Patrimoine canadien | Canadian Heritage

Canada

Audit de la Politique sur le contrôle interne – Audit des contrôles généraux des technologies de l'information (CGTI)

Bureau de la dirigeante principale de la vérification
Direction des services de vérification et d'assurance

Mars 2015

This publication is also available in English.

Cette publication est disponible en format PDF accessible à l'adresse Internet suivante : http://www.pch.gc.ca

Nº de catalogue : CH6-31/2015F-PDF
ISBN : 978-0-660-02112-6

Table des matières

Sommaire

Introduction

Le Secrétariat du Conseil du Trésor a adopté la Politique sur le contrôle interne en 2008, et a fixé le 1er avril 2009 comme date d'entrée en vigueur. L'objectif de la politique est de faire en sorte que les risques reliés à la gérance des ressources publiques soient gérés adéquatement grâce à des contrôles internes efficaces et efficients au sein des ministères et à l'échelle du gouvernement. La Politique sur le contrôle interne appuie les principes fondamentaux de la *Loi sur la gestion des finances publiques* (LGFP), qui est la pierre angulaire du cadre juridique de la gestion financière générale et de la responsabilisation des organisations qui composent la fonction publique fédérale et des sociétés d'État.

Compte tenu de la dépendance continue à l'égard des systèmes d'information et des contrôles financiers, des contrôles généraux des technologies de l'information (CGTI) qui sont bien conçus et qui fonctionnent efficacement sont nécessaires pour appuyer adéquatement le contrôle interne en matière de rapports financiers (CIRF). De bons contrôles généraux des TI sont essentiels pour déterminer si on peut se fier sur les contrôles de processus opérationnels automatisés qui prennent en charge les comptes importants présentés dans les états financiers.

L'autorisation de mener le projet d'audit découle du Plan d'audit pluriannuel axé sur les risques de 2014-2015 à 2016-2017, qui a été recommandé par le Comité ministériel de vérification (CMV) et approuvé par le sous-ministre en juin 2014.

L'audit avait pour objectif de fournir l'assurance que les CGTI, en tant que parties intégrantes du contrôle interne des rapports financiers et de la gérance globale des biens des TI, soient clairement établis et utilisés pour aider le Ministère à réaliser son mandat et à atteindre ses objectifs, plus particulièrement grâce au soutien fourni par les CGTI en ce qui concerne le fonctionnement efficace des contrôles d'applications, notamment les contrôles relatifs à l'entrée, au traitement et à la sortie.

L'audit porte sur les CGTI relativement aux quatre secteurs de contrôle suivants :

1. Sécurité logicielle de l'accès aux programmes d'applications et aux données;
2. Modifications des programmes aux applications, y compris l'application de correctifs ou le versionnage (version; doublage);
3. Activités d'élaboration de programmes (toutefois, il a été confirmé qu'il n'y a pas eu de telles activités dans la période en cours);
4. Activités opérationnelles, y compris la planification des tâches et travaux, la gestion des problèmes et les copies de sauvegarde.

Les secteurs de contrôle susmentionnés ne tombent sous la portée de l'audit qu'en raison de leur rapport avec les applications appuyant le contrôle interne en matière de rapports financiers. Dans le cadre de la phase de planification, ces applications ont été définies comme suit :

- SAP – Système financier de dossiers de PCH.
- SIGPAA – Système d'information sur la gestion du Programme d'aide aux athlètes. Ce système gère les paiements d'aide aux athlètes amateurs.
- SRP – Système régional de paye. Cette application ne tombe sous la portée de l'audit qu'en raison de son rapport avec la gestion des utilisateurs ayant accès au SRP, car tous les autres aspects des CGTI relèvent de Travaux publics et Services gouvernementaux Canada, qui fournit l'application aux ministères.

La période couverte par l'audit correspond à l'exercice financier en cours, soit du 1er avril 2014 jusqu'à l'achèvement du travail d'audit sur le terrain en décembre 2014.

Principales constatations

Des tests ont été effectués pour chaque application tombant sous la portée de l'audit et chaque secteur de contrôle applicable à chacune de ces applications. Tout au long de l'audit, l'équipe d'audit a observé de nombreux secteurs de contrôle dans la gestion des CGTI, ainsi que certains secteurs où les activités de contrôle devraient être renforcées. Le tableau ci-dessous résume les résultats globaux des tests.

		SAP	SIGPAA	SRP
Accès aux programmes et aux données	Politique et normes de sécurité des TI	PCH		
	Authentification de l'utilisateur	PCH	PCH	TPSGC
	Administration de l'accès des utilisateurs	PCH	PCH	PCH
	Revalidation de l'accès des utilisateurs	PCH	PCH	PCH
	Séparation des tâches entre les demandes et les autorisations d'accès	PCH	PCH	PCH
Modifications des programmes	Politique et procédures	PCH	PCH	TPSGC
	Caractéristiques et suivi des demandes de modifications	PCH et AAC	PCH	TPSGC
	Autorisation	PCH	PCH	TPSGC
	Tests et assurance de la qualité	PCH	PCH	TPSGC
	Mise en production	PCH et AAC	PCH	TPSGC
	Modifications d'urgence	PCH	PCH	TPSGC
Opérations informatiques	Gestion et surveillance des travaux	PCH	PCH	TPSGC
	Gestion des copies de sauvegarde	AAC et SPC	PCH et SPC	TPSGC
	Centre des services et gestion des problèmes	PCH	PCH	TPSGC

Légende	Description
Vert	Il existe des contrôles, et la preuve de l'efficacité du contrôle est démontrée constamment.
Jaune	Il existe des contrôles partiels, et/ou on observe un manque d'uniformité dans l'efficacité du contrôle.
Rouge	Il n'existe pas de contrôles, ou on observe un manque important d'uniformité dans l'efficacité du contrôle.

Comme l'indiquent les cellules vertes dans le tableau ci-dessus, PCH a de nombreux contrôles solides en place en ce qui a trait aux CGTI, et on a pu constater que ces contrôles fonctionnaient efficacement au cours de la période visée par l'audit.

Chacune des cellules jaunes indique une constatation qui a été notée à la suite des tests effectués sur les CGTI pertinents, par rapport à la conception des procédures de contrôle ou au fonctionnement uniforme de ces procédures tout au long de la période des tests. Ci-dessous figurent les constatations relatives aux contrôles pour chaque cellule jaune.

SAP

- L'accès de l'utilisateur au SAP n'est pas toujours retiré en temps opportun lorsque les utilisateurs cessent d'exercer leur emploi ou autrement quittent le Ministère.
- Un certain nombre de contrôles de surveillance de l'accès des utilisateurs au SAP sont en place, mais ils devraient être améliorés de façon à comprendre :
- un examen et une reconfirmation périodiques des droits d'accès pour les utilisateurs de l'administration centrale;
- une réalisation en temps opportun des examens actuels de la séparation des tâches.
- Il n'y a pas de politique ni de procédures documentées en place relatives à la gestion des modifications pour guider toutes les étapes du traitement des modifications à l'application SAP.

SIGPAA

- Les mots de passe ne sont pas modifiés régulièrement.
- Il existe un conflit lié à la séparation des tâches dans le cas d'un utilisateur qui approuve les modifications à l'accès et qui peut aussi configurer les paramètres d'accès de l'application.
- Il n'y a pas de politique ni de procédures documentées en place relatives à la gestion des modifications pour guider toutes les étapes du traitement des modifications à l'application du SIGPAA.
- Il n'existe aucun processus défini pour le suivi et la gestion des problèmes et des incidents liés au SIGPAA.

