Emploi et Développement social Canada
Employment and Social Development Canada
Canada

Non classifié

Audit de suivi sur l'examen des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Mars 2019

Direction générale des services de vérification interne

Audit de suivi sur l'examen des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Vous pouvez télécharger cette publication en ligne sur le site canada.ca/publicentre-EDSC .
Ce document est aussi offert sur demande en médias substituts (gros caractères, MP3, braille, audio sur DC, fichiers de texte sur DC, DAISY, ou accessible PDF) auprès du 1 800 O-Canada (1-800-622-6232).
Si vous utilisez un téléscripteur (ATS), composez le 1-800-926-9105.

PDF
Nº de cat. : Em20-128/2019F-PDF
ISBN : 978-0-660-30712-1

EDSC
Nº de cat. : SP-1207-05-19F

TABLE DES MATIÈRES

1. RENSEIGNEMENTS GÉNÉRAUX

1.1 Contexte

À la suite des résultats de l'audit de la Mise en œuvre de la délégation des pouvoirs de signature dans SAP en mars 2015 et du suivi des recommandations effectué par la Direction générale des services de vérification interne en avril 2017, un audit de suivi de la Conformité à l'article 34 dans SAP a été inclus dans le Plan d'audit ministériel axé sur les risques de 2018-2020.

1.2 Objectif de l'audit

L'objectif de l'audit de suivi consistait à vérifier si les mesures prévues dans le Plan d'action de la direction (PAD) découlant de l'audit réalisé en 2015 portant sur l'examen des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP ont été entièrement exécutées.

1.3 Portée

La portée du présent mandat englobe un examen des activités effectuées pour la mise en œuvre du PAD.

1.4 Méthodologie

L'audit a été effectué en utilisant un certain nombre de méthodes, notamment les suivantes :

- Observation et analyse des processus;
- Examen et analyse de la documentation;
- Entrevues auprès des gestionnaires et du personnel de la Direction générale du Dirigeant principal des finances (DGDPF), y compris le Centre d'expertise SAP, les Comptes créditeurs nationaux et la Direction intégrée de la responsabilité et de la comptabilité ministérielle (DIRCM);
- Examen et analyse pendant la période visée, soit du 1er avril 2017 au 30 juin 2018 :
    - Examen d'un échantillon de directions générales qui faisaient partie de l'examen annuel des droits d'accès aux fonctions de nature délicate exécuté par l'équipe du Centre d'expertise SAP;
    - Examen d'un échantillon d'accès aux fonctions clés de SAP, exécuté par l'équipe de sécurité SAP.

2. CONSTATATIONS DE L'AUDIT

2.1 Bien que la DGDPF ait pris des mesures de contrôle et accompli certaines activités pour détecter les droits d'accès de nature délicate inappropriés, les transactions qui y sont liées ne sont pas surveillées

Recommandation 1.1 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait examiner les exigences opérationnelles entourant les droits d'accès de nature délicate et mettre en œuvre des mesures de contrôle pour veiller à ce que ces droits soient octroyés aux utilisateurs qui en ont absolument besoin pour exécuter leurs tâches. Une surveillance devrait être exercée pour détecter l'usage inadéquat des droits d'accès de nature délicate.

Réponse de la direction

La DGDPF déterminera, consignera et mettra en œuvre des mesures d'atténuation et des activités de surveillance pour détecter l'utilisation inappropriée des droits d'accès de nature délicate (mars 2016).

Examen annuel des postes nécessitant des droits d'accès de nature délicate

L'équipe du Centre d'expertise SAP, au sein de la DGDPF, a consigné et réalisé un examen annuel destiné à confirmer le caractère approprié des droits d'accès de nature délicate. Le plus récent examen a eu lieu en mars 2018.

