Gouvernement du Canada | Government of Canada

Audit collectif des contrôles internes du SAP

2015-2016

Bureau de la vérification et de l'évaluation d'Agriculture et Agroalimentaire Canada

Direction générale de la vérification et de l'évaluation de l'Agence canadienne d'inspection des aliments

Direction de l'audit de Ressources naturelles Canada

Canada

Le Comité de vérification d'Agriculture et Agroalimentaire Canada (AAC) a recommandé au sous-ministre d'approuver le présent rapport d'audit le 4 décembre 2015.

Le Comité de vérification de l'Agence canadienne d'inspection des aliments (ACIA) a recommandé au président d'approuver le présent rapport d'audit le 13 janvier 2016.

Le Comité de vérification de Ressources naturelles Canada (RNCan) a recommandé au sous-ministre d'approuver le présent rapport d'audit le 17 décembre 2015.

© Sa Majesté la Reine du chef du Canada, représentée par le ministre de l'Agriculture et de l'Agroalimentaire (2016)

Version électronique disponible sur le site d'AAC : http://www.agr.gc.ca/fra/a-propos-de-nous/bureaux-et-emplacements/bureau-de-la-verification-et-de-levaluation/?id=1231423632566
ACIA : http://www.inspection.gc.ca/au-sujet-de-l-acia/responsabilisation/autres-activites/verifications-evaluations-et-revues/fra/1299843498252/1299843588592
RNCan : https://www.rncan.gc.ca/verification/rapports/2015/17353

No de catalogue : A29-1/9-2016F-PDF
ISBN : 978-0-660-04665-5
No d'AAC : 12487E

Issued also in English under the title
Joint Audit of SAP Internal Controls

Pour en savoir davantage :
AAC : www.agr.gc.ca ou appelez-nous sans frais au 1-855-773-0241
ACIA : www.inspection.gc.ca ou appelez-nous sans frais au 1-800-442-2342
RNCan : www.nrcan.gc.ca ou appelez-nous au 343-292-6096

TABLE DES MATIÈRES

Page

SOMMAIRE 1

1.0 INTRODUCTION 3
1.1 CONTEXTE 3
1.2 OBJECTIF DE L'AUDIT 4
1.3 PORTÉE DE L'AUDIT 4
1.4 MÉTHODE DE L'AUDIT 4
1.5 CONCLUSION 6
1.6 ÉNONCÉ DE CONFORMITÉ 6

2.0 OBSERVATIONS DÉTAILLÉES, RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION 7
2.1 GOUVERNANCE DES PARTENARIATS 7
2.2 CONTRÔLES DES TECHNOLOGIES DE L'INFORMATION 9
2.3 PLANIFICATION DE LA CONTINUITÉ DES ACTIVITÉS ET PLANIFICATION DE LA REPRISE APRÈS SINISTRE 16
2.4 GOUVERNANCE DES FOURNISSEURS DE SERVICES 20

ANNEXE A : SIGLES 23

ANNEXE B : CRITÈRES DE L'AUDIT 24

SOMMAIRE

Le SAP est le système standard de planification des ressources d'entreprise (PRE) du gouvernement du Canada utilisé dans le cadre du Système intégré des finances et du matériel (SIFM). En tant qu'administrateur du SIFM, Agriculture et Agroalimentaire Canada (AAC) est chargé de la prestation des services de gestion de l'application SAP ainsi que de la gestion de l'infrastructure de la base de données SAP pour divers partenaires des grappes.

Les dirigeants principaux de l'audit d'AAC et deux de ses partenaires des grappes, l'Agence canadienne d'inspection des aliments (ACIA) et Ressources naturelles Canada (RNCan), ont convenu de mener un audit collectif afin de donner à leurs organisations respectives l'assurance de l'efficacité de l'application de PRE du SAP à fournir des informations financières exactes, fiables, accessibles et opportunes.

Objectif

L'objectif de l'audit est de fournir l'assurance que :

- des structures de gouvernance sont en place et fonctionnent de façon efficace pour permettre une planification saine et équitable des investissements ainsi que l'affectation de ressources dans la maintenance et l'évolution constante de l'application PRE du SAP hébergée par AAC;

- des contrôles des technologies de l'information (TI) sont en place et fonctionnent de façon efficace pour permettre la production d'informations financières exactes, fiables, accessibles et opportunes.

Sommaire des observations

Afin de répondre à son objectif, l'audit a porté sur la structure de gouvernance globale qui guide l'exploitation et la maintenance du SAP, les contrôles des TI (y compris les contrôles généraux des TI [CGTI] et les contrôles automatisés des applications), la planification de la continuité des activités et la planification de la reprise après sinistre ainsi que sur la gouvernance entre le partenariat et les fournisseurs de services tiers tels que Services partagés Canada (SPC). En résumé :

- ***Gouvernance du partenariat*** – L'audit a permis de déterminer que la structure de gouvernance du partenariat a été mise en œuvre comme conçue dans l'accord sur les niveaux de service en vigueur et que celle-ci fonctionne de façon efficace au niveau opérationnel; toutefois, l'audit recommande des améliorations visant à renforcer les couches tactiques et stratégiques de la structure de gouvernance pour lesquelles la participation aux réunions et la fréquence de ces dernières n'étaient pas conformes aux exigences de l'accord sur les niveaux de service.

- ***Contrôles des TI*** – Il a été établi que la conception et le fonctionnement des principaux contrôles dans les secteurs de la gestion des changements dans les TI, des opérations des TI et des contrôles des applications ont été efficaces tout au long de la période de l'audit. À l'issue de cette dernière, il est recommandé d'apporter des améliorations aux essais d'acceptation par l'utilisateur (EAU) et aux processus de gestion de l'accès des utilisateurs.

- ***Planification de la continuité des activités et planification de la reprise après sinistre*** – L'audit a permis de déterminer que les plans de continuité des activités d'AAC et de l'ACIA doivent être mis à jour et améliorés afin qu'en cas de sinistre ou de perturbation des activités, les organisations soient en mesure d'assurer les fonctions et services essentiels comme ils sont définis dans les analyses des répercussions sur les activités.

- ***Gouvernance des pourvoyeurs de services*** – L'audit recommande que les mécanismes de gouvernance entre le partenariat et SPC soient améliorés de façon à veiller à la reprise efficace et opportune du SAP et de l'infrastructure informatique sous-jacente en cas de sinistre ainsi qu'à la communication et à l'escalade appropriées de toute préoccupation concernant le calendrier et les répercussions possibles des modifications de l'infrastructure informatique.

Conclusion

L'audit a permis de déterminer que des structures de gouvernance étaient en place pour favoriser la planification saine et équitable des investissements et l'affectation des ressources dans la maintenance et l'évolution constante de l'application PRE du SAP; toutefois, les principaux groupes de gouvernance ne se réunissent pas à la fréquence définie dans l'accord sur les niveaux de service du partenariat et la participation n'a pas toujours lieu au niveau approprié. Dans l'ensemble, l'audit a permis de déterminer que le Centre d'excellence d'AAC exécute de façon uniforme, efficace et opportune les principaux contrôles des TI sous sa responsabilité. On a cerné des possibilités d'amélioration de certains contrôles des TI appartenant à des partenaires clients ou détenus collectivement par le partenariat ainsi que dans la continuité des activités et la reprise après sinistre. Enfin, l'audit a permis de déterminer que les structures de gouvernance pour les fournisseurs de services pourraient être renforcées.

1.0 INTRODUCTION

1.1 CONTEXTE

1.1.1 Dans le contexte des systèmes de gestion des finances et du matériel, un groupe de grappes est un regroupement de ministères qui travaillent ensemble pour promouvoir et mettre en œuvre des solutions normalisées et axées sur les activités commerciales pour la gestion interopérable des finances et du matériel. La *Politique sur la gérance des systèmes de gestion financière* du Conseil du Trésor reconnaît que les groupes de grappes jouent un rôle important dans l'assurance de la normalisation de la gestion financière en agissant à titre de centre d'expertise et d'organisme central de coordination pour le développement et la gestion des systèmes ministériels de gestion financière les plus courants à l'échelle du gouvernement.