Recommandations

SAP

Le dirigeant principal des finances devrait :

1. Examiner et réviser le processus actuel par lequel l'équipe de sécurité du SAP est avisée des personnes ayant cessé d'exercer leur emploi ou ayant autrement quitté le Ministère, afin que l'accès de l'utilisateur au SAP puisse être retiré en temps opportun.
2. Améliorer les activités de contrôle liées à la surveillance de l'accès des utilisateurs, plus particulièrement :
    a) Mettre en œuvre un processus de revalidation d'accès périodique des utilisateurs du SAP à l'administration centrale, et des rôles assignés à chacun, qui se déroulerait au moins une fois l'an et qui serait documenté officiellement. Toutes les modifications d'accès des utilisateurs nécessaires à la suite de la revalidation devraient être traitées rapidement.
    b) Établir un calendrier pour la réalisation des examens de la séparation des tâches, y compris le traitement immédiat des modifications d'accès des utilisateurs nécessaires afin d'éliminer les conflits liés la séparation des tâches.
3. Exiger qu'une directive de gestion des modifications soit documentée, approuvée et mise en œuvre pour guider l'application uniforme des procédures de gestion des modifications apportées à l'application SAP.

SIGPAA

Le directeur exécutif, Excellence sportive, devrait :

4. Mettre en œuvre une procédure exigeant à tous les utilisateurs ayant accès au SIGPAA de modifier régulièrement leurs mots de passe.
5. Mettre en œuvre une exigence selon laquelle aucun utilisateur ne peut à la fois approuver les demandes d'accès au SIGPAA et autoriser l'accès à l'application.
6. Exiger qu'une politique et des procédures d'envergure appropriée de gestion des modifications soient documentées, approuvées et mises en œuvre pour guider l'application uniforme des procédures de gestion des modifications apportées à l'application.
7. Mettre en œuvre un processus par lequel les problèmes et les incidents d'application liés au SIGPAA sont suivis et analysés, et dont la résolution est consignée dans un registre.

Énoncé de conformité

Selon mon jugement professionnel en tant que dirigeante principale de l'audit, l'audit est conforme aux normes de vérification interne du gouvernement du Canada, comme le confirment les résultats du programme d'assurance et d'amélioration de la qualité.

Opinion d’audit

À mon avis, les contrôles de gestion des CGTI comportent divers secteurs de risque qui nécessitent l’attention de la direction, avec un faible degré d’exposition au risque en ce qui concerne l’incidence globale du contrôle interne en matière de rapports financiers et de la gérance des biens de TI.

Signé par

_____

Maria Lapointe-Savoie
Dirigeante principale de l’audit
Ministère du Patrimoine canadien

Membres de l’équipe d’audit

Maria Lapointe-Savoie, directrice

Dylan Edgar, gestionnaire de l’audit

Jean-Phillipe Rioux, auditeur

Avec l’aide de ressources externes

1. Introduction et contexte

1.1 Autorisation du projet

L'autorisation de mener ce projet d'audit découle du Plan de vérification pluriannuel axé sur les risques de 2014-2015 à 2016-2017, qui a été recommandé par le Comité ministériel de vérification (CMV) et approuvé par le sous-ministre en juin 2014.

1.2 Contexte

En tant qu'institution du gouvernement du Canada, le ministère du Patrimoine canadien (PCH) est tenu de gérer le domaine des contrôles généraux de la technologie de l'information (CGTI) de manière à appuyer les objectifs généraux du gouvernement et à fournir des informations et des services aux Canadiens. Ces exigences sont officiellement exposées dans la législation, les politiques et les normes de l'ensemble du gouvernement.

Le Secrétariat du Conseil du Trésor a adopté la Politique sur le contrôle interne en 2008, et a fixé le 1er avril 2009 comme date d'entrée en vigueur. L'objectif de la politique est de faire en sorte que les risques liés à la gérance des ressources publiques soient gérés adéquatement au moyen de contrôles internes efficaces et efficients au sein des ministères et à l'échelle du gouvernement.

Les principaux résultats attendus de la Politique sur le contrôle interne sont les suivants :

- Des systèmes de contrôle interne efficaces, fondés sur les risques, sont en place dans chaque ministère et sont adéquatement maintenus, et ils font l'objet d'une surveillance continu, d'évaluations périodiques et de mesures correctives en temps opportun lorsque des problèmes sont identifiés.
- Des systèmes de contrôle interne efficace en matière de rapports financiers sont en place dans chaque ministère comme le démontre la Déclaration de responsabilité de la direction englobant le contrôle interne en matière de rapports financiers du Ministère (échelonnée sur une période de trois ans).
- Les intervenants de tous les niveaux connaissent et comprennent bien leurs rôles, responsabilités et obligations redditionnelles en matière de contrôles internes.

La Politique sur le contrôle interne appuie les principes fondamentaux de la *Loi sur la gestion des finances publiques* (LGFP), qui est la pierre angulaire du cadre juridique de la gestion financière générale et de la responsabilisation des organisations qui composent la fonction publique fédérale et des sociétés d'État.

Compte tenu de la dépendance continue à l'égard des systèmes d'information et des contrôles financiers, des contrôles généraux des TI qui sont bien conçus et qui fonctionnent efficacement sont nécessaires pour appuyer adéquatement le contrôle interne en matière de rapports financiers (CIRF). De bons contrôles généraux de la technologie de l'information (CGTI) sont essentiels pour déterminer si on peut se fier sur les contrôles de processus opérationnels automatisés qui prennent en charge les comptes importants présentés dans les états financiers.

2. Objectif

L'audit avait pour objectif de fournir l'assurance que les CGTI, en tant que parties intégrantes du contrôle interne des rapports financiers et de la gérance globale des biens de TI, soient clairement établis et utilisés pour aider le Ministère à réaliser son mandat et à atteindre ses objectifs, plus particulièrement grâce au soutien fourni par les CGTI en ce qui concerne le fonctionnement efficace des contrôles d'applications, notamment les contrôles relatifs à l'entrée, au traitement et à la sortie.

3. Portée

L'audit porte sur les CGTI relativement aux quatre secteurs de contrôle suivants :

1. Sécurité logicielle de l'accès aux programmes d'applications et aux données;
2. Modifications des programmes aux applications, y compris l'application de correctifs ou le versionnage (version; doublage);
3. Activités d'élaboration de programmes, y compris les conversions de données;
4. Activités opérationnelles, y compris la gestion des travaux, la gestion des problèmes et les copies de sauvegarde.

Les secteurs de contrôle susmentionnés ne tombent sous la portée de l'audit qu'en raison de leur rapport avec les applications appuyant les CIRF. Dans le cadre de la phase de planification, ces applications ont été définies comme suit :

- SAP – Système financier de dossiers de PCH. L'application SAP de PCH est gérée par le personnel de PCH et hébergée par Agriculture et Agroalimentaire Canada (AAC) qui, conformément au protocole d'entente, fournit du soutien technique pour le SAP et du soutien en matière de bases de données. Parcs Canada partage la même application que PCH, et l'équipe du SAP de PCH administre le SAP au nom de Parcs Canada.
- SIGPAA – Système d'information sur la gestion du Programme d'aide aux athlètes. Ce système gère les paiements d'aide aux athlètes amateurs. Il s'agit d'une plus petite application qui compte un nombre limité d'utilisateurs et qui est gérée à l'interne par PCH.
- SRP – Système régional de paye. Cette application ne tombe sous la portée de l'audit qu'en raison de son rapport avec la gestion des utilisateurs ayant accès au SRP, car tous les autres aspects des CGTI relèvent de Travaux publics et Services gouvernementaux Canada, qui fournit l'application aux ministères.

En outre, l'audit n'inclut que les secteurs de contrôle ayant un rapport avec les contrôles exercés par PCH, et elle exclut les contrôles qui relèvent d'un autre ministère.
Deux autres ministères sont responsables de parties de l'environnement des CGTI à PCH, soit Services partagés Canada (SPC) et AAC. Voici l'approche favorisée par chacun de ces deux ministères à l'égard des CGTI :

- SPC possède l'infrastructure, ce qui comprend les centres de données, le matériel et les logiciels des systèmes. Conformément à l'approche adoptée dans l'ensemble du

gouvernement, le présent audit exclut tous les contrôles de SPC. Les responsables de SPC ont reconnu leur responsabilité sur le plan du contrôle, et ils se sont engagés à tester leurs CGTI et à communiquer les résultats aux ministères, comme l'indiquait un courriel de SPC aux ministères, le 30 mai 2014.

