Correctional Service Canada | Service correctionnel Canada

Safety, Respect and Dignity for All

La sécurité, la dignité et le respect pour tous

# Vérification des Plans de reprises après sinistre des SGI

*Vérification interne*

*378-1-615*

*29 avril 2009*

Canada

# TABLE DES MATIÈRES

**RÉSUMÉ** ..... **II**

**1.0 INTRODUCTION** ..... **5**

**2.0 OBJECTIFS ET PORTÉE DE LA VÉRIFICATION** ..... **7**

**3.0 APPROCHE ET MÉTHODOLOGIE DE VÉRIFICATION** ..... **7**

**4.0 CONCLUSIONS ET RECOMMANDATIONS** ..... **8**

4.1 CADRE DE CONTRÔLE DE GESTION POUR LA PLANIFICATION DE LA REPRISE APRÈS SINISTRE ..... 8

*4.1.1 Cadre des plans de reprise (processus DS4.1 de COBIT)* ..... *8*

*4.1.2 Plans de reprise après sinistre, ressources essentielles, récupération et reprise (processus DS4.2, 4.3 et 4.8 de COBIT)* ..... *10*

*4.1.3 Plans de reprise – Maintenance, essais et formation (processus DS4.4, 4.5 et 4.6 de COBIT)* ..... *11*

*4.1.4 Diffusion des plans de reprise après sinistre (processus DS4.7 de COBIT)* ..... *13*

*4.1.5 Stockage hors site des bandes de sauvegarde (processus DS4.9 de COBIT)* ..... *14*

*4.1.6 Évaluation post-reprise (processus DS4.10 de COBIT)* ..... *14*

4.2 PROGRÈS RÉALISÉS DANS LA MISE EN ŒUVRE DE LA GSTI ET DES AMÉLIORATIONS DÉCOULANT DES EXERCICES DE SIMULATION ..... 15

*4.2.1 Mise en œuvre des exigences de GSTI reliées aux plans de reprise* ..... *16*

*4.2.2 Mise en œuvre des améliorations* ..... *16*

***Annexe A* – Critères de vérification**

***Annexe B* – Suites à donner – Reprise sûre I**

***Annexe C* – Plan d'action de gestion**

# RÉSUMÉ


## Contexte, portée et approche

Afin de continuer à atteindre ses objectifs et à satisfaire aux exigences de la Politique du gouvernement sur la sécurité (PGS), le SCC a élaboré, par l'entremise de ses Services de gestion de l'information (SGI), des plans de reprise après sinistre pour ses applications jugées essentielles.

Cette vérification vise à donner des assurances raisonnables que le cadre de contrôle de gestion qui est en place pour appuyer la préparation de la reprise après sinistre des systèmes de technologie de l'information est adéquat et efficace. La vérification a également examiné les progrès réalisés dans la mise en œuvre des exigences reliées aux plans de reprise de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du SCT et les améliorations entreprises dans la foulée de l'exercice de simulation des plans de reprise réalisé par les SGI en 2005.

La vérification portait sur les plans de reprise des applications essentielles des SGI, sur les contrôles en place à l'administration centrale (AC) et au centre de Laval pour soutenir la mise en œuvre rapide des plans de reprise, et sur les liens entre les plans de reprise et les plans de continuité des opérations (PCO), mais pas sur les PCO comme tels. Les régions ont récemment commencé à élaborer des plans de reprise, mais les bureaux régionaux n'ont que très récemment commencé à participer aux activités reliées aux plans de reprise dans le contexte des exercices de simulation des plans de reprise. La vérification des plans de reprise englobait donc un examen des plans de reprise régionaux, mais il n'a pas été jugé nécessaire de faire des visites dans chaque région, compte tenu des activités de contrôle limitées effectuées dans les régions et du fait que toutes les applications essentielles sont gérées centralement à l'AC.

Les applications essentielles qui ont été identifiées dans le cadre du projet de passage à l'an 2000 et qui s'inscrivent dans le cadre de cette vérification sont les suivantes :

| Système/ Applica-tion | Aperçu | Nombre d'utilisateurs |
|---|---|---|
| Réseau | L'infrastructure de réseau du SCC permet au personnel et aux partenaires du SCC d'interagir avec diverses formes de magasins d'information et d'applications électroniques. | |
| PTCEV2 | Le Poste de travail commun de l'entreprise, version 2 (PTCEV2), est le système d'exploitation commun tournant sur tous les postes de travail des utilisateurs du SCC et donnant accès aux applications du SCC. | 13 000 |

| | | |
|---|---|---|
| Courriel | Le courrier électronique (courriel) est un système de messagerie clé, utilisé au sein du SCC. | 14 000 |
| SGD | Le Système de gestion des délinquant(e)s (SGD) est une application informatique développée pour le Service correctionnel du Canada (SCC) et la Commission nationale des libérations conditionnelles (CNLC) pour gérer l'information sur les délinquantes. Grâce au SGD, le SCC est connecté à la Commission nationale des libérations conditionnelles, à la GRC et à l'ADRC (Immigration), ce qui lui permet de partager de l'information pertinente sur les délinquantes. | 10 000 |
| SCD | Le Système de la comptabilité des détenus (SCD) est une application utilisée par les commis des établissements du SCC pour gérer la paye et les comptes d'épargne (fonds) des délinquantes. | 150 |
| SGRH | Le Système de gestion des ressources humaines (SGRH) est un composant de l'application PeopleSoft. PeopleSoft est une application commerciale répandue dans les secteurs privé et public, qui offre un éventail de produits, dont des modules de Gestion des ressources humaines, de Gestion financière, de Gestion du matériel et de Programmation du temps et du travail. | 3 200 |
| SIGFM | Le Système intégré de gestion des finances et du matériel (SIGFM) est le système de gestion financière du SCC. | 600 |
| Paye en direct | Le système de paye en direct est utilisé par le SCC pour traiter les données de paye. | |
| RADAR | RADAR (Rapports automatisés de données appuyant la réinsertion) est une application de production de rapports qui permet au personnel et aux gestionnaires du SCC d'accéder de façon conviviale à l'information sur les délinquantes contenue dans le SGD. | 10 000 |

L'approche et la méthodologie utilisées sont conformes aux normes de vérification interne de l'Institute of Internal Auditors et respectent la Politique de vérification interne du gouvernement du Canada. Les critères de vérification ont été élaborés à partir des exigences du processus DS4 de COBIT 4.1 (www.isaca.org) et comprennent aussi les exigences spécifiques reliées aux plans de reprise après sinistre de la Politique du gouvernement sur la sécurité et de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du SCT. Les critères de vérification sont présentés à l'Annexe A.

## Conclusion

Plusieurs contrôles clés pour le programme de plans de reprise ont été mis en œuvre. Plus précisément, le SCC a établi un programme de plans de reprise pour les applications opérationnelles essentielles qui comprend une ressource spécialisée et qui a été basé sur un cadre de référence établie. Des plans de reprise des services d'application essentiels sont en place, le programme utilise le stockage de sauvegardes et la reprise hors site, et a également fait l'objet de tests et d'exercices de simulation.

Plusieurs améliorations possibles du programme actuel ont été identifiées. Des accords officiels sur les niveaux de service décrivant les exigences en matière de disponibilité des systèmes devraient être établis entre les SGI et leurs clients, une analyse officielle des incidences opérationnelles devrait être réalisée, un test complet de basculement devrait être effectué pour toutes les applications essentielles, et les efforts actuels de mise en œuvre et de mise à l'essai des plans de reprise dans les régions devraient se poursuivre.

