



Chef – Service d'examen

EXAMEN DE LA CONFORMITÉ DU MDN ET DES FC
À LA POLITIQUE DU GOUVERNEMENT
SUR LA SÉCURITÉ (PGS) –
POINT DE VUE DE L'UNITÉ

Avril 2002

7050-7 (CS Ex)

SYNOPSIS

Le présent rapport fait état des résultats d'un examen réalisé en collaboration avec KPMG Consulting, dans le but d'évaluer la conformité du MDN et des FC à la Politique du gouvernement sur la sécurité (PGS). L'examen s'est surtout intéressé au niveau local/unités. On a visité plus de 20 endroits en 2000. L'« instantané » ainsi pris à l'échelon des unités offre un point de vue raisonnable, même s'il n'est pas définitif, de la conformité du MDN et des FC à la PGS. Bien que l'examen portait effectivement sur certains aspects de la sécurité de l'information, un autre examen, qui ciblait davantage ce sujet, a été réalisé parallèlement à celui-ci et fait l'objet d'un rapport distinct.

L'examen a permis de relever certains cas de non-conformité et de conformité partielle. Par la suite, des recommandations pertinentes ont été faites en vue d'améliorer la situation. Les domaines où il faut apporter des améliorations intéressent surtout la sensibilisation aux plans d'urgence et de contingence locaux et leur mise à l'essai. Les méthodes de surveillance de la sécurité des TI pourraient profiter d'une modernisation et d'une amélioration de l'orientation de la gestion du risque.

Sous réserve de ce qui précède, les résultats, dans l'ensemble, montrent que les unités se conforment à la PGS de façon satisfaisante. Cette conclusion est renforcée par les mesures rapides prises par le Grand prévôt adjoint (Sécurité) et le plan détaillé qu'il a fourni, en ce qui a trait aux questions soulevées par l'examen. Il faut de plus reconnaître que cet examen a eu lieu avant les récents événements qui ont fait en sorte que les besoins en matière de sécurité se sont accrus de façon appréciable. En conséquence, on travaille actuellement à d'autres examens ciblés. Il faut aussi préciser que la PGS fait actuellement l'objet de modifications et tout changement important devra se refléter dans de tels plans d'action.

Le présent examen a été effectué dans le cadre du plan de travail approuvé par le Service. Les conclusions de cet examen n'ont pas le poids d'une vérification, il ne faut donc pas les considérer comme telles. Bien qu'elles suffisent à permettre d'élaborer des recommandations qui seront étudiées par la direction, les évaluations fournies et les conclusions proposées ne se fondent pas sur le type d'enquête rigoureuse et de preuves requises que représente une vérification. En conséquence, elles ne sont pas proposées comme telles et le lecteur est donc mis en garde.

TABLE DES MATIÈRES

SYNOPSIS	i
Sommaire	1
Objectif et portée	1
Sommaire des résultats	1
Introduction	4
Contexte	4
Objectif et portée	4
Approche	4
Présentation de diapositives de KPMG	7
Plan d'action de la direction	8
Organisation de la sécurité	8
Administration de la sécurité	9
Sécurité matérielle	10
Gestion des mesures d'urgence et des marchés	10
Sécurité des technologies de l'information	10
Figure :	
1 Sites vérifiés	4
Tableau :	
1 Conformité du MDN et des FC à la PGS — Évaluation de la conformité et sommaire des recommandations	2

SOMMAIRE

OBJECTIF ET PORTÉE

Le principal objectif du présent examen visait à évaluer la conformité, aux échelons locaux et des unités du MDN et des FC, à la Politique du gouvernement sur la sécurité (PGS) mise en œuvre par le Conseil du Trésor (CT).

Les sept principaux éléments qui ont fait l'objet de cet examen sont les suivants :

- organisation de la sécurité;
- administration de la sécurité;
- sécurité matérielle;
- sécurité du personnel;
- gestion des mesures d'urgence;
- gestion des marchés;
- sécurité des technologies de l'information.

On a procédé aux examens sur place au cours de l'an 2000 dans plus de 20 unités choisies à la fois au hasard et par échantillonnage discrétionnaire.

Le présent examen ne portait toutefois pas sur la sécurité des armements et des autres inventaires de nature délicate.

SOMMAIRE DES RÉSULTATS

Dans l'ensemble, les résultats montrent que le Programme de sécurité du MDN et des FC est conforme à la PGS. Bien que certains domaines demandent des améliorations, nous ne les avons pas jugés à ce point importants et avons accordé une note globale « conforme ».

Les indices de conformité, de même que les principales recommandations et les organisations responsables sont présentés dans le tableau de la page qui suit. Ensuite, les résultats, évaluations et recommandations détaillés sont inscrits dans la présentation de diapositives de KPMG, qui sont annexées au présent rapport. Enfin, la fin du présent rapport propose des mesures correctives prises et prévues.

TABLEAU 1
Conformité du MDN et des FC à la PGS — Évaluation de la conformité et sommaire des recommandations

<u>Élément</u>	<u>Évaluation</u>	<u>Portée des principales recommandations</u>	<u>BPR/BC</u>
1. Organisation de la sécurité	Conforme	Rappeler l'importance des rôles et des responsabilités de l'officier de sécurité du Ministère (O Sécur M) Il faudra officialiser les examens/inspections Uniformiser les rôles des officiers de sécurité d'unité (OSU) Renforcer les programmes de formation et de sensibilisation à la sécurité	GPA (Sécur) ¹
2. Administration de la sécurité	Conforme	Simplifier et uniformiser les politiques et directives de classification des renseignements Les processus d'évaluation de la menace et des risques doivent être améliorés	O Sécur M ² GPA (Sécur)
3. Sécurité matérielle	Conforme	Il faut procéder à des examens de sécurité réguliers dans toutes les unités La gestion des dossiers doit être uniformisée dans toutes les unités	GPA (Sécur) O Sécur M
4. Sécurité du personnel	Conforme	Les mesures de sélection et de départ doivent être améliorées	O Sécur M et BPR RH ³
5. Contrats et mesures d'urgence	Conformité partielle	Le personnel des unités doit être au courant des plans d'urgence Les plans d'urgence doivent faire l'objet de mises à l'essai régulières Les questions de sécurité des contrats doivent être incluses dans les documents de politique	O Sécur M O Sécur M GPA (Sécur)

¹ GPA (Sécur) — Grand prévôt adjoint (Sécurité).