- AAC fournit l'environnement d'hébergement pour l'application SAP. Les responsabilités d'AAC et de PCH sont énoncées dans un protocole d'entente. L'équipe d'audit a tenté d'obtenir d'AAC les tests distincts effectués et les résultats de ces tests pour les éléments des CGTI qu'ils fournissent à PCH, mais les responsables d'AAC ont indiqué qu'ils ne disposent pas de rapports distincts pour PCH. Par conséquent, on a communiqué directement avec les responsables d'AAC au cours de l'audit afin qu'ils répondent à des questions précises concernant les contrôles sur le soutien en matière de bases de données et la gestion des copies de sauvegarde. Les réponses reçues ont été utilisées à titre de preuve aux fins de l'audit, bien qu'il convienne de souligner que ces secteurs n'ont pas été testés indépendamment dans le cadre de l'audit.

Le tableau ci-dessous résume les secteurs de contrôle tombant sous la portée de l'audit, selon l'environnement d'applications. Seules les parties ombragées en gris ont été testées pour chaque environnement d'applications.

		SAP	AAPMIS	SRP
Accès aux programmes et aux données	Politique et normes de sécurité des TI	PCH	PCH	S/O
	Authentification de l'utilisateur	PCH	PCH	TPSGC
	Administration de l'accès des utilisateurs	PCH	PCH	PCH
	Revalidation de l'accès des utilisateurs	PCH	PCH	PCH
	Séparation des tâches entre les demandes et les autorisations d'accès	PCH	PCH	TPSGC
	Sécurité des bases de données	AAC	PCH	TPSGC
	Sécurité du système d'exploitation	SPC	SPC	SPC
Program Changes	Politique et procédures	PCH	PCH	TPSGC
	Caractéristiques, autorisation et suivi des demandes de modifications	PCH et AAC	PCH	TPSGC
	Tests et assurance de la qualité	PCH	PCH	TPSGC
	Mise en production	PCH	PCH	TPSGC
	Modifications d'urgence	PCH et AAC	PCH	TPSGC
Modifications des programmes	Gestion des activités d'élaboration et de mise en œuvre	Sans objet pour le moment, car il n'y a pas eu de fait nouveau important en 2014-2015.	Sans objet pour le moment, car il n'y a pas eu de fait nouveau important en 2014-2015.	TPSGC
	Lancement, analyse et conception de projet			TPSGC
	Élaboration et sélection de la trousse			TPSGC
	Tests et assurance de la qualité			TPSGC
	Conversion de données			TPSGC
	Mise en œuvre en production			TPSGC
Élaboration de programmes	Gestion et surveillance des travaux	PCH	PCH	TPSGC
	Gestion des copies de sauvegarde	AAC et SPC	PCH et SPC	TPSGC
	Centre des services et gestion des problèmes	PCH	PCH	TPSGC

La période couverte par l'audit correspond à l'exercice financier en cours, soit du 1er avril 2014 jusqu'à l'achèvement du travail d'audit sur le terrain en décembre 2014.

4. Approche et méthodologie

Tout le travail d'audit a été effectué conformément aux *Normes relatives à la vérification interne au sein du gouvernement du Canada* et à la *Politique sur la vérification interne* du Secrétariat du Conseil du Trésor ainsi qu'aux *Normes internationales pour la pratique professionnelle de l'audit interne* de l'Institut des auditeurs internes.

Les critères d'audit déterminent les normes en fonction desquelles une évaluation est faite, et ils constituent le fondement du plan de travail et de l'exécution de l'audit. Ils sont propres aux objectifs et à la portée de chaque audit. Les critères d'audit détaillés pour les objectifs d'audit des CGTI sont énoncés à l'annexe A. Les critères d'audit ont été élaborés à partir des objectifs de contrôle dans le domaine de l'information et des technologies connexes (*Control Objectives for Information Technology [COBIT]*), une publication internationale largement reconnue qui énonce des pratiques exemplaires pour la gouvernance et la gestion des TI. De nombreux ministères ont eu recours au cadre COBIT dans la détermination de la portée de leurs CGTI et des tests à effectuer à l'appui du contrôle interne en matière de rapports financiers.

La méthodologie de l'audit comprenait notamment ce qui suit :

- l'examen de la documentation, des lignes directrices, des procédures, des politiques et des lois pertinentes du Ministère;
- l'analyse de divers autres documents et rapports, notamment les rapports sur les systèmes ou la visualisation à l'écran des paramètres de configuration des systèmes, en présence des administrateurs de systèmes compétents de PCH;
- la collecte de données au moyen d'observations et d'entrevues auprès du personnel du Ministère afin d'examiner les pratiques, procédures et processus utilisés;
- le contrôle d'une sélection d'opérations pour la période du 1er avril 2014 jusqu'à l'achèvement du travail d'audit sur le terrain afin de déterminer si les principaux CGTI pour chaque application tombant sous la portée de l'audit fonctionnaient efficacement tout au long de la période visée.

L'audit a été mené à partir de la région de la capitale nationale, avec une faible participation régionale, étant donné qu'il a été déterminé lors de la phase de planification que les CGTI pour les applications tombant sous la portée de l'audit sont administrés par les équipes de soutien des systèmes en poste dans la région de la capitale nationale.

5. Observations et recommandations

Cette section présente en détail les constatations et les recommandations connexes de l'audit des CGTI. Les constatations sont fondées sur une combinaison de preuves recueillies au cours de l'examen des documents, des analyses, du contrôle des opérations et des dossiers, et des entrevues effectuées pour chacun des critères d'audit. L'annexe A présente un résumé de toutes les constatations et conclusions pour chacun des critères

évalués par l'équipe d'audit. Au cours de l'audit, des observations mineures ont été communiquées directement à la direction.

La matrice de contrôle sommaire ci-dessous donne un aperçu clair des résultats des tests.

		SAP	SIGPAA	SRP
Accès aux programmes et aux données	Politique et normes de sécurité des TI	PCH		
	Authentification de l'utilisateur	PCH	PCH	TPSGC
	Administration de l'accès des utilisateurs	PCH	PCH	PCH
	Revalidation de l'accès des utilisateurs	PCH	PCH	PCH
	Séparation des tâches entre les demandes et les autorisations d'accès	PCH	PCH	PCH
Modifications des programmes	Politique et procédures	PCH	PCH	TPSGC
	Caractéristiques et suivi des demandes de modifications	PCH et AAC	PCH	TPSGC
	Autorisation	PCH	PCH	TPSGC
	Tests et assurance de la qualité	PCH	PCH	TPSGC
	Mise en production	PCH et AAC	PCH	TPSGC
	Modifications d'urgence	PCH	PCH	TPSGC
Opérations informatiques	Gestion et surveillance des travaux	PCH	PCH	TPSGC
	Gestion des copies de sauvegarde	AAC et SPC	PCH et SPC	TPSGC
	Centre des services et gestion des problèmes	PCH	PCH	TPSGC

La légende de la matrice est la suivante.

Évaluation	Description
Vert	Il existe des contrôles, et la preuve de l'efficacité du contrôle est démontrée constamment.
Jaune	Il existe des contrôles partiels, et/ou on observe un manque d'uniformité dans l'efficacité du contrôle.
Rouge	Il n'existe pas de contrôles, ou on observe un manque important d'uniformité dans l'efficacité du contrôle.

Comme l'indiquent les cellules vertes dans le tableau ci-dessus, PCH a de nombreux contrôles solides en place en ce qui a trait aux CGTI, et on a pu constater que ces contrôles fonctionnaient efficacement tout au long de la période visée par l'audit.