Des progrès ont été réalisés dans la mise en œuvre des améliorations identifiées dans la norme de GSTI et lors de l'exercice de simulation des plans de reprise de 2005. Il faut cependant poursuivre les efforts pour satisfaire pleinement aux exigences de GSTI visant les tests et la révision des plans de reprise.

Ce rapport contient des recommandations qui permettront d'améliorer ces aspects. La haute direction a examiné et approuvé les constats présentés dans ce rapport et un Plan d'action de gestion a été élaboré pour donner suite à ces recommandations (voir l'Annexe C).

# 1.0 INTRODUCTION

En tant qu'organisme du gouvernement fédéral, le Service correctionnel du Canada (SCC) est responsable de la gestion des établissements de divers niveaux de sécurité et de la surveillance des délinquants en liberté sous condition dans la collectivité. À titre de composante du système de justice pénale, le SCC travaille en étroite collaboration avec plusieurs partenaires, comme les autres organismes du portefeuille de la Sécurité publique, en particulier la Gendarmerie royale du Canada (GRC) et la Commission nationale des libérations conditionnelles (CNLC), ainsi que tous les services de police.

Afin de continuer à atteindre ses objectifs et à satisfaire aux exigences de la Politique du gouvernement sur la sécurité (PGS), le SCC a élaboré, par l'entremise de ses Services de gestion de l'information (SGI), des plans de reprise après sinistre pour ses applications jugées essentielles. En raison de l'importance pour le SCC des plans de reprise après sinistre et des résultats de l'évaluation préliminaire des risques liés à la fonction de TI réalisée en 2006 par la Direction générale de la vérification interne, le Comité de vérification a approuvé une vérification des plans de reprise des Services de gestion de l'information, dans le cadre du plan de vérification de 2008-2009 de la Direction générale de la vérification interne.

Les SGI ont identifié, au sein du groupe de Sécurité et gestion des projets (ITSEC), un gestionnaire responsable des plans de reprise, ont affecté un agent de projet principal à temps plein aux plans de reprise, et commencé à examiner tous les plans de reprise existants et à réaliser des essais de simulation et des tests de reprise afin d'améliorer les plans de reprise existants. Alors que la Direction ITSEC est responsable de la coordination, de la surveillance, des essais et des activités normalisées de reprise après sinistre, la Direction de la gestion de l'infrastructure et des opérations (GIO) et la Direction du développement de systèmes sont responsables de l'élaboration et de la mise à jour des plans de reprise visant les opérations de TI et les applications essentielles. Tous les employés qui participent aux activités de reprise après sinistre relèvent, centralement, des SGI, mais peuvent travailler à l'administration centrale, au centre de traitement de Laval (Québec), ou au sein des régions ou de l'établissement qu'ils soutiennent.

La planification de la continuité des opérations relève de l'agent de sécurité du SCC, qui a demandé aux différents secteurs d'activité de préparer des plans de continuité des opérations (PCO). Ces plans devraient décrire de façon détaillée, notamment, les exigences sectorielles en termes des ressources de TI nécessaires pour assurer la continuité de leurs opérations. Les SGI sont responsables de la préparation de plans de reprise qui tiennent compte des ressources nécessaires en cas de sinistre.

Les applications essentielles qui ont été identifiées dans le cadre du projet de passage à l'an 2000 et qui s'inscrivent dans le cadre de cette vérification sont les suivantes :

| Système/ Applica-tion | Aperçu | Nombre d'utilisateurs |
|---|---|---|
| Réseau | L'infrastructure de réseau du SCC permet au personnel et aux partenaires du SCC d'interagir avec diverses formes de magasins d'information et d'applications électroniques. | |
| PTCEV2 | Le Poste de travail commun de l'entreprise, version 2 (PTCEV2), est le système d'exploitation commun tournant sur tous les postes de travail des utilisateurs du SCC et donnant accès aux applications du SCC. | 13 000 |
| Courriel | Le courrier électronique (courriel) est un système de messagerie clé, utilisé au sein du SCC. | 14 000 |
| SGD | Le Système de gestion des délinquant(e)s (SGD) est une application informatique développée pour le Service correctionnel du Canada (SCC) et la Commission nationale des libérations conditionnelles (CNLC) pour gérer l'information sur les délinquantes. Grâce au SGD, le SCC est connecté à la Commission nationale des libérations conditionnelles, à la GRC et à l'ADRC (Immigration), ce qui lui permet de partager de l'information pertinente sur les délinquantes. | 10 000 |
| SCD | Le Système de la comptabilité des détenus (SCD) est une application utilisée par les commis des établissements du SCC pour gérer la paye et les comptes d'épargne (fonds) des délinquantes. | 150 |
| SGRH | Le Système de gestion des ressources humaines (SGRH) est un composant de l'application PeopleSoft. PeopleSoft est une application commerciale répandue dans les secteurs privé et public, qui offre un éventail de produits, dont des modules de Gestion des ressources humaines, de Gestion financière, de Gestion du matériel et de Programmation du temps et du travail. | 3 200 |
| SIGFM | Le Système intégré de gestion des finances et du matériel (SIGFM) est le système de gestion financière du SCC. | 600 |
| Paye en direct | Le système de paye en direct est utilisé par le SCC pour traiter les données de paye. | |
| RADAR | RADAR (Rapports automatisés de données appuyant la réinsertion) est une application de production de rapports qui permet au personnel et aux | 10 000 |

gestionnaires du SCC d'accéder de façon conviviale à l'information sur les délinquantes contenue dans le SGD.

# 2.0 OBJECTIFS ET PORTÉE DE LA VÉRIFICATION

## 2.1 Objectifs de la vérification

Cette vérification vise à donner des assurances raisonnables que le cadre de contrôle de gestion qui est en place pour appuyer la préparation de la reprise après sinistre des systèmes de technologie de l'information est adéquat et efficace. La vérification a également examiné les progrès réalisés dans la mise en œuvre des exigences reliées aux plans de reprise de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du SCT et les améliorations entreprises dans la foulée de l'exercice de simulation des plans de reprise réalisé par les SGI en 2005.

## 2.2 Portée de la vérification

La vérification était basée sur une évaluation initiale des risques. Ainsi, la vérification portait sur les plans de reprise des applications essentielles des SGI et sur les contrôles en place à l'administration centrale (AC) et au centre de Laval pour soutenir la mise en œuvre rapide des plans de reprise. Compte tenu des risques identifiés, la vérification portait également sur les liens entre les plans de reprise et les plans de continuité des opérations (PCO), mais pas sur les PCO comme tels. Les contrôles des plans de reprise n'ont été testés que sur le plan de la conception et de la mise en œuvre (c.-à-d. à un moment précis dans le temps) et non sur le plan de leur efficacité opérationnelle (c.-à-d. au cours d'une période de temps).

Les régions ont récemment commencé à élaborer des plans de reprise, mais les bureaux régionaux n'ont que très récemment commencé à participer aux activités reliées aux plans de reprise dans le contexte des exercices de simulation des plans de reprise. La vérification des plans de reprise englobait donc un examen des plans de reprise régionaux, mais il n'a pas été jugé nécessaire de faire des visites dans chaque région, compte tenu des activités de contrôle limitées effectuées dans les régions et du fait que toutes les applications essentielles sont gérées centralement à l'AC. La seule visite à l'extérieur de la région de la capitale nationale (RCN) a été effectuée au centre de traitement secondaire de Laval.