1.1.2 En tant que responsable d'une grappe SAP, AAC est chargé de la prestation des services de gestion de l'application SAP ainsi que de la gestion de l'infrastructure de la base de données SAP pour divers partenaires des grappes.

1.1.3 Les dirigeants principaux de l'audit d'AAC et deux de ses partenaires des grappes, l'ACIA et RNCan, ont convenu de mener un audit collectif afin de donner à leurs organisations respectives l'assurance de l'efficacité de l'application SAP à fournir des informations financières exactes, fiables, accessibles et opportunes.

1.1.4 Étant donné la dépendance des partenaires des grappes sur les contrôles internes d'AAC, la conduite d'un audit collectif des contrôles internes du SAP fournira à toutes les parties un moyen efficient d'obtenir une assurance concernant la question de savoir si les contrôles mis en place appuient la fourniture d'informations financières d'une manière qui préserve l'intégrité des transactions financières entrées dans l'application SAP.

1.1.5 AAC, l'ACIA et RNCan (ci-après dénommés les « partenaires clients » et, ensemble, « le partenariat ») ont établi des ententes qui définissent les mécanismes de gouvernance ainsi que les rôles et les responsabilités des diverses parties concernées, y compris le Centre d'excellence, lequel forme l'équipe de soutien d'AAC chargée de la coordination et de la fourniture de la solution SAP et des services au partenariat. Les ententes entre les partenaires clients comprenaient un droit d'audit, que les organisations partenaires ont choisi de ne pas exercer. Ces dernières ont plutôt décidé de se coordonner pour mener un audit collectif des contrôles internes du SAP et des structures de gouvernance à l'appui, y compris les accords sur les niveaux de service.

1.1.6 Les sigles utilisés dans le rapport figurent à l'annexe A.

1.2 OBJECTIF DE L'AUDIT

1.2.1 Un audit interne des contrôles internes du SAP est inclus dans les plans triennaux d'audit axé sur les risques de chacun des ministères partenaires (AAC, ACIA et RNCan) pour l'exercice 2015–2016. L'objectif de l'audit est de fournir l'assurance que :

- des structures de gouvernance sont en place et fonctionnent de façon efficace pour permettre une planification saine et équitable des investissements et l'affectation des ressources dans la maintenance et l'évolution constante de l'application PRE du SAP hébergée par AAC;

- des contrôles des TI sont en place et fonctionnent de façon efficace pour permettre la production d'informations financières exactes, fiables, accessibles et opportunes.

1.2.2 Il convient de noter que les « contrôles des TI » comprenaient les contrôles généraux des TI (CGTI) et les principaux contrôles de l'application SAP qui appuient les processus financiers.

1.3 PORTÉE DE L'AUDIT

1.3.1 La portée de l'audit a englobé des contrôles relatifs à l'application SAP et à son environnement informatique de soutien en place entre le 1er avril 2014 et le 30 juin 2015 et sous la responsabilité des partenaires clients suivants : AAC, ACIA et RNCan. L'audit ne s'est pas étendu aux contrôles relatifs à d'autres services de grappes dirigés par AAC tels que PeopleSoft ou SAP Business Warehouse.

1.3.2 SPC est propriétaire de l'infrastructure informatique qui héberge la solution SAP utilisée par le partenariat. Cet audit exclut la mise à l'essai des contrôles sous la responsabilité de SPC, mais les structures de gouvernance et la surveillance relatives aux secteurs de responsabilité de SPC ont été vérifiées.

1.4 MÉTHODE DE L'AUDIT

1.4.1 L'approche et la méthode de l'audit sont fondées sur les risques et sont conformes aux *Normes relatives à la vérification interne pour le gouvernement du Canada*, comme l'exige la *Politique sur la vérification interne* du Conseil du Trésor. Ces normes exigent que l'audit soit planifié et réalisé de manière à obtenir la garantie raisonnable que son objectif est atteint. L'audit a été mené selon un programme qui définit les tâches pour l'évaluation de chacun des critères d'audit. Diverses méthodes ont été utilisées pour recueillir les éléments probants de l'audit, y compris des

entrevues, des observations, des visites sur place, l'examen de documents et des analyses.

1.4.2 Nous avons passé en revue les travaux d'audit et d'évaluation antérieurs effectués par d'autres vérificateurs et évaluateurs en ce qui concerne l'environnement de contrôle SAP, cela afin de déterminer si une stratégie de confiance pouvait être adoptée. Nous avons pris en considération divers facteurs, dont les suivants :

- la période visée;
- la nature et l'étendue des travaux exécutés;
- l'objectivité et la compétence des autres vérificateurs.

1.4.3 La période d'audit couverte par les travaux d'audit antérieurs n'était pas suffisante pour adopter une stratégie de confiance; par conséquent, nous avons effectué des essais indépendants pour réaliser le programme d'audit.

1.4.4 Les Objectifs de contrôle de l'information et des technologies connexes (COBIT), norme industrielle fournissant des exigences relatives au contrôle, sont harmonisés avec les risques informatiques et commerciaux. Les COBIT ont été mis à profit pendant l'évaluation des risques et dans l'élaboration des critères d'évaluation en harmonisant les travaux prévus avec certains éléments des COBIT.

1.4.5 La Politique du Conseil du Trésor sur la gérance des systèmes de gestion financière et les instruments connexes de même que les éléments clés de l'accord sur les niveaux de service entre les partenaires clients ont aussi servi à élaborer des critères et sous-critères.

1.4.6 Les critères d'audit sont organisés selon les trois secteurs d'examen ci-après qui, ensemble, ont permis à l'audit d'atteindre son objectif :

- **Gouvernance du partenariat** – Le partenariat possède une structure de gouvernance qui lui permet de discuter collectivement des priorités et des objectifs stratégiques, de les établir et de les communiquer. Ces priorités et objectifs visent à guider la planification et l'établissement de l'ordre de priorité des investissements et des ressources, et ce, conformément aux besoins opérationnels et à l'orientation pangouvernementale.

- **Contrôles des TI** – Des contrôles des TI sont en place au Centre d'excellence et chez les partenaires clients pour appuyer la production d'informations financières exactes, fiables, accessibles et opportunes.

- **Gouvernance des fournisseurs de services** – Des structures de gouvernance sont en place pour gérer les risques relatifs aux services de CGTI fournis par des tiers.

1.4.7 Les critères et sous-critères d'audit figurent à l'annexe B.

1.4.8 La phase d'exécution de l'audit a commencé en juin 2015 et s'est terminée en septembre 2015.

1.5 CONCLUSION

1.5.1 L'audit a permis de déterminer que des structures de gouvernance étaient en place pour favoriser la planification saine et équitable des investissements et l'affectation des ressources dans la maintenance et l'évolution constante de l'application PRE du SAP; toutefois, les principaux groupes de gouvernance ne se réunissent pas à la fréquence définie dans l'accord sur les niveaux de service du partenariat et la participation n'a pas toujours lieu au niveau approprié. Dans l'ensemble, l'audit a permis de déterminer que le Centre d'excellence d'AAC exécute de façon uniforme, efficace et opportune les principaux contrôles des TI sous sa responsabilité. On a cerné des possibilités d'amélioration de certains contrôles des TI appartenant à des partenaires clients ou détenus collectivement par le partenariat ainsi que dans la continuité des activités et la reprise après sinistre. Enfin, l'audit a permis de déterminer que les structures de gouvernance pour les fournisseurs de services pourraient être renforcées.

1.6 ÉNONCÉ DE CONFORMITÉ

1.6.1 Selon l'opinion professionnelle des dirigeants principaux de l'audit, des procédures suffisantes et adéquates d'audit ont été menées et des preuves ont été recueillies pour étayer la justesse de la conclusion présentée et contenue dans le présent rapport. La conclusion repose sur une comparaison des circonstances, telles qu'elles existaient à l'époque, par rapport à des critères d'audit préétablis convenus avec la direction. La conclusion ne s'applique qu'à l'entité vérifiée.