Chacune des cellules jaunes indique une constatation qui a été notée à la suite des tests effectués sur les CGTI pertinents, par rapport à la conception des procédures de contrôle ou au fonctionnement uniforme de ces procédures tout au long de la période des tests. Ci-dessous figurent les constatations relatives aux contrôles pour chaque cellule jaune. Les constatations sont présentées par application et par secteur de contrôle de l'application.

5.1 SAP

5.1.1 Administration de l'accès des utilisateurs

L'accès de l'utilisateur au SAP n'est pas toujours retiré en temps opportun lorsque les utilisateurs cessent d'exercer leur emploi ou autrement quittent le Ministère.

Critères de contrôle

Il existe des procédures, qui sont suivies, pour faire en sorte que les mesures nécessaires soient prises en temps opportun en ce qui concerne les demandes, l'établissement, la délivrance, la suspension et la fermeture des comptes d'utilisateur.

Observations

L'équipe de sécurité du SAP suit des procédures définies pour gérer l'accès des utilisateurs au SAP, y compris les procédures pour ajouter, modifier et supprimer l'accès des utilisateurs. Les procédures pour ajouter et modifier l'accès des utilisateurs ont été testées, et aucune exception n'a été notée. Pour tester la rapidité des retraits de l'accès, des rapports d'utilisateurs ayant cessé d'exercer leur emploi ont été obtenues directement des Ressources humaines ainsi que des rapports du système de billetterie qui permet de suivre les demandes de modifications d'accès, et les dates de cessation d'emploi figurant sur ces rapports ont été comparées aux dates où l'accès de l'utilisateur a réellement été retiré du SAP. Ce tests ont permis de constater ce qui suit :

- Cinq utilisateurs ayant quitté leur poste, dont les dates de cessation d'emploi allaient d'avril à octobre 2014, avaient encore des comptes actifs dans le SAP en date du 26 novembre 2014, soit la date à laquelle les tests ont été effectués.
- Parmi les utilisateurs visés par les tests, dont l'accès au SAP avait été retiré, l'accès pour 11 des 34 utilisateurs ayant cessé d'exercer leur emploi n'a pas été retiré en temps opportun. Pour ces 11 utilisateurs ayant quitté leur emploi, l'accès au SAP a été retiré entre 9 et 211 jours après la date de cessation d'emploi de l'utilisateur.

La capacité d'accéder au SAP nécessite d'abord d'ouvrir une session sur le réseau, puis sur l'application SAP, ce qui fournit deux niveaux de contrôle de l'accès. Si la procédure d'annulation de l'accès de l'utilisateur au niveau du réseau donne lieu au retrait en temps opportun des comptes d'utilisateur à ce niveau, le risque de retards dans le retrait de l'accès au SAP est réduit. Nous n'avons pas pu tester la rapidité des retraits de l'accès au réseau, car la date de retrait n'est pas évidente sur chaque compte réseau. Cependant, outre les procédures liées au retrait de l'accès au réseau, chaque équipe des applications doit s'assurer que l'accès demeure à jour pour tous les utilisateurs.

Évaluation des risques

Le défaut de retirer l'accès en temps opportun aux utilisateurs qui n'en ont plus besoin, peut donner lieu à un accès non autorisé à l'application SAP. En outre, cela va à l'encontre de l'article 5.2 de la « Norme sur l'identification et l'authentification » du Ministère qui énonce ce qui suit : « Les utilisateurs auront accès aux seuls renseignements nécessaires à leur fonction de travail et niveau d'habilitation. »

Recommandation nº 1

Le dirigeant principal des finances devrait :

Examiner et réviser le processus actuel par lequel l'équipe de sécurité du SAP est avisée des personnes ayant cessé d'exercer leur emploi ou ayant autrement quitté le Ministère, afin que l'accès de l'utilisateur au SAP puisse être retiré en temps opportun.

5.1.2 Revalidation de l'accès des utilisateurs

Un certain nombre de contrôles de surveillance de l'accès des utilisateurs au SAP sont en place, mais ils devraient être améliorés de façon à comprendre :

- un examen et une reconfirmation périodiques des droits d'accès pour les utilisateurs de l'administration centrale;
- une réalisation plus rapide des examens actuels de la séparation des tâches.

Critères de contrôle
Il existe un processus de contrôle, qui est suivi, pour examiner périodiquement les droits d'accès et les confirmer, y compris la désactivation des comptes d'utilisateur inactifs.

Observations

L'équipe de sécurité du SAP effectue un certain nombre d'activités de surveillance de la sécurité qui sont menées sur une base hebdomadaire, mensuelle, trimestrielle ou semestrielle. Un examen de ces activités a révélé qu'ils comprennent de nombreuses procédures rigoureuses de contrôle pour améliorer et maintenir la sécurité de l'application SAP.

Au nombre des activités de surveillance de la sécurité figure une exigence d'envoyer des rapports de tous les noms d'utilisateurs du SAP à chaque région sur une base trimestrielle afin de reconfirmer que ces utilisateurs ont encore besoin de leur accès au SAP. Cependant, cela n'est pas nécessaire pour les utilisateurs de l'administration centrale, bien que ceux-ci représentent le plus grand pourcentage d'utilisateurs du SAP.

Une autre activité importante de surveillance est l'examen semi-annuel pour déceler les conflits potentiels liés à la séparation des tâches en lien avec des affectations de l'utilisateur dans le système SAP. L'examen de la séparation des tâches couvre tous les utilisateurs du SAP quel que soit le niveau de risque. Cependant, les conflits liés à la séparation des tâches incombent aux utilisateurs des Opérations comptables, des

Systèmes et d'AAC. Les conflits liés à la séparation des tâches qui ont été identifiés sont affectés à des personnes désignées pour évaluer et indiquer les modifications nécessaires, lesquelles sont ensuite traitées par l'équipe des systèmes du SAP. Les tests ont indiqué que, bien que le processus soit en place, il y a des retards dans la réalisation des examens. L'examen fondé sur les rapports à partir du 26 mai 2014 a été réalisé comme suit :

- Opérations comptables – examen réalisé le 18 juillet, la modification d'accès demandée a été effectuée le 9 septembre.
- Systèmes – examen réalisé le 2 juillet, la modification d'accès demandée a été effectuée le 16 juillet.
- AAC – examen réalisé le 24 juin, la modification d'accès demandée le 30 juin.
- Parcs Canada – les utilisateurs de Parcs Canada étaient inclus dans l'examen de mai 2014, mais Parcs Canada a indiqué qu'il n'avait pu réaliser l'examen en raison d'autres priorités. Étant donné que Parcs Canada est une entité distincte, il incombe à PCH de lui fournir l'information sur les conflits à risque élevé liés à la séparation des tâches à l'intérieur de l'application, mais pas de s'assurer que Parcs Canada réalise l'examen.

Évaluation des risques

L'absence d'un processus pour revalider l'accès des utilisateurs au SAP à l'administration centrale sur une base périodique augmente le risque qu'il existe un accès inapproprié pour les utilisateurs qui ont quitté le Ministère ou qui ont changé de poste et qui ont donc acquis un droit d'accès dont ils n'ont plus besoin pour exercer les responsabilités de leur poste.

Les retards dans l'examen des conflits potentiels liés à la séparation des tâches en lien avec l'accès de l'utilisateur, et les retards dans l'élimination de ces conflits lorsque leur annulation est prévue, pourraient donner lieu au traitement non autorisé d'opérations dans le SAP et, par conséquent, à des résultats financiers inexacts.

Recommandation n^{o} 2

Le dirigeant principal des finances devrait :

Améliorer les activités de contrôle liées à la surveillance de l'accès des utilisateurs, notamment :

a) Mettre en œuvre un processus de revalidation d'accès périodique des utilisateurs du SAP à l'administration centrale, et des rôles assignés à chacun, qui se déroulerait au moins une fois l'an et qui serait documenté officiellement. Toutes les modifications d'accès des utilisateurs nécessaires à la suite de la revalidation devraient être traitées rapidement.
b) Établir un calendrier pour la réalisation des examens de la séparation des tâches, y compris le traitement immédiat des modifications d'accès des utilisateurs nécessaires afin d'éliminer les conflits liés la séparation des tâches.