² O Sécur M — Officier de sécurité du Ministère.

³ BPR RH — Bureau de première responsabilité - Ressources humaines

6. Sécurité des technologies de l'information	Conformité partielle	Il faudra tenir compte des questions de sécurité dans toutes les activités de planification Des mesures de contrôle et d'examen de sécurité des TI doivent être mises en place Le processus d'attestation et d'accréditation des TI demande des améliorations	O Sécur M GPA (Sécur) GOIFC ⁴
---	----------------------	---	--

⁴ GOIFC — Groupe des opérations d'information des Forces canadiennes

INTRODUCTION

CONTEXTE

La Politique du gouvernement sur la sécurité (PGS) énonce à l'intention des ministères fédéraux les règles de base en matière de sécurité auxquelles les organismes doivent se conformer. On y a néanmoins tenu compte de l'hétérogénéité des priorités, des ressources budgétaires et de la culture des ministères en définissant les exigences générales qui garantissent une sécurité minimale à l'intérieur d'un ministère ou même du gouvernement.

Le Grand prévôt adjoint (Sécurité) [GPA (Sécur)] qui relève du Vice-chef d'état-major de la Défense (VCEMD) et le Groupe des opérations d'information des Forces canadiennes (GOIFC) qui relève du Sous-ministre adjoint (Gestion de l'information) [SMA(GI)] sont les deux principaux organismes qui s'occupent des questions se rapportant à la PGS au sein du MDN et des FC.

Les lignes directrices du Conseil du Trésor relatives à la PGS contiennent, à l'intention des ministères fédéraux, des directives et des conseils sur l'organisation d'examens et de vérifications internes de leur programmes de sécurité ministériels.

Le présent examen fait suite à une évaluation préalable de conformité à la PGS réalisée par le GPA (Sécur) en février 2000.

OBJECTIF ET PORTÉE

Le présent examen avait pour objectif d'évaluer la conformité du MDN et des FC à la PGS et aux normes opérationnelles publiées par le Conseil du Trésor.

L'examen portait sur la conformité à la PGS à l'échelon des unités. Il ne portait pas cependant sur la sécurité des armements, et autres biens de nature délicate⁵ qui font l'objet d'un examen distinct.

APPROCHE

Entrevues préliminaires

Les questions de conformité et les attentes ont été examinées avec les autorités du Conseil du Trésor. Les contacts ont été établis avec les intervenants clés du Ministère, et des entrevues préliminaires ont eu lieu. Les renseignements recueillis dans le cadre de ces entrevues ont été mis à profit dans la définition du plan d'examen. L'idée était de dresser une liste de contrôle de conformité et de questions clés sur lesquelles porterait l'examen.

⁵ Il s'agit d'articles qui, s'ils sont perdus, endommagés ou mal utilisés, peuvent avoir des conséquences négatives sur les capacités opérationnelles des FC, mettre en danger le grand public ou nuire aux accords de partage de technologies conclus avec les alliés du Canada.

L'examen se subdivisait en sept principaux éléments, indiqués ci-dessous, qui sont prévus dans la structure de politique et les directives connexes de la PGS :

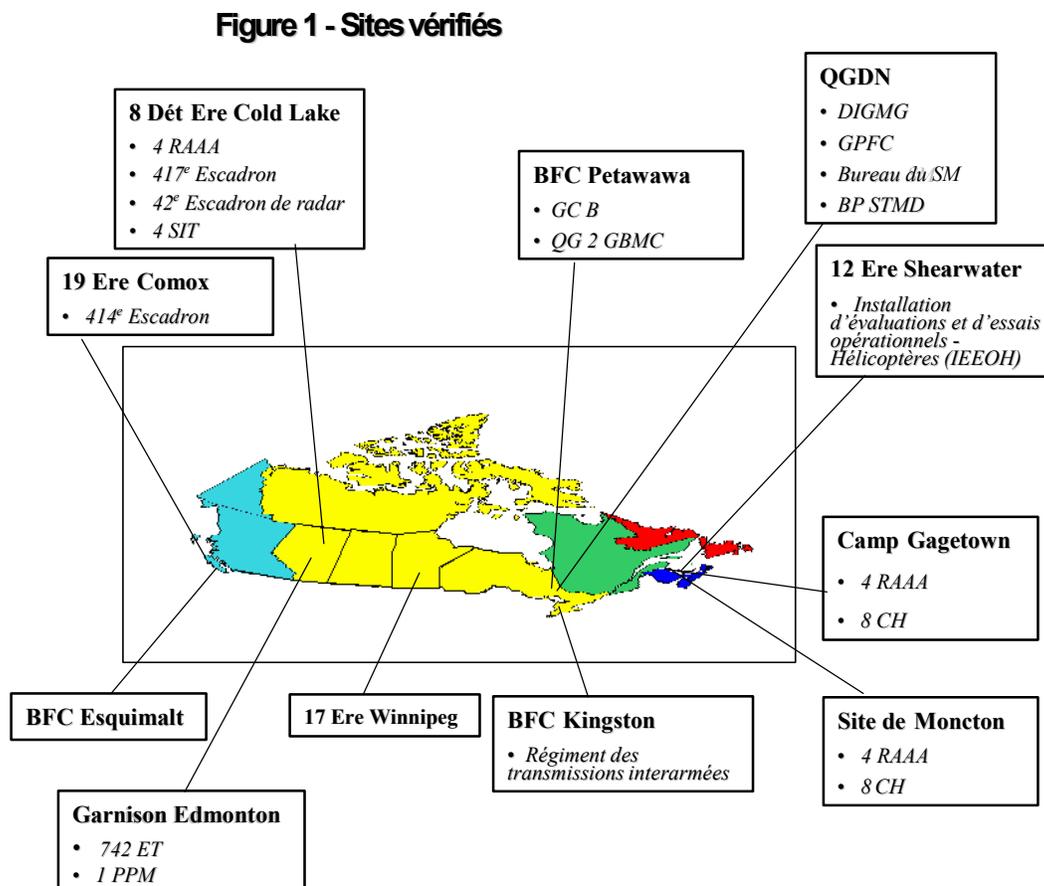
- organisation de la sécurité;
- administration de la sécurité;
- sécurité matérielle;
- sécurité du personnel;
- gestion des mesures d'urgence;
- gestion des marchés;
- sécurité des technologies de l'information.