L'équipe d'audit a conçu des tests et obtenu un échantillon représentatif de cinq directions générales qui faisaient partie de l'examen annuel pour la période visée, afin de déterminer si l'examen des droits d'accès de nature délicate a été exécuté conformément aux directives établies. L'équipe d'audit a notamment vérifié si on avait approuvé et confirmé les droits d'accès de nature délicate au Centre d'expertise SAP et si l'on avait pris les mesures correctives afin de remédier aux exceptions accordées, le cas échéant. L'équipe d'audit a conclu que l'examen annuel des postes nécessitant des droits d'accès de nature délicate a été exécuté de manière appropriée et que les mesures correctives avaient été prises lorsque cela était nécessaire.

Nonobstant le fait que l'examen soit exécuté annuellement, les transactions faisant appel aux droits d'accès de nature délicate ne sont pas surveillées. Il existe donc un risque que des transactions anormales ou douteuses ne soient pas repérées. La direction pourrait souhaiter envisager la surveillance des droits d'accès de nature délicate.

Examen des droits d'accès aux fonctions clés dans SAP

L'équipe de sécurité SAP est chargée d'examiner l'accès aux fonctions clés de SAP; cela comprend la vérification de l'accès accordé aux superutilisateurs et de leurs activités, la gestion des utilisateurs et l'attribution des fonctions, la répartition entre les groupes, le contrôle des mots de passe et les paramètres de sécurité. Ces vérifications se font à

intervalle hebdomadaire ou mensuel, comme il est indiqué dans les directives de sécurité et de surveillance du Programme de renouvellement des services habilitants.

L'équipe d'audit a conçu des tests et obtenu un échantillon représentatif des vérifications faites par l'équipe de sécurité SAP au cours de la période visée. L'échantillon qui a été analysé avait pour objet de vérifier si les examens ont été réalisés conformément aux directives établies.

L'équipe d'audit a constaté que les activités de surveillance liées aux examens menés par l'équipe de sécurité SAP ont été exécutées comme prévu.

Sur cette base, les actions prises pour répondre à la recommandation 1.1 ont été partiellement mises en œuvre.

2.2 La DGDPF a formellement documenté la limite qui est en place et a mis en œuvre un contrôle automatisé pour repérer les transactions atypiques

Recommandation 1.2 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait officialiser les activités de surveillance portant sur les transactions relatives aux cartes d'achat afin de démontrer qu'elles cadrent avec la stratégie de gestion des risques visant la vérification des comptes. Le DPF devrait également envisager d'instituer des activités de surveillance supplémentaires pour repérer et vérifier les transactions traitées de manière atypique.

Réponse de la direction

La DGDPF documentera formellement la limite qui est en place et les mesures d'atténuation figurant déjà dans la stratégie de gestion des risques visant la vérification des comptes (septembre 2015).

La DGDPF s'est dotée d'un contrôle automatisé pour prévenir la plupart des erreurs de ce type. Bien que le nombre de ces erreurs soit négligeable, la DGDPF consignera et appliquera également des mesures de surveillance (septembre 2015).

Harmonisation avec la stratégie de gestion des risques

La DGDPF a formellement consigné la limite existante que l'audit précédent avait mis en évidence (c'est-à-dire qu'il est impossible de bloquer les paiements reliés aux achats faits au moyen d'une carte d'achat) dans les documents intitulés « Méthodologie d'échantillonnage statistique » et « Guide de l'utilisateur – Échantillonnage statistique ». Ces deux documents ont récemment été fusionnés et remplacés par le « Cadre de contrôle en vertu de l'article 33 - Plan d'assurance de la qualité des comptes créditeurs » le 31 octobre 2018.

Ajout d'activités de surveillance supplémentaires

Des entrevues avec l'équipe des Comptes créditeurs nationaux et une étude de la documentation ont permis de confirmer qu'il existe un processus de blocage dans myEMS

(SAP) et que ce processus classe les transactions en fonction du niveau de risque qu'elles présentent (élevé ou moyen-faible).