1.6.2 La présente évaluation est conforme aux *Normes relatives à la vérification interne au sein du gouvernement du Canada,* comme le confirment les résultats du programme d'assurance et d'amélioration de la qualité.

2.0 OBSERVATIONS DÉTAILLÉES, RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION

2.1 GOUVERNANCE DES PARTENARIATS

2.1.1 La structure de gouvernance du partenariat a été créée pour permettre une discussion collective ainsi que l'établissement et la communication des priorités et des objectifs stratégiques (voir la figure 1). Le modèle de gouvernance créé pour établir, déployer et surveiller les couches stratégiques, tactiques et opérationnelles du partenariat SAP comprend les structures suivantes :

- **Comité directeur du partenariat SAP (CDPS)** – Un comité permanent des sous-ministres adjoints qui assure une direction et établit l'orientation stratégique du partenariat et qui est l'organisme d'approbation définitive pour les modifications, la gestion des questions escaladées et l'atténuation des risques. Ce comité est composé de représentants de chacun des partenaires clients.

- **Comité de gestion du partenariat SAP (CGPS)** – Un comité permanent dirigé par le directeur général et axé sur la fonctionnalité, l'exploitation et la gestion du service SAP pour le partenariat. Ce comité est composé de représentants de chacun des partenaires clients.

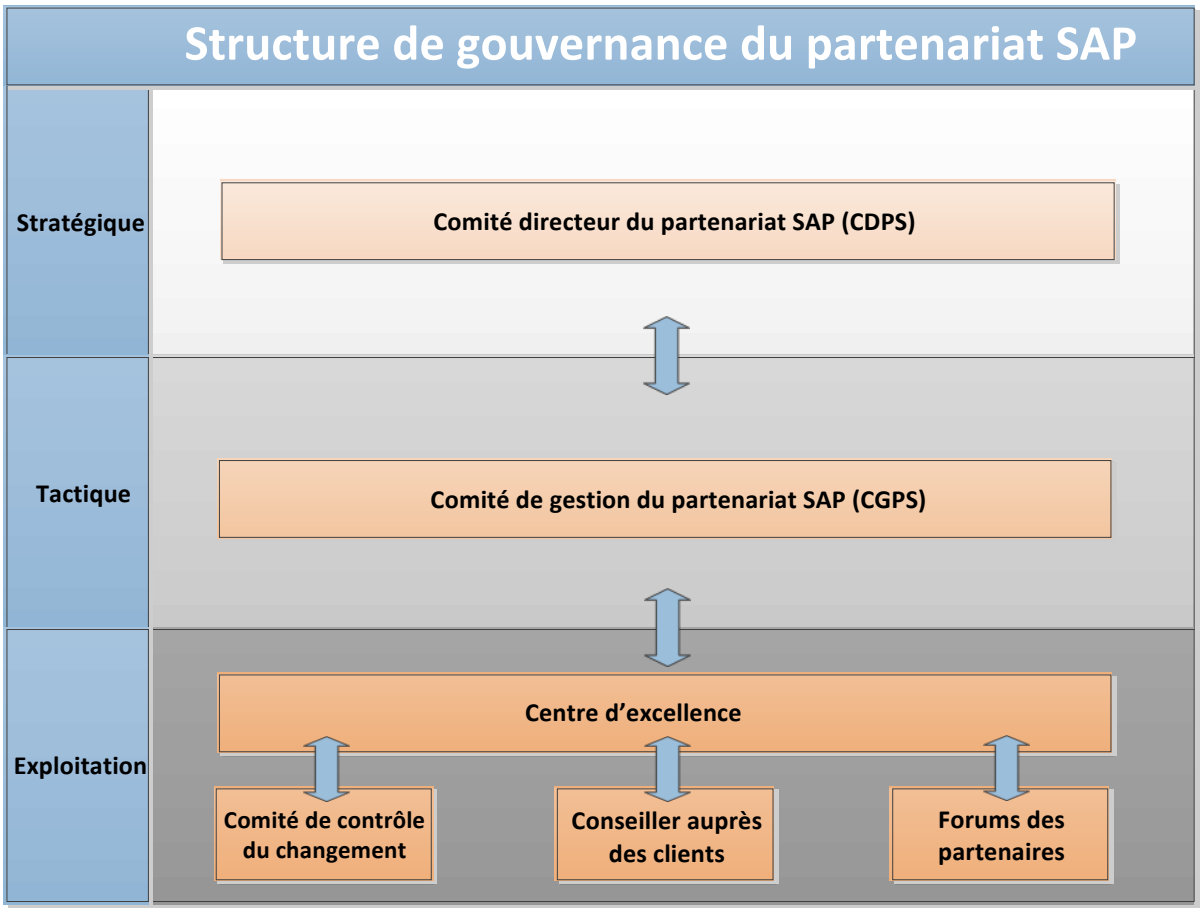
- **Centre d'excellence** – Organisation relevant d'AAC responsable de fournir des solutions du système SAP qui respectent les objectifs et les priorités stratégiques fixés par le CDPS et le CGPS. Le Centre d'excellence offre des services de développement et de soutien des systèmes pour la solution SAP.

- **Comité de contrôle du changement (CCC)** – Groupe dirigé par AAC qui participe à l'évaluation des changements ainsi qu'à l'établissement de leur ordre de priorité et de leur calendrier.

- **Conseiller auprès des clients** – Personne désignée par chaque partenaire client pour agir à titre de personne-ressource clé et assurer la liaison avec le partenariat.

- **Forums des partenaires clients** – Groupes qui appuient la gouvernance en travaillant en étroite collaboration avec le Centre d'excellence pour fournir une expertise en matière d'opérations au partenariat en participant à la planification et à l'établissement de l'ordre de priorité des besoins opérationnels, à la détermination des problèmes opérationnels et à l'assurance de l'échange d'information et du transfert des connaissances.

Figure 1 – Structure de gouvernance du partenariat



Constatation

L'audit a permis de déterminer que la structure de gouvernance du partenariat a été mise en œuvre telle que conçue dans l'accord sur les niveaux de service en vigueur pour la solution SAP (voir la figure 1); toutefois, des points à améliorer ont été relevés. Le CDPS et le CGPS ne se réunissent pas à des fréquences qui sont conformes à celles précisées dans l'accord sur les niveaux de service. Le CDPS s'est réuni seulement une fois pendant les 15 mois qu'a duré la période d'audit (une fois seulement lorsqu'on s'attendait à trois ou plus) et seulement deux rencontres du CGPS ont été organisées pendant la même période (lorsque l'on s'attendait à cinq). Par conséquent, il existe un risque accru que des problèmes qui nuisent à la réalisation des priorités et des objectifs stratégiques ne soient pas repérés et résolus en temps opportun. L'accord sur les niveaux de service qui définit la fréquence prévue des réunions de gouvernance a été élaboré à un moment où le partenariat SAP était nouveau pour toutes les parties. Maintenant que les partenaires connaissent bien la solution SAP pour l'avoir utilisée plusieurs années et qu'ils sont habitués à travailler ensemble, il est possible que la fréquence précisée dans l'accord ne reflète plus la fréquence exigée ou attendue des partenaires. De plus, l'audit interne a

observé que la participation n'a pas toujours lieu aux niveaux désignés, car des délégués assistent aux réunions au nom des invités.

2.1.2

Constatation 1 : Une structure de gouvernance assurant la participation de la haute direction à la planification stratégique, à la prise de décisions et à la résolution des problèmes est conçue et établie de façon adéquate; toutefois, elle ne fonctionne pas de la façon décrite dans l'accord du partenariat sur les niveaux de service. Le Comité directeur du partenariat SAP et le Comité de gestion du partenariat SAP ne se réunissent pas à des fréquences conformes à l'accord sur les niveaux de service et la participation n'a pas toujours lieu aux paliers désignés (c.-à-d. que des délégués assistent aux réunions).