Évaluation préliminaire

Les résultats d'une évaluation préliminaire faite par le GPA (Sécur) au sujet de la conformité à la PGS (février 2000) ont été évalués dans le présent examen. On a d'ailleurs utilisé les renseignements provenant de l'évaluation du GPA (Sécur) pour élaborer une liste de contrôle de conformité.

Visites des unités

La liste de contrôle de conformité a été utilisée dans le cadre des visites d'unités partout dans le MDN et les FC. Afin qu'elles soient le plus représentatives possible, les unités ont été choisies à



la fois au hasard et par échantillonnage discrétionnaire. Étant donné que l'unité est l'élément opérationnel principal tant du MDN que des FC, les évaluations d'unités étaient importantes pour déterminer l'ensemble des forces et faiblesses de conformité au sein du MDN et des FC. Comme l'illustre la figure 1, plus de 20 unités du MDN et des FC partout au Canada ont fait l'objet de l'examen.

Période visée

Le présent examen tenait compte de la période qui se terminait à la fin de mars 2001. Toutes les entrevues et visites d'unités ont eu lieu pendant les deux derniers trimestres de l'an 2000.

Examen de la sécurité des renseignements du MDN et des FC

Cet examen s'est déroulé séparément de celui qui a été effectué parallèlement par le Chef – Service d'examen (CS Ex) sur la sécurité des renseignements du MDN et des FC. Cependant, les deux ont été alignés par souci d'uniformité et d'efficacité des ressources. On rédige actuellement un rapport distinct destiné à l'examen de la sécurité de l'information.

PRÉSENTATION DE DIAPOSITIVES DE KPMG

Examen de la conformité à la Politique du gouvernement sur la sécurité



Novembre 2001



Table des matières

1.0 Introduction

- Contexte et but
- Objectifs
- Approche et méthodologie
- Visites des unités

2.0 Constatations et recommandations

- Organisation de la sécurité
- Administration de la sécurité
- Sécurité matérielle
- Sécurité du personnel
- Gestion de la sécurité et des mesures d'urgence
- Gestion de la sécurité et des marchés
- Sécurité des TI

3.0 Conclusion

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



1.1 Contexte et but

- La Politique du gouvernement sur la sécurité (PGS) du Conseil du Trésor vise à fournir aux ministères fédéraux des lignes directrices de haut niveau en matière de politique.
- La PGS tient compte de l'hétérogénéité des priorités, des ressources budgétaires et de la culture des ministères. Pour ce faire, elle définit les exigences générales qui garantissent une sécurité minimale au sein d'un ministère ou à l'échelle du gouvernement.
- Le personnel du CS Ex a collaboré avec une équipe de KPMG pour effectuer un examen de la conformité du MDN et des FC à la PGS.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



1.2 Objectifs

L'examen réalisé par le CS Ex/KPMG poursuivait trois grands objectifs :

- évaluer la conformité des ministères aux normes opérationnelles de la Politique sur la sécurité;
- évaluer l'efficacité du MDN et des FC à mettre en œuvre les normes opérationnelles de la Politique sur la sécurité;
- vérifier l'efficacité des ministères à mettre en œuvre les normes opérationnelles de la Politique sur la sécurité.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



1.3 Approche et méthodologie

- *But* : L'évaluation avait globalement pour but d'examiner et d'évaluer la conformité du MDN et des FC aux dispositions de la Politique du gouvernement sur la sécurité (PGS) du Conseil du Trésor.
- *Portée* : L'examen portait sur un certain nombre d'organisations et d'unités du MDN et des FC et intéressait des organismes de l'extérieur, le Programme de sécurité actuel et le programme prévu de politique de sécurité du MDN, ainsi que les politiques, normes et directives connexes. Il ne portait pas sur la sécurité des armes et des munitions et autres inventaires de nature délicate.
- *Principales questions* : Confirmer/valider l'évaluation préliminaire du GPA (Sécur) au sujet de la conformité à la PGS.
- *Techniques* : Le présent examen a été réalisé à l'aide d'entrevues, de l'examen de documents, des meilleures pratiques, de la recherche documentaire et des visites à des unités choisies.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



1.4 Visites des unités

8 Dét Ere Cold Lake

- 4 RAAA
- 417^e Escadron
- 42^e Escadron de radar
- 4 SIT

19 Ere Comox

- 414^e Escadron

BFC Petawawa

- GC B
- QG 2 GBMC

QGDN

- DIGMG
- GPFC
- Bureau du SM
- BP STMD

12 Ere Shearwater

- Installation d'évaluations et d'essais opérationnels - Hélicoptères (IEEOH)