Les transactions à risque élevé sont repérées en fonction des profils de risque établis afin d'être examinées. Les paiements à risques faibles ou moyens, comme les acquisitions faites grâce à une carte d'achat, sont assujettis à une vérification postérieure au paiement après l'exécution de l'article 33 et l'émission du paiement.

L'équipe responsable de la coordination nationale des cartes d'achat s'est dotée d'un mécanisme de surveillance des cartes. En 2016, elle a entrepris cette surveillance en examinant mensuellement un échantillon de transactions, conformément au plan établi à cette fin. L'équipe a également réalisé un examen semestriel des cartes d'achat inactives. Le dernier examen a été mené en avril 2018. Sur cette base, les actions prises pour répondre à la recommandation 1.2 ont été entièrement mises en œuvre.

2.3 La DGDPF a mis en place des activités de surveillance et des contrôles financiers à l'égard des processus manuels

Recommandation 1.3 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait envisager d'instituer des vérifications supplémentaires pour les transactions effectuées au moyen de ces processus ou encore, dans la mesure du possible, de les automatiser.

Réponse de la direction

La DGDPF a déjà adopté des activités de surveillance et des contrôles financiers à l'égard des processus manuels et considère que ces mesures sont suffisantes pour atténuer les risques éventuels associés à ces processus. Aucune autre intervention n'est requise.

La DGDPF a déjà indiqué que des activités de surveillance et des contrôles financiers avaient été mis en place à l'égard des processus manuels et qu'elle considère que ces mesures sont suffisantes pour en atténuer les risques éventuels. La direction a conclu qu'aucune autre intervention n'est requise. Par conséquent, aucun travail de suivi n'a été réalisé dans le cadre de cet audit.

2.4 La DGDPF a corrigé le bogue dans le système qui permettait qu'aucune date d'échéance pour la formation ne soit saisie dans SAP

Recommandation 1.4 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait rechercher la cause de l'absence d'une date d'échéance et examiner les mesures de contrôle s'appliquant aux dates non inscrites dans le tableau des pouvoirs de signature des documents financiers (PSDF); il devrait également s'assurer que les dossiers relatifs à ces pouvoirs sont complets. À défaut, le système SAP devrait interpréter l'absence de cette date comme étant synonyme que le PSDF n'est pas valable.

Réponse de la direction

Le bogue du système qui permettait qu'aucune date d'échéance ne soit saisie pour la formation a été corrigé. Il n'est plus possible de laisser ce champ vierge. La DGDPF a également confirmé que tous les dossiers où aucune date n'apparaît ont été examinés et qu'il n'en existe plus aucun qui soit encore actif. Aucune autre intervention n'est requise.

Pour se conformer à cette recommandation, la DGDPF a apporté des modifications au système SAP pour s'assurer que :

- les PSDF ne soient pas autorisés dans le système SAP en l'absence d'une date d'échéance (sauf pour certains postes comme les ministres et les sous-ministres, puisqu'on ne peut pas la déterminer à l'avance à leur égard);
- la date d'échéance pour la formation soit toujours mentionnée dans SAP;
- « 9999 » ne puisse jamais être saisie comme date de fin de la formation dans SAP.

Après avoir étudié les données à l'appui (document ayant trait à la conception du système et sa mise en service, l'équipe d'audit a confirmé que le bogue permettant qu'une date de validité ne soit pas saisie pour la formation a été corrigé et qu'il est désormais impossible de laisser vierge le champ correspondant dans les PSDF.

Sur cette base, les actions prises pour répondre à la recommandation 1.4 ont été entièrement mises en œuvre.

2.5 La mesure de contrôle automatisée visant la séparation des fonctions aux termes de l'article 32 et la passation des marchés a été instaurée dans le processus des comptes créditeurs

Recommandation 2.1 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait établir si cette mesure de contrôle joue un rôle critique dans le processus des comptes créditeurs et s'assurer de la soumettre à une vérification proportionnelle à l'importance des changements apportés à SAP qui pourraient avoir des répercussions sur les contrôles touchant les comptes créditeurs.