5.1.3 Politique et procédures de gestion des modifications

Il n'y a pas de politique ni de procédures documentées en place relatives à la gestion des modifications pour guider toutes les étapes du traitement des modifications à l'application SAP.

Critères de contrôle

Il existe une politique de gestion des modifications et des procédures connexes, qui ont été approuvées par un niveau approprié de gestion, et qui sont communiquées au personnel concerné.

Observations

Même si l'équipe des systèmes du SAP a pu décrire le processus suivi pour gérer une modification à l'application SAP, il n'y a pas de politique ni de procédures documentées en place relatives à la gestion des modifications pour guider toutes les étapes du traitement des modifications à l'application SAP. Il existe un document sur les pratiques de gestion des modifications au système STAR, daté du 16 mars 2010; toutefois, ce document a plus de quatre ans, et il est encore à l'état d'ébauche avec des sections qui sont incomplètes. En outre, l'équipe de gestion des modifications a indiqué qu'il n'est pas à jour et qu'il n'est pas entièrement suivi. Les pratiques exemplaires au sein de l'industrie indiquent qu'un tel document devrait aborder, à tout le moins, les principales étapes du processus de gestion des modifications ainsi que les points de contrôle et les approbations nécessaires, y compris les exigences relatives à ce qui suit :

- la documentation des demandes de modifications;
- les demandes de modifications sont autorisées par un niveau de gestion approprié;
- les modifications sont entièrement testées, validées et approuvées avant d'être mises en production;
- des restrictions s'appliquent sur l'accès à la migration des modifications à l'environnement de production.

Évaluation des risques

L'absence d'une directive formelle et documentée de gestion des modifications augmente le risque que les activités effectuées pour traiter les modifications aux programmes soient inadéquates ou qu'elles ne soient pas suivies de manière uniforme, ce qui comporte le risque que des erreurs de traitement se glissent dans l'environnement de production.

En outre, comme il s'agit d'une application ministérielle qui donne lieu à des opérations financières, le manque d'officialisation des procédures crée un risque pour le Ministère dans l'éventualité d'un roulement du personnel.

Recommandation no 3

Le dirigeant principal des finances devrait :

Exiger qu'une directive de gestion des modifications soit documentée, approuvée et mise en œuvre pour guider l'application uniforme des procédures de gestion des modifications apportées à l'application.

5.2 SIGPAA

5.2.1 Authentification de l'utilisateur

Les mots de passe ne sont pas modifiés régulièrement.

Critères de contrôle
Il existe des procédures, qui sont suivies, pour authentifier tous les utilisateurs du système afin d'appuyer la validité des opérations.

Observations

Un nom d'utilisateur et un mot de passe uniques donnent accès à l'application du SIGPAA. Lorsque de nouveaux utilisateurs sont créés, un mot de passe qui répond aux exigences de longueur et de complexité est choisi et créé par l'équipe de la base de données. Il n'existe actuellement pas de fonction dans l'application du SIGPAA ni de fonction établie au niveau de la base de données qui exige que les mots de passe soient modifiés régulièrement, ou qui permette aux utilisateurs de modifier leur mot de passe dans l'application. Il s'ensuit que les mots de passe de l'utilisateur peuvent ne pas être modifiés pendant une période prolongée. Conformément aux exigences du Ministère énoncées dans la « Norme sur l'identification et l'authentification » du Ministère, les mots de passe doivent être modifiés au moins tous les six mois, comporter au moins huit caractères et suivre certaines exigences de composition.

Les modifications de mots de passe devraient être mises en œuvre par l'application. Toutefois, comme cela pourrait ne pas être pratique pour le SIGPAA, et comme le nombre d'utilisateurs de celui-ci est petit, une procédure manuelle pourrait être instaurée par laquelle l'équipe du SIGPAA programme les modifications de mots de passe et met en œuvre un processus manuel afin que tous les utilisateurs du SIGPAA communiquent avec l'administrateur de la base de données de l'application chaque six mois pour traiter les modifications demandées.

Évaluation des risques

Le défaut de modifier les mots de passe des applications sur une base régulière augmente le risque que d'autres personnes connaissent les mots de passe, ce qui pourrait donner lieu à un accès non autorisé à l'application.

Recommandation nº 4

Le directeur exécutif, Excellence sportive, devrait :

Mettre en œuvre une procédure exigeant à tous les utilisateurs ayant accès au SIGPAA de modifier régulièrement leurs mots de passe.

5.2.2 Séparation des tâches entre les demandes et les autorisations d'accès au SIGPAA

Il existe un conflit lié à la séparation des tâches lorsqu'un utilisateur approuve les modifications à l'accès et qu'il peut aussi configurer les paramètres d'accès de l'application.

Critères de contrôle

Il existe des contrôles relatifs à la séparation appropriée des tâches en ce qui concerne les demandes et les autorisations d'accès aux systèmes et aux données, et ces contrôles sont mis en application.

Observations

En raison du petit nombre d'utilisateurs ayant accès au SIGPAA, le processus d'autorisation ou de modification de l'accès de l'utilisateur est informel, s'effectuant à partir d'un courriel de l'analyste de programme présentant la demande de modification, laquelle demande est approuvée par le gestionnaire, et transmise à l'équipe de la base de données afin qu'elle configure les paramètres d'accès. Toutefois, un examen des utilisateurs en mesure de configurer ou de modifier les paramètres d'accès au niveau de la base de données a révélé que le gestionnaire dispose également de cet accès en raison de son appartenance au groupe « admin », quoique nous ayons été informés qu'il ne l'utilise jamais. Le fait d'avoir la responsabilité d'approuver les demandes d'accès et de traiter ces demandes crée un conflit lié à la séparation des tâches.

Évaluation des risques

Il est important de maintenir une séparation appropriée des tâches afin que personne ne puisse traiter une opération d'un bout à l'autre. Dans ce cas, un accès inapproprié pourrait être accordé au SIGPAA avec le risque d'un traitement non autorisé d'opérations.

Recommandation nº 5

Le directeur exécutif, Excellence sportive, devrait :

Mettre en œuvre une exigence selon laquelle aucun utilisateur ne peut à la fois approuver les demandes d'accès au SIGPAA et autoriser l'accès à l'application. En ce qui concerne

l'utilisateur qui peut actuellement exercer ces deux fonctions, il faudrait réattribuer la capacité d'autoriser l'accès à un autre membre de l'équipe afin d'éliminer la source de conflit.

5.2.3 Politique et procédures de gestion des modifications

Il n'y a pas de politique ni de procédures documentées en place relatives à la gestion des modifications pour guider toutes les étapes du traitement des modifications à l'application du SIGPAA.

Critères de contrôle

Il existe une politique de gestion des modifications et des procédures connexes, qui ont été approuvées par un niveau approprié de gestion, et qui sont communiquées au personnel concerné.

Observations

Même si le nombre de modifications de programme apportées au SIGPAA est petit, il n'y a pas de politiques ni de procédures documentées en place relatives à la gestion des modifications pour guider toutes les étapes du traitement des modifications à l'application. Les modifications apportées à l'application sont programmées par un consultant externe. Toutefois, les procédures pour donner des instructions au consultant et les exigences relatives aux tests et aux approbations de l'équipe du SIGPAA reposent sur les connaissances et l'expérience d'un personnel de longue date. Les pratiques exemplaires au sein de l'industrie indiquent qu'un tel document devrait adresser, à tout le moins, les principales étapes du processus de gestion des modifications ainsi que les points de contrôle et les approbations nécessaires, y compris les directives relatives à ce qui suit :

- les exigences relatives à la documentation des demandes de modifications;
- les demandes de modifications sont autorisées par un niveau de gestion approprié;
- les modifications sont entièrement testées, validées et approuvées avant d'être mises en production;
- des restrictions s'appliquent sur l'accès à la migration des modifications à l'environnement de production.

