articles sont perdus, selon les résultats d'une enquête;
- si tous les employés détiennent une carte d'identification où figurent, à tout le moins, le nom du ministère, la photographie du porteur, un numéro unique, la signature de l'employé et une date de péremption;
- si les fournisseurs et les visiteurs sont tenus de s'inscrire à l'entrée de l'installation et de porter des insignes d'identité sur les lieux;

- si les visiteurs, les fournisseurs et le personnel de service doivent être accompagnés;
- si les employés interpellent les personnes qui ne portent pas les insignes de sécurité appropriés dans l'installation;
- si le système de laissez-passer prévoit une façon d'émettre une carte temporaire qui indique clairement que les visiteurs et les fournisseurs ne sont pas des employés.

17.2.3 Vérifier si une politique et des procédures ont été mises en œuvre relativement à l'utilisation des systèmes de contrôle d'accès et de surveillance dans les installations et les zones à accès restreint. Examiner la politique et les procédures, en discuter avec l'ASM et vérifier si les systèmes répondent aux besoins du ministère.

17.2.4 Lorsque des cartes ou des clés d'accès sont utilisées pour contrôler l'accès aux installations ou aux zones de sécurité, vérifier si une politique et des procédures ont été mises en œuvre pour l'application du principe de la « nécessité d'accéder » et pour la délivrance, la récupération et l'annulation des cartes et des clés.

17.2.5 Se rendre dans les installations et vérifier, en observant et en parlant aux employés, si la surveillance exercée sur les zones à accès restreint est conforme aux procédures.

17.2.6 Lorsque des gardes de sécurité sont employés dans les installations, déterminer les directives et la formation qu'ils ont reçues. Vérifier s'ils ont reçu des consignes de poste écrites approuvées par l'ASM.

17.2.7 Lorsque l'accès aux installations ou aux zones à accès restreint est contrôlé ou surveillé au moyen de dispositifs électroniques, demander aux employés qui utilisent le matériel de confirmer qu'ils en connaissent bien le fonctionnement.

17.2.8 Vérifier si des procédures ont été mises en œuvre quant aux mesures à prendre en cas d'atteinte à l'intégrité d'un système de contrôle.

17.2.9 Vérifier si l'ASM dispose d'un processus de surveillance pour garantir la conformité aux procédures de contrôle d'accès.

Critère n^{o} 17.3 Les renseignements de nature délicate sont conservés dans les coffres appropriés, énumérés dans le *Guide de l'équipement de sécurité*. (Il y a exception lorsque la quantité de renseignements et de biens est telle qu'il est nécessaire d'utiliser une zone à accès restreint à cette fin).

Procédés de vérification

17.3.1 Obtenir une vue d'ensemble des pratiques et procédures mises en œuvre pour la conservation des renseignements de nature délicate lorsqu'ils ne sont pas utilisés. Vérifier si ces procédures sont mises à la disposition de tous les employés. Vérifier si les employés sont informés du niveau de sécurité le plus élevé des renseignements de nature délicate qui peuvent être conservés dans les coffres de sécurité auxquels ils ont accès.

17.3.2 Vérifier si l'ASM dispose d'un processus pour faire en sorte que la conservation des renseignements et des biens de nature délicate se fasse conformément à la politique et aux procédures ou si les exceptions ont été évaluées comme il se doit.

17.3.3 Examiner une installation de gestion des documents et d'autres installations et, par des entrevues et des observations, vérifier :

- si les renseignements de nature délicate sont conservés dans des coffres de sécurité adaptés aux zones où ils sont placés;
- si les gestionnaires et les employés connaissent le plus haut niveau de sécurité des renseignements de nature délicate qui peuvent être conservés dans les coffres de sécurité utilisés dans leur installation.

Critère n^{o} 17.4 Les renseignements et les biens de nature délicate sont transportés et transmis selon les normes.

Procédés de vérification

17.4.1 Obtenir une vue d'ensemble des pratiques, politiques et procédures mises en œuvre pour le transport et la transmission de renseignements de nature délicate, qui figurent habituellement dans le *Guide de classification de l'information*; lorsque le ministère n'a pas de guide, on peut consulter les normes opérationnelles de sécurité du Secrétariat.

17.4.2 Choisir des installations de gestion des documents et vérifier si elles respectent les normes du ministère ou du Secrétariat.

Critère n° 17.5 Les renseignements de nature délicate sont détruits au moyen des appareils figurant dans le *Guide d'équipement de sécurité* (sauf les documents contenant des renseignements désignés de nature peu délicate qui peuvent être déchiquetés à la main).

Procédés de vérification

17.5.1 Obtenir une vue d'ensemble des pratiques et procédures mises en œuvre pour la destruction des renseignements de nature délicate. Les examiner et vérifier si elles sont suffisamment exhaustives et complètes.

17.5.2 Interroger les employés afin de déterminer s'ils connaissent et suivent la procédure requise pour la destruction des renseignements de nature délicate.

17.5.3 Vérifier si tous les appareils de destruction figurent dans le *Guide de l'équipement de sécurité*. Si tel n'est pas le cas, vérifier si l'ASM a approuvé l'utilisation des autres appareils.

17.5.4 Vérifier si des procédures ont été mises en vigueur relativement à l'entretien du matériel utilisé pour détruire des renseignements de nature délicate et des biens de valeur. Sélectionner des appareils et vérifier si le processus est suivi.

Critère n° 17.6 Les biens de nature délicate sont contrôlés et protégés à toutes les étapes de leur cycle de vie.

Procédés de vérification

17.6.1 Obtenir une vue d'ensemble des pratiques et procédures mises en œuvre pour assurer le contrôle et la protection des biens de nature délicate, à partir de leur acquisition jusqu'à leur élimination.

17.6.2 Obtenir des listes où figurent les différents types de biens de nature délicate, tels les ordinateurs portables, les agendas électroniques, les assistants numériques, les appareils BlackBerry et les téléphones cellulaires. Examiner les mesures particulières de contrôle et de protection qui s'appliquent à ces biens entre le moment où ils sont achetés et celui où ils sont éliminés. Choisir un échantillon d'articles afin de vérifier s'ils existent et si les listes sont complètes.

17.6.3 Vérifier s'il existe un processus pour examiner les mesures de protection et les contrôles mis en vigueur lorsque des biens de nature délicate sont perdus, volés ou vandalisés, et pour réaliser une étude d'impact.

17.6.4 Déterminer les incidents qui se sont traduits par la perte, le vol ou le saccage de biens de nature délicate et examiner les mesures de protection et les contrôles qui étaient appliqués au moment où les incidents se sont produits ainsi que les mesures qui ont été prises pour réduire les risques à l'avenir.

Critère n^{o} 17.7 Des mesures de protection appropriées sont adoptées pour assurer la sécurité matérielle.

Procédés de vérification

17.7.1 Vérifier les mesures de protection utilisées aux points d'accès de l'installation, par exemple :

- les barrières physiques;
- les écrans acoustiques;
- les fils-pièges;
- les systèmes de détection par rupture des faisceaux infra-rouges/photoélectriques;
- les détecteurs magnétiques;
- les détecteurs thermiques;
- les détecteurs de capacité;
- autres (préciser).

17.7.2 Vérifier si des moniteurs (télévisions en circuit fermé, dispositifs de surveillance, etc.) et des dispositifs d'alarme sont installés aux principaux points d'accès.

17.7.3 Vérifier si les registres d'accès électroniques sont examinés périodiquement afin de déceler les activités inhabituelles. Déterminer qui procède à l'examen et si les résultats sont communiqués à l'ASM.

17.7.4 Vérifier si les clés et les jetons font l'objet d'un contrôle adéquat. Sait-on où sont toutes les clés, les cartes magnétiques et les cartes de proximité? Les clés de rechange, les cartes magnétiques et les cartes de proximité sont-elles toutes sécurisées dans un lieu à accès restreint? Tient-on un registre indiquant l'entrée et la sortie des clés, des cartes magnétiques et des cartes de proximité? Vérifier l'efficacité du processus et comment son application est vérifiée.