Réponse de la direction

La DGDPF continuera de suivre la demande de changement et la mettra à l'épreuve conformément aux protocoles d'acceptation par l'utilisateur établis, avant la fixation d'une date de diffusion (mars 2016).

Se fondant sur l'examen des éléments probants à l'appui transmis par le Centre d'expertise SAP, l'équipe d'audit a confirmé qu'un contrôle automatisé visant la séparation des fonctions aux termes de l'article 32 et la passation des marchés fait maintenant partie des mesures de contrôle critiques du processus des comptes créditeurs. Ce contrôle a été choisi, conçu, mis à l'épreuve avec succès et déployé par le Centre d'expertise SAP dans ce processus en avril 2015.

Sur cette base, les actions prises pour répondre à la recommandation 2.1 ont été entièrement mises en œuvre.

2.6 L'échantillonnage des transactions à risque faible est effectué à partir de l'ensemble des transactions

Recommandation 2.2 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait s'assurer que l'échantillonnage des transactions à risque faible se fait à partir de l'ensemble des transactions en instaurant des mesures de contrôle automatisées ou des contrôles manuels compensatoires, dont il vérifiera périodiquement l'efficacité opérationnelle.

Réponse de la direction

La DIRCM collaborera avec l'Organisation de soutien aux services internes (OSSI) pour remédier à ce problème (mars 2016).

Des entrevues et un examen de la documentation ont permis de confirmer que le « Cadre de contrôle en vertu de l'article 33 – Plan d'assurance de la qualité des comptes créditeurs » a été mis à jour, de sorte que l'échantillonnage des transactions à risque faible est dorénavant fait à partir de l'ensemble des transactions.

Sur cette base, les actions prises pour répondre à la recommandation 2.2 ont été entièrement mises en œuvre.

2.7 Les mesures d'atténuation et les activités de surveillance destinées à repérer les droits d'accès incompatibles ont été consignées et mises en œuvre

Recommandation 3.1 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait examiner les rôles relatifs à la sécurité et les accès des postes affectés à la vérification des comptes afin de s'assurer qu'aucun droit d'accès incompatible n'est

octroyé. La portée de l'examen devrait englober notamment toute question relative aux droits incompatibles et le risque que la situation actuelle représente.

Lorsque les exigences opérationnelles requièrent des droits d'accès incompatibles, il faut instaurer des contrôles manuels compensatoires pour repérer les utilisateurs qui exercent leurs PSDF à l'égard de leurs propres fournisseurs.

Les mesures de contrôle critiques, en matière de droits d'accès, devraient être mises à l'épreuve périodiquement afin de vérifier qu'elles fonctionnent conformément aux attentes.

Réponse de la direction

La DGDPF déterminera, consignera et mettra en œuvre des mesures d'atténuation et des activités de surveillance pour s'assurer de repérer les droits d'accès incompatibles qui ont été utilisés (mars 2016).

L'équipe d'audit a confirmé que le Centre d'expertise SAP examine annuellement les rapports produits par SAP dans lesquels sont identifiés les utilisateurs qui ont des droits d'accès incompatibles. Le plus récent examen a eu lieu en mai 2018.

Sur cette base, les actions prises pour répondre à la recommandation 3.1 ont été entièrement mises en œuvre.

2.8 La DGDPF a évalué les accès des postes qui effectuent la vérification des comptes et a révoqué les accès non requis selon les exigences opérationnelles

Recommandation 3.2 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait établir des critères clairs pour l'octroi des droits d'accès aux postes qui font la vérification des comptes, en tenant compte des exigences opérationnelles et des compétences, et s'assurer que ces droits sont accordés en conséquence. Ceux-ci devraient être soumis à une révision périodique pour s'assurer qu'ils demeurent appropriés.