Camp Gagetown

- 4 RAAA
- 8 CH

Site de Moncton

- 4 RAAA
- 8 CH

BFC Kingston

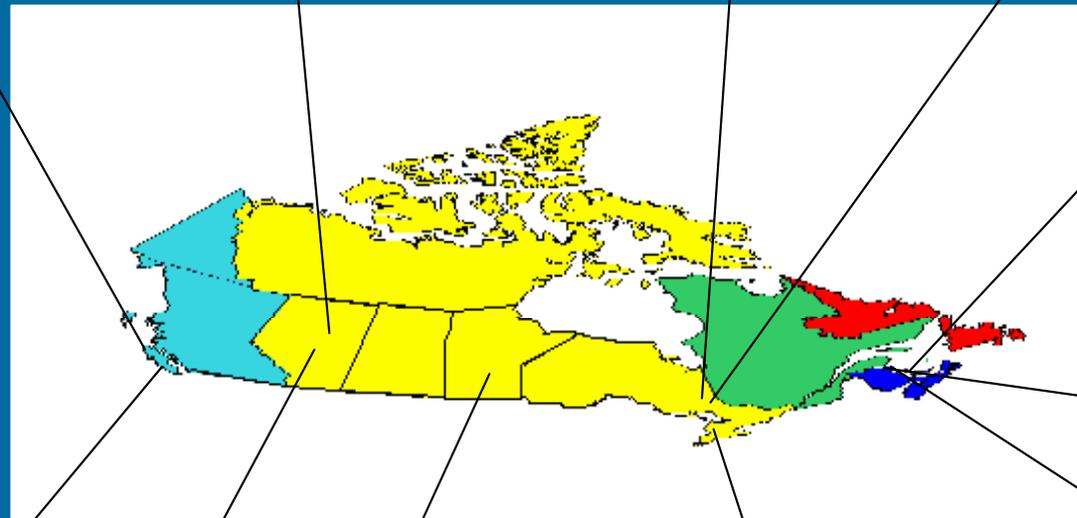
- Régiment des transmissions interarmées

17 Ere Winnipeg

BFC Esquimalt

Garnison Edmonton

- 742 ET
- 1 PPM



● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

● Gestion de la sécurité et des marchés

● Sécurité des TI

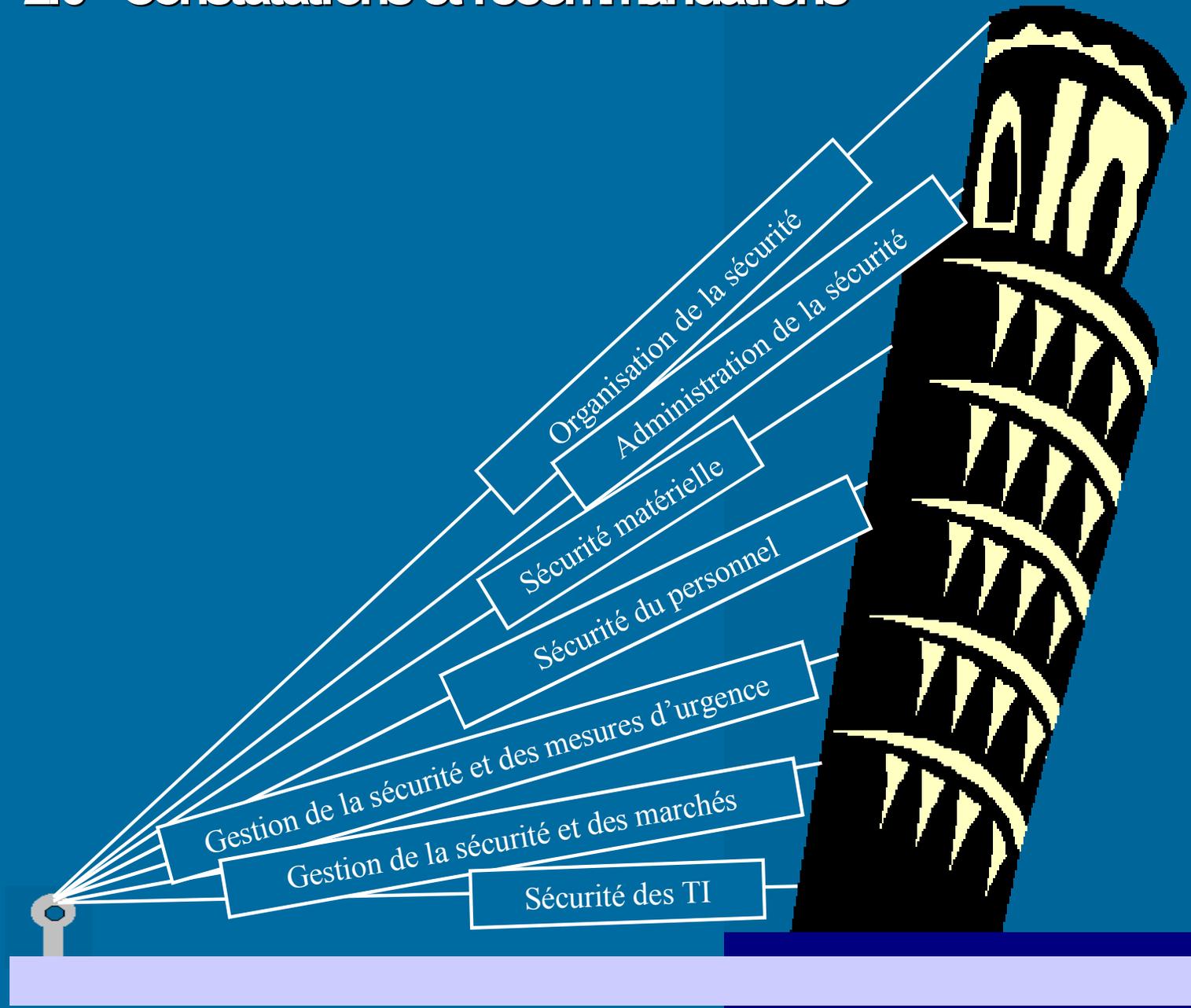
● Conclusion

d'évaluations et d'essais opérationnels - Hélicoptères



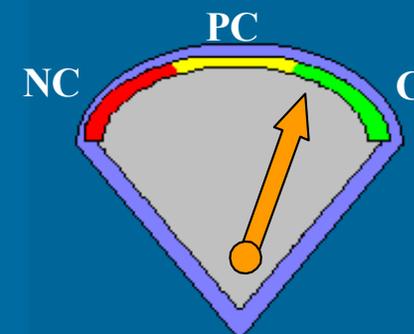
20 Constatations et recommandations

- Introduction
- Organisation de la sécurité
- Administration de la sécurité
- Sécurité matérielle
- Sécurité du personnel
- Gestion de la sécurité et des mesures d'urgence
- Gestion de la sécurité et des marchés
- Sécurité des TI
- Conclusion