2.1.3 Recommandation

AAC 1 – AAC, en collaboration avec d'autres partenaires, doit renforcer les processus de gouvernance en réévaluant collectivement les exigences de l'accord sur les niveaux de service en vue de déterminer si la fréquence des réunions de gouvernance est appropriée pour les besoins du partenariat. Si cela s'avère nécessaire, l'accord doit être mis à jour. AAC doit désigner un responsable ou élaborer un processus visant à établir le calendrier des réunions du comité de gouvernance à la fréquence convenue et avec la représentation appropriée.

AAC 1
Réponse de la direction : Recommandation acceptée.

Plan d'action :
Au cours des prochaines réunions de gouvernance des directeurs généraux et des sous-ministres adjoints, la fréquence des réunions de gouvernance sera réévaluée collectivement en fonction des besoins du partenariat. L'accord sur les niveaux de service sera mis à jour en conséquence. Un responsable sera désigné pour établir le calendrier des réunions du comité de gouvernance à la fréquence convenue et avec la représentation appropriée.

Date cible d'achèvement : 31 janvier 2016

Responsable(s) : Dirigeant principal de l'information

2.2 CONTRÔLES DES TECHNOLOGIES DE L'INFORMATION

2.2.1 D'une manière générale, les contrôles des TI sont définis comme des activités réalisées par des personnes ou des systèmes informatiques pour s'assurer que les applications fonctionnent toujours comme prévu pour appuyer l'atteinte des objectifs opérationnels et préserver l'intégrité des

données. Les contrôles des TI sont évalués dans deux catégories principales : les CGTI et les contrôles des applications.

Contrôles généraux des technologies de l'information

2.2.2 Les CGTI sont le fondement de l'environnement de contrôle des TI et leur fonctionnement est principalement manuel. Les CGTI relèvent traditionnellement de trois catégories : la gestion des changements dans les TI, la gestion de l'accès des utilisateurs et les opérations des TI. Les résultats de chaque catégorie sont décrits en détail ci-après.

Gestion des changements informatiques

2.2.3 Les contrôles de la gestion des changements dans les TI sont essentiels à l'appui de la continuité des opérations et de l'évolution des applications. Ils contribuent à veiller à ce que ces dernières et l'infrastructure de soutien fonctionnent comme prévu de manière uniforme. Le Centre d'excellence est chargé d'exécuter les services de développement et de soutien des systèmes, notamment l'établissement des priorités, la planification, la conception, le développement, les essais et la mise en œuvre des demandes de service.

2.2.4 Afin d'effectuer le suivi des changements et de contrôler le processus complet de gestion des changements, le Centre d'excellence d'AAC utilise un module personnalisé du SAP appelé « système de gestion des changements ». L'audit a permis de constater que tous les changements examinés sont conformes au processus de gestion des changements défini dans l'accord sur les niveaux de service et à l'entente de service de gestion des changements. De plus, les points de contrôle clés suivants sont en place et fonctionnent de façon efficace :

- **Amorçage des changements** – Les changements sont mis en route par le personnel approprié en fonction des exigences fonctionnelles, techniques et opérationnelles.

- **Essais de fonctionnement** – Les changements font l'objet d'essais de fonctionnement par les membres du Centre d'excellence.

- **Approbation des changements** – Les changements sont approuvés par le personnel approprié avant d'être mis en œuvre.

- **Surveillance des changements** – L'utilisation des comptes de superutilisateurs destinés à faire avancer les changements à l'étape de la mise en œuvre et d'autres activités privilégiées relatives à la gestion des changements sont surveillées de façon efficace par le Centre d'excellence.

- **Ségrégation des tâches incompatibles** – Il y a une ségrégation appropriée des tâches incompatibles parmi celles qui sont reliées à des responsabilités clés (approuver, développer et faire avancer les changements à l'étape de la mise en œuvre).

Point fort : Tous les changements qui ont été examinés suivent le processus de gestion des changements de manière contrôlée et les changements sont planifiés de façon à réduire au minimum les incidences sur les opérations.

Constatation

2.2.5 Dans le cycle de vie de développement des logiciels, l'essai d'acceptation par les utilisateurs (EAU) (aussi appelé « essai par l'utilisateur final ») est une activité dans le cadre de laquelle les logiciels sont mis à l'essai par l'auditoire ou les utilisateurs professionnels visés avant d'avancer à l'étape de la mise en œuvre. L'EAU est un élément clé de la série de contrôles de la gestion des changements dans les TI parce qu'il est essentiel que les changements aient l'effet prévu dans le contexte des processus opérationnels touchés. Dans l'environnement du partenariat, l'EAU revêt une importance accrue, car il peut y avoir des différences nuancées entre les processus opérationnels de chaque partenaire client que le Centre d'excellence ne connaît pas; par conséquent, le risque que les changements puissent avoir un effet imprévu est plus élevé s'ils ne sont pas mis à l'essai par les partenaires clients avant de passer à l'étape de la mise en œuvre.

2.2.6 L'audit a permis de constater que les partenaires clients ne participent pas de façon uniforme aux EAU des changements apportés au SAP et les exigences relatives aux EAU n'ont pas été officialisées dans le cadre du processus de gestion des changements. Il y a un risque que les changements ne répondent pas aux besoins des clients ou ne fonctionnent pas comme prévu par tous les partenaires clients. Dans certains cas, le manque de participation des clients a donné lieu à des inefficacités parce que des demandes de changement supplémentaires ont dû être satisfaites pour répondre aux besoins des clients.

Constatation 2 : Les partenaires clients ne participent pas de façon uniforme aux essais d'acceptation par les utilisateurs des changements apportés au SAP.

2.2.7 Recommandation

AAC 2 – AAC, en collaboration avec les partenaires clients, doit augmenter le processus de gestion des changements pour tenir compte des essais d'acceptation par les utilisateurs fondés sur les risques avant que les changements ne soient apportés à l'application SAP et à son environnement informatique de soutien.

AAC 2

Réponse de la direction : Recommandation acceptée.

Plan d'action :
En collaboration avec les partenaires clients, le processus de gestion des changements sera amélioré pour tenir compte à l'avenir des essais d'acceptation par les utilisateurs.

Date cible d'achèvement : 1er avril 2016

Responsable(s) : Dirigeant principal de l'information

Gestion de l'accès des utilisateurs

2.2.8 Les contrôles de la gestion de l'accès des utilisateurs régissent la façon dont l'accès aux applications est restreint, assuré, modifié et retiré afin de veiller à ce que seules les personnes autorisées aient accès aux données et aux applications connexes et puissent exécuter uniquement les fonctions expressément autorisées. Les environnements solides de contrôle d'accès logique se fondent en parts égales sur les contrôles de prévention et les contrôles de détection. Les contrôles relatifs aux approbations de l'accès des utilisateurs, à la révocation de l'accès des utilisateurs, aux exigences relatives aux mots de passe et aux paramètres de configuration de la sécurité sont considérés comme des contrôles importants de prévention tandis que les contrôles de détection consistent généralement en un examen périodique des droits d'accès et en une surveillance des activités des utilisateurs. L'audit a permis d'évaluer les contrôles dans les secteurs clés suivants de la gestion de l'accès des utilisateurs:

- mots de passe;
- configuration de la sécurité;
- accès aux fonctions informatiques privilégiées;
- surveillance de l'accès des utilisateurs;
- attribution de l'accès aux utilisateurs;
- retrait de l'accès des utilisateurs;
- examen périodique de l'accès des utilisateurs et certification.

Points forts :

- Les contrôles des mots de passe sont appropriés et conformes aux normes du Centre de la sécurité des télécommunications Canada.
- Les paramètres clés de configuration et de sécurité du SAP sont appropriés.
- Les fonctions informatiques privilégiées à la couche d'application SAP, y compris l'accès aux transactions sensibles, aux profils SAP par défaut et aux objets d'autorisation SAP, sont limitées aux personnes appropriées.
- La conception et le fonctionnement des contrôles visant à surveiller les droits

d'accès et les activités des utilisateurs sensibles et à risque plus élevé sont efficaces pendant la période de l'audit.

- Le Centre d'excellence, en collaboration avec les partenaires clients, a élaboré un processus d'approbation conçu de façon efficace pour les nouveaux accès, lequel comprend la définition des rôles et l'identification des approbateurs. De plus, le processus d'assurance de l'accès est exécuté de façon uniforme par le Centre d'excellence.
- Le Centre d'excellence retire l'accès de façon uniforme et en temps opportun lorsqu'il reçoit des demandes de la part des partenaires clients.