17.7.5 Vérifier si les combinaisons des chambres fortes et des classeurs à tiroirs protégés sont gardées confidentielles. Vérifier s'il existe une norme à cet effet. Change-t-on les combinaisons :

- lorsque quelqu'un qui connaît la combinaison quitte le ministère;

- tous les six mois;
- lorsqu'on soupçonne une atteinte à l'intégrité?

17.7.6 Vérifier si les listes d'autorisations logiques et matérielles et les mécanismes de contrôles donnant accès à l'installation sont mis à jour lorsque l'autorisation d'une personne est révoquée.

17.7.7 Vérifier si les mesures de sécurité matérielle suivantes sont appliquées et justifiées par des exigences de sécurité de base ou par une EMR :

- L'éclairage du périmètre est suffisant pour observer les lieux et pour assurer la sécurité des employés. Vérifier s'il y a une alimentation d'appoint pour l'éclairage du périmètre et des principaux points d'entrée.
- Toutes les fenêtres au rez-de-chaussée sont fixes ou peuvent être verrouillées à l'aide d'une quincaillerie de qualité industrielle.
- Toutes les ouvertures du périmètre sont protégées contre les entrées non autorisées.
- Des panneaux de mise en garde lisibles à une distance moyenne sont installés adéquatement à tous les 100 pieds environ.
- L'alimentation de secours est suffisante pour assurer la sécurité des employés en cas d'évacuation (p. ex. service partiel d'ascenseur et éclairage d'urgence).

Objectif n° 18

Des zones de sécurité matérielle de plus en plus restrictives sont établies et maintenues, ainsi que des mécanismes permettant de contrôler l'accès aux renseignements et aux biens de nature délicate (article 10.11 de la PGS).

Procédés de vérification

18.1.1 Obtenir une vue d'ensemble des pratiques et procédures touchant les zones de sécurité et les mesures et procédures de contrôle d'accès visant à créer des zones d'accueil, de réception et de travail, ainsi que des zones de sécurité et de haute sécurité dans les installations. Vérifier si ces mesures sont fondées sur les résultats d'une EMR. Déterminer de quelle façon l'ASM s'assure que les zones appropriées sont créées et maintenues et comment il évalue le caractère raisonnable des pratiques en vigueur.

18.1.2 Vérifier si les limites de sécurité sont bien définies et si les dessins, esquisses, plans ou schémas des installations sont à jour et faciles à obtenir, notamment en ce qui concerne :

- le périmètre des installations;
- la topographie des installations;
- les barrières du périmètre;
- les installations voisines;
- les points d'entrée et de sortie;
- la chaussée dans l'installation et à l'extérieur;
- l'emplacement des installations;
- les espaces de rangement;
- l'emplacement du matériel d'urgence et les points de rendez-vous en cas d'évacuation;
- l'emplacement des portes, fenêtres et ouvertures semblables;
- la disposition et les diagrammes des dispositifs d'alarme (schémas).

18.1.3 Évaluer l'emplacement des zones connexes et des zones de commodités (garderies, cafétérias, aires de repos, salles de réunion, etc.) afin de déterminer si elles sont situées à distance des zones de travail ou des zones sensibles.

Objectif n° 19

Les mesures de protection matérielles sont constamment examinées afin de tenir compte de l'évolution du contexte de la menace et de tirer avantage des économies qui peuvent être réalisées grâce aux nouvelles technologies (article 10.11 de la PGS).

Procédés de vérification

19.1.1 Déterminer qui est responsable de mener l'examen continu. Comment les résultats sont-ils communiqués à l'ASM? Quelle latitude l'ASM a-t-il pour modifier les mesures de protection de la sécurité matérielle en fonction de l'évolution de la menace et des nouvelles technologies?

19.1.2 Déterminer le processus mis en œuvre pour mener des consultations et des inspections de sécurité dans les installations. Vérifier si l'ASM reçoit les résultats de toutes les inspections de sécurité.

19.1.3 Déterminer quelles consultations et inspections de sécurité ont été menées au ministère au cours des deux dernières années et vérifier si l'ASM a donné suite aux recommandations (ou si les raisons de ne pas y donner suite ont été consignées). Vérifier si les arguments invoqués pour ne pas donner suite aux recommandations ont été approuvés par la haute direction.

19.1.4 Déterminer le processus mis en œuvre par l'ASM pour réaliser des examens internes des mesures de protection matérielle aux installations, ainsi que toute autre consultation ou inspection réglementaire.

SÉCURITÉ DU PERSONNEL

Objectif n° 20

Toutes les personnes qui ont accès aux biens du gouvernement (à l'exception des personnes nommées par le gouverneur en conseil) doivent avoir à tout le moins une cote de fiabilité (article 10.9 de la PGS).

Critère n° 20.1 Les contrôles nécessaires sont autorisés, acceptés et terminés avant l'entrée en fonction des titulaires

Procédés de vérification

20.1.1 Examiner des dossiers correspondant à différents types et niveaux de contrôle de sécurité du personnel et vérifier :

- si le formulaire Demande d'enquête de sécurité sur le personnel et autorisation a été rempli et si les contrôles obligatoires et facultatifs ont été versés au dossier comme il se doit;
- si les contrôles ont été acceptés par les personnes ou par leurs parents ou tuteurs si elles ne sont pas majeures;
- si les contrôles ont été effectués et si le type et le niveau de sécurité requis ont été autorisés avant l'entrée en fonction des titulaires;
- si les personnes ont signé le formulaire Certificat d'enquête de sécurité et profil de sécurité.

20.1.2 Examiner les dossiers des postes nécessitant une cote de sécurité et s'assurer que les exigences relatives aux enquêtes de sécurité préalables ont été satisfaites avant de procéder à l'évaluation de sécurité.

20.1.3 Vérifier si une cote de sécurité a été attribuée à chaque poste du ministère et si un processus est en vigueur pour confirmer qu'aucun employé ne peut accéder à des renseignements de nature délicate ou à des biens de valeur sans avoir satisfait aux exigences relatives à l'accès restreint.

Critère n^{o} 20.2 Les employés qui ont des rapports avec le ministère possèdent la cote de sécurité requise.

Procédés de vérification

20.2.1 Vérifier si les fonctionnaires qui ont accès aux installations ont fait l'objet, à tout le moins, d'une vérification de base de la fiabilité.

20.2.2 Vérifier si les employés qui ont accès à des renseignements classifiés ont obtenu une autorisation de sécurité et si les employés ayant accès à des renseignements classifiés PROTÉGÉ ont fait l'objet d'une vérification approfondie de la fiabilité.

20.2.3 Vérifier, à partir d'un échantillon, si les employés sont informés de leur cote de sécurité et si cette cote est à jour.

Objectif n° 21

Les enquêtes de sécurité sur les personnes sont menées conformément à la PGS et à la Norme sur la sécurité du personnel (article 10.9 de la PGS).

Critère n° 21.1 Le programme de contrôle de sécurité du ministère est conforme à la PGS et à la Norme sur la sécurité du personnel.

Procédés de vérification

21.1.1 Obtenir une vue d'ensemble des pratiques et procédures adoptées relativement au processus de contrôle de la sécurité et aux vérifications nécessaires pour chaque type et niveau de contrôle. Vérifier si l'ASM les a examinées et approuvées.

21.1.2 Examiner la politique et les procédures et vérifier si elles sont conformes à la PGS et à la Norme sur la sécurité du personnel.

21.1.3 Interroger les gestionnaires et le personnel responsable de la dotation afin de vérifier s'ils connaissent bien le processus de contrôle de sécurité, notamment le fait que les employés doivent obtenir une attestation de sécurité pour être à l'emploi du gouvernement, et les autorisations de sécurité exigées pour certains postes au ministère.

Critère n° 21.2 L'enquête de sécurité nécessaire pour remplir des postes est définie et documentée.