# 3.0 APPROCHE ET MÉTHODOLOGIE DE VÉRIFICATION

L'approche et la méthodologie utilisées sont conformes aux normes de vérification interne de l'Institute of Internal Auditors et respectent la Politique de vérification interne du gouvernement du Canada.

À la suite d'une analyse des cadres de contrôle potentiels à utiliser pour la vérification, un programme de vérification basé sur les risques a été élaboré à partir des exigences du processus DS4 de COBIT 4.1 (www.isaca.org), et comprend aussi les exigences reliées spécifiquement aux plans de reprise de la Politique du gouvernement sur la sécurité et la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information du SCT (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328). Les critères de vérification sont présentés à l'Annexe A.

Les travaux de vérification ont été réalisés dans la RCN entre septembre et décembre 2008, et comprenaient une visite au centre de traitement secondaire de Laval. Des entrevues ont été réalisées avec de nombreux représentants du SCC responsables des activités reliées aux plans de reprise. Les tests comprenaient un examen des directives et des lignes directrices, de la structure organisationnelle, des rôles et responsabilités, et l'observation de l'exercice de simulation mené pour l'AC en novembre 2008. En ce qui concerne l'AC, le cycle complet des plans de reprise a été testé, soit : l'élaboration initiale, les essais, la formation, la maintenance et la mise à jour. Pour les régions, les tests se sont limités à un examen des plans de reprise régionaux et à un nombre limité d'entrevues.

Après avoir terminé le travail sur le terrain, l'équipe a tenu une réunion de débreffage à l'administration centrale avec le dirigeant principal de l'information, Services de gestion de l'information, et le directeur, Sécurité de la TI et gestion de projet.

# 4.0 CONCLUSIONS ET RECOMMANDATIONS

## 4.1 Cadre de contrôle de gestion pour la planification de la reprise après sinistre

Nous avons évalué dans quelle mesure le cadre de contrôle de gestion pour les plans de reprise après sinistre est en place.

### 4.1.1 Cadre des plans de reprise (processus DS4.1 de COBIT)

Nous nous attendions à trouver un cadre pour soutenir la planification de la reprise après sinistre dans l'ensemble de l'entreprise, qui utiliserait un processus cohérent et systématique. L'objectif du cadre devrait être d'aider à déterminer la résilience requise de l'infrastructure et d'orienter l'élaboration de plans de reprise. Ce cadre devrait englober la structure organisationnelle, y compris les rôles, les tâches et les responsabilités des fournisseurs de services internes et externes, leur gestion et leurs clients, ainsi que les processus de planification qui créent les règles et les structures utilisées pour documenter, tester et exécuter les plans de reprise après sinistre et de mesures d'urgence pour les TI. Les plans de reprise devraient aussi comprendre l'identification des ressources essentielles, en notant les dépendances importantes, la

surveillance et la déclaration de la disponibilité des ressources essentielles, les installations de traitement d'appoint, et les principes de sauvegarde et de récupération.

***Le cadre des plans de reprise est bien conçu en ce qui concerne les applications essentielles se trouvant à l'AC, mais il n'est pas entièrement mis en œuvre, car il y a encore de nombreux aspects à améliorer. Le cadre n'est pas encore mis en œuvre de façon suffisante dans les régions.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Le SCC n'a pas évalué officiellement l'adéquation de n'avoir qu'une seule ressource qui se consacre aux activités reliées aux plans de reprise, ce qui accroît le risque que le programme de plans de reprise manque de personnel.*
- *Un modèle standard pour l'élaboration des plans de reprise régionaux et des autres documents connexes n'a pas été élaboré et distribué aux régions du SCC pour faire en sorte que les plans régionaux soient complets et cohérents. Par exemple, la plupart des plans de reprise régionaux n'identifient pas les personnes affectées à diverses responsabilités, et on n'y retrouve pas certaines informations clés, comme la liste des applications essentielles et les délais de récupération ciblés. Ce manque de cohérence accroît le risque que les efforts de reprise seront plus difficiles à coordonner advenant un sinistre exigeant l'activation de multiples plans de reprise.*
- *Les SGI n'ont pas conclu avec leurs clients d'accords internes sur les niveaux de service décrivant la disponibilité exigée des systèmes, ce qui accroît le risque que les SGI ne soient pas informés ni capables de répondre aux besoins de disponibilité des secteurs opérationnels.*
- *Il n'existe aucune preuve que les plans de reprise ont été approuvés par la haute direction, ce qui accroît le risque que les plans ne répondent pas aux besoins de la haute direction.*

**Recommandation n$^{o}$ 1**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait évaluer officiellement l'adéquation du niveau de ressources actuellement affectées au programme de plans de reprise.

**Recommandation n$^{o}$ 2**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait préparer un modèle standard pour la documentation, les essais et la diffusion des plans de reprise au niveau régional au sein du SCC.

**Recommandation n$^{o}$ 3**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait s'assurer que des accords officiels sur les niveaux de service décrivant les exigences en matière de disponibilité des systèmes sont établis entre les SGI et leurs clients dans l'ensemble du SCC.

**Recommandation n$^{o}$ 4**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait s'assurer que tous les plans de reprise existants sont examinés et officiellement approuvés par les mêmes parties qui sont les signataires des accords internes sur les niveaux de service spécifiant les exigences de disponibilité. Tous les changements importants apportés aux plans de reprise devraient aussi faire l'objet d'une évaluation et d'une approbation officielle de la part des gestionnaires/propriétaires d'applications.

### 4.1.2 Plans de reprise après sinistre, ressources essentielles, récupération et reprise (processus DS4.2, 4.3 et 4.8 de COBIT)

Nous nous attendions à trouver des plans de reprise basés sur le cadre et conçus pour réduire l'impact d'une interruption majeure des fonctions et des processus opérationnels clés. Les plans devraient être basés sur la compréhension des risques liés aux impacts opérationnels potentiels et tenir compte des exigences en matière de résilience, de traitement d'appoint et de capacité de reprise de tous les services essentiels de TI. Ils devraient également englober les lignes directrices en matière d'utilisation, les rôles et responsabilités, les procédures, les processus de communication et l'approche en matière de tests et d'essais. Les plans de reprise devraient mettre l'accent sur les éléments identifiés comme étant les plus essentiels et établir les priorités à respecter en cas de reprise. Les plans de reprise devraient prévoir des interventions de récupération concordant avec les besoins opérationnels prioritaires, tout en assurant que les coûts sont maintenus à un niveau acceptable et en respectant les exigences réglementaires et contractuelles. Enfin, nous nous attendions à trouver des plans décrivant les mesures à prendre pendant la période de récupération et de rétablissement des services de TI.