Évaluation des risques

Même si le nombre de modifications de programme apportées au SIGPAA a été faible, des lacunes dans la gestion des modifications pourraient avoir une incidence considérable sur l'intégrité de l'application. En outre, comme il s'agit d'une application ministérielle qui donne lieu à des opérations financières, le manque d'officialisation des procédures crée un risque pour le Ministère dans l'éventualité d'un roulement du personnel.

Recommandation nº 6

Le directeur exécutif, Excellence sportive, devrait :

Exiger qu'une politique et des procédures d'envergure appropriée de gestion des modifications soient documentées, approuvées et mises en œuvre pour guider l'application uniforme des procédures de gestion des modifications apportées à l'application.

5.2.4 Gestion des problèmes

Il n'existe aucun processus défini pour le suivi et la gestion des problèmes et des incidents liés au SIGPAA.

Critères de contrôle

Un système de gestion des problèmes a été défini et mis en œuvre afin que les événements opérationnels qui ne sont pas pratique courante (incidents, problèmes et erreurs) soient enregistrés, analysés et résolus en temps opportun.

Observations

Dans le cadre de l'audit, l'équipe avait prévu de tester si les problèmes ou incidents liés au SIGPAA étaient analysés et résolus en temps opportun, mais n'a pu obtenir une liste de tels incidents s'étant produits au cours de l'exercice financier. Bien que l'équipe d'audit ait été informée de l'occurrence de quelques problèmes et incidents liés au SIGPAA, il n'y a pas de système de tickets ni d'autre processus en place pour le suivi des incidents liés au SIGPAA et leur résolution finale. Idéalement, les problèmes et les incidents devraient faire l'objet d'un suivi dans un système de tickets; cependant, en raison du signalement d'un faible nombre d'incidents liés au SIGPAA, cela pourrait être réalisé en faisant le suivi par le biais d'Excel ou d'un autre moyen qui se trouve à un emplacement accessible, au besoin, à tous les membres de l'équipe du SIGPAA.

Évaluation des risques

Le défaut de faire le suivi des incidents liés à l'application peut entraîner l'une ou l'autre des conséquences suivantes :

- des incidents non résolus qui continuent de causer des problèmes de système;
- l'absence d'un registre des incidents antérieurs et de leur résolution fournissant de la documentation sur la résolution des incidents dans l'éventualité d'une réoccurrence de ceux-ci;
- le manque de connaissances dans l'éventualité d'un roulement du personnel.

Recommandation nº 7

Le directeur exécutif, Excellence sportive, devrait :

Mettre en œuvre un processus par lequel les problèmes et les incidents d'application liés au SIGPAA sont suivis et analysés, et dont la résolution est consignée dans un registre. Idéalement, les problèmes et les incidents feraient l'objet d'un suivi dans un système de tickets; cependant, en raison du signalement d'un faible nombre d'incidents liés au SIGPAA, cela pourrait être réalisé en faisant le suivi par le biais d'Excel ou d'un autre moyen qui se trouve à un emplacement accessible, au besoin, à tous les membres de l'équipe du SIGPAA.

Annexe A – Critères d'audit

Les conclusions énoncées pour chacun des critères d'audit utilisés dans l'audit ont été développées selon les définitions suivantes.

Catégorisation numérique	Conclusion relative aux critères d'audit	Définition de la conclusion
1	Bien contrôlé	• Bien géré, aucune faiblesse importante constatée; • efficace.
2	Contrôlé	• Bien géré, mais certaines améliorations sont nécessaires; • efficace.
3	Problèmes modérés	Certains problèmes modérés nécessitent l'attention de la direction (satisfaire à au moins un des deux critères suivants) : • faiblesses en matière de contrôle, mais l'exposition au risque est limitée, car la probabilité d'occurrence du risque n'est pas élevée; • faiblesses en matière de contrôle, mais l'exposition au risque est limitée, car l'incidence du risque n'est pas élevée.
4	Améliorations importantes requises	Il est nécessaire d'apporter des améliorations importantes (satisfaire à au moins un des trois critères suivants) : • des redressements financiers s'imposent à l'égard de certains postes ou domaines ou pour le Ministère; • des lacunes en matière de contrôle entraînent une exposition grave au risque; • des lacunes importantes dans la structure decontrôle globale. Nota : Chaque critère d'audit qui est classé **« 4 »** doit immédiatement être communiqué au DPV et au directeur général concerné ou à un niveau plus élevé pour la prise de mesures correctives.

Voici les critères d'audit employés et un résumé des données en fonction desquelles l'équipe d'audit a tiré ses conclusions.

<table>
<tr><td colspan="5">Sous-objectif d'audit nº 1 : Accès aux programmes et aux données : Les contrôles fournissent une assurance raisonnable que les systèmes et les sous-systèmes de rapports financiers sont adéquatement sécurisés de façon à protéger les renseignements qu'ils contiennent contre leur utilisation non autorisée, leur communication et leur modification, ou la perte de données.</td></tr>
<tr><th>Nos des critères</th><th>Critères d'audit</th><th colspan="2">Conclusion</th><th>Preuves/observations clés</th></tr>
<tr><td></td><td></td><td>SAP</td><td>SIGPAA</td><td></td></tr>
<tr><td>1.1</td><td>Une politique sur la sécurité de l'information et des normes connexes existent, elles ont été approuvées par un niveau de gestion approprié, et elles sont communiquées au personnel concerné.</td><td colspan="2">2</td><td>• Une politique, une directive, un cadre et des normes connexes de sécurité des TI sont en place, et elles peuvent être consultées par les utilisateurs dans l'intranet.
• Tous ces éléments ont été examinés la dernière fois en 2010. À l'article 1.3 de la Politique sur la sécurité des TI, il est énoncé ce qui suit : « Cette politique sur la sécurité des TI fera l'objet d'un examen au moins tous les trois ans après cela et elle sera actualisée s'il y a lieu. » Compte tenu de ce qui précède, ces documents sont en retard pour un examen et toute mise à jour nécessaire.</td></tr>
<tr><td>1.2</td><td>Il existe des procédures, qui sont suivies, pour authentifier tous les utilisateurs du système afin d'appuyer la validité des opérations.</td><td>1</td><td>2</td><td>• Toutes les applications nécessitent des identificateurs et des profils d'utilisateur uniques pour gérer l'accès.
• L'accès des utilisateurs privilégiés est restreint aux administrateurs qui en ont besoin.
• L'utilisation de mots de passe complexes est appliquée pour le SAP. Quant au SIGPAA, celui-ci n'impose pas de modifier les mots de passe.
• On peut visualiser les pistes d'audit pour assurer le suivi des opérations.</td></tr>
</table>

Nos des critères	Critères d'audit	Conclusion		Preuves/observations clés
		SAP	SIGPAA	
1.3	Il existe des procédures, qui sont suivies, pour faire en sorte que les mesures nécessaires soient prises rapidement en ce qui concerne les demandes, l'établissement, la délivrance, la suspension et la fermeture des comptes d'utilisateur.	3	SIGPAA = 1 SRP = 1	• Des procédures ont été établies pour ajouter des accès de l'utilisateur et les modifier, ce qui nécessite l'approbation du gestionnaire. • En ce qui concerne le SAP, même si des procédures sont en place pour retirer l'accès de l'utilisateur, il a été constaté qu'il ne fonctionne pas efficacement pour retirer l'accès en temps opportun. • Quant au SIGPAA et au SRP, de petits groupes d'utilisateurs permettent une gestion plus étroite des modifications des utilisateurs.
1.4	Il existe un processus de contrôle, qui est suivi, pour examiner périodiquement les droits d'accès et les confirmer, y compris la désactivation des comptes d'utilisateur inactifs.	2	SIGPAA = 1 SRP = 2	• En ce qui concerne le SAP, on effectue une revalidation de l'accès de l'utilisateur sur une base semestrielle pour les utilisateurs dans les régions, mais pas pour les utilisateurs à l'administration centrale, lesquels représentent le groupe le plus important d'utilisateurs. Des contrôles compensatoires partiels sont indiqués ci-dessous : – Sur une base trimestrielle, tous les comptes inactifs sont signalés et examinés, et l'accès est retiré au besoin. – Sur une base semestrielle, une analyse de la séparation des tâches est effectuée pour les principales opérations financières, et elle est examinée par Opérations comptables, Systèmes et AAC, mais il a été constaté que cela n'est pas effectué en temps opportun. • Pour ce qui est du SIGPAA, compte tenu du fait qu'il n'y a que neuf comptes d'utilisateur pour l'application, l'accès est revu chaque fois qu'une modification d'accès est traitée.