Procédés de vérification

21.2.1 Examiner une ventilation en pourcentage des types et niveaux d'enquêtes de sécurité autorisées pour les employés et déterminer si les pourcentages semblent raisonnables compte tenu du mandat du ministère, des types et des quantités de renseignements de nature délicate et de biens de valeur détenus. Si quelque chose semble anormal, parler de la question avec l'ASM et voir s'il y a une explication raisonnable à ce sujet.

21.2.2 Interroger les gestionnaires afin de déterminer comment ils prennent des décisions sur le type et le niveau d'enquête de sécurité requis pour un poste.

21.2.3 Examiner des formules de mesure de classification, ou un autre formulaire semblable en usage, et vérifier si le type et le niveau d'enquête de sécurité y ont été consignés.

21.2.4 Interroger les titulaires de postes et déterminer le plus haut niveau de renseignements de nature délicate dont ils prennent connaissance et à quelle fréquence. Déterminer si cette situation correspond au type et au niveau d'enquête de sécurité qui ont été autorisés pour ces personnes. Vérifier, au moyen d'entrevues, si elles comprennent leurs responsabilités

en ce qui concerne la protection des renseignements de nature délicate qui leur sont confiés.

Critère n^{o} 21.3 Il existe un processus pour hausser et mettre à jour la cote de fiabilité approfondie et la cote de sécurité des personnes au besoin.

Procédés de vérification

21.3.1 Déterminer s'il existe un dossier centralisé des types et niveaux d'enquêtes de sécurité autorisées pour les employés et d'autres personnes travaillant au ministère, ainsi que la date à laquelle ces enquêtes ont été autorisées. Vérifier si ce dossier est mis à la disposition de l'ASM.

21.3.2 Déterminer si les procédures s'appliquent au processus visant à hausser et à mettre à jour la cote de fiabilité et la cote de sécurité et si elles sont conformes à la PGS et à la Norme de sécurité du personnel.

21.3.3 Examiner les dossiers pour les postes où le type et le niveau d'enquête de sécurité ont été haussés et s'assurer que les vérifications nécessaires ont été faites.

Critère n^{o} 21.4 Le ministère informe par écrit les personnes dont la cote de fiabilité ou de sécurité est refusée ou révoquée de leurs droits à une révision ou à des mesures de redressement.

Procédés de vérification

21.4.1 Vérifier si des procédures ont été mises en œuvre afin que les personnes dont la cote de fiabilité ou de sécurité a été refusée ou révoquée en soient informées par écrit et déterminer comment ce processus peut être amorcé.

21.4.2 Examiner les dossiers relatifs aux cotes de fiabilité et aux cotes de sécurité qui ont été refusées ou révoquées au cours des deux dernières années et vérifier si les personnes concernées ont été informées par écrit de leur droit à une révision ou à des mesures de redressement.

Critère n^{o} 21.5 Les documents dans un dossier de sécurité du personnel sont transférés et détruits conformément à la PGS et à la *Norme de sécurité du personnel*.

Procédés de vérification

21.5.1 Obtenir une vue d'ensemble des pratiques et procédures mises en œuvre pour le traitement des documents relatifs à la mutation dans un autre ministère, au départ à la retraite ou à la cessation d'emploi d'un employé dans un dossier de sécurité du personnel.

Vérifier les exigences particulières relatives aux casiers judiciaires ou aux autres renseignements défavorables.

21.5.2 Comparer les pratiques en vigueur et les évaluer en fonction de la PGS et de la *Loi sur les Archives nationales du Canada* afin de déterminer :

- si les renseignements défavorables sont retirés des dossiers et détruits lorsque les dossiers sont transférés à un autre ministère, sauf dans les cas où les renseignements sont encore valables et utiles;
- si l'ASM conseille la haute direction en ce qui a trait aux renseignements qui doivent être retirés des dossiers du personnel;
- si les dossiers d'enquêtes de sécurité reçus par un ministère et portant sur un employé qui y est affecté ou détaché doivent être détruits lorsque la mutation n'a pas lieu ou lorsque l'affectation ou le détachement est terminé;
- si les documents d'enquête de sécurité des employés partis à la retraite ou ayant quitté leur emploi sont détruits conformément au calendrier de conservation et d'élimination de la *Loi sur les Archives nationales du Canada*.

Objectif n^{o} 22

Lorsqu'une personne quitte son emploi, des mesures doivent être prises afin de réduire ou d'éliminer tout risque pour les renseignements, les systèmes et les biens de nature délicate ou pour le personnel du ministère (implicite dans l'article 10.9 de la PGS).

Procédés de vérification

22.1.1 Obtenir une vue d'ensemble des pratiques et procédures mises en œuvre relativement au processus à suivre lorsqu'il a été décidé de mettre fin à l'emploi d'une personne. Vérifier si le processus prévoit :

- la récupération de tous les articles de sécurité matérielle, comme les cartes d'identité, les insignes d'accès, les clés et les cadenas;
- la modification des combinaisons que connaît la personne et la suppression des autorisations dans les systèmes électroniques;
- la consignation dans un document écrit du fait que ces mesures ont été prises et l'envoi de ce document à l'ASM.

22.1.2 Examiner les dossiers de personnes dont l'emploi a pris fin et s'assurer que la politique et les procédures ont été suivies.

22.1.3 Déterminer si la politique et les procédures exigent que, lorsqu'une personne perd son emploi avec motif, elle doit immédiatement quitter les lieux où elle peut poser une menace pour les renseignements et les biens de nature délicate, ou les systèmes essentiels du ministère. Vérifier si des mesures sont prises afin que la personne puisse récupérer plus tard ses effets personnels en étant accompagnée d'un employé du ministère.

PROTECTION DES EMPLOYÉS

Objectif n° 23

Une évaluation de la menace et des risques (EMR) a été menée afin de déterminer les situations où les employés sont menacés de violence en raison de leurs fonctions ou à cause des situations auxquelles ils sont exposés (article 10.10 de la PGS).

Procédés de vérification

23.1.1 Vérifier si des scénarios de menaces touchant la sécurité des employés ont été élaborés et évalués dans le cadre du processus permanent d'évaluation de la menace et des risques au ministère.

23.1.2 Vérifier le processus de surveillance de la sécurité mis en place par l'ASM afin de contrôler les incidents touchant la sûreté et la sécurité des employés et examiner la pertinence des mesures de protection qui ont été prises dans des installations où des incidents se sont produits.

23.1.3 Examiner les rapports sur les incidents touchant la sécurité et la protection des employés qui se sont produits au cours des deux dernières années. Déterminer les mesures de protection qui étaient en vigueur au moment où les incidents se sont produits, les recommandations visant à éviter d'autres incidents et les changements apportés en réponse aux recommandations. Si rien n'a été fait, évaluer les raisons données à l'appui de cette décision et vérifier si elles ont été approuvées par l'ASM ou par la haute direction.

Objectif n° 24

Des mécanismes sont en vigueur afin d'identifier, de protéger et d'appuyer les employés (et leurs familles, le cas échéant) menacés de violence ou travaillant dans des secteurs à risque élevé (article 10.10 de la PGS).

Critère n° 24.1 Des politiques et des procédures ont été mises en œuvre et des normes ont été élaborées afin d'assurer la sûreté et la sécurité des employés qui travaillent dans des secteurs à risque élevé.

Procédés de vérification

24.1.1 Examiner la politique, les procédures et les normes et vérifier si elles sont complètes et exhaustives en ce qui a trait à la protection des employés.

24.1.2 Vérifier si les responsabilités de tous les gestionnaires relativement à la santé et à la sécurité des employés au travail sont consignées par écrit et disponibles.

24.1.3 Vérifier si des procédures ont été établies et si des normes ont été élaborées pour assurer la sûreté et la sécurité des employés travaillant dans des secteurs à risque élevé.

Critère n° 24.2 Les situations dangereuses ou pouvant devenir violentes ont été déterminées et des mesures ont été prises dans le but d'atténuer les risques.