***Les plans de reprise sont bien conçus en ce qui concerne les applications essentielles situées à l'AC, mais ils ne sont pas pleinement mis en œuvre, car il reste encore plusieurs aspects à améliorer. Les plans de reprise n'ont pas été suffisamment mis en œuvre dans les régions.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Étant donné que le SCC se fiait à la liste des applications essentielles identifiées pour les efforts de reprise liés au passage à l'an 2000, aucune analyse des incidences opérationnelles n'a été réalisée, ce qui accroît le risque que les applications essentielles n'ont peut-être pas toutes été identifiées correctement et que les délais de reprise cibles définis ne sont pas adéquats. Une analyse des*

*incidences opérationnelles est généralement effectuée dans le cadre du processus de PCO, qui relève de l'agent de sécurité du SCC.*

- *Les plans de reprise des applications essentielles de l'AC sont basés sur des délais de reprise définis, mais l'on ne sait pas si tous ces objectifs peuvent être atteints, tout particulièrement en cas de sinistre général où toutes les applications essentielles doivent être restaurées, ce qui accroît le risque que des ressources de TI ne seront pas rétablies à temps pour satisfaire aux exigences des secteurs opérationnels.*
- *Il n'existe pas d'orientations claires quant au délai à l'intérieur duquel un sinistre devrait être déclaré (les délais de reprise cibles n'entrent en jeu qu'après la déclaration d'un sinistre), ce qui accroît le risque qu'un sinistre ne soit pas déclaré assez rapidement pour répondre aux besoins des secteurs opérationnels.*
- *Le rôle de reprise après sinistre et la formation du personnel qui travaille au centre de traitement secondaire (à Laval) ont été réduits, et les plans de reprise dépendent surtout du personnel de l'AC, ce qui accroît le risque de retarder encore davantage les efforts de reprise, advenant que le personnel de l'AC mette du temps à se rendre au centre de traitement secondaire.*
- *Les plans de reprise pourraient tirer parti du Collège du personnel situé à côté du centre de traitement secondaire, mais ils dépendent de la disponibilité de chambres d'hôtel à proximité pour héberger les ressources de l'AC, ce qui accroît le risque d'un retard supplémentaire des efforts de reprise, advenant que le personnel de l'AC mette du temps à s'installer au site secondaire.*

**Recommandation n$^{o}$ 5**

Directeur, Sûreté, sécurité et protection civile devrait s'assurer qu'une analyse officielle des incidences opérationnelles est réalisée par les responsables des opérations/applications pour confirmer l'identification des applications essentielles et pour valider de nouveau que les délais de reprise prévus demeurent appropriés et pertinents.

**Recommandation n$^{o}$ 6**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait élaborer un programme de formation sur les plans de reprise spécifiquement conçu pour permettre aux ressources du centre de Laval de mieux connaître les plans de reprise, ce qui accroîtra la disponibilité de ressources qualifiées en cas de sinistre.

### 4.1.3 Plans de reprise – Maintenance, essais et formation (processus DS4.4, 4.5 et 4.6 de COBIT)

Nous nous attendions à ce que des procédures de contrôle du changement soient en place pour faire en sorte que les plans de reprise soient tenus à jour et continuent à refléter les exigences opérationnelles réelles, et à ce que les changements apportés

aux procédures et aux responsabilités soient communiqués clairement et rapidement. Nous nous attendions aussi à ce que des tests périodiques des plans de reprise soient effectués pour faire en sorte que les systèmes de TI soient rétablis de façon efficace, que les lacunes soient corrigées et que les plans demeurent pertinents. Cela exige de faire une préparation minutieuse, de documenter les tests, de rendre compte des résultats, et de mettre en place un plan d'action en fonction de ces résultats. Enfin, nous nous attendions à constater que toutes les parties concernées ont accès à des séances de formation périodiques sur les procédures et sur leurs rôles et responsabilités en cas d'incident ou de sinistre.

***Un plan de tests a été conçu et partiellement mis en œuvre pour les applications essentielles et les régions, ce plan consistant essentiellement en des tests de simulation et en des tests de basculement limités. L'on procède à la mise à jour régulière des plans de reprise, mais il n'est pas clair si ces mises à jour tiennent compte de toutes les leçons tirées des tests réalisés.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Bien que des tests de basculement aient été réalisés pour trois applications essentielles, des tests complets n'ont pas été effectués pour toutes les applications essentielles, ce qui accroît le risque que les délais de reprise définis ne répondent pas aux besoins de tous les secteurs opérationnels, et que les plans de reprise actuels omettent des étapes importantes pour permettre la reprise complète de toutes les applications essentielles.*
- *La capacité du centre de traitement secondaire à assurer l'exploitation de toutes les applications essentielles n'a pas fait l'objet d'une évaluation officielle, ce qui accroît le risque que des applications essentielles ne fonctionnent pas si elles sont exploitées depuis le centre de traitement secondaire.*
- *Les plans de reprise ne sont pas toujours mis à jour sur une base au moins annuelle, comme l'exigent les lignes directrices des SGI, ce qui accroît le risque que ces plans soient désuets et omettent des étapes essentielles à la reprise des applications essentielles.*
- *Les leçons et plans d'action découlant des séances d'essai n'ont pas été systématiquement documentés, ce qui accroît le risque que les problèmes identifiés lors des tests n'aient pas été corrigés ou mis à jour dans le cadre du plan de reprise. Des vingt améliorations potentielles identifiées lors de l'exercice de simulation du plan de reprise de 2005, onze ont été effectuées (55 %), deux ont été mises en œuvre partiellement (10 %), et sept n'ont pas encore été réalisées (35 %).*
- *Il n'existe pas de plan de formation officiel. La formation des ressources affectées à la reprise après sinistre passe essentiellement par la participation aux exercices de simulation, mais cette participation n'est pas obligatoire. Cela accroît le risque que le personnel ne reçoive pas toujours la formation requise.*

**Recommandation n$^{o}$ 7**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait élargir le programme d'essai actuel en incorporant la mise à l'essai annuelle de la capacité de traitement du centre de traitement secondaire.

**Recommandation n$^{o}$ 8**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait s'assurer que tous les documents de plans de reprise sont mis à jour au moins chaque année ou à la suite d'un changement important. Dans le cadre de cette mise à jour, le dirigeant principal de l'information devrait aussi s'assurer que les plans de reprise sont officiellement évalués et approuvés par les propriétaires d'applications.

**Recommandation n$^{o}$ 9**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait mettre en œuvre un processus visant à faire en sorte que les leçons tirées des tests des plans de reprise soient systématiquement documentées et appliquées de façon proactive.

### 4.1.4 Diffusion des plans de reprise après sinistre (processus DS4.7 de COBIT)

Nous nous attendions à constater l'existence d'une stratégie de diffusion définie et gérée, pour s'assurer que les plans sont distribués de façon correcte et sûre, et qu'ils sont accessibles à toutes les parties autorisées, en temps et lieu nécessaires. Il faudrait veiller à ce que les plans soient accessibles dans tous les scénarios de sinistre.

***Un plan limité de diffusion des plans de reprise a été préparé et mis en œuvre à l'AC, mais pas dans les régions. Les plans de reprise sont conservés dans un référentiel central à l'AC, et une copie est envoyée chaque jour au centre de traitement de Laval, mais ces processus de diffusion pourraient être améliorés.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Les plans de reprise ne prévoient pas, actuellement, un plan de diffusion complet, listant toutes les personnes qui devraient avoir une copie du plan de reprise le plus récent et la méthode de diffusion, ce qui accroît le risque que les plans de reprise ne seront pas immédiatement disponibles dans l'éventualité d'un sinistre.*
- *Lors de nos tests, le personnel responsable de la reprise après sinistre du centre de traitement de Laval ne pouvait pas accéder immédiatement aux documents pertinents, ce qui accroît le risque que les plans de reprise ne seront pas immédiatement disponibles en cas de sinistre.*

**Recommandation n$^{o}$ 10**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait s'assurer que les plans de reprise comprennent un plan de diffusion complet, listant toutes les personnes qui devraient avoir une copie du plan de reprise le plus récent et la méthode de diffusion, et que le personnel du centre de traitement secondaire a immédiatement accès aux documents relatifs à la reprise après sinistre.