Réponse de la direction

La DGDPF évaluera la définition des agents financiers et la consignera aux fins de l'assurance de la qualité. Les droits d'accès seront octroyés en conséquence ou, au besoin, on consignera des mesures d'atténuation adaptées aux exigences opérationnelles (mars 2016).

Les entrevues avec les représentants des Comptes créditeurs nationaux et l'examen de la documentation ont confirmé que la DGDPF a évalué la définition des agents financiers et l'a consignée dans la « Méthodologie d'échantillonnage statistique ». Comme il est indiqué à la section 2.2, la « Méthodologie d'échantillonnage statistique » et le « Guide de l'utilisateur – Échantillonnage statistique » ont récemment été fusionnés, puis remplacés par le « Cadre de contrôle en vertu de l'article 3 - Plan d'assurance de la qualité des comptes créditeurs ».

L'équipe d'audit a confirmé que la DGDPF a examiné les accès accordés aux utilisateurs qui exécutent la vérification des comptes et qu'elle a retiré tous les droits d'accès non requis, en se basant sur les exigences opérationnelles et les compétences.

Sur cette base, les actions prises pour répondre à la recommandation 3.2 ont été entièrement mises en œuvre.

2.9 Les droits d'accès non nécessaires dans SAP ont été supprimés, mais les pistes de vérification n'ont pas été examinées durant la période de mise en œuvre

Recommandation 3.3 de l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Le DPF devrait appliquer des mesures pour s'assurer que les droits d'accès temporaires ne sont pas utilisés de manière inappropriée pendant la période de mise en œuvre et que les droits accordés en trop sont supprimés une fois l'environnement de production stabilisé.

Réponse de la direction

Les droits d'accès seront supprimés après l'exécution des activités critiques de fin d'exercice. Entre-temps, on peut avoir accès aux pistes de vérification aux fins de surveillance (septembre 2015).

Des droits d'accès excessifs ont été accordés aux employés du groupe de l'OSSI SAP (au nombre d'environ 80), comme mesure temporaire, afin de permettre aux équipes techniques de résoudre des problèmes liés à l'environnement de production dans la première année de mise en œuvre du système SAP.

Après s'être informée auprès du Centre d'expertise SAP (qui a pris la relève du groupe de l'OSSI) et avoir examiné la documentation, l'équipe d'audit a confirmé que le problème des droits d'accès excessifs a été réglé et que ceux-ci ont été révoqués dans SAP.

La direction a indiqué que les pistes de vérification étaient accessibles aux fins de surveillance, mais l'équipe de sécurité SAP ne les a pas examinées. Les utilisateurs bénéficiant de droits d'accès excessifs (superutilisateurs) auraient pu créer des utilisateurs ou des fournisseurs inappropriés ou encore traiter des transactions non autorisées. Il existe donc un risque que des transactions inappropriées découlant de droits d'accès excessifs puissent avoir été exécutées dans SAP pendant la période de mise en œuvre (soit entre avril 2015 et le règlement du problème en septembre 2015).

Sur cette base, les actions prises pour répondre à la recommandation 3.3 ont été entièrement mises en œuvre.

3. Conclusion

Toutes les mesures à prendre dans le PAD, relatifs à l'Examen de 2015 des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP, ont été entièrement exécutées, à l'exception de la recommandation 1.1, qui a partiellement été mise en œuvre. La DGDPF examine annuellement les droits d'accès de nature délicate, mais ne surveille pas les transactions qui y font appel. Nous sommes d'avis qu'une surveillance devrait être effectuée pour détecter l'utilisation inappropriée des droits d'accès de nature délicate.

4. Énoncé d'assurance

Selon notre jugement professionnel, les procédures d'audit appliquées et les éléments probants recueillis sont suffisants et appropriés pour étayer l'exactitude des constatations présentées dans ce rapport. Ces dernières sont fondées sur des observations et des analyses des situations qui existaient au moment de l'audit. Les conclusions ne s'appliquent qu'à l'Audit de suivi sur l'examen des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP. Les éléments probants ont été recueillis conformément à la *Politique sur l'audit interne* du Conseil du Trésor et aux *Normes internationales pour la pratique professionnelle de l'audit interne*.