				• Quant au SRP, une revalidation de l'accès de l'utilisateur n'est pas effectuée régulièrement. Une revalidation, qui a été effectuée à notre demande, a révélé que l'accès aurait dû être retiré à trois utilisateurs.
1.5	Il existe des contrôles relatifs à la séparation appropriée des tâches en ce qui concerne les demandes et les autorisations d'accès aux systèmes et aux données, et ces contrôles sont mis en application.	1	SIGPAA = 2 SRP = 1	• En ce qui concerne le SAP, les gestionnaires utilisateurs doivent demander l'accès, alors que seuls les membres de l'équipe des systèmes du SAP peuvent autoriser l'accès. • Pour ce qui est du SIGPAA, une analyse de la séparation des tâches a permis de constater que le gestionnaire, qui approuve tous les accès, a également accès à la base de données administrative. Il pouvait donc configurer les paramètres d'accès, bien que l'équipe d'audit ait été informée que ce compte n'est jamais utilisé. • Quant au SRP, PCH ne peut demander que des modifications d'accès. La capacité de traiter les modifications d'accès au SRP est réservée à TPSGC.

Sous-objectif d'audit n° 2 : **Gestion des modifications aux applications :** Les contrôles fournissent une assurance raisonnable que les modifications apportées aux applications sont autorisées, testées, documentées et approuvées avant d'être mises en production.				
N°s des critères	**Critères d'audit**	**Conclusion**		**Preuves/observations clés**
		SAP	**SIGPAA**	
2.1	Il existe une politique de gestion des modifications et des procédures connexes, qui ont été approuvées par un niveau approprié de gestion, et qui sont communiquées au personnel	3	3	• En ce qui concerne le SAP, même si l'équipe des systèmes du SAP a pu décrire les procédures suivies pour gérer les modifications, et que nous n'avons relevé aucune exception dans le cadre de nos tests des contrôles, conformément aux articles 2.2 à 2.6, la politique et les procédures de gestion des modifications n'ont pas été documentées. • Pour ce qui est du SIGPAA, il y a très peu de modifications chaque année – une en 2014 – et les modifications sont programmées par un consultant externe. Toutefois, les procédures de gestion des

	concerné.			modifications n'ont pas été documentées, et elles reposent en bonne partie sur deux employés à long terme pour la gestion de tous les aspects des modifications de programme.
2.2	Les demandes de modifications de programme, les modifications de configuration de système et la maintenance (y compris les modifications de logiciels de système) sont normalisées et documentées, et elles sont assujetties aux procédures de gestion des modifications.	1	1	• En ce qui concerne le SAP, une sélection de modifications a été testée, et aucune exception n'a été relevée. • Pour ce qui est du SIGPAA, la seule modification effectuée en 2014 a été testée, et aucune exception n'a été relevée.
2.3	Les modifications de système et d'application assurant un contrôle en matière de rapports financiers sont autorisées par un niveau approprié de gestion.	1	1	• En ce qui concerne le SAP, une sélection de modifications a été testée, et aucune exception n'a été relevée. • Pour ce qui est du SIGPAA, la seule modification effectuée en 2014 a été testée, et aucune exception n'a été relevée.
2.4	Les modifications d'application et de système sont testées, validées et approuvées avant d'être mises en production.	1	1	• En ce qui concerne le SAP, une sélection de modifications a été testée, et aucune exception n'a été relevée. • Pour ce qui est du SIGPAA, la seule modification effectuée en 2014 a été testée, et aucune exception n'a été relevée.

2.5	Des contrôles sont en place pour restreindre l'accès à la migration des modifications à l'environnement de production.	1	1	• En ce qui concerne le SAP, nous avons obtenu des listes d'utilisateurs du système ayant accès au transfert des modifications à la production, et nous avons pu confirmer que les restrictions à l'accès étaient bien appliquées. • Pour ce qui est du SIGPAA, l'accès à la migration des modifications à l'environnement de production est restreint à deux membres de l'équipe de la base de données.
2.6	Les modifications d'urgence aux applications et à la configuration sont documentées et assujetties aux procédures officielles de gestion des modifications.	1	1	• En ce qui concerne le SAP et le SIGPAA, les modifications d'urgence sont rares, car ni l'une ni l'autre des applications n'est disponible 24 heures par jour, 7 jours par semaine. • Pour ce qui est du SAP, un examen du registre des modifications et une enquête menée par l'équipe des systèmes du SAP n'a indiqué aucune modification d'urgence en 2014. • Quant au SIGPAA, la seule modification effectuée au cours de l'année n'était pas une modification d'urgence.

Sous-objectif d'audit n° 3 : **Opérations informatiques :** Les contrôles fournissent une assurance raisonnable que les fonctions de soutien des TI sont effectuées régulièrement et de façon ordonnée.				
N^{os} des critères	**Critères d'audit**	**Conclusion**		**Preuves/observations clés**
		SAP	**SIGPAA**	
3.1	Des procédures normalisées de gestion et de surveillance des travaux ont été définies et mises en œuvre.	1	1	• Pour ce qui est du SAP, les rapports du système d'accès pour maintenir la gestion des travaux et les tâches de production par lot ont été examinés, et on a pu confirmer que l'accès était adéquatement restreint à l'équipe de base/sécurité. • Pour ce qui est du SAP, la surveillance des travaux est effectuée sur une base quotidienne au moyen de l'écran de SM37. L'équipe d'audit a inspecté la preuve de suivi d'une tâche non réussie,

				ainsi qu'une liste cumulative de toutes les tâches non réussies et non éliminées, et nous avons pu déterminer que les tâches non réussies sont en train d'être éliminées. • En ce qui concerne le SIGPAA, il n'y a pas de gestion des travaux distincte, et il n'y a qu'une seule tâche principale, qui est le cycle de paiement. Celui-ci est soumis à une surveillance manuelle pour s'assurer de la production et de l'exactitude des rapports de paiement, lesquels font l'objet d'un rapprochement manuel avec le montant affiché sur le SAP.
3.2	Un système de gestion des problèmes a été défini et mis en œuvre afin que les événements opérationnels qui ne sont pas pratique courante (incidents, problèmes et erreurs) soient enregistrés, analysés et résolus en temps opportun.	1	2	• En ce qui concerne le SAP, les problèmes et les incidents sont suivis par l'entremise du Bureau d'aide de Remedy. Une sélection d'incidents du SAP a été testée, et on a pu constater que tous les incidents ont été analysés et résolus en temps opportun. • Quant au SIGPAA, bien que l'équipe d'audit ait été informée qu'il y a très peu de problèmes et d'incidents, ceux-ci ne font pas l'objet d'un suivi distinct. Par conséquent, nous n'avons pas été en mesure de confirmer cette information et de recommander que le suivi et la documentation de la résolution soient mis en œuvre.
3.3	La direction a mis en œuvre une stratégie de sauvegarde cyclique des données et des programmes, y compris les périodes de conservation et	1 (selon les réponses fournies par AAC)	1	• En ce qui concerne le SAP, les copies de sauvegarde sont gérées par AAC. Selon les réponses fournies par AAC, elles sont exécutées quotidiennement en ligne et hebdomadairement hors ligne les fins de semaine, avec un délai de conservation de quatre semaines. Elles sont stockées hors site la semaine (SPC en assure la gestion). • Pour ce qui est du SIGPAA, les