Constatations

2.2.9 L'audit a aussi permis de relever des possibilités d'améliorer l'environnement de contrôle de la gestion de l'accès des utilisateurs. Bien que le Centre d'excellence retire l'accès de façon uniforme et en temps opportun lorsqu'il reçoit des demandes de la part des partenaires clients, il a été observé que ce dernier n'est pas avisé du départ des utilisateurs de façon uniforme et en temps opportun par les partenaires clients. Par conséquent, les droits d'accès au SAP pour les utilisateurs qui quittent les organisations ne sont pas retirés de façon uniforme et en temps opportun. Cela tient au fait que le processus relatif au départ d'employés de chaque partenaire client n'est pas bien intégré aux processus de retrait des droits d'accès au SAP. Il y a un risque que des utilisateurs non autorisés puissent accéder à l'application SAP par l'entremise des comptes utilisateur d'employés qui ont quitté les organisations.

Constatation 3 : Le Centre d'excellence n'est pas avisé de façon uniforme et en temps opportun du départ des utilisateurs du SAP; par conséquent, les droits d'accès au SAP des utilisateurs qui quittent les organisations ne sont pas retirés de façon uniforme et en temps opportun.

2.2.10 Afin de favoriser la pertinence continue des droits d'accès des utilisateurs exigés pour effectuer les transactions financières ou les transactions qui pourraient avoir une incidence sur les composantes de l'environnement informatique, on s'attendait, dans le cadre de l'audit, à ce qu'il y ait un examen périodique des droits d'accès des utilisateurs. On s'attendait aussi à ce que ces examens soient effectués par des informaticiens ou du personnel de gestion des activités appropriés et réalisés à une fréquence raisonnable et en suivant une approche fondée sur les risques, et ce, afin que les efforts nécessaires pour effectuer l'examen correspondent aux risques connexes (p. ex. les utilisateurs à risque modéré ou plus élevé devraient faire l'objet d'examens plus fréquents que les utilisateurs à faible risque, qui peuvent n'exiger qu'un examen annuel). L'audit a permis de déterminer que l'examen périodique de l'accès des utilisateurs de chaque partenaire client n'est effectué qu'une fois par année, ce qui n'est pas suffisant pour atténuer les

risques relatifs aux lacunes dans le processus de retrait de l'accès (voir le paragraphe 2.2.9). Les comptes utilisateur appartenant aux employés qui ont quitté les organisations pourraient demeurer actifs pendant un an et des utilisateurs non autorisés pourraient y accéder (c.-à-d. si le compte est utilisé de façon suffisamment fréquente pour empêcher le verrouillage automatique habituellement prévu après 30 jours en raison d'inactivité).

Constatation 4 : L'examen périodique de l'accès des utilisateurs de chaque partenaire client n'est effectué qu'une fois par année, ce qui n'est pas suffisant pour atténuer les risques relatifs aux lacunes dans le processus de retrait de l'accès.

2.2.11 Recommandation

AAC 3/ACIA 1/RNCan 1 – Chaque partenaire client doit réévaluer ce qui suit :

- le processus relatif au départ des employés afin de s'assurer que le Centre d'excellence soit avisé en temps opportun de tous les départs d'employés qui disposent de droits d'accès au SAP;
- le processus d'examen périodique de l'accès des utilisateurs et l'adoption d'une approche comportant des examens plus fréquents (p. ex. tous les trimestres) fondés sur les risques.

AAC 3
Réponse de la direction : Recommandation acceptée.

Plan d'action :
AAC 3 (première puce) : AAC réévaluera son processus relatif au départ d'employés afin de s'assurer que le Centre d'excellence SAP soit avisé en temps opportun de tous les départs. AAC réévaluera son processus d'examen de l'accès des utilisateurs et envisagera d'adopter une approche comportant des examens plus fréquents fondés sur les risques.

Date cible d'achèvement : 1er mars 2016

Responsable(s) : Sous-ministre adjoint, Direction générale de la gestion intégrée

Plan d'action :
AAC 3 (deuxième puce) : Le Centre d'excellence SAP communiquera et échangera avec ses partenaires afin de mettre en place un processus standard d'examen de l'accès des utilisateurs.

Date cible d'achèvement : 31 mars 2016

Responsable(s) : Dirigeant principal de l'information

ACIA 1
Réponse de la direction : Recommandation acceptée.

Plan d'action :
Le groupe chargé des opérations comptables s'efforce d'aviser le Centre d'excellence du départ d'un employé qui dispose de droits d'accès au SAP. Le problème concerne davantage les employés qui sont mutés à un autre poste à l'ACIA. L'examen périodique proposé (ci-après) aidera à résoudre ces situations.

Bien que l'Agence effectue un examen intensif des utilisateurs du SAP, elle ne le fait qu'une fois par année. La Division des opérations comptables effectuera un examen trimestriel ou semestriel qui vise davantage les utilisateurs que leurs rôles afin de s'assurer 1) que les personnes occupent toujours leur poste et 2) qu'elles ont toujours besoin d'accéder au SAP. Les secteurs ciblés (p. ex. les comptes créditeurs) peuvent aussi être utilisés lorsqu'on adopte une approche fondée sur les risques.

Date cible d'achèvement : 31 mars 2016

Responsable(s) : Directeur, Opérations comptables

RNCan 1
Réponse de la direction : Recommandation acceptée. Cependant, on doit noter que l'audit a révélé un nombre minime de cas où des employées ayant quitté leurs postes avaient toujours un accès potentiel au SAP.

Plan d'action :
RNCan a récemment mis en œuvre un nouveau processus relatif au départ d'employés (mars 2015), lequel est intégré aux droits d'accès au SAP. En ce qui concerne l'adoption d'un processus comportant des examens de l'accès plus fréquents, RNCan mettra en œuvre un examen semestriel pour les profils d'accès à risque plus élevé tels que ceux des agents chargés des rapports ministériels et les fonctionnaires chargés d'appliquer l'article 33.

De plus, les nouveaux rapports automatisés compareront les informations relatives à l'accès au SAP à d'autres systèmes tels que le module de prévisions salariales et l'Annuaire du personnel et des services. Ce contrôle compensatoire additionnel permettra d'atténuer davantage le risque connexe. Aussi, il faut noter que des contrôles compensatoires existent actuellement pour s'assurer que les comptes sont désactivés lorsque les usagers n'utilisent pas le SAP pendant une période de 90 jours.

Date cible d'achèvement : 31 mars 2016

Responsable(s) : Directeur, Services liés aux finances et à l'approvisionnement, Direction des finances et de l'approvisionnement

Opérations des technologies de l'information

2.2.12 Les contrôles des opérations des TI visent à fournir un environnement de traitement fiable et à atténuer les risques relatifs à la perte d'applications et de données ainsi qu'au traitement incomplet de l'information. Les secteurs clés de contrôle évalués dans le cadre de l'audit étaient la sauvegarde des données et le traitement programmé (c.-à-d. les travaux exécutés par lots). Le Centre d'excellence est chargé d'exécuter les contrôles clés relatifs aux opérations des TI.

2.2.13 L'audit a permis de déterminer que la série de contrôles des sauvegardes et de redondances intégrée à l'architecture atténue raisonnablement le risque relatif aux sauvegardes des données. De plus, la conception et le fonctionnement des contrôles visant à repérer et résoudre les déviations du traitement prévu (p. ex. échecs des travaux exécutés par lots) en temps opportun sont efficaces pendant la période de l'audit. L'accès permettant d'apporter des modifications aux calendriers des travaux est restreint aux personnes appropriées du Centre d'excellence.

Point fort : Les contrôles des opérations des technologies de l'information relatifs à la sauvegarde des données et au traitement programmé sont gérés de manière contrôlée et une surveillance du traitement automatisé est effectuée.