2.1 Organisation de la sécurité



Principales constatations

- Il n'y a pas de centre de coordination.
- La plupart des unités ont adopté des politiques et des procédures de sécurité qui sont accessibles et compréhensibles, mais elles ne sont pas forcément à jour ni uniformes.
- Les capacités, les responsabilités, l'obligation de rendre compte et les fonctions varient d'un officier de sécurité à l'autre. Le poste d'OSSI n'est pas reconnu officiellement.
- La majorité des unités ne font pas régulièrement d'examen ni de vérification de la sécurité.
- Il y a un manque de formation et de sensibilisation à la sécurité au sein du Ministère.

Principales recommandations

- Même si la structure organisationnelle actuelle est conforme à la PGS, des améliorations d'efficacité et d'efficacités pourraient être réalisées grâce à une réorganisation.
- L'O Sécur M doit assurer l'uniformité des politiques locales et des ordonnances de sécurité par rapport aux normes minimales de sécurité.
- L'O Sécur M doit s'assurer que les unités procèdent régulièrement à des examens et vérifications de la sécurité et signalent les résultats.
- Le GPA (Sécur) et le GOIFC doivent uniformiser les rôles et les responsabilités de l'OSU et des OSSI partout dans les unités. Cela suppose une reconnaissance officielle de la part de la direction.
- Des programmes de sensibilisation et de formation doivent être institués.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

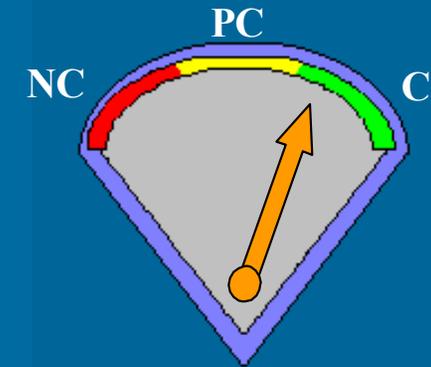
● Gestion de la sécurité et des marchés

● Sécurité des TI

Conclusion



2.2 Administration de la sécurité



Principales constatations

- Les renseignements sont généralement bien classifiés et désignés.
- Un certain nombre d'unités n'ont pas fait d'évaluations de la menace et des risques (EMR) en raison de la confusion qui subsistait quant à la responsabilité des évaluations.
- Les recommandations provenant d'examens/enquêtes de sécurité récentes ont été ou sont actuellement mises en œuvre.
- Les infractions et les manquements à la sécurité sont rares.

Principales recommandations

- Les politiques et les directives de classification des renseignements du Ministère devraient être simplifiées et uniformisées. Pour éviter la surclassification des renseignements, une personne qualifiée de l'unité peut revoir la classification de l'information. La déclassification et le déclassement doivent aussi suivre une méthode uniformisée, définie par l'O Sécur M.
- On doit fournir des modèles d'EMR et une formation appropriée.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

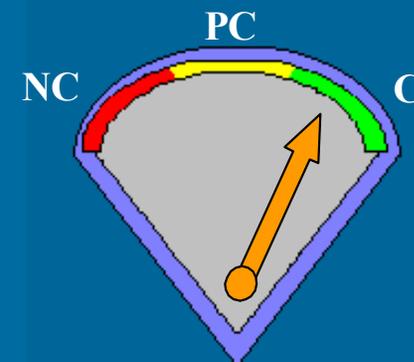
● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



2.3 Sécurité matérielle



Principales constatations

- Très peu d'incidents relatifs à la sécurité matérielle des employés ont été signalés au cours des deux dernières années. Les OSU ne reçoivent pas systématiquement de copie des rapports d'incidents.
- Le contrôle et l'examen des mesures de sécurité ne se font pas uniformément dans toutes les unités (p. ex., rapports sur l'état de la sécurité).
- La majorité des unités observées ont institué des systèmes autonomes de gestion des dossiers (SGD).
- La majorité des unités observées ont un contrôle limité sur les biens de nature délicate.

Principales recommandations

- Les OSU devraient obtenir une copie de tous les rapports d'incidents relatifs à la sécurité.
- Le manque de rapports empêche la tenue d'examen internes exhaustifs pour assurer la conformité. Cela empêche aussi de prendre des mesures correctives en cas d'infractions à la sécurité.
- Il faudra mettre en place un SGD uniforme dans toutes les unités pour que les documents soient classés et classifiés convenablement.
- Les articles transportables devraient être obtenus contre signature.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion

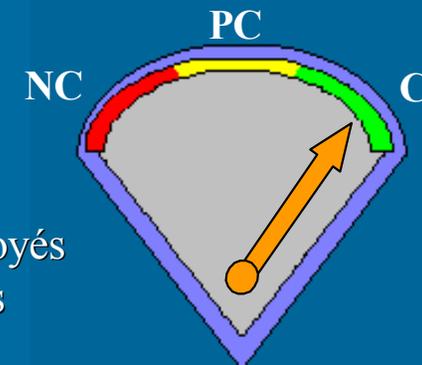
2.4 Sécurité du personnel

Principales constatations

- Il n'y a pas de procédures officielles à l'égard des employés qui partent et le fait de ne pas modifier les combinaisons ou les codes d'accès n'entraîne aucune conséquence.
- Les employés ne sont pas tenus dans toutes les unités de signer leur habilitation.
- Le dossier des niveaux d'habilitation est gardé dans une base de données centrale (*PeopleSoft*). Les unités ne savent pas au juste si les niveaux d'habilitation conviennent ou non.
- Les autorisations d'accès au système informatique sont retirées au moment du départ des employés, mais l'efficacité du processus reste à confirmer.
- Le client peut accéder au système de traitement des habilitations de la sécurité du GPA (Sécur) sur le site Web du GPFC.