Procédés de vérification

24.2.1 Vérifier si les classifications et les postes qui peuvent présenter un danger pour la santé et la sécurité des employés ont été recensés; le cas échéant, vérifier si les types de danger sont mentionnés dans les descriptions de travail.

24.2.2 Vérifier si le ministère a un programme de protection des cadres supérieurs et, le cas échéant, les personnes qui sont protégées en vertu de ce programme (dresser la liste des noms et des postes). Vérifier si le programme s'étend aux membres de la famille.

24.2.3 Vérifier à qui sont confiées les fonctions liées à la protection des cadres supérieurs (dresser la liste des noms et des fonctions). Déterminer le nombre d'employés qui s'acquittent de ces fonctions. Vérifier si des critères d'embauche ont été élaborés pour le personnel affecté à ces fonctions, p. ex. une enquête sur les antécédents, le niveau de formation et l'expérience.

24.2.4 Vérifier si les employés dont les postes ont été désignés comme pouvant devenir dangereux ont reçu des séances de formation initiales et périodiques sur la santé et la

sécurité au travail (SST). Vérifier si les séances d'information sont données séparément ou dans le cadre du programme de sécurité ministériel. Déterminer si l'ASM participe à la supervision ou à la prestation des cours sur la SST.

24.2.5 Vérifier si les employés sont encouragés à signaler tous les incidents violents qu'ils subissent ou dont ils sont témoins. Déterminer s'il existe une politique de « tolérance zéro » en matière de violence au travail.

24.2.6 Vérifier si tous les incidents signalés font rapidement l'objet d'une enquête et si la direction, les responsables des ressources humaines, l'ASM et les autorités policières en sont informés, le cas échéant.

24.2.7 Existe-t-il un processus officiel ou officieux pour décider de faire appel aux autorités policières? Qui participe au processus décisionnel (la haute direction, l'ASM, les responsables des ressources humaines, les représentants syndicaux, etc.)?

24.2.8 Au moyen d'un échantillon d'incidents, vérifier si des documents exhaustifs sont préparés pour tous les incidents signalés. Qui conserve ces documents (Ressources humaines, ASM, etc.)? Vérifier si un rapport annuel à la haute direction est exigé et préparé.

Critère n^{o} 24.3 Les victimes de violence professionnelle ou de violence au travail obtiennent des services-conseils et du soutien.

Procédés de vérification

24.3.1 Vérifier s'il y a un programme en vigueur pour offrir des services-conseils et du soutien aux employés qui ont été victimes de violence et à leurs familles.

24.3.2 Déterminer comment les dispositions relatives aux services-conseils sont prises. Les services sont-ils offerts automatiquement dans le cadre d'un processus administratif ou faut-il en faire la demande? Vérifier si les pratiques en vigueur permettent d'offrir les services rapidement à la suite d'un incident.

SÉCURITÉ ET GESTION DES CAS D'URGENCE

Le Programme relatif au plan de poursuite des activités complète la protection civile qui est requise par des textes législatifs ou une politique gouvernementale (*Normes de sécurité opérationnelle, Programme relatif au plan de poursuite des activités, Préambule*).

Objectif n° 25

Les gestionnaires des installations du ministère ont pris les mesures nécessaires pour assurer la protection des renseignements et des biens de nature délicate et celle des employés pendant tous les cas d'urgence et de menace accrue (article 10.14 de la PGS).

Critère n° 25.1 Les gestionnaires des installations ont élaboré et documenté des plans pour réagir à divers cas d'urgence.

Procédés de vérification

25.1.1 Vérifier si des directives ont été mises en vigueur pour l'élaboration de plans par les gestionnaires visant à fournir des services essentiels et à protéger des biens connexes pendant les situations qui causent des perturbations.[12]

25.1.2 Vérifier si des plans d'urgence et d'intervention ont été élaborés pour chaque installation et si un point de contact a été prévu pour chacune. Déterminer les moyens utilisés pour faire en sorte que les plans soient harmonisés et gardés à jour.

25.1.3 Déterminer quel processus l'ASM a mis en place pour confirmer que les plans sont à jour, logiques, exhaustifs et complets.

25.1.4 Examiner un échantillon des plans de certaines installations et déterminer s'ils sont raisonnables, exhaustifs et complets.

Critère n° 25.2 Les plans de mesures d'urgence sont tenus à jour et mis à l'essai.

Procédés de vérification

25.2.1 Vérifier si des directives ont été émises pour la mise à jour régulière des plans en cas d'urgence et la fréquence à laquelle ils doivent être mis à l'essai, et pour déterminer s'il s'agit d'essais en situation réelle ou d'essais théoriques, ou les deux. De quel processus l'ASM dispose-t-il pour s'assurer que les essais ont lieu?

[12] Il peut s'agir notamment d'incendies, d'alertes à la bombe, de désastres environnementaux, d'agressions contre les employés, de manifestations, mais aussi d'autres situations.

25.2.2 Vérifier s'il existe des procédures pour permettre au personnel affecté aux urgences d'accéder aux installations en cas d'incendie ou de panne d'électricité majeure ou dans d'autres cas d'urgence ou de catastrophe.

25.2.3 Vérifier si un processus permet de garantir que le souci du détail augmente lorsque les mesures de sécurité sont resserrées. Procède-t-on à des vérifications plus fréquentes dans les installations et contrôle-t-on plus rigoureusement les visiteurs et les entrepreneurs? Vérifier les résultats des essais.

25.2.4 Vérifier s'il existe des plans et des procédures pour l'établissement et le fonctionnement d'un centre des opérations d'urgence. Vérifier s'il a été décidé d'ouvrir un tel centre (qui a pris la décision) et si l'ASM a été consulté.

25.2.5 Vérifier si le personnel du centre des opérations d'urgence a reçu une formation adéquate. Examiner la nature de la formation qu'il a reçue.

25.2.6 À l'aide d'un échantillon, faire des essais afin de déterminer si les listes de rappel au travail des employés du centre des opérations d'urgence sont à jour.

Critère n^{o} 25.3 Il existe un processus pour assurer la coordination des principaux services de sécurité (sécurité ministérielle, sécurité des TI, planification de la poursuite des activités, santé et sécurité au travail, etc.) en vue de resserrer les mesures de sécurité, sous la direction de l'ASM.

Procédés de vérification

25.3.1 Vérifier s'il existe des rapports hiérarchiques de communication entre la haute direction et l'ASM en vue d'ordonner le resserrement des mesures de sécurité. Vérifier si ces rapports sont officiels ou officieux et si l'ASM siège au comité des cadres supérieurs responsables des mesures d'urgence.

25.3.2 Vérifier s'il existe des rapports hiérarchiques entre l'ASM et les principaux responsables de la sécurité en vue d'ordonner le resserrement des mesures de sécurité. Existe-t-il un comité chargé de planifier les mesures de sécurité en cas d'urgence? L'ASM siège-t-il à ce comité?

25.3.3 Vérifier si le plan prévoit un resserrement partiel des mesures de sécurité. Identifier le principal coordonnateur de ce plan s'il ne s'agit pas de l'ASM.

25.3.4 Identifier la personne à contacter lorsque les mesures de sécurité sont resserrées sur ordre du gouvernement.

Objectif n° 26

Des plans sont élaborés afin d'assurer la poursuite des activités, des services et des biens essentiels à l'échelle du ministère après une interruption imprévue (article 10.4 de la PGS).

Critère n° 26.1 Le ministère dispose d'un programme de poursuite des activités (PPA) efficace.

Procédés de vérification

26.1.1 Obtenir une vue d'ensemble du PPA et des activités de planification et de surveillance.

26.1.2 Examiner les directives stratégiques et fonctionnelles afin de vérifier si le programme :

- Met en valeur la responsabilisation et les responsabilités de l'ASM, notamment celle d'approuver les priorités en matière de poursuite et de rétablissement des activités;
- Désigne le coordonnateur du PPA en tant que champion du programme;
- Explique les rapports fonctionnels entre le coordonnateur du PPA et l'ASM;
- Décrit la structure ministérielle utilisée pour superviser, coordonner et surveiller l'élaboration et la mise à jour des PPA;
- Donne une orientation adéquate et pertinente en présentant une politique, des procédures et des directives connexes.