Contrôles des applications

2.2.14 Les contrôles des applications sont automatisés et ils sont intégrés aux processus opérationnels (p. ex. le SAP ne permet pas d'enregistrer une transaction non équilibrée).

2.2.15 Dans certains cas, les descriptions des contrôles automatisés des applications relatifs aux processus opérationnels d'AAC, de l'ACIA et de RNCan ne sont pas harmonisées avec exactitude avec la fonctionnalité du système SAP. Bien que des possibilités mineures d'amélioration aient été relevées en ce qui concerne l'exactitude des descriptions des contrôles documentées, l'audit a permis de déterminer que les contrôles automatisés des applications sont conçus et fonctionnent de façon efficace. La liste des contrôles pour lesquels il existe des possibilités d'améliorer l'exactitude des descriptions des contrôles a été fournie à la direction.

2.3 PLANIFICATION DE LA CONTINUITÉ DES ACTIVITÉS ET PLANIFICATION DE LA REPRISE APRÈS SINISTRE

2.3.1 Chaque organisation est vulnérable aux interruptions possibles des activités causées par divers incidents et sinistres, qui pourraient comprendre les suivants :

- catastrophes naturelles comme des tornades, des inondations, des blizzards, des tremblements de terre et des incendies;
- accidents;
- sabotage;
- interruption de l'alimentation en courant ou en énergie;
- panne dans les secteurs des communications, des transports, de la sécurité ou des services publics;
- catastrophe environnementale causée par la pollution ou par le déversement de matières dangereuses;
- cyberattaques et actes de piratage informatique.

2.3.2 Le plan de continuité des activités permet aux partenaires clients de répondre aux interruptions des activités afin de continuer d'assurer les fonctions et les services essentiels.

2.3.3 La planification de la reprise après sinistre est axée sur la récupération des actifs informatiques après un sinistre ou une interruption. Le plan de reprise après sinistre est un élément essentiel qui permet au partenariat, à la suite d'un incident ou d'une interruption, de continuer à exploiter la solution SAP et l'infrastructure informatique connexe et de maintenir la disponibilité des données à un niveau acceptable pour les partenaires clients. Le plan de reprise après sinistre décrit les procédures et les arrangements en place pour récupérer les actifs informatiques dans un délai prédéterminé.

Constatations

2.3.4 Conformément à l'accord sur les niveaux de service du partenariat SAP, chaque partenaire client est responsable d'effectuer sa propre analyse des répercussions sur les activités et d'élaborer le plan de continuité des activités correspondant (si les résultats de l'analyse précitée l'exigent) pour les services supportés par l'application SAP. L'audit a permis d'évaluer l'analyse des répercussions sur les activités ainsi que le plan de continuité des activités de chaque partenaire client et de déterminer que le dernier plan de continuité des activités complet et approuvé d'AAC date de mars 2012, quoiqu'une mise à jour de ce dernier soit en cours. Il existe un risque qu'AAC ne soit pas bien positionné pour poursuivre ses activités en temps opportun en cas d'interruption des activités.

2.3.5 En ce qui concerne l'ACIA, les documents du plan de continuité des activités fournis dans le cadre du présent audit ne prévoyaient pas de scénarios où l'application SAP serait touchée. Un temps d'arrêt maximal admissible d'un à trois jours a été identifié par les unités fonctionnelles dans les analyses des répercussions sur les activités. Par ailleurs, la continuité des activités peut ne pas être atteignable en l'absence de plan, ce qui pourrait empêcher l'ACIA de poursuivre des activités critiques en bas d'interruption des activités.

2.3.6 L'analyse des répercussions sur les activités de RNCan ne fait pas état de fonctions ou de services critiques qui se fondent sur SAP; par conséquent, on ne s'attendait pas, dans le cadre de l'audit, à trouver des preuves de l'existence d'un plan de continuité des activités et d'un plan de reprise après sinistre relatifs au SAP.

Constatation 5 : Les documents relatifs à la continuité des activités doivent être mis à jour et améliorés afin qu'AAC et l'ACIA soient prêts à poursuivre, en temps opportun, l'exploitation des fonctions et des services critiques en cas d'interruption des activités.

2.3.7 Conformément à l'accord du partenariat sur les niveaux de service, chaque partenaire a des responsabilités individuelles en ce qui concerne la planification de la reprise après sinistre. L'accord sur les niveaux de service entre les partenaires clients énonce que « le modèle de coût pour la solution SAP ne comprend pas la planification de la reprise après sinistre ou la planification de la continuité des activités »; toutefois, « si un partenaire client souhaite créer un plan de reprise après sinistre avec l'aide d'AAC, cela serait examiné séparément ». Dans le cadre de l'audit, on s'attendait à ce que chaque membre du partenariat ait des arrangements en place pour veiller à ce que les exigences opérationnelles et informatiques soient satisfaites en cas de sinistre; toutefois, les arrangements liés à la planification de la reprise après sinistre et les coûts connexes n'ont pas été acceptés de façon officielle par le partenariat. Par conséquent, le plan de reprise après sinistre d'AAC n'a pas été élaboré en collaboration avec RNCan et l'ACIA. Bien que les données de RNCan et de l'ACIA soient dupliquées et sauvegardées au moyen des mêmes méthodes utilisées à cette fin par AAC, il n'y a pas de disposition qui prévoit la fourniture, au centre de secours immédiat, d'espace de travail et de connectivité pour le personnel des partenaires clients en cas d'interruption des activités ou de sinistre. Selon l'analyse des répercussions sur les activités de RNCan, cela n'aurait pas d'incidence sur la capacité de ce dernier d'assurer les fonctions ou les services essentiels. Les exigences opérationnelles de l'ACIA pour le SAP, telles que définies dans son analyse des répercussions sur les activités, peuvent ne pas être respectées en cas de sinistre. Toutefois, la direction a déclaré qu'à son avis le système SAP n'est pas un service essentiel et que, par conséquent, les exigences opérationnelles et informatiques définies dans son analyse des répercussions sur les activités ne sont pas exactes.

Constatation 6 : En ce qui concerne l'application SAP, l'ACIA n'a pas d'arrangements en place visant à permettre de satisfaire aux exigences opérationnelles et informatiques telles que définies dans son analyse des répercussions sur les activités en cas de sinistre.

2.3.8 Recommandations

AAC 4 – AAC devrait terminer la mise à jour du plan de continuité des activités présentement en cours et approuver ce dernier pour démontrer que le Ministère est prêt à faire face aux situations d'urgence.

AAC 4
Réponse de la direction : Recommandation acceptée.

Plan d'action :
Le plan de continuité des activités du SAP est terminé et approuvé au niveau des directeurs généraux et sera présenté en vue de son approbation définitive.

Date cible d'achèvement : 1er décembre 2015

Responsable(s) : Dirigeant principal de l'information

ACIA 2 – L'ACIA devrait réévaluer le caractère critique de l'application SAP. Si l'on détermine subséquemment que les services supportés par le SAP ne sont plus essentiels, l'analyse des répercussions sur les activités devrait être revue en conséquence. Si l'on confirme que le système SAP est essentiel, les améliorations des documents du plan de continuité des activités et des arrangements liés à la reprise, mentionnées ci-après, devraient être apportées pour permettre la continuité des fonctions et des services essentiels :

- L'ACIA devrait mettre à jour les documents du plan de continuité des activités afin d'inclure des scénarios dans le cadre desquels le système SAP et l'infrastructure informatique sont touchés ou non disponibles. Les exigences relatives à la continuité des services essentiels en cas de non-disponibilité du système SAP et de l'infrastructure informatique devraient être documentées dans le plan de continuité des activités.

- L'ACIA devrait mobiliser AAC pour mettre en œuvre des arrangements visant à assurer la satisfaction des exigences opérationnelles et informatiques en cas de sinistre. Les arrangements devraient être étayés par des documents officiels décrivant l'entente, le modèle de coût et les ressources et qui seront rendus disponibles à l'ACIA en cas de sinistre.

ACIA 2
Réponse de la direction : Recommandation acceptée.