Principales recommandations

- Il faudrait élaborer une liste de contrôle des départs et l'appliquer uniformément dans toutes les unités.
- Les unités devraient instituer un processus d'examen et de contrôle pour s'assurer que les habilitations de sécurité sont signées, que les niveaux d'habilitation des employés conviennent à leur poste et que les mesures à prendre au départ des employés sont bien suivies.



● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

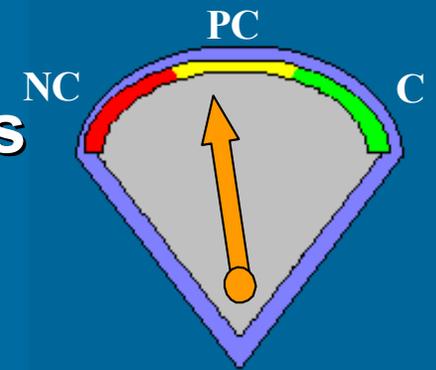
● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



2.5 Gestion de la sécurité et des mesures d'urgence



Principales constatations

- Les employés ne connaissent pas leurs plans locaux de gestion des mesures d'urgence.
- La majorité des unités observées ont établi des plans d'urgence. Ces plans ne semblent cependant pas complets et n'étaient pas mis à l'essai régulièrement.

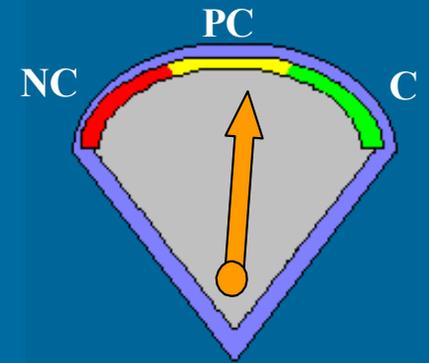
Principales recommandations

- Le personnel de toutes les unités devrait être mis au courant des plans de reprise des activités et des plans d'urgence. Si l'unité n'a pas de plan, il faudrait en fournir un (p. ex., le plan du QGDN).
- Tous les plans doivent être régulièrement mis à jour en fonction du contexte actuel du MDN et des FC et mis à l'essai pour s'assurer qu'ils fonctionnent bien.

- Introduction
- Organisation de la sécurité
- Administration de la sécurité
- Sécurité matérielle
- Sécurité du personnel
- Gestion de la sécurité et des mesures d'urgence
- Gestion de la sécurité et des marchés
- Sécurité des TI
- Conclusion



2.6 Gestion de la sécurité et des marchés



Principales constatations

- Beaucoup d'unités n'ont pas de rapport avec les entrepreneurs, puisque le génie de construction local est responsable des marchés. Par conséquent, les OSU ne connaissent pas les habilitations de sécurité des entrepreneurs sur place.
- La gestion de la sécurité des marchés (y compris ceux avec l'étranger) n'est pas parfaitement couverte dans la PSDN, mais elle sera précisée dans les ISDN.

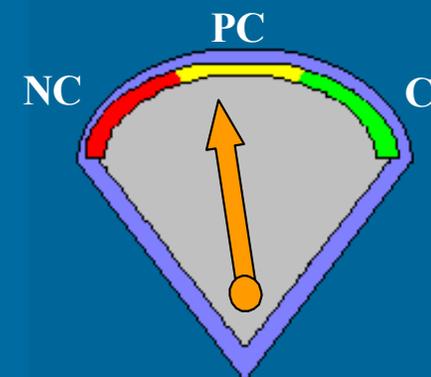
Principales recommandations

- Les unités locales qui font appel à des entrepreneurs devraient assumer la responsabilité de voir à ce que tous ces entrepreneurs aient obtenu les habilitations de sécurité appropriées.
- La sécurité des marchés est une question importante qui devrait être abordée explicitement dans les procédures de sécurité des unités.

- Introduction
- Organisation de la sécurité
- Administration de la sécurité
- Sécurité matérielle
- Sécurité du personnel
- Gestion de la sécurité et des mesures d'urgence
- Gestion de la sécurité et des marchés
- Sécurité des TI
- Conclusion



2.7 Sécurité des TI



Principales constatations

- La planification de la sécurité n'est pas toujours vue comme une priorité et il s'ensuit qu'on n'en tient pas toujours compte dès le début du cycle de mise en œuvre des projets.
- Les contrôles et les examens ne sont pas uniformes dans toutes les unités et à ce sujet certaines unités sont moins dynamiques que d'autres.
- La sécurité du personnel et la sécurité du matériel est plus ou moins conforme à la politique dans toutes les unités observées, mais la gestion du matériel de TI pourrait être améliorée.
- Les procédures d'attestation et d'accréditation sont complexes et périmées, il s'ensuit que de nombreux systèmes sont utilisés sans attestation.
- Les pratiques de configuration des logiciels ne sont ni structurées ni appliquées uniformément par les unités. Le personnel ne connaît pas bien les modules de base de sécurité des systèmes.
- L'architecture de sécurité est périmée.
- La visite d'une unité a révélé qu'une imprimante du réseau local approuvée pour imprimer des documents « PROTÉGÉS » avait servi pour traiter des documents « CLASSIFIÉS ».
- Il existe une certaine préoccupation quant aux mesures de contrôle insuffisantes des comptes des administrateurs du système.