### 4.1.5 Stockage hors site des bandes de sauvegarde (processus DS4.9 de COBIT)

Nous nous attendions à ce que tous les éléments essentiels et nécessaires à l'exécution des plans de reprise et de continuité des opérations de TI – supports de sauvegarde, documentation et autres ressources de TI – soient conservés hors site. La gestion de l'installation de stockage hors site devrait respecter la politique de classification des données et les pratiques de stockage des supports du SCC. Les services de gestion de la TI devraient s'assurer d'évaluer le contenu, la protection environnementale et la sécurité des aménagements de stockage hors site. Ils devraient également assurer la compatibilité des matériels et logiciels nécessaires à la restauration des données archivées, aux tests et au rafraîchissement périodiques des données archivées.

***Un processus de stockage hors site des bandes de sauvegarde a été établi et mis en œuvre. Certaines applications essentielles utilisent la réplication des données pour réduire les risques de perte, mais les processus de stockage hors site devraient être améliorés.***

*Plus précisément, lors de nos tests, nous avons fait l'observation suivante :*

- *Les bandes de sauvegarde des applications essentielles et des régions ne sont pas cryptées, ce qui accroît le risque d'accès non autorisé aux données de sauvegarde, en particulier pendant le transit des bandes entre le SCC et les Archives nationales ou le centre de traitement secondaire.*

**Recommandation n$^{o}$ 11**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait mettre en œuvre une solution qui permet au SCC de crypter les bandes de sauvegarde pour les données d'applications jugées de nature sensible sur le plan de la sécurité ou de l'accès à l'information.

### 4.1.6 Évaluation post-reprise (processus DS4.10 de COBIT)

Nous nous attendions à ce que les services de gestion de la TI aient établi des procédures pour évaluer l'adéquation du plan pour ce qui est du rétablissement réussi de la fonction de TI après un sinistre, et pour actualiser le plan en conséquence.

***Un processus d'évaluation post-reprise n'a pas encore été établi et mis en œuvre.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Nous n'avons trouvé aucune preuve que les leçons tirées des tests des plans de reprise et des incidents et sinistres réels sont officiellement prises en compte pour améliorer les plans de reprise, ce qui accroît le risque que les plans de reprise omettent des étapes importantes permettant la reprise complète des applications essentielles.*
- *Les plans de reprise ne prévoient pas actuellement d'étapes pour la reprise des activités à l'installation de traitement principale, ce qui accroît le risque que le retour aux opérations de TI normales soit retardé.*

**Recommandation n° 12**

Le dirigeant principal de l'information, Services de gestion de l'information, devrait s'assurer que le plan de reprise incorpore un plan de rétablissement des activités à l'AC ou, encore, un nouveau plan de reprise qui guiderait le personnel responsable de la reprise après sinistre dans l'éventualité d'un sinistre au centre de traitement secondaire (avant la reprise à l'AC).

### CONCLUSION

Dans l'ensemble, le SCC a défini et mis en œuvre certains éléments importants du cadre de gestion des plans de reprise. Cependant, il sera important que le SCC établisse, entre les SGI et leurs clients, des accords officiels sur les niveaux de service qui décrivent de façon détaillée les exigences de disponibilité des systèmes. Pour permettre l'établissement de tels accords, une analyse officielle des incidences opérationnelles devrait être réalisée. En outre, un test complet de basculement devrait être effectué pour toutes les applications essentielles, et les efforts actuels de mise en œuvre et de mise à l'essai des plans de reprise dans les régions devraient se poursuivre.

## 4.2 Progrès réalisés dans la mise en œuvre de la GSTI et des améliorations découlant des exercices de simulation

La vérification avait pour deuxième objectif d'évaluer les progrès réalisés dans la mise en œuvre des exigences liées aux plans de reprise énoncées dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du SCT, et des améliorations entreprises à la suite de l'exercice de simulation des plans de reprise effectué par les SGI en 2005.

### 4.2.1 Mise en œuvre des exigences de GSTI reliées aux plans de reprise

Nous nous attendions à trouver des preuves que le SCC a officiellement mis en œuvre l'exigence de GSTI reliée aux plans de reprise, plus précisément :

- Dans le cadre de la planification de la continuité des activités, les ministères doivent d'abord élaborer un plan de continuité pour la GI et un autre pour les TI, puis les tester et les réviser régulièrement. (GSTI 12.8)
- Les ministères doivent rétablir les fonctions essentielles dans les limites de temps et selon les exigences de disponibilité précisées dans le Plan de continuité des activités du ministère. (GSTI 18.5)
- Des procédures de sauvegarde et de reprise existent et sont documentées. (GSTI 18.5)
- Des données de sauvegarde sont créées régulièrement et des copies sont conservées hors site. (GSTI 18.5)

***Le SCC a donné suite aux exigences relatives aux plans de reprise de la GSTI, à l'exception des exigences relatives aux tests et à la révision des plans de reprise.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Des plans de reprise ont été produits pour les applications essentielles à l'AC et pour les régions, mais n'ont pas été systématiquement révisés et testés, ce qui accroît le risque que les plans de reprise omettent des étapes nécessaires à la reprise des applications régionales essentielles.*
- *Le SCC n'a pas entièrement testé sa capacité de restaurer toutes les applications essentielles dans les délais prescrits et selon les exigences de disponibilité spécifiées dans les PCO, ce qui accroît le risque que des applications essentielles ne soient pas restaurées rapidement, ou qu'elles fonctionnent aux niveaux de traitement attendus lorsqu'elles sont exploitées au centre de traitement secondaire.*
- *Les procédures de sauvegarde et de reprise sont documentées. Des données de sauvegarde sont créées régulièrement et des copies sont conservées hors site.*

Ces observations ont déjà été présentées dans la Section 4.1 et les recommandations pertinentes y sont également incluses.

### 4.2.2 Mise en œuvre des améliorations

Nous nous attendions à trouver des preuves que le SCC a officiellement apporté les améliorations identifiées lors de l'exercice de simulation des plans de reprise réalisé par les SGI en 2005.

***Des vingt améliorations potentielles identifiées lors de l'exercice de simulation du plan de reprise de 2005, onze ont été effectuées (55 %), deux ont été mises en œuvre partiellement (10 %), et sept n'ont pas encore été réalisées (35 %). La liste complète des améliorations et de leur état actuel est présentée à l'Annexe B.***

*Plus précisément, lors de nos tests, nous avons fait les observations suivantes :*

- *Les plans de reprise ne documentent pas spécifiquement quelles ressources de l'AC seront réinstallées au centre de traitement secondaire, dans quel délai ces ressources devraient être réinstallées, où elles seront logées et pendant combien de temps. Cela accroît le risque de retarder l'installation du personnel de l'AC au centre de Laval et, par conséquent, de retarder les efforts de reprise.*
- *Les plans de reprise ne prévoient pas de processus documenté pour le transport sécurisé des bandes de sauvegarde au centre de traitement secondaire, ce qui accroît le risque d'accès non autorisé, de perte ou de vol des bandes de sauvegarde.*

Ces observations ont déjà été présentées dans la Section 4.1 et les recommandations pertinentes y sont également incluses.