26.1.3 Interroger le coordonnateur du PPA et les membres des comités supérieurs concernés afin de vérifier si la diversité des points de vue est prise en compte. Examiner la représentation des fonctions suivantes dans la structure du programme :

- vérification;
- environnement;
- gestion financière;
- santé et sécurité au travail;
- services informatiques;
- activités de fonctionnement ministérielles;
- planification ministérielle;
- gestion du matériel;
- gestion des biens immobiliers et des installations;
- sécurité.

Critère n^{o} 26.2 Le ministère a élaboré des plans adéquats de poursuite des activités et ceux-ci sont bien documentés afin d'atténuer le risque de perturbation des fonctions essentielles.

Procédés de vérification

26.2.1 Vérifier si des politiques et procédures ont été mises en vigueur pour l'élaboration de PPA par les gestionnaires dans le but d'assurer la poursuite des activités essentielles.

26.2.2 Obtenir un résumé pour l'ensemble de l'organisation, dans la mesure du possible, et d'autres documents afin de déterminer si les problèmes du ministère y sont exposés avec exactitude et si le ministère est prêt à prendre des mesures prioritaires pour la poursuite et le rétablissement des activités. Déterminer si une analyse des répercussions sur les activités a été effectuée dans le but de vérifier et de classer par ordre de priorité les services et les biens essentiels du ministère.

26.2.3 Vérifier s'il existe un répertoire des services, activités et programmes essentiels du ministère. Déterminer qui en est responsable et la méthode officielle ou officieuse utilisée pour le mettre à jour. L'ASM est-il informé des modifications et des mises à jour? Interroger le fonctionnaire responsable du plan de poursuite des activités et vérifier s'il estime que toutes les activités essentielles ont été recensées.

26.2.4 Vérifier si des PPA ont été préparés pour toutes les activités et tous les systèmes essentiels à la mission. En examiner un échantillon afin de s'assurer qu'ils sont complets, exhaustifs et logiques.

Critère n^{o} 26.3 Les PPA sont examinés et mis à l'essai, puis vérifiés par l'ASM.

Procédés de vérification

26.3.1 Vérifier s'il existe un processus pour surveiller la mise en œuvre d'un PPA, notamment l'élaboration et la mise à jour d'un plan adapté aux besoins de chaque site.

26.3.2 Vérifier s'il existe des directives pour la mise à jour des PPA, la fréquence recommandée des essais et la méthode utilisée (p. ex. essais en situation réelle ou essais théoriques, ou les deux).

26.3.3 Choisir des PPA et vérifier s'ils font l'objet de mises à jour et d'essais périodiques.

26.2.4 Obtenir un exemplaire d'un rapport d'étape récent préparé à l'intention de la haute direction. Vérifier l'exactitude et l'exhaustivité de l'information en comparant le rapport à l'échantillon mis à l'essai précédemment.

SÉCURITÉ ET GESTION DES MARCHÉS

Objectif n° 27

Les exigences de sécurité relatives à la protection des renseignements, des biens et du personnel sont respectées dans le processus de passation des marchés (article 10.4 de la PGS).

Critère n° 27.1 Les exigences de sécurité sont prises en compte dans la passation des marchés et elles sont décrites dans les documents remis aux entrepreneurs.

Procédés de vérification

27.1.1 Obtenir une vue d'ensemble de la façon de traiter les exigences de sécurité dans le processus de passation des marchés.

27.1.2 Examiner la politique et les procédures relatives aux exigences de sécurité dans les marchés qui nécessitent l'accès à des renseignements et à des biens de nature délicate, et vérifier si elles sont exhaustives et si elles s'appliquent aux demandes de marchés, aux appels d'offres, à la négociation, à l'adjudication, à l'évaluation du rendement et à la résiliation des marchés.

27.1.3 Vérifier si la politique établit que les marchés auxquels participent des entrepreneurs étrangers ayant accès à des renseignements ou à des biens de nature délicate détenus par le gouvernement du Canada ou qui comportent des renseignements de nature délicate détenus par un gouvernement étranger doivent être administrés par l'entremise de Travaux publics et Services gouvernementaux Canada (TPSGC).

27.1.4 Examiner un échantillon de marchés qui comportent des renseignements et des biens de nature délicate et vérifier si les exigences de sécurité nécessaires ont été incluses dans tous les documents.

Critère n^{o} 27.2 Des activités de surveillance sont prévues pour garantir le respect des exigences de sécurité à toutes les étapes du processus de passation des marchés.

Procédés de vérification

Dans les cas où TPSGC est l'autorité contractante

27.2.1 Vérifier si la politique et les procédures exigent l'utilisation d'une liste de vérification des exigences relatives à la sécurité (LVES) pour tous les marchés qui comportent des renseignements et des biens de nature délicate où TPSGC est l'autorité contractante.

27.2.2 Examiner un échantillon de marchés administrés par TPSGC et vérifier si les dossiers contiennent une LVES dûment remplie.

Dans les cas où le ministère est l'autorité contractante

27.2.3 Obtenir une vue d'ensemble des mesures prises pour confirmer que les entrepreneurs respectent les exigences de sécurité.

27.2.4 Vérifier si la politique explique dans quelles circonstances le ministère demande à TPSGC de s'assurer que les exigences de sécurité ont été respectées.

27.2.5 Examiner un échantillon de marchés dans lesquels le ministère a assumé la pleine responsabilité de veiller à ce que l'entrepreneur respecte les exigences de sécurité et vérifier :

- si la situation de l'entrepreneur a été vérifiée auprès de TPSGC au début du processus;
- si l'entrepreneur a commencé à exécuter le marché seulement après que les exigences de sécurité ont été respectées;
- si TPSGC a été avisé lorsque l'entrepreneur a respecté toutes les exigences de sécurité;
- si le fait que l'entrepreneur a respecté les exigences de sécurité est consigné au dossier.

27.2.6 Vérifier s'il existe des processus pour l'inspection périodique des lieux de travail des entrepreneurs, s'il y a lieu. Vérifier s'il existe un processus prévoyant que l'ASM doit coordonner les inspections et être informé des résultats.

Critère n^{o} 27.3 Tous les entrepreneurs sont assujettis au programme de sécurité ministériel.

Procédés de vérification

27.3.1 Vérifier s'il existe une liste à jour des entrepreneurs qui travaillent pour le compte du ministère. Déterminer si cette liste et la cote de sécurité (exigée et effective) de chaque entrepreneur sont mises à la disposition de l'ASM.

27.3.2 Vérifier si un processus est en vigueur pour aviser l'ASM que les entrepreneurs ont reçu les séances d'information nécessaires sur la sécurité et qu'ils ont accès au programme de sécurité ministériel et aux documents connexes.

27.3.3 Vérifier si un processus est en vigueur pour que l'ASM s'assure que les exigences de sécurité nécessaires sont incluses dans les conditions de tout document contractuel.

ANNEXE A—AUTORISATIONS ET RÉFÉRENCES

Le pouvoir relatif à la Politique du gouvernement sur la sécurité (PGS) découle d'une décision du gouvernement et de l'article 7 de la *Loi sur la gestion des finances publiques*.

http://lois.justice.gc.ca/fr/F-11/index.html

Les textes législatifs ayant un lien avec la Politique figurent à la section 13 de la PGS.