● Introduction

● Organisation de la sécurité

● Administration de la sécurité

● Sécurité matérielle

● Sécurité du personnel

● Gestion de la sécurité et des mesures d'urgence

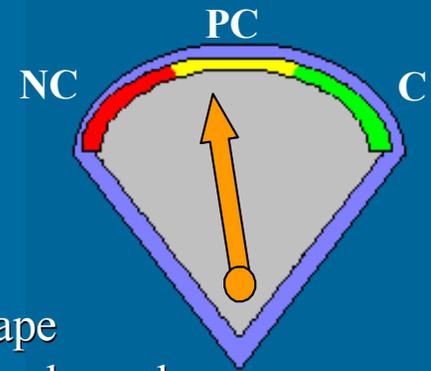
● Gestion de la sécurité et des marchés

● Sécurité des TI

● Conclusion



2.7 Sécurité des TI (suite)



Principales recommandations

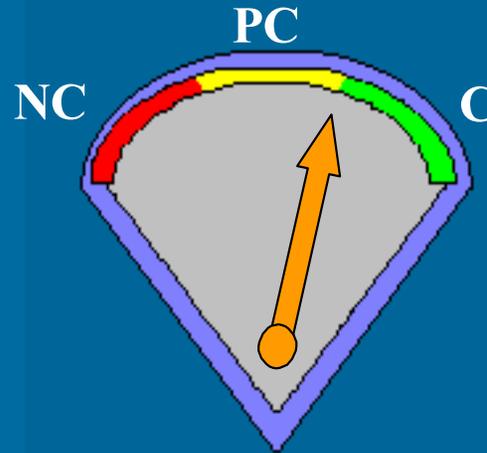
- S'assurer que la sécurité des TI est instaurée dès l'étape de planification d'un projet; il faudra y affecter les fonds voulus.
- Les mesures de contrôle et d'examen doivent être uniformisées et proactives.
- Les renseignements de nature délicate qui sont enregistrés dans les ordinateurs portatifs, sur les disquettes, etc. doivent être encryptés afin de minimiser le risque de divulgation en cas de perte.
- Le processus d'attestation et d'accréditation devrait être modernisé afin de tenir compte du contexte actuel du MDN et des FC.
- Les politiques et les pratiques de gestion de la configuration doivent être élaborées et/ou améliorées en fonction de directives énoncées pour tout le Ministère.
- L'architecture de sécurité doit être actualisée en fonction du contexte actuel du MDN et des FC afin de minimiser les risques.
- Les documents classifiés doivent être imprimés sur des imprimantes autonomes.
- Il faudra contrôler toutes les personnes qui ont accès aux systèmes (c.-à-d. les administrateurs des systèmes).

- Introduction
- Organisation de la sécurité
- Administration de la sécurité
- Sécurité matérielle
- Sécurité du personnel
- Gestion de la sécurité et des mesures d'urgence
- Gestion de la sécurité et des marchés
- Sécurité des TI
- Conclusion



3.0 Conclusion

- Dans l'ensemble, on a constaté que le MDN et les FC étaient conformes à la Politique du gouvernement sur la sécurité (PGS).



- L'examen de la PGS a révélé un certain nombre d'éléments qui peuvent être améliorés. La majeure partie de ces améliorations se rapportaient aux éléments où l'on avait constaté une conformité partielle. Les recommandations présentées dans le cadre de l'examen portent sur ces améliorations.
- Le BPR principal du MDN, le GPFC/GPA (Sécur), a présenté un plan d'action de gestion acceptable qui porte sur les recommandations de l'examen.

- Introduction
- Organisation de la sécurité
- Administration de la sécurité
- Sécurité matérielle
- Sécurité du personnel
- Gestion de la sécurité et des mesures d'urgence
- Gestion de la sécurité et des marchés
- Sécurité des TI
- Conclusion

FIN DE LA PRÉSENTATION DES DIAPOSITIVES DE KPMG

PLAN D'ACTION DE LA DIRECTION

En réponse au présent examen, la principale autorité sur ce sujet, le GPFC/GPA (Sécur) a mis sur pied une équipe chargée de l'élaboration du plan d'action. Les principaux aspects du plan sont présentés ci-dessous, regroupés selon les principales catégories de notre examen. Les dates d'échéance et les BPR à l'intérieur du GPFC sont indiqués dans la mesure du possible.

ORGANISATION DE LA SÉCURITÉ

Réorganisation (Centre de coordination) – Date d'échéance : AF 2002-2003

Il existe déjà un centre de coordination offrant des directives en matière de sécurité. Il s'agit du bureau de l'officier de sécurité du Ministère⁶. La principale fonction de ce bureau consiste à formuler et à mettre en œuvre des politiques en répondant aux besoins de la haute direction des secteurs administratifs et opérationnels du MDN et des FC.

Cette fonction a disparu avec les réductions d'effectifs et la restructuration. De plus, la plupart des gens ignorent l'existence de ce bureau et sa fonction. Pour régler cette question, l'*O Sécur M* devra, au cours de l'AF 2001-2002 :

- effectuer six visites d'état-major dans des unités où des lacunes ont été constatées sur le plan de la sécurité;
- organiser des entrevues avec les gestionnaires de niveau 1 afin de discuter avec eux et de connaître leurs préoccupations et leurs besoins en matière de sécurité;
- continuer de relever, au Ministère et à l'extérieur, les comités auxquels le personnel de l'*O Sécur M* et du GPA (Sécur) devraient participer;
- continuer d'élaborer le plan de mise en œuvre du renouveau du Programme de sécurité du Ministère.

Contrôle — Date d'échéance : juillet 2001

Le cadre essentiel à l'exécution d'examen/de vérifications de sécurité sera élaboré et déterminé dans les mandats du projet et dans le plan de mise en œuvre du Programme de surveillance de la sécurité du Ministère. *BPR – GPA (Sécur)*.

Normalisation — Date d'échéance : décembre 2001

Dans le cadre de la révision de la Politique de sécurité de la Défense nationale (PSDN) actuellement en vigueur, on réglera la question de l'uniformisation des rôles et responsabilités des OSU. *BPR — GPA (Sécur)*

⁶ L'OSU en titre est le GPA (Sécur), qui relève du GPFC et est rattaché à l'organisation du VCEMD.