## CONCLUSION

Des progrès ont été réalisés dans la mise en œuvre des améliorations identifiées dans la norme de GSTI et lors de l'exercice de simulation des plans de reprise de 2005. Il faut cependant poursuivre les efforts pour satisfaire pleinement aux exigences de GSTI visant les tests et la révision des plans de reprise.

# Annexe A

## Critères de vérification

Les critères de vérification ont été élaborés à partir des exigences des processus DS4 de COBIT 4.1 (www.isaca.org), et comprennent aussi les exigences relatives aux plans de reprise de la Politique sur la sécurité du gouvernement et la Norme de gestion de la sécurité de l'information du SCT (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328).

**1. Cadre de référence de la continuité des opérations de TI**
Développer un cadre de référence de la continuité informatique pour soutenir la gestion de la continuité des opérations dans l'ensemble de l'entreprise selon un processus cohérent. L'objectif de ce cadre de référence est d'aider à déterminer la résilience requise de l'infrastructure et d'induire le développement de plans de reprise informatique. Il doit prendre en compte la structure organisationnelle de gestion de la continuité des opérations, y compris les rôles, les tâches et les responsabilités des fournisseurs de services internes et externes, leur gestion et leurs clients, ainsi que les processus de planification qui créent les règles et les structures permettant de documenter, de tester et d'exécuter les plans de reprise après sinistre et de mesures d'urgence pour les TI. Les plans de reprise devraient aussi comprendre l'identification des ressources essentielles, en notant les dépendances importantes, la surveillance et la déclaration de la disponibilité des ressources essentielles, les installations de traitement de secours, et les principes de sauvegarde et de restauration.

**2. Plans de continuité des opérations de TI**
Développer des plans de reprise basés sur le cadre et conçus pour réduire l'impact d'une interruption majeure des fonctions et des processus opérationnelles clés. Les plans devraient être basés sur la compréhension des risques liés aux impacts opérationnels potentiels et tenir compte des exigences en matière de résilience, de traitement d'appoint et de capacité de reprise de tous les services essentiels de TI. Ils devraient également englober les lignes directrices en matière d'utilisation, les rôles et responsabilités, les procédures, les processus de communication et l'approche en matière de tests et d'essais.

**3. Ressources de TI essentielles**
Concentrer l'attention sur les éléments considérés comme les plus vitaux dans le plan de continuité des opérations de TI pour en renforcer la résilience et établir les priorités lorsqu'il s'agit de rétablir une situation dégradée. Éviter de perdre du temps à récupérer les éléments les moins importants et tenir compte des besoins opérationnels prioritaires, tout en s'assurant que les coûts restent à un niveau acceptable et en se conformant aux exigences réglementaires et contractuelles. Prendre en compte les exigences de durée en matière de résilience, de réactivité et de restauration pour différents laps de temps, p. ex. 1 à 4 heures, 4 à 24 heures, plus de 24 heures et les périodes critiques d'activités opérationnelles.

**4. Maintenance du Plan de continuité des opérations de TI**
Encourager les gestionnaires de la TI à définir et à appliquer des procédures de contrôle du changement pour s'assurer que le plan de continuité est tenu à jour et reflète toujours les exigences opérationnelles réelles. Communiquer clairement et rapidement les changements apportés aux procédures et aux responsabilités.

**5. Tests du Plan de continuité des opérations de TI**
Tester régulièrement le plan de continuité des opérations de TI pour s'assurer que les systèmes de TI peuvent être restaurés de façon efficace, que les lacunes sont corrigées et que le plan demeure pertinent. Cela exige de faire une préparation minutieuse, de documenter les tests, de rendre compte des résultats, et de mettre en place un plan d'action en fonction de ces résultats. Envisager d'étendre les tests de restauration d'applications individuelles à des scénarios de tests intégrés, à des tests exhaustifs et à l'intégration de tests fournisseurs.

**6. Formation sur le Plan de continuité des opérations de TI**
S'assurer que toutes les parties concernées bénéficient de séances de formation périodiques sur les procédures et sur leurs rôles et responsabilités en cas d'incident ou de sinistre. Vérifier et améliorer la formation en fonction des résultats des tests de situations d'urgence.

**7. Diffusion du Plan de continuité des opérations de TI**
Vérifier ou faire en sorte qu'il existe une stratégie de diffusion définie et gérée, pour s'assurer que tous les plans sont distribués de façon sûre et qu'ils sont disponibles pour les parties dûment autorisées et intéressées, à l'endroit et au moment où elles en ont besoin. Bien vérifier que les plans soient accessibles selon tous les scénarios de sinistres.

**8. Reprise et rétablissement des services de TI**
Prévoir les actions à entreprendre pendant la période de restauration et de redémarrage des services de TI. Cela peut concerner l'activation de sites de secours, le lancement de traitements alternatifs, la communication à l'intention des parties prenantes et des clients, et les procédures de redémarrage. S'assurer que les secteurs opérationnels comprennent les délais de restauration et les investissements technologiques nécessaires pour répondre aux besoins de restauration et de redémarrage.

**9. Stockage hors site des bandes de sauvegarde**
Stocker hors site tous les supports de sauvegarde critiques, la documentation et les autres ressources de TI nécessaires à la restauration des opérations de TI et aux plans de continuité. Le contenu de ce stockage de sauvegarde doit être déterminé par une collaboration entre les propriétaires de processus opérationnels et le personnel informatique. Les responsables de l'installation de stockage hors site doivent s'aligner sur la politique de classification des données et sur les pratiques de stockage des supports de l'entreprise. La direction informatique doit s'assurer que les équipements hors site sont évalués périodiquement, au moins annuellement, en ce qui concerne leur

contenu, leur protection vis-à-vis de l'environnement, et leur sécurité. S'assurer que la compatibilité des matériels et de logiciels permet de restaurer les données archivées, et tester et rafraîchir périodiquement les archives.

**10. Évaluation post-reprise**

Déterminer si les gestionnaires de la TI ont établi des procédures pour évaluer l'adéquation du plan quant à la reprise réussie de la fonction TI après un sinistre, et mettre le plan à jour en conséquence.

# *Annexe B*

## Suites à donner – Reprise sûre I

| Réf. | Suites à donner/ Leçons tirées de l'expérience/ Commentaires | Constatation | État |
|---|---|---|---|
| **Phase d'alerte** | | | |
| i. | Il faut tenir compte du délai nécessaire aux équipes de reprise pour se réunir avant le déploiement au site de reprise. | Les plans ne font pas état du temps nécessaire. Il n'a pas été possible de documenter cette question lors de la rencontre du 23 décembre 2008 avec le coordonnateur de la reprise après sinistre. Il incombe aux groupes de reprise de respecter les délais cibles. | Pas mis en œuvre |
| ii. | La liste de contacts posait problème. Leçon tirée de l'expérience : les membres des équipes devraient avoir tous les numéros de contact de leur équipe, et un plan d'appel. | Lors de la rencontre de 2005, Bruno était chargé d'appeler tous les membres. Cela a changé pour l'exercice de simulation de 2007. Le plan d'appel est documenté dans le PCO. | Mis en œuvre |
| iii. | Leçon tirée de l'expérience : la haute direction devrait tenir une réunion pour discuter des mesures à prendre avant la déclaration d'un sinistre. | Cela n'était pas inclus dans le plan en 2005. En 2008, le PCO situait le Centre des opérations d'urgence au 100, rue Metcalfe. | Mis en œuvre |
| iv. | Prévoir un processus de notification pour informer le contact suppléant désigné qu'il est le responsable principal en cas d'absence du responsable principal. | En 2005, des suppléants n'étaient pas identifiés. Le PCO et les plans de reprise de 2008 prévoient des responsables principaux et des suppléants. | Mis en œuvre |
| **Phase de déploiement** | | | |
| i | **Équipe de reprise** | | |
| i.1 | Le point de rendez-vous doit être clairement identifié. | En 2005, le point de rendez-vous n'était pas documenté. En 2008, le point de rendez-vous, à savoir le Centre commercial Carlingwood, est documenté dans le PCO. | Mis en œuvre |
| i.2 | Les employés habitent dans tous les quartiers d'Ottawa. L'autobus à destination de Laval pourrait cueillir ces employés en cours de route. | Il y a un point de rendez-vous unique et central. | Mis en œuvre |
| i.3 | Il est prévu que le déploiement | Ceci est un commentaire. En | Pas mis en |