Politique et normes

Sécurité du gouvernement - Politique de 1er niveau et normes opérationnelles de 2e niveau
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/siglist_f.asp

Politiques et lignes directrices du gouvernement ayant un lien avec la PGS

Accès à l'information
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_121/siglist_f.asp

Politique sur l'autorisation et l'authentification électroniques
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TBM_142/2-2_f.asp

Politique sur les pertes de deniers et infractions et autres actes illégaux commis contre la Couronne
http://www.tbs-sct.gc.ca/Pubs_pol/dcgpubs/TBM_142/4-7_f.asp

Protection des renseignements personnels
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_f.asp

Politique sur la gestion des risques
http://www.tbs-sct.gc.ca/Pubs_pol/dcgpubs/RiskManagement/siglist_f.asp

Politique sur les marchés
http://www.tbs-sct.gc.ca/Pubs_pol/dcgpubs/contracting/siglist_f.asp

Sécurité du gouvernement - normes techniques et lignes directrices de 3e niveau pour la sécurité matérielle

Construction d'une aire protégée (DSS/GS-21), août 1988

Devis de construction de pièces sécuritaires de type C (DSS/GS-23), mars 1991

Devis de construction de pièces sécuritaires de type D (DSS/GS-22), mars 1991

Cloisons de protection pour cage d'escalier (DSS/GS-13), novembre 1987

Portes et cadres de porte (DSS/GS-16), mars 1985

Contrôles des accès, portes basculantes (DSS/GS-9), décembre 1981

Devis de construction d'une barrière pour échelle extérieure fixe (DSS/GS-8), août 1987

Vitrage (DSS/GS-11), février 1988

Guide pour la gestion des services d'agents de sécurité (DSS/GS-29), mai 1993

Guide des institutions locataires pour la préparation d'un énoncé de sécurité matérielle (DSS/GS-25), octobre 1992

Quincaillerie (DSS/GS-15), février 1985

Cartes d'identité/Cartes d'accès (DSS/GS-27), juin 1992

Les systèmes de clés maîtresses (DSS/GS-10), décembre 1981

Normes d'insonorisation des nouvelles constructions (DSS/GS-12), décembre 1986

Devis de construction de portes escamotables en plafond (DSS/GS-4), août 1987

Éléments du Code national du bâtiment qui intéressent la sécurité, 1980 (DSS/GS-14), septembre 1983

Éléments du Code national du bâtiment, 1985, qui intéressent la sécurité (DSS/GS-26), mars 1990

L'isolation acoustique (DSS/GS-3), janvier 1981

Besoins en espace des centres de surveillance (DSS/GS-7), juillet 1987

Sommaire de la conception sécuritaire pour les immeubles de la GRC (DSS/GS-18), août 1988

Guide de sécurité pour les immeubles à bureaux (DSS/GS-19), novembre 1987

Guide d'équipement de sécurité (DSS/GS-20), octobre 1992 (distribution limitée strictement aux ministères du gouvernement fédéral et non disponible électroniquement)

Éclairage de sécurité (DSS/GS-2), août 1987

Fermeture des édifices en cas d'urgence (clés maîtresses ou codes des serrures) (DSS/GS-28), mars 1991

Norme pour la transmission et le transport de renseignements et de biens de nature délicate (DSS/GS-30), juin 1994

Plafonds suspendus (DSS/GS-6), août 1987

Chambres fortes (DSS/GS-17), mars 1985

Panneaux d'usage courant et fonctionnels, Appendice A, Panneaux normalisés, *Manuel du Programme de coordination de l'image de marque*, Secrétariat du Conseil du Trésor, mars 1990

Lignes directrices relatives au traitement des incidents et à la protection des propriétés de DRH (Bulletin de sécurité n^{o} 92-1), Développement des ressources humaines Canada, 1992

Sécurité des employés et services au public, Développement des ressources humaines Canada, 1994

Approvisionnements d'articles en stock, catalogue publié par Travaux publics et Services gouvernementaux Canada (aucune date)

ANNEXE B—GLOSSAIRE

Accréditation *(accreditation)*—approbation donnée par le gestionnaire compétent en vue de l'exploitation d'un système de technologies de l'information avec un ensemble de mesures de protection.

Agent de sécurité du ministère *(departmental security officer)*—personne chargée d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller le programme ministériel de sécurité selon la *Politique du gouvernement sur la sécurité* et les normes opérationnelles.

Aire insonorisée *(sensitive discussion area)*—local spécialement conçu et géré pour prévenir l'écoute, électronique ou autre, de discussions portant sur des renseignements classifiés ou désignés.

Aires de service *(service spaces)*—aires telles les vestiaires, les toilettes, les cafétérias, les passages, les bureaux d'inscription, ainsi que les aires de service de l'immeuble telles les cabines téléphoniques et les placards pour l'électricité et le matériel de nettoyage.

Atteinte à l'intégrité *(compromise)*—situation résultant de la communication, de la destruction, de la suppression, de la modification ou de l'interruption non autorisée de renseignements ou de biens de nature délicate.

Autres gouvernements *(other governments)*—les gouvernements municipaux, régionaux, provinciaux, ainsi que ceux d'autres pays.

Avec motif *(for cause)*—terme indiquant la nécessité d'une enquête plus approfondie suivant les renseignements disponibles. Cette décision relève d'un ministère ou d'un organisme menant l'enquête dans les cas particuliers, ou conjointement pour certains groupes ou catégories.

Biens classifiés *(classified assets)*—tout bien matériel, autre qu'un renseignement, ayant une importance pour l'intérêt national et dont la protection est justifiée.

Biens de nature délicate *(sensitive assets)*—bien classifié ou désigné.

Biens désignés *(designated assets)*—tout bien matériel, autre que des renseignements, que le ministère a reconnu important pour ses activités en raison de son usage ou de sa valeur et qui mérite donc d'être protégé; par exemple, l'argent et tout effet négociable, et les technologies de l'information dont la protection est nécessaire pour garantir la confidentialité, l'intégrité et la disponibilité des renseignements qu'ils contiennent.

Bureau à aires ouvertes *(open-office area)*—bureau comportant de nombreux postes de travail qui ne sont séparés ni par des portes ni par des murs.

Carte d'identité *(identification card)*—document délivré par le ministère et servant à identifier le porteur en tant qu'employé de ce ministère.

Clé d'accès *(access key)*—méthode utilisée par un ministère pour autoriser une personne à franchir un point de contrôle d'accès à une installation ou dans une zone de sécurité, par exemple, les caractéristiques physiques, les connaissances de la personne ou un dispositif.

Coffre *(container)*—tout espace, y compris un classeur ou une pièce, utilisé pour ranger des renseignements ou des biens.

COMSEC *(COMSEC)*—protection résultant de l'application de mesures de sécurité cryptographique, de sécurité de la transmission et de sécurité d'émission aux télécommunications et au matériel d'acheminement des données ainsi que de l'application d'autres mesures pertinentes aux renseignements et au matériel visés par la COMSEC.

Confidentialité *(confidentiality)*—sensibilité des renseignements ou biens classifiés ou désignés à la communication non autorisée, dont la mention indique le préjudice qui pourrait être causé en cas de communication non autorisée.

Confidentiel *(confidential)*—niveau de classification des renseignements et biens lorsqu'une atteinte à l'intégrité est vraisemblablement susceptible de causer un préjudice à l'intérêt national; en majuscules, signe indiquant le niveau de sensibilité.

Conséquence *(consequence)*—résultat, effet; synonyme d'impact

Cote de fiabilité approfondie *(enhanced reliability status)*—type d'enquête de sécurité qui, en raison du besoin de savoir, est obligatoire pour l'accès aux renseignements et aux biens désignés.

Cote de fiabilité de base *(basic reliability status)*—type d'enquête de sécurité minimale; donne uniquement accès à des renseignements et à des biens de nature non délicate.

Cote de sécurité *(security clearance)*—type d'enquête de sécurité qui, en raison du besoin de savoir, est obligatoire pour l'accès aux renseignements et aux biens classifiés.

Cote de sécurité donnant accès aux sites *(site-access security clearance)*—type d'enquête de sécurité sur le personnel nécessaire dans certaines circonstances limitées et spécifiques lorsque certaines tâches exigent que l'employé ait accès, normalement durant de courtes périodes, à des lieux ou à des installations du gouvernement et non à des renseignements de nature délicate.