Instruction — Date d'échéance : mai 2001

Les discussions auront lieu avec des responsables du Service du recrutement, de l'éducation et de l'instruction (SREIFC) des Forces canadiennes concernant les normes de qualification du cours de formation de l'OSU. **BPR — GPA (Sécur).**

Sensibilisation — Date d'échéance : avril 2001

Le GPA (Sécur) discutera avec le responsable de la cellule de protection des ressources nommé récemment au sein de l'organisation du GPFC dans le but de promouvoir les questions de sensibilisation à la sécurité. **BPR — GPA (Sécur).**

ADMINISTRATION DE LA SÉCURITÉ**Politiques et directives — Date d'échéance : décembre 2002**

Il faut élaborer un guide de classification pour permettre aux employés du Ministère et des Forces canadiennes de bien identifier et classer les documents/renseignements qu'ils produisent. Cette procédure qui a été, à tort, associée au domaine de la sécurité en raison du fait que l'on attribue aux renseignements/documents une marque d'identification appelée « *Cote de sécurité* ». L'O Sécur M a pour rôle de relever dans la Politique la nécessité d'attribuer une cote de sécurité et la façon d'appliquer le « *critère subjectif* » dans le but de déterminer s'il est nécessaire d'attribuer une cote aux renseignements/documents du fait qu'ils sont considérés comme étant « d'intérêt national » ou « autre que national ». Il incombe aux commandants de repérer au sein de leurs organisations les « *experts en la matière (EM)* » qui sont autorisés à classer et à divulguer les renseignements/documents.

Le guide doit servir d'outil de référence pour les auteurs, leur permettant de mieux déterminer les domaines/sujets auxquels le Ministère a, par mesure de protection, attribué un niveau de sensibilité. La rédaction d'un tel guide devra se faire avec la collaboration des diverses organisations et il faudra ensuite nommer un gestionnaire qui sera chargé de veiller à sa mise à jour. **BPR — GPA (Sécur).**

Politique d'évaluation de la menace et des risques — Date d'échéance : décembre 2001

La Politique sur les évaluations de la menace et des risques (EMR) permettra de régler cette question. L'O Sécur M examine également les logiciels qui pourraient apporter une solution technique à l'exécution des EMR en matière de sécurité et de technologie de l'information. **BPR — GPA (Sécur).**

SÉCURITÉ MATÉRIELLE

Rapports

Tous les OSU devraient recevoir une copie des rapports d'incidents relatifs à la sécurité de leur unité. Cette question sera traitée en détail dans les Politiques sur le rôle et les responsabilités des OSU et sur la présentation de rapports concernant les incidents relatifs à la sécurité. Il est aussi prévu que cette question sera traitée parallèlement à l'élaboration d'un Cadre de référence en matière de responsabilité de la gestion en fonction des résultats (CRRG) pour la régie du Programme de surveillance de la sécurité du Ministère du MDN et des FC.

Amélioration des rapports

Les examens annuels sur « l'état de la sécurité » et les rapports produits par toutes les unités seront exécutés grâce aux nouvelles Instructions de sécurité de la Défense nationale (ISDN) et au Programme de surveillance de la sécurité du Ministère. Le BPR et les dates d'échéance seront établis une fois le CRRG mis sur pied pour la régie de ce programme.

Amélioration du contrôle des articles transportables — Date d'échéance : décembre 2002

Les exigences concernant la signature pour l'emprunt des articles transportables visent à rendre les personnes responsables des biens empruntés, et cette question sera réglée avec l'entrée en vigueur des nouvelles ISDN. *BPR — GPA (Sécur).*

GESTION DES MESURES D'URGENCE ET DES MARCHÉS

Un « Groupe de travail sur la sécurité des marchés (GTSM) » a été mis sur pied par le GPA (Sécur) afin de régler les questions de sécurité et améliorer la procédure d'adjudication des contrats et de sensibiliser davantage les intervenants du Ministère afin de rationaliser et d'éliminer le double emploi. *BPR — GPA (Sécur).*

SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION⁷

Amélioration de la planification de la sécurité des TI — Date d'échéance : 31 décembre 2001

Cette question sera réglée avec la publication des nouvelles ISDN et sera imposée par la PGS. *BPR — GPA (Sécur)/GOIFC.*

⁷ Ces interventions se rapportent aux questions liées à la conformité qui ont été soulevées dans le présent rapport. On prévoit prendre d'autres mesures parallèlement à l'examen du CS Ex portant sur la sécurité de l'information du MDN et des FC mentionné précédemment.

Amélioration des contrôles — Date d'échéance : 31 juillet 2001

Le plan de mise en œuvre du projet d'un Programme de surveillance de la sécurité du Ministère permettra de régler cette question. Nous savons que le CPI/GOIFC élabore actuellement un Programme de surveillance de la sécurité des systèmes d'information (SSI). **BPR — GPA (Sécur)/GOIFC.**

Protection des renseignements de nature délicate — Date d'échéance : 31 décembre 2001

La question de la protection des biens de valeur sera réglée par la publication des ISDN pertinentes. Cette même question peut également être réglée par la mise en place du cadre de l'Infrastructure à clés publiques (ICP) que le gouvernement du Canada et le Ministère n'ont pas encore fini de mettre au point. **BPR — GPA (Sécur)/GOIFC.**

Attestation et accréditation — Date d'échéance : octobre 2001

Il est convenu que le processus d'attestation et d'accréditation du Ministère est laborieux et axé sur la technique. Par conséquent, nous devons examiner ce processus en mettant l'accent sur le concept et les principes.

Un groupe de travail doit être mis sur pied dans le but de rédiger un nouveau Guide d'attestation et d'accréditation (GAA). **BPR — GPA (Sécur)/GOIFC.**