| Réf. | Suites à donner/ Leçons tirées de l'expérience/ Commentaires | Constatation | État |
|---|---|---|---|
| | initial de tout le personnel sera de 30 jours, ce qui est trop long. Après la reprise, il ne faut qu'un nombre limité d'employés de l'AC au site de Laval. | 2005, la durée n'était pas précisée. En 2008, il était entendu que le personnel n'était nécessaire au site de Laval que jusqu'à ce que le site soit fonctionnel, soit trois jours. Cela n'est pas documenté. La plupart des employés ont l'impression qu'ils ne sont pas obligés d'être sur les lieux. Ils croient qu'ils travailleront via un réseau privé virtuel. | œuvre |
| i.4 | Un aide-mémoire devrait être créé pour rappeler aux membres de l'équipe ce qu'ils devraient apporter au site de reprise. | Cet aide-mémoire n'a pas été créé. | Pas mis en œuvre |
| i.5 | Il n'est pas prévu de payer le personnel contractuel au-delà des 37,5 heures de travail par semaine. | Lors de la rencontre du 23 décembre 2008 avec Terry, il a été indiqué que des clauses de disponibilité pour les plans de reprise sont ajoutées aux contrats à mesure qu'ils sont renouvelés. | Mis en œuvre en partie |
| i.6 | Le gestionnaire désigné responsable de l'organisation des services d'autobus devrait être informé de cette responsabilité. | Mentionné dans le PCO. Lors de la rencontre du 23 décembre 2008 avec Terry, le gestionnaire de la reprise pour le PCO (Murray) avait cette responsabilité. Cela a été confirmé par Murray lors de son entrevue. | Mis en œuvre |
| i.7 | D'autres moyens de transport devraient être examinés. | Lors de la rencontre avec le coordonnateur de la reprise après sinistre, il a été indiqué que le gestionnaire du PCO avait cette responsabilité. | Pas mis en œuvre |
| **Droit de refus** | | | |
| ii.1 | Il faut revoir la composition de l'équipe de reprise, car le déploiement à un autre site avec quelques heures d'avis pose problème pour certains membres. | Selon le coordonnateur de la reprise, le SCC ne peut pas obliger un employé à répondre lors d'un sinistre, mais la plupart des responsables principaux comprennent qu'ils doivent être présents. Cependant, lors des entrevues, la plupart d'entre eux ont indiqué qu'ils ne pensent pas | Pas mis en œuvre |

| Réf. | Suites à donner/ Leçons tirées de l'expérience/ Commentaires | Constatation | État |
|---|---|---|---|
| | | qu'il sera nécessaire de se rendre à Laval. | |
| ii.2 | Prévoir des mécanismes pour les membres d'équipe pour lesquels la relocalisation au site de reprise pose des problèmes familiaux ou de santé. | Le mécanisme en question réside dans le personnel suppléant. En 2005, les suppléants n'étaient pas définis. Chaque responsable principal et membre clé a un suppléant désigné. | Mis en œuvre |
| **Espace physique** | | | |
| iii.1 | Au site de reprise, l'espace physique est limité à 15 personnes. Beaucoup plus de 15 personnes sont désignées pour se rendre au site de reprise. | Il est entendu officieusement qu'on pourra utiliser le Collège du personnel. | Mis en œuvre en partie |
| **Bandes de sauvegarde** | | | |
| iv.1 | Contradiction dans les plans : les bandes sont en fait récupérées du centre King Edward, et non des Archives nationales. | Lors des entrevues et de l'examen du processus, il a été indiqué que les bandes sont conservées aux Archives nationales et au centre King Edward (2 copies). Les bandes seront récupérées des Archives nationales. | Mis en œuvre |
| iv.2 | Transport des bandes de sauvegarde – La norme de sécurité matérielle du Secrétariat du Conseil du Trésor (SCT) exige le transport sécurisé des bandes. Il faut mettre en place un processus selon lequel, en cas d'accident, la police serait informée que le véhicule contient une cargaison précieuse et que le contenant devrait être protégé et remis uniquement à une personne autorisée. | Les plans ne prévoient pas de transport sécurisé. | Pas mis en œuvre |
| **Hébergement du personnel à Laval** | | | |
| v.1 | Les documents ne précisent pas où le personnel sera hébergé à Laval. | Cette question demeure en suspens. Il est entendu officieusement que Normand Vermette à Laval prendra les mesures nécessaires pour loger le personnel dans la région de Laval ou au Collège du | Pas mis en œuvre |

| Réf. | Suites à donner/ Leçons tirées de l'expérience/ Commentaires | Constatation | État |
|---|---|---|---|
| | | personnel. Il n'existe pas d'ententes officielles. | |
| **Phase de récupération/restauration/reprise** | | | |
| i | Lorsqu'on leur donne la possibilité de se rencontrer, les équipes de reprise apprécient l'occasion d'examiner et de réviser leurs plans. | Des exercices de simulation sont réalisés chaque année, et les plans sont actualisés en conséquence. | Mis en œuvre |
| ii | Le Bureau de service n'avait pas de plan de reprise détaillé. | Le Bureau de service a un plan de reprise détaillé. Nous avons observé les procédures de reprise du Bureau de service lors de l'exercice de simulation. | Mis en œuvre |
| iii | Les plans de reprise ne prévoient pas l'établissement d'un « centre de commandement » (CC) ou d'un « poste de commandement » (PC). | Il n'y avait pas de poste de commandement en 2005. En 2007, le 441 MacLean était défini comme le centre de commandement. En 2008, il s'agissait du 100, rue Metcalfe. | Mis en œuvre |