ANNEXE A : GLOSSAIRE

DGDPF	Direction générale du dirigeant principal des finances
DIRCM	Direction intégrée de la responsabilité et de la comptabilité ministérielle
DPF	Dirigeant principal des finances
OSSI	Organisation de soutien aux services internes
PAD	Plan d'action de la direction
PSDF	Pouvoir de signature des documents financiers

Annexe B : Plan d'action de la direction

Examen des contrôles de la délégation des pouvoirs et de la vérification des comptes dans SAP

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
1.1 Contournement des flux de travail Il est possible de contourner les flux de travail automatisés si l'on a recours à certaines fonctions de saisie ou de modification des transactions dans SAP, qui sont de nature délicate. Par exemple, en accédant directement au module FI plutôt qu'en empruntant le flux de travail typique pour approuver une transaction, de nombreux commis aux Comptes créditeurs et agents financiers, dans les centres de traitement régionaux, sont en mesure d'approuver des demandes pour voyager (article 32) ou des notes de frais de déplacement (article 34) au nom du gestionnaire du centre de fonds. De la même manière, un agent des achats peut établir un bon de commande sans l'appui d'une demande à cette fin, ce qui lui permet de contourner les dispositions de l'article 32.	En ayant recours à des transactions de nature délicate, les employés peuvent exercer des pouvoirs qui ne leur ont pas été octroyés ou encore contourner certains pouvoirs.	Le DPF devrait examiner les exigences opérationnelles entourant les droits d'accès de nature délicate et mettre en œuvre des mesures de contrôle pour veiller à ce que ces droits soient octroyés aux utilisateurs qui en ont absolument besoin pour exécuter leurs tâches. Une surveillance devrait être exercée pour détecter l'usage inadéquat des droits d'accès de nature délicate.	La nécessité d'une exception se rapportant aux déplacements et aux bons de commande a été analysée. Cette exception a été jugée à faible risque et indispensable au bon fonctionnement des activités opérationnelles. La DGDPF convient qu'il faut établir des mesures d'atténuation officielles. Mesure : La DGDPF déterminera, consignera et mettra en œuvre des mesures d'atténuation et des activités de surveillance pour détecter l'utilisation inappropriée des droits d'accès de nature délicate. Date d'achèvement : 31 mars 2016

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
1.2 Traitement atypique des transactions La conception de la vérification des comptes ne soutient pas entièrement les catégories de risque définies par le DPF pour les transactions qui comportent des attributs atypiques ou qui ne correspondent pas aux flux de travail normaux. Par exemple, les achats effectués au moyen d'une carte d'achat ne peuvent être bloqués avant le paiement et ne sont donc jamais assujettis à la vérification des comptes avant le paiement. D'autre part, l'équipe d'audit a analysé les données associées aux transactions affichées dans le système SAP tout au long de la période d'audit et a pris note de celles ayant des combinaisons d'attributs (ex. : type de document et grand livre) atypiques qui n'ont pas été bloquées. Ces transactions n'ont pas fait l'objet d'une vérification des comptes même si elles comportaient des attributs correspondant aux catégories de risque définies par le DPF.	Les paiements qui ne sont pas traités selon un flux de travail typique ne sont pas assujettis à la vérification des comptes (ni avant ni après le paiement); ce qui empêche le DPF de compter sur le processus de vérification des comptes pour ces transactions.	a) Le DPF devrait officialiser les activités de surveillance portant sur les transactions relatives aux cartes d'achat afin de démontrer qu'elles cadrent avec la stratégie de gestion des risques visant la vérification des comptes. b) Le DPF devrait également envisager d'instituer des activités de surveillance supplémentaires pour repérer et vérifier les transactions traitées de manière atypique.	a) Les documents liés aux cartes d'achat ne peuvent être soumis au blocage du paiement et à la vérification avant paiement, car les transactions ne sont pas traitées dans myEMS/SAP. Toutefois, les contrôles automatisés existants font en sorte que les transactions par carte d'achat ayant un risque élevé sont soumises à une vérification postérieure complète. Mesure : La DGDPF documentera formellement la limite qui est en place et les mesures d'atténuation figurant déjà dans la stratégie de gestion des risques visant la vérification des comptes. Date d'achèvement : 30 septembre 2015 b) La plupart des transactions atypiques relevées ont été délibérément exclues car il s'agissait de notes de crédit qui ne constituent pas des dépenses. La DGDPF convient qu'un nombre minime de dépenses ont été faites par inadvertance au moyen du mauvais type de document. Mesure : La DGDPF s'est dotée d'un contrôle automatisé pour prévenir la plupart des erreurs de ce type. Bien que le nombre de ces erreurs soit négligeable, la DGDPF consignera et appliquera également des mesures de surveillance. Date d'achèvement : 30 septembre 2015