Plan d'action :
L'Agence admet que le temps d'arrêt maximal admissible d'un à trois jours (niveau 2) indiqué dans l'analyse des répercussions sur les activités n'est pas adéquat. Il sera modifié à un temps d'arrêt maximal admissible de huit à vingt et un jours (niveau 4) au cours du prochain examen.

Avec la rectification du temps d'arrêt maximal admissible, les services passent d'essentiels à non essentiels; par conséquent, d'autres mises à jour du plan de continuité des activités ne sont pas justifiées.

Date cible d'achèvement : 31 juillet 2016

Responsable(s) : Directeur, Opérations comptables

2.4 GOUVERNANCE DES FOURNISSEURS DE SERVICES

2.4.1 Travailler en partenariat avec des fournisseurs de services tiers peut procurer des avantages importants tels que des coûts réduits et une efficience accrue; toutefois, le recours à de tels fournisseurs introduit également des risques additionnels qui doivent être gérés en conséquence. Le fournisseur de services le plus essentiel à l'appui de l'environnement SAP du partenariat est Services partagés Canada (SPC), car ce dernier est responsable de l'hébergement et de la maintenance de l'infrastructure informatique. SPC a été créé le 4 août 2011 et les services relatifs à l'infrastructure informatique qui étaient officiellement exécutés par AAC lui ont subséquemment été transférés.

2.4.2 L'audit a permis d'évaluer la gouvernance des fournisseurs de services dans les secteurs clés suivants : la planification de la reprise après sinistre et la gestion des changements dans l'infrastructure informatique.

Planification de la reprise après sinistre

Constatation

2.4.3 Il est essentiel d'assurer un niveau élevé de communication et de coordination entre le partenariat et SPC en raison du rôle crucial de ce dernier dans la reprise après sinistre. L'audit a permis de déterminer qu'AAC et SPC ne se rencontrent pas de façon régulière pour discuter des exigences stratégiques ou opérationnelles à l'appui de la reprise après sinistre pour l'environnement SAP.

2.4.4 L'audit a permis de déterminer que la dernière mise à jour du plan de reprise après sinistre d'AAC date de mars 2012 et qu'elle ne reflète pas le transfert des responsabilités du centre de données à SPC. Ce dernier a subséquemment transféré l'emplacement du centre de données de relève du système SAP de Winnipeg à Ottawa; toutefois, le plan de reprise après

sinistre du SAP n'a pas été mis à jour afin de refléter l'environnement actuel. De plus, en raison de la relocalisation du centre de données de relève, les centres de données principal et de relève à l'appui de l'application SAP sont maintenant situés à proximité l'un de l'autre (~5 km), ce qui n'est pas conforme aux pratiques exemplaires. Les centres de données principal et de relève devraient être suffisamment éloignés l'un de l'autre et comporter des différences sur les plans de la géographie, du climat, de la séismologie et des réseaux électriques. Il existe un risque qu'AAC ne soit pas bien positionné pour récupérer les actifs informatiques rapidement en cas de sinistre. Dans l'ensemble, il existe un risque que les plans d'urgence à l'appui de la reprise après sinistre ne soient pas suffisants pour réparer rapidement les dégâts causés par certains types de sinistres.

Constatation 7 : Le plan de reprise après sinistre ne reflète pas l'environnement actuel ou ne distingue pas de façon claire les rôles et les responsabilités du partenariat de ceux de Services partagés Canada. Les centres de données principal et de relève sont situés très près l'un de l'autre, ce qui accroît la possibilité qu'un sinistre ou qu'une interruption en particulier puisse toucher les deux centres de données en même temps, nuisant ainsi à la reprise opportune de l'environnement SAP.

Gestion des changements dans l'infrastructure informatique

Constatation

2.4.5 L'audit a permis de déterminer qu'aucun canal de communication efficace n'était en place pour permettre d'informer AAC de façon uniforme et en temps opportun des changements dans l'infrastructure informatique qui peuvent entraîner la non-disponibilité de l'application SAP, ce qui empêche de prévenir les partenaires clients. Depuis la création de SPC, l'étendue de la communication et de la collaboration avec son personnel dans le processus de gestion des changements d'AAC a diminué et les représentants de SPC ne participent plus aux réunions relatives au contrôle des changements à AAC. Bien que des réunions entre AAC et SPC aient lieu au niveau de la haute direction, les représentants des deux ministères ne participent à aucune réunion relative à la gestion des changements.

Constatation 8 : Aucune structure de gouvernance efficace n'est en place pour veiller à l'uniformité et à la rapidité des messages au sujet de changements à l'infrastructure pouvant entraîner la non-disponibilité de l'application SAP, leur transmission à tous les partenaires et la minimalisation des incidences sur les activités.

2.4.6 Recommandation

AAC 5 – AAC devrait collaborer avec SPC dans le but d'officialiser des accords sur les niveaux de service ou d'autres arrangements opérationnels afin que :

- le plan de reprise après sinistre soit mis à jour de façon continue pour refléter l'environnement actuel; les documents du plan de reprise après sinistre distinguent avec précision les rôles et les responsabilités du partenariat de ceux de SPC en cas de sinistre;

- l'emplacement du centre de données de relève et du centre de secours immédiat soit réévalué et que des mesures correctives soient prises si cela est nécessaire;

- les changements prévus dans l'infrastructure qui pourraient avoir une incidence sur la disponibilité du système SAP soient abordés de façon uniforme et en temps opportun avec les partenaires clients.

AAC 5
Réponse de la direction : Recommandation acceptée.

Plan d'action :
AAC collaborera avec SPC pour s'assurer que les attentes et les besoins relatifs au service SAP sont pleinement compris. De plus, il travaillera avec SPC dans les buts suivants :

- officialiser l'examen périodique et l'actualisation du plan de reprise après sinistre pour refléter l'environnement SAP actuel, y compris la distinction des rôles et des responsabilités d'AAC et de SPC en cas de sinistre;

- demander que l'emplacement du centre de données de relève (centre de secours immédiat) pour le SAP soit réévalué et que des mesures correctives soient prises si cela est nécessaire;

- définir l'approche qui permettra à SPC de tenir des discussions opportunes avec AAC au sujet des changements proposés dans l'infrastructure ayant une incidence anticipée sur le système SAP.

Date cible d'achèvement : 1er avril 2016

Responsable(s) : Dirigeant principal de l'information

ANNEXE A : SIGLES

AAC	Agriculture et Agroalimentaire Canada
ACIA	Agence canadienne d'inspection des aliments
BCG	Bureau du contrôleur général
CCC	Comité de contrôle du changement d'AAC
CDPS	Comité directeur du partenariat SAP
CGPS	Comité de gestion du partenariat SAP
CGTI	Contrôles généraux des technologies de l'information
COBIT	Objectifs de contrôle de l'information et des technologies connexes
EAU	Essais d'acceptation par les utilisateurs
PRE	Planification des ressources d'entreprise
RNCan	Ressources naturelles Canada
SIFM	Système intégré des finances et du matériel
SPC	Services partagés Canada
TI	Technologies de l'information

ANNEXE B : CRITÈRES DE L'AUDIT

Secteur d'intérêt 1
Le partenariat possède une structure de gouvernance qui lui permet de discuter collectivement des priorités et des objectifs stratégiques, de les établir et de les communiquer. Ces priorités et objectifs visent à guider la planification et l'établissement de l'ordre de priorité des investissements et des ressources, et ce, conformément aux besoins opérationnels et à l'orientation pangouvernementale.

1.1. Une structure de gouvernance comportant la participation des cadres supérieurs pour la prise des décisions et la résolution des problèmes est établie pour veiller à ce que les investissements et les ressources de la solution SAP appuient les partenaires clients de façon efficace et équitable.

***Source** : Accord entre AAC, RNCan et l'ACIA sur les niveaux de service pour la solution SAP*

1.1.1. Le Comité directeur du partenariat SAP examine et approuve les ressources de la solution SAP et s'assure que les investissements prévus sont harmonisés avec les objectifs stratégiques des partenaires clients. Le Comité se réunit régulièrement et la participation aux réunions est appropriée.