	le stockage.			copies de sauvegarde sont gérées par la Direction générale du dirigeant principal de l'information (DGDPI).
3.4	Les registres de sauvegarde sont surveillés pour assurer la réussite des opérations.	1 (selon les réponses fournies par AAC)	1	• Selon les réponses fournies par AAC, les registres de sauvegarde du SAP sont surveillés quotidiennement par AAC au moyen de HPDataprotector et d'alertes automatiques. Selon les réponses fournies par AAC, les copies de sauvegarde non réussies sont surveillées quotidiennement conformément aux procédures documentées. • En ce qui concerne le SIGPAA, les registres de sauvegarde sont surveillés quotidiennement par la DGDPI. Les copies de sauvegarde non réussies sont surveillées quotidiennement et généralement simplement récupérées dans le cadre des activités de sauvegarde du jour suivant.
3.5	Il existe des procédures, qui son suivies, pour tester périodiquement l'efficacité du processus de restauration et la qualité des supports de sauvegarde.	1 (selon les réponses fournies par AAC)	1	• Selon les réponses fournies par AAC, des mises à jour périodiques du SAP sont effectuées chaque fois qu'il y a une demande de client, la dernière mise à jour ayant été réalisée en janvier 2015. Il existe également une procédure de mise à jour documentée. • En ce qui concerne le SIGPAA, la restauration des copies de sauvegarde est testée une fois l'an, ou plus souvent, lorsque les développeurs le demandent.

Annexe B – Plan d'action de la direction

Audit de la Politique sur le contrôle interne – Audit des contrôles généraux des technologies de l'information (CGTI)

5.1 SAP			
Recommandation	**Mesures**	**Responsable**	**Date cible**
1. Le dirigeant principal des finances devrait examiner et réviser le processus actuel par lequel l'équipe de sécurité du SAP est avisée des personnes ayant cessé d'exercer leur emploi ou ayant autrement quitté le Ministère, afin que l'accès de l'utilisateur au SAP puisse être retiré en temps opportun.	*En accord* Un processus sera mis en place visant à assurer l'accès de l'utilisateur est retiré en temps opportun lorsque les employés qui ont accès à SAP quittent le Ministère. L'inactivation de l'accès au système financier est un contrôle secondaire puisqu'un employé qui a quitté le Ministère aurait besoin d'un accès à la bâtisse, d'une connexion au réseau active et d'un matériel afin d'accéder au système SAP. Ainsi, ce processus considéré à faible risque, a déjà été fait comme un travail périodique au lieu d'une étape de contrôle.	*Gestionnaire, Système financier; Direction générale de la gestion financière*	*Juin 2015*
Recommandation	**Mesures**	**Responsable**	**Date cible**
2. a) Le dirigeant principal des finances devrait mettre en œuvre un processus de revalidation d'accès périodique des utilisateurs du SAP à l'administration centrale, et des rôles assignés à chacun, qui se déroulerait au moins une fois l'an et qui serait documenté officiellement. Toutes les	*En accord* Un procédé pour une revalidation d'accès périodique des utilisateurs du SAP à l'administration centrale sera mis en place.	*Gestionnaire, Système financier; Direction générale de la gestion financière*	*Décembre 2015*

modifications d'accès des utilisateurs nécessaires à la suite de la revalidation devraient être traitées rapidement.			
Recommandation	**Mesures**	**Responsable**	**Date cible**
2. b) Le dirigeant principal des finances devrait établir un calendrier pour la réalisation des examens de la séparation des tâches, y compris le traitement immédiat des modifications d'accès des utilisateurs nécessaires afin d'éliminer les conflits liés à la séparation des tâches.	*En accord* Il ya suffisamment de personnes impliquées dans le processus de paiement pour éviter même les moindres chevauchements d'accès qui pourrait être interprétéré comme conflit lié à la séparation des tâches. Un calendrier fixe pour des examens futurs sera mis en place.	*Gestionnaire, Système financier; Direction générale de la gestion financière*	*Juin 2015*
Recommandation	**Mesures**	**Responsable**	**Date cible**
3. Le dirigeant principal des finances devrait exiger qu'une directive de gestion des modifications soit documentée, approuvée et mise en œuvre pour guider l'application uniforme des procédures de gestion des modifications apportées à l'application.	*En accord* Une directive officielle de gestion du changement sera mise en place. Ceci est considéré à faible risque, étant donné que même le processus non-entièrement documenté a toujour assuré les essaies et tests approprié de système avec toutes les modifications apportées à SAP.	*Gestionnaire, Système financier; Direction générale de la gestion financière*	*Juin 2015*

5.2 SIGPAA			
Recommandation	**Mesures**	**Responsable**	**Date cible**
4. Le directeur exécutif, Excellence sportive, devrait mettre en œuvre une procédure exigeant à tous les utilisateurs ayant accès au SIGPAA de modifier régulièrement leurs mots de passe.	*En accord* L'Unité Programme d'aide aux athlètes (PAA) demandera que la Direction du dirigeant principal de l'information (DDPI) change, chaque six mois, le mot de passe généré aléatoirement pour chaque utilisateur et informer l'utilisateur.	*Gestionnaire, PAA*	*Avril 2015*
Recommandation	**Mesures**	**Responsable**	**Date cible**
5. Le directeur exécutif, Excellence sportive, devrait mettre en œuvre une exigence selon laquelle aucun utilisateur ne peut à la fois approuver les demandes d'accès au SIGPAA et autoriser l'accès à l'application. En ce qui concerne l'utilisateur qui peut actuellement exercer ces deux fonctions, il faudrait réattribuer la capacité d'autoriser l'accès à un autre membre de l'équipe afin d'éliminer la source de conflit.	*En accord* L'Unité PAA demandera au DDPI d'annuler la capacité du gestionnaire du PAA de faire les changements d'accès aux utilisateurs de SIGPAA. Une sauvegarde est nécessaire pour l'analyste en politiques et programmes, qui a également la possibilité d'apporter des modifications d'accès aux utilisateurs de SIGPAA.	*Analyste en politiques et programmes, PAA*	*Avril 2015*

Recommandation	Mesures	Responsable	Date cible
6. Le directeur exécutif, Excellence sportive, devrait exiger qu'une politique et des procédures d'envergure appropriée de gestion des modifications soient documentées, approuvées et mises en œuvre pour guider l'application uniforme des procédures de gestion des modifications apportées à l'application.	*En accord* Une politique et des procédures d'envergure appropriée de gestion des modifications seront développées pour l'utilisation par l'Unité PAA dans la gestion des modifications à la SIGPAA.	*Gestionnaire, PAA*	*Septembre 2015*
Recommandation	**Mesures**	**Responsable**	**Date cible**
7. Le directeur exécutif, Excellence sportive, devrait mettre en œuvre un processus par lequel les problèmes et les incidents d'application liés au SIGPAA sont suivis et analysés, et dont la résolution est consignée dans un registre. Idéalement, les problèmes et les incidents devraient faire l'objet d'un suivi dans un système de tickets; cependant, en raison du signalement d'un faible nombre d'incidents liés au SIGPAA, cela pourrait être réalisé en faisant le suivi par le biais d'Excel ou d'un autre moyen qui se trouve à un emplacement accessible, au besoin, à tous les membres de l'équipe du SIGPAA.	*En accord* L'Unité PAA va développer un système pour documenter et suivre les problèmes / incidents liés au SIGPAA, et ce, depuis l'identification initiale du problème jusqu'à sa résolution.	*Gestionnaire, PAA*	*Septembre 2015*