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
1.3 Processus manuels Bien que de nombreux types de transactions suivent un flux de travail automatisé pour l'obtention des approbations, l'exercice des PSDF, pour les processus suivants, se fait en grande partie manuellement et ces transactions ne sont donc pas assujetties aux processus automatisés : factures qui ne sont pas appuyées par un bon de commande, paiements effectués au moyen d'une carte d'achat et notes de frais pour les déplacements de personnes ne faisant pas partie du personnel du Ministère.	Dans le cadre du présent audit, nous n'avons pas relevé des lacunes plus importantes au niveau des contrôles appliqués aux transactions traitées manuellement qu'à celles assujetties au flux de travail automatisé. Par contre, les processus manuels sont généralement plus susceptibles de comporter des erreurs que les processus plus automatisés.	Le DPF devrait envisager d'instituer des vérifications supplémentaires pour les transactions effectuées au moyen de ces processus ou encore, dans la mesure du possible, de les automatiser.	La DGDPF a déjà adopté des activités de surveillance et des contrôles financiers à l'égard des processus manuels et considère que ces mesures sont suffisantes pour atténuer les risques éventuels associés à ces processus. Mesure : Aucune autre intervention n'est requise. Date d'achèvement : S. O.

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
1.4. Tableaux des PSDF Les pouvoirs délégués aux employés figurent dans la base de données de la délégation des PSDF. Chaque inscription dans cette base est composée du code d'identification de la personne, des pouvoirs précis qui lui ont été délégués, de la date de validité de sa formation et de celle de ses pouvoirs. Pour déterminer qui a le droit d'approuver une transaction, le sous-système du flux de travail des approbations consulte les tableaux des pouvoirs de la base de données des pouvoirs délégués. L'équipe d'audit a noté que ce flux acheminait des transactions vers des personnes à l'égard desquelles aucune date de validité des pouvoirs n'était inscrite.	Les employés qui n'ont pas dans leurs dossiers ni la date d'achèvement de la formation appropriée, ni la date d'échéance des pouvoirs peuvent approuver des transactions, même si cela contrevient aux exigences de la Directive sur l'administration de la formation indispensable ou, de manière générale, à l'instrument de délégation de pouvoir.	Le DPF devrait rechercher la cause de l'absence d'une date d'échéance et examiner les mesures de contrôle s'appliquant aux dates non inscrites dans le tableau des PSDF; il devrait également s'assurer que les dossiers relatifs à ces pouvoirs sont complets. À défaut, le système SAP devrait interpréter l'absence de cette date comme étant synonyme que le PSDF n'est pas valable.	Le bogue du système qui permettait qu'aucune date d'échéance ne soit saisie pour la formation a été corrigé. Il n'est plus possible de laisser ce champ vierge. La DGDPF a également confirmé que tous les dossiers où aucune date n'apparaît ont été examinés et qu'il n'en existe plus aucun qui soit encore actif. Mesure : Aucune autre intervention n'est requise. Date d'achèvement : S. O.