# *Annexe C*

## Plan d'action de gestion

| Recommandation | Résumé des mesures prises | BPR | Date d'achèvement prévue |
|---|---|---|---|
| **Recommandation n° 1**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait évaluer officiellement l'adéquation du niveau de ressources actuellement affectées au programme de plans de reprise. | 1.) La Gestion de l'infrastructure et des opérations et la Sécurité de la technologie de l'information effectueront ensemble l'analyse de rentabilisation et la soumettront à l'approbation du dirigeant principal de l'Information. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) juin 2009 |
| **Recommandation n° 2**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait préparer un modèle standard pour la documentation, les essais et la diffusion des plans de reprise au niveau régional au sein du SCC. | 1.) Le modèle a été créé en 2008. Les plans régionaux de reprise des activités après sinistre ont été conçus à l'exercice 2007-2008.<br>Des simulations ont eu lieu dans toutes les régions, y compris à l'administration centrale, à l'exercice 2008-2009, selon les modèles conçus.<br><br>2.) Le modèle sera envoyé aux administrateurs régionaux des services de gestion de l'information afin d'obtenir leurs commentaires. Ces administrateurs régionaux seront chargés de la mise en œuvre. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Terminé<br><br>2.) Avril 2009 |
| **Recommandation n° 3**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait s'assurer que des accords officiels sur les niveaux de service décrivant les exigences en matière de disponibilité des systèmes sont établis entre les SGI et leurs clients dans l'ensemble du SCC. | 1.) La Gestion de l'infrastructure et des opérations doit élaborer le modèle d'accord sur les niveaux de service.<br>Le modèle comprendra les objectifs sur les points de reprise et sur le temps de récupération en fonction des éléments de Certification et accréditation.<br><br>2.) La Gestion de l'infrastructure et des opérations doit établir des accords sur les niveaux de service pour toutes les applications essentielles à la mission.<br><br>3.) Approbation des accords sur les niveaux de service. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Terminé<br><br>2.) Avril 2010<br><br>3.) Avril 2010 |

| Recommandation | Résumé des mesures prises | BPR | Date d'achèvement prévue |
|---|---|---|---|
| **Recommandation n° 4**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait s'assurer que tous les plans de reprise existants sont examinés et officiellement approuvés par les mêmes parties qui sont les signataires des accords internes sur les niveaux de service spécifiant les exigences de disponibilité. Tous les changements importants apportés aux plans de reprise devraient aussi faire l'objet d'une évaluation et d'une approbation officielle de la part des gestionnaires/propriétaires d'applications. | 1.) Les plans de reprise en cas de sinistre seront revus d'ici le 31 mars 2009.<br><br>2.) Le coordonnateur de la reprise en cas de sinistre concevra des processus officiels d'examen et d'approbation des plans de reprise en cas de sinistre et les mettra à jour chaque année.<br><br>3.) Le dirigeant principal de l'Information doit approuver et mettre en œuvre le processus. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Terminé<br><br>2.) Juin 2009<br><br>3.) Juillet 2009 |
| **Recommandation n° 5**<br>L'agent de sécurité du SCC devrait s'assurer qu'une analyse officielle des incidences opérationnelles est réalisée par les responsables des opérations/applications pour confirmer l'identification des applications essentielles et pour valider de nouveau que les délais de reprise prévus demeurent appropriés et pertinents. | La Division de la sécurité du Ministère analysera les répercussions sur les opérations de l'AC au cours des prochains mois. Cette analyse comprendra un dialogue entre la Sécurité du Ministère, la Sécurité de la technologie de l'information ainsi que les gestionnaires/propriétaires des applications en vue de déterminer les applications essentielles et leurs objectifs en matière de temps de récupération. La participation active de tous les intervenants sera cruciale afin de veiller à ce que l'analyse des répercussions sur les opérations soit juste, bien conçue et pertinente à la mission du Service correctionnel du Canada. | L'agent de sécurité du SCC | Octobre 2009 |
| **Recommandation n° 6**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait élaborer un programme de formation sur les plans de reprise spécifiquement conçu pour permettre aux ressources du centre de Laval de mieux connaître les plans de reprise, ce qui accroîtra la disponibilité de ressources qualifiées en cas de sinistre**.** | 1.) La Gestion de l'infrastructure et des opérations doit concevoir et exécuter un plan de formation complémentaire pour les activités et les responsabilités relatives à la reprise après sinistre à Laval, y compris le calendrier de mise en œuvre. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Juin 2009 |

| Recommandation | Résumé des mesures prises | BPR | Date d'achèvement prévue |
|---|---|---|---|
| **Recommandation n° 7**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait élargir le programme d'essai actuel en incorporant la mise à l'essai annuelle de la capacité de traitement du centre de traitement secondaire. | 1.) Des essais sur la capacité et sur les répertoires anti-panne ont été effectués au site de reprise des activités en cas de sinistre en 2008 pour les applications du Système intégré de gestion des finances et du matériel ainsi que du Système de gestion des ressources humaines.<br><br>2.) Les essais sur la capacité et sur les répertoires anti-panne seront effectués chaque année pour les applications essentielles à la mission. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Terminé<br><br>2.) Mars 2010 |
| **Recommandation n° 8**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait s'assurer que tous les documents de plans de reprise sont mis à jour au moins chaque année ou à la suite d'un changement important. Dans le cadre de cette mise à jour, le dirigeant principal de l'Information devrait aussi s'assurer que les plans de reprise sont officiellement évalués et approuvés par les propriétaires d'applications. | 1.) Le coordonnateur de reprise après sinistre concevra un processus officiel d'examen et d'approbation des plans de reprise des activités après sinistre. Le dirigeant principal de l'Information des Services de gestion de l'information approuvera et mettra en œuvre le processus. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Juin 2009 |
| **Recommandation n° 9**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait mettre en œuvre un processus visant à faire en sorte que les leçons tirées des tests des plans de reprise soient systématiquement documentées et appliquées de façon proactive. | 1.) Le plan d'action a été créé afin de régler les problèmes relevés dans le document sur les leçons apprises 2007-2008.<br><br>2.) Le processus sera élaboré, approuvé et mis en œuvre par le dirigeant principal de l'Information des Services de gestion de l'information. Ce processus comprendra notamment les plans d'action visant à répondre aux recommandations formulées dans les leçons apprises. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Terminé<br><br>2.) Avril 2010 |
| **Recommandation n° 10**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait s'assurer que les plans de reprise comprennent un plan de diffusion complet, listant toutes les personnes qui devraient avoir une copie du plan de reprise le plus récent et la méthode de diffusion, et que le personnel du centre de traitement secondaire a immédiatement accès aux documents relatifs à la reprise après sinistre. | 1.) Les gestionnaires/propriétaires des applications doivent inclure une liste de diffusion dans les plans de reprise des activités après sinistre et maintenir cette liste à jour.<br><br>2.) Les employés de Laval ont déjà accès à tous les plans de reprise des activités après sinistre. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Juin 2009<br><br>2.) Terminé |

| Recommandation | Résumé des mesures prises | BPR | Date d'achèvement prévue |
|---|---|---|---|
| **Recommandation n° 11**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait mettre en œuvre une solution qui permet au SCC de crypter les bandes de sauvegarde pour les données d'applications jugées de nature sensible sur le plan de la sécurité ou de l'accès à l'information. | 1.) La Gestion de l'infrastructure et des opérations doit élaborer et mettre en œuvre une solution permettant de crypter les bandes de sauvegarde ou proposer une solution de rechange.<br><br>2.) Exécution de la solution | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Mars 2010<br><br>2.) Juin 2010 |
| **Recommandation n° 12**<br>Le dirigeant principal de l'Information, Services de gestion de l'information, devrait s'assurer que le plan de reprise incorpore un plan de rétablissement des activités à l'AC ou, encore, un nouveau plan de reprise qui guiderait le personnel responsable de la reprise après sinistre dans l'éventualité d'un sinistre au centre de traitement secondaire (avant la reprise à l'AC). | 1.) La Sécurité de la technologie de l'information dirigera l'élaboration du plan de rétablissement des activités en étroite collaboration avec la Gestion de l'infrastructure et des opérations.<br><br>2.) Le dirigeant principal de l'Information examinera et approuvera le plan de rétablissement des activités de l'administration centrale. | Le dirigeant principal de l'Information, Services de gestion de l'information | 1.) Mars 2010<br><br>2.) Mai 2010 |