Déclassement *(downgrading)*—décision écrite de l'auteur des renseignements de nature délicate ou de tout autre agent autorisé par l'administrateur général ou responsable d'un organisme, d'abaisser le niveau de classification des renseignements ou de ne plus les considérer comme désignés.

Déclassification *(declassification)*—la décision écrite de l'auteur des renseignements classifiés ou d'un autre agent autorisé par l'administrateur général ou responsable d'un organisme, de ne plus considérer les renseignements comme classifiés.

Défense du Canada ou de tout État allié ou associé *(defence of Canada or any state allied or associated with Canada)*—les efforts déployés par le Canada ou des États étrangers pour découvrir, empêcher ou réprimer les activités d'un État étranger en vue d'attaquer réellement ou éventuellement le Canada ou l'un de ses États alliés ou associés, ou encore de commettre d'autres actes d'agression envers eux.

Disponibilité *(availability)*—état de ce qui est disponible sur demande pour soutenir les activités.

Données *(data)*—représentation de faits, de concepts ou d'instructions sous une forme convenant aux télécommunications, à l'interprétation ou au traitement par des personnes ou par des moyens automatisés.

Efficacité *(effectiveness)*—un terme utilisé en vérification de l'optimisation des ressources – qui a trait à l'atteinte des objectifs ou à la production d'autres effets voulus d'un programme, d'opérations ou d'activités.

Efficience *(efficiency)*—un terme utilisé en vérification de l'optimisation des ressources – qui a trait à l'utilisation de ressources financières, humaines et matérielles de manière à maximiser les intrants des ressources pour toute quantité donnée d'extrants.

Énoncé de la conception de la sécurité *(security design brief)*—description de la conception de la sécurité matérielle et de l'aménagement des zones à accès restreint élaborés en réponse à une évaluation de la menace et des risques.

Énoncé de la nature délicate *(statement of sensitivity)*—description des exigences quant au caractère confidentiel, à l'intégrité ou à la disponibilité des renseignements ou des biens stockés ou traités dans un système des technologies de l'information ou transmis par un tel système.

Énoncé de sécurité du site *(security site brief)*—document énumérant les qualités d'un site dont il faut tenir compte pour choisir l'emplacement d'une installation.

Équipement de sécurité *(security equipment)*—matériel qui a été évalué ou mis à l'essai par rapport à des normes élaborées par l'organisme conseil. Le *Guide de l'équipement de sécurité* énumère le matériel de sécurité devant être utilisé au gouvernement du Canada.

Évaluation de la menace *(threat assessment)*—évaluation de la nature, de la probabilité et de la conséquence d'actes ou d'événements qui pourraient mettre en péril des renseignements et des biens de nature délicate.

Évaluation des risques *(risk assessment)*—analyse de la probabilité que les points vulnérables puissent être exploités, compte tenu de l'efficacité des mesures de sécurité actuelles ou proposées.

Évaluation sécuritaire *(security assessment)*—évaluation d'une personne relativement à sa loyauté au Canada et à sa fiabilité dans ce contexte; condition préalable à l'obtention d'une cote de sécurité.

Garde de sécurité *(security guard)*—personne dont la tâche principale consiste à protéger des renseignements et des biens.

Guide de classification et désignation *(classification and designation guide)*—document interne, approuvé par l'administrateur général d'un ministère ou le chef d'un organisme, indiquant les types de renseignements devant être classifiés ou désignés.

Guide de désignation *(designation guide)*—voir « Guide de classification et de désignation ».

Heures d'accès limité *(limited-access hours)*—périodes en dehors des heures d'ouverture pendant lesquelles seules les personnes autorisées, normalement les employés et exceptionnellement les visiteurs autorisés, ont accès aux zones de réception et aux aires contrôlées.

Heures d'ouverture *(business hours)*—heures affichées pendant lesquelles les zones de réception sont accessibles au public et où toute personne autorisée ou visiteur peut avoir accès aux zones contrôlées.

Incident de sécurité *(security incident)*—infraction à la sécurité ou violation de la sécurité, ou tout autre événement ayant une incidence sur les mesures prises pour protéger des renseignements et des biens de nature délicate.

Infraction à la sécurité *(breach of security)*—toute atteinte, y compris une atteinte probable, à l'intégrité de renseignements et de biens de nature délicate.

Insigne d'accès *(access badge)*—document fourni par un ministère permettant d'indiquer la zone ou l'installation à laquelle le détenteur est autorisé à avoir accès.

Inspection de sécurité *(security inspection)*—vérification courante des lieux où des renseignements de nature délicate sont traités ou stockés par le personnel ou par des gardes de sécurité (sur place) à la fin des heures de travail habituelles.

Installation *(facility)*—désigne un aménagement physique qui sert à une fin précise. On entend par installation une partie ou la totalité d'un immeuble; soit un immeuble, son emplacement et ses alentours, ou encore une structure qui n'est pas un immeuble. Le terme désigne non seulement l'objet même mais aussi son usage.

Intégrité *(integrity)*—exactitude et intégralité des renseignements et des biens et authenticité des transactions.

Intérêt national *(national interest)*—s'entend de la protection et du maintien de la stabilité sociopolitique et économique du Canada.

Interruption *(interruption)*—non-disponibilité de renseignements, biens, systèmes ou services. L'interruption peut être accidentelle ou délibérée.

Lieu contrôlé *(controlled area)*—lieu réunissant un agencement quelconque des trois zones à accès restreint.

Manquement à la sécurité *(violation of security)*—tout acte ou omission qui contrevient à une disposition de la Politique sur la sécurité, notamment négliger de classifier ou de désigner des renseignements conformément à la Politique; classifier ou désigner des renseignements sans respecter la Politique ou maintenir une telle classification ou désignation; modifier, garder, détruire ou supprimer sans autorisation des renseignements de nature délicate, et interrompre sans autorisation leur transmission.

Menace *(threat)*—tout événement ou acte qui pourrait amener une ou plusieurs des situations suivantes à se produire : communication, destruction, suppression, modification ou interruption non autorisée de renseignements, de biens ou de services de nature délicate, ou encore un préjudice à des personnes. Une menace peut être volontaire ou accidentelle.

Ministère *(department)*—toute institution fédérale à laquelle s'applique la *Politique du gouvernement sur la sécurité*.

Ministères gardiens *(custodian departments)*—ministères chargés de l'administration d'une installation attribuée à d'autres ministères pour l'administration de programmes gouvernementaux.

Ministère tuteur *(sponsoring department)*—ministère qui demande au Conseil du Trésor d'approuver les objectifs et les dépenses d'un projet, et qui gère le projet.

Modification *(modification)*—le fait de modifier des renseignements, des données, des logiciels ou du matériel informatique, accidentellement ou volontairement.

Norme de sécurité *(security standard)*—niveau considéré comme une mesure suffisante; exigences et lignes directrices en matière de sécurité approuvées pour l'ensemble du gouvernement fédéral. (Les normes opérationnelles font partie du *Manuel du Conseil du Trésor*; les normes techniques proviennent des organismes-conseils en matière de sécurité.)

Organisations *(organizations)*—organisations non assujetties à la PGS, dont les organisations internationales comme l'Organisation du Traité de l'Atlantique Nord.

Organisme-conseil *(lead agency)*—organisme responsable à l'échelle du gouvernement de la Politique sur la sécurité, selon la définition qui figure dans la Politique.

Périmètre de sécurité *(secure perimeter)*—obstacles matériels ininterrompus qui peuvent vraisemblablement contrer des menaces anticipées.

Planification de la continuité opérationnelle *(business continuity planning)*—terme global s'appliquant notamment à l'élaboration et à l'exécution opportune de plans, de mesures, de procédures et de préparatifs afin d'éviter ou de minimiser tout arrêt de la disponibilité des services et des biens essentiels.

Planification des cas d'urgence *(contingency planning)*—processus d'élaboration d'un plan pour la reprise des activités des technologies de l'information en cas d'interruption.