1.1.2. Le Comité de gestion du partenariat SAP examine et approuve les initiatives des partenaires clients, y compris les changements importants dans la fonctionnalité de la solution SAP, et détermine les plans et les priorités dans le cadre de négociations. Le Comité se réunit régulièrement et la participation aux réunions est appropriée.

1.1.3. Lorsqu'il élabore des plans de solutions et d'applications, le Centre d'excellence interagit en temps opportun avec les secteurs opérationnels et fonctionnels ainsi que les organisations de prestation de services des partenaires clients afin de s'assurer que les exigences opérationnelles des partenaires clients sont respectées et que le partenariat bénéficie le plus possible des initiatives de chaque partenaire client.

1.1.4. Les partenaires clients sont représentés par les personnes appropriées à chaque forum des partenaires; ces forums ont lieu de façon périodique pour discuter de l'élaboration prochaine de la solution SAP et permettre aux partenaires clients de fournir une rétroaction en temps opportun.

1.2. Des investissements prudents sont faits dans le Système intégré des finances et du matériel (SIFM) SAP qui satisfont aux exigences opérationnelles et sont harmonisés avec l'orientation stratégique pour les systèmes de gestion financière à l'échelle du gouvernement, conformément aux directives du Conseil du Trésor.

***Source** : Politique du Conseil du Trésor sur la gérance des systèmes de gestion financière*

1.2.1. Des représentants du partenariat ont été affectés aux comités du groupe de grappes du SIFM du gouvernement du Canada et ils y participent activement afin de s'assurer que les besoins opérationnels du partenariat sont pris en considération dans le cadre de ce forum tout en respectant l'orientation du Bureau du contrôleur général (BCG) du Canada pour les systèmes de gestion financière.

1.2.2. Les nouvelles informations ou exigences opérationnelles qui touchent le SIFM au niveau pangouvernemental font l'objet de discussions avec les partenaires clients. Le partenariat, le BCG et le groupe de grappes du SIFM du gouvernement du Canada travaillent en collaboration pour élaborer un processus approprié de gestion des changements dans les systèmes et un plan de mise en œuvre.

1.2.3. La collaboration entre le partenariat et le BCG vise à harmoniser, dans la mesure du possible, le SIFM du partenariat avec l'orientation pangouvernementale.

Secteur d'intérêt 2
Des contrôles des TI sont en place au sein du Centre d'excellence et parmi les partenaires clients pour appuyer la production d'informations financières exactes, fiables, accessibles et opportunes.

2.1. Des contrôles efficaces sont en place pour ajouter, mettre à jour et supprimer les droits d'accès des utilisateurs aux données et aux programmes financiers et l'accès à ceux-ci est restreint de façon appropriée.

***Source** : COBIT5 – DSS05.04 Gérer l'identité de l'utilisateur et l'accès logique*

2.1.1. Les paramètres de configuration du SAP, y compris les exigences relatives aux mots de passe, sont appropriés et harmonisés avec les normes de l'industrie.

2.1.2. L'accès aux fonctions informatiques privilégiées, y compris les comptes puissants, est limité aux personnes appropriées.

2.1.3. L'accès des utilisateurs est autorisé, établi de façon appropriée, surveillé, examiné de façon périodique et retiré en temps opportun lorsqu'il n'est plus requis.

2.1.4. Une ségrégation des tâches incompatibles existe dans le processus de gestion de l'accès logique.

2.2. Les changements au niveau de l'application sont apportés de manière contrôlée, y compris les changements standards et la maintenance d'urgence. Cela comprend les normes et les procédures relatives aux changements, l'évaluation de l'incidence, l'établissement des priorités, l'autorisation, les changements d'urgence, le suivi, la production des rapports, la clôture et la documentation.

***Source** : COBIT5 – BAI06 Gérer les changements*

2.2.1. Les changements sont mis en route par le personnel approprié en fonction des exigences fonctionnelles, techniques et opérationnelles.

2.2.2. La mise à l'essai des changements est effectuée par le personnel approprié selon la nature du changement et avant que celui-ci ne passe à l'étape de la mise en œuvre. Les partenaires clients participent au besoin.

2.2.3. Les changements sont approuvés par le personnel approprié avant de passer à l'étape de la mise en œuvre.

2.2.4. Les changements prévus à l'environnement de production et aux activités de maintenance sont abordés par le Comité de contrôle du changement et programmés de façon à réduire au minimum l'incidence sur les activités.

2.2.5. Une ségrégation des tâches incompatibles existe dans le processus de gestion des changements.

2.3. Les opérations des TI sont gérées d'une manière contrôlée et une surveillance du traitement automatisé est effectuée.

***Source** : COBIT5 – DSS01.01 Exécuter les procédures opérationnelles*

2.3.1. Les sauvegardes des données financières du système SAP sont effectuées de façon régulière et mises à l'essai afin de s'assurer que ces données peuvent être restaurées. Les échecs de sauvegardes sont surveillés et des mesures correctives sont prises.

2.3.2. Les déviations du traitement prévu sont relevées et résolues en temps opportun et l'accès permettant d'apporter des changements au calendrier

des travaux est restreint aux personnes appropriées. Les changements au calendrier des travaux sont approuvés.

2.4. Un plan est établi et maintenu pour permettre à l'entreprise et aux TI de répondre aux incidents et aux interruptions afin de continuer l'exploitation de la solution SAP et de maintenir la disponibilité des données à un niveau acceptable pour les partenaires clients.

***Source** : COBIT5 – DSS04 Gérer la continuité*

2.4.1. Chaque partenaire client a effectué une analyse des répercussions sur les activités et une évaluation des menaces et des risques de la solution SAP, y compris l'établissement d'objectifs cibles en matière de temps de reprise.

2.4.2. Un plan de reprise après sinistre a été établi en collaboration avec les partenaires clients et ce dernier est harmonisé avec les analyses des répercussions sur les activités.

2.4.3. Un plan de continuité des activités a été établi par chaque partenaire client lorsque cela a été jugé nécessaire selon l'analyse des répercussions sur les activités.

2.5. Les contrôles des applications clés à l'appui des processus opérationnels financiers identifiés par le dirigeant principal des finances des partenaires clients fonctionnent comme prévu.

***Source** : Politique du Conseil du Trésor sur le contrôle interne*

2.5.1. Les contrôles des applications ont été conçus et configurés de façon adéquate.

2.5.2. L'accès permettant de modifier les paramètres clés et les éléments configurables est restreint au personnel autorisé.

Secteur d'intérêt 3
Des structures de gouvernance sont en place pour gérer les risques relatifs aux services fournis par des tiers.

3.1. Les changements ou les activités de maintenance ayant une incidence sur l'infrastructure qui héberge la solution SAP du partenariat sont abordés à l'avance avec les représentants du partenariat afin d'atténuer les incidences imprévues sur les activités ou les interruptions imprévues de celles-ci.

***Source** : COBIT5 – APO10.04 Gérer les risques liés aux fournisseurs*

3.1.1. Un mécanisme est en place pour assurer la liaison des tiers avec les représentants du partenariat et discuter des changements à venir dans l'infrastructure.

3.1.2. Les changements à venir dans l'infrastructure qui peuvent entraîner un temps d'arrêt sont abordés parmi les partenaires clients et les problèmes sont soulevés auprès de tiers.

3.2. Des mécanismes sont en place pour s'assurer que les services fournis par des tiers peuvent être restaurés à un niveau et dans un délai acceptables pour les partenaires clients en cas de sinistre ou que des mesures d'atténuation sont en place.

***Source** : COBIT5 – APO10.04 Gérer les risques liés aux fournisseurs*

3.2.1. Les exigences à l'appui de la continuité des activités, y compris la disponibilité de données de sauvegarde complètes à l'intérieur de l'objectif en matière de temps de reprise, sont abordées de façon officielle avec les tiers.

3.2.2. Les rôles et les responsabilités du partenariat en cas de sinistre ont été clairement distingués de ceux des tiers.

3.2.3. Un plan intégré de reprise après sinistre a été élaboré et communiqué au partenariat. Ce plan est harmonisé avec les objectifs du partenariat ou des mesures d'atténuation sont en place si un tel plan n'a pas été établi.