Principe d'accès sélectif *(need-to-access principle)*—disposition permettant de limiter l'accès à certains endroits aux personnes qui doivent y travailler.

Principe de connaissance sélective *(need-to-know principle)*—disposition permettant de limiter la diffusion de renseignements aux personnes qui en ont besoin pour leur travail.

Processus de passation des marchés *(contracting process)*—invitation à soumissionner, négociation, adjudication, exécution et résiliation des marchés

***PROTÉGÉ** (PROTECTED)*—mention indiquant que les renseignements sont désignés et nécessitent plus qu'une protection de base.

***Rapport hiérarchique** (line reporting relationship)*—Rapport entre un subordonné et le gestionnaire de l'organisation à laquelle il appartient. En général, le gestionnaire a la responsabilité d'attribuer les travaux au subordonné, d'assurer son bien-être et son perfectionnement professionnel et d'évaluer son rendement.

***Rapport hiérarchique fonctionnel** (functional reporting relationship*—rapport hiérarchique entre un gestionnaire et un subordonné qui n'appartient *pas* à l'organisation du gestionnaire mais à qui celui-ci confie des fonctions spécifiques pour lesquelles le subordonné possède une expertise particulière. Ces fonctions de portée limitée comprennent habituellement la participation à des réunions, des groupes de travail et des comités ainsi que la communication systématique de statistiques. Un subordonné dans un rapport hiérarchique fonctionnel peut être assujetti à un rapport hiérarchique avec le gestionnaire d'une autre organisation en cas d'urgence ou de menace accrue.

***Renseignements classifiés** (classified information)*—renseignements liés à l'intérêt national qui pourraient faire l'objet d'une exception en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* et dont on peut croire que toute atteinte à leur intégrité pourrait porter préjudice à l'intérêt national.

***Renseignements de nature délicate** (sensitive information)*—renseignements classifiés ou désignés.

***Renseignements désignés** (designated information)*—renseignements non liés à l'intérêt national, qui sont de nature peu délicate, particulièrement délicate ou extrêmement délicate et qui pourraient faire l'objet d'une exception ou d'une exemption en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*.

***Renseignements désignés de nature extrêmement délicate** (extremely sensitive, designated information)*—sous-catégorie de renseignements désignés pouvant vraisemblablement causer un très grave préjudice entraînant même la mort, s'il y avait atteinte à leur intégrité; peuvent porter la mention PROTÉGÉ C

***Renseignements désignés de nature particulièrement délicate** (particularly sensitive, designated information)*—sous-catégorie de renseignements désignés qui pourraient vraisemblablement causer un sérieux préjudice s'il y avait atteinte à leur intégrité; peuvent porter la mention PROTÉGÉ B.

Renseignements désignés de nature peu délicate *(low-sensitive, designated information)*—sous-catégorie de renseignements désignés qui pourraient vraisemblablement causer un préjudice s'il y avait atteinte à leur intégrité; peuvent porter la mention PROTÉGÉ A.

Renseignements détenus *(information holdings)*—renseignements qu'un ministère a en sa possession, peu importe l'objet matériel dans lequel les renseignements sont stockés. Cette définition ne tient pas compte du matériel conservé par les bibliothèques du gouvernement fédéral, qui n'a pas été préparé ou fabriqué par ou pour des gouvernements.

Renseignements personnels *(personal information)*—toute forme de renseignements consignés au sujet d'une personne donnée. Voir l'art. 3 de la *Loi sur la protection des renseignements personnels* pour une liste d'exemples. La Loi indique également quelques exceptions à la définition. Les renseignements personnels, une sous-catégorie des autres renseignements de nature délicate, méritent une protection accrue et peuvent porter la mention : « PROTÉGÉ-Renseignements personnels ».

Risque *(risk)*—i) possibilité que des points vulnérables soient exploités; ii) incertitude.

Secret *(secret)*—niveau de classification attribué aux renseignements ou biens lorsque toute atteinte à leur intégrité risquerait vraisemblablement de porter un sérieux préjudice à l'intérêt national.

Sécurité des technologies de l'information *(information technology security)*—protection résultant d'une série de mesures de protection intégrées visant à protéger la confidentialité de renseignements stockés, traités ou transmis par voie électronique, l'intégrité des renseignements et des processus connexes, et la disponibilité des systèmes et des services.

Sécurité matérielle *(physical security)*—mécanismes de protection, de détection et de réaction utilisés sur place afin de contrôler l'accès aux renseignements et aux biens de nature délicate.

Suppression *(removal)*—perte de renseignements ou de biens qui peut être accidentelle, par exemple, lorsqu'ils sont jetés avec les rebuts, ou délibérée, dans le cas d'un vol.

Surveiller *(monitor)*—faire en sorte que les renseignements et les biens, ou les mesures de protection les protégeant, soient vérifiés par le personnel qui en est responsable, par le personnel de sécurité ou par des moyens électroniques, à intervalles assez fréquents, d'après l'évaluation de la menace et des risques.

Très secret *(top secret)*—niveau de classification attribué aux renseignements ou aux biens lorsque toute atteinte à leur intégrité risquerait vraisemblablement de causer un préjudice exceptionnellement grave à l'intérêt national.

Valeur *(value)*—coût approximatif

Vérification approfondie de la fiabilité *(enhanced reliability check)*—évaluation de l'intégrité d'une personne; condition pour obtenir la cote de fiabilité approfondie.

Vérification de base de la fiabilité *(basic reliability check)*—évaluation de l'intégrité d'une personne; condition préalable de l'obtention de la cote de fiabilité de base.

Vulnérabilité *(vulnerability)*—menace pouvant causer du tort en raison d'une sécurité insuffisante.

Zone d'accueil *(reception zone)*—aire située à l'entrée de l'installation où le premier contact entre le public et le ministère se produit, où les services sont fournis, où des renseignements sont échangés et où l'accès aux zones restreintes est contrôlé. Le public peut n'y avoir accès qu'à certaines heures de la journée ou pour des motifs précis, et la surveillance se fait, à des degrés divers, par le personnel qui travaille à cet endroit, par d'autres employés ou par le personnel de sécurité.

Zone de haute sécurité *(high-security zone)*—aire à laquelle l'accès est contrôlé au moyen d'un point d'entrée et qui est réservée au personnel autorisé ayant fait l'objet de l'enquête de sécurité nécessaire, ainsi qu'aux visiteurs autorisés et dûment accompagnés. La zone ne devrait être accessible qu'à partir des zones de sécurité et elle doit être séparée des zones de sécurité et des zones d'opérations par un périmètre aménagé d'après les spécifications recommandées dans l'évaluation de la menace et des risques. La surveillance se fait 24 heures sur 24 et 7 jours sur 7 par du personnel de sécurité, par d'autres employés ou par des moyens électroniques.

Zone de sécurité *(security zone)*—aire dont l'accès est réservé au personnel autorisé et aux visiteurs autorisés et dûment accompagnés. La zone devrait être préférablement accessible à partir d'une zone d'opérations et par un point d'entrée, mais elle n'est pas nécessairement séparée de la zone des opérations par un périmètre de sécurité. La surveillance se fait 24 heures sur 24 et 7 jours sur 7 par le personnel de sécurité, par d'autres employés ou par des moyens électroniques.

Zone de travail *(operations zone)*—aire dont l'accès est réservé au personnel qui y travaille et aux visiteurs dûment accompagnés, qui doit être surveillée périodiquement, d'après une

évaluation de la menace et des risques, et qui devrait être de préférence accessible à partir d'une zone de réception.

Zone publique *(public zone)*—aire qui entoure généralement les installations d'un ministère ou qui en fait partie. Mentionnons par exemple les terrains qui entourent un immeuble, les couloirs publics et les halls d'ascenseur dans un immeuble occupé par plusieurs locataires.

Zones restreintes *(restricted zones)*—zones de travail, de sécurité et de haute sécurité.