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
2.1. Mesures de contrôle visant la séparation des fonctions aux termes de l'article 32 et la passation des marchés Bien qu'une mesure de contrôle automatisée ait été conçue dans le but d'assurer la séparation des fonctions touchant l'approbation des bons de commande de celles qui ont trait à l'approbation des demandes d'approvisionnement (article 32), elle ne fonctionnait pas de manière efficace au moment de l'audit en raison d'une mise à niveau récente du système SAP. Par conséquent, les employés disposant de droits d'accès et de pouvoirs à l'égard des bons de commande et des demandes d'approvisionnement pouvaient exercer les deux pouvoirs pour la même transaction. L'équipe d'audit a cependant été informée qu'une demande de changement visant le système SAP avait été amorcée pour remédier à cette erreur.	Bien que cela ne soit pas une exigence de la politique, la séparation des pouvoirs en matière d'engagement et de passation des marchés fait partie des meilleures pratiques reconnues. L'équipe d'audit a remarqué que les droits d'accès permettant d'établir et d'approuver les bons de commande étaient réservés au personnel du groupe des approvisionnements, ce qu'elle a jugé approprié car on peut ainsi atténuer les risques liés à la séparation des tâches incompatibles dans un modèle d'achat centralisé.	Le DPF devrait établir si cette mesure de contrôle joue un rôle critique dans le processus des comptes créditeurs et s'assurer de la soumettre à une vérification proportionnelle à l'importance des changements apportés à SAP qui pourraient avoir des répercussions sur les contrôles touchant les comptes créditeurs.	Ce contrôle est important, même si le risque qu'il atténue est jugé faible. Comme il est mentionné, le droit d'accès pour approuver un bon de commande (c'est-à-dire l'exercice du pouvoir de passation des marchés dans un processus automatisé allant de l'approvisionnement au paiement) est exclusif à l'équipe de l'approvisionnement. Au sein de cette équipe se trouvent quelques postes supérieurs auxquels on pourrait aussi accorder le pouvoir d'approuver les demandes d'approvisionnement (ce dont traite l'article 32). Malgré la faiblesse du risque, le contrôle automatisé lorsqu'il fonctionne comme prévu ferait en sorte que les deux pouvoirs ne puissent être exercés par la même personne, pour la même transaction. À cette fin, une demande de changement au système SAP est en cours de traitement. Mesure : La DGDPF continuera de suivre la demande de changement et la mettra à l'épreuve conformément aux protocoles d'acceptation par l'utilisateur établis, avant la fixation d'une date de diffusion. Date d'achèvement : 31 mars 2016

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
2.2. Exhaustivité de l'échantillonnage après paiement Les paramètres d'échantillonnage doivent être saisis manuellement pour chaque compte inclus dans l'échantillon assujetti à la vérification des comptes après paiement. L'équipe d'audit, pendant ses enquêtes, a constaté que l'exhaustivité des comptes n'a pas été validée au moment de l'échantillonnage; elle a observé des incohérences quant à la taille de la population parmi laquelle l'échantillon est choisi.	Toutes les transactions pertinentes qui présentent un risque faible pourraient ne pas être soumises à une vérification appropriée des comptes, ce qui ne concorde pas avec l'approche de vérification fondée sur le risque.	Le DPF devrait s'assurer que l'échantillonnage des transactions à risque faible se fait à partir de l'ensemble des transactions en instaurant des mesures de contrôle automatisées ou des contrôles manuels compensatoires, dont il vérifiera périodiquement l'efficacité opérationnelle.	La DGDPF reconnaît cette incohérence liée à la taille de la population et s'affaire à en cerner la cause. Mesure : La DIRCM collaborera avec l'OSSI pour remédier à ce problème. Date d'achèvement : 31 mars 2016

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
3.1. Séparation des tâches incompatibles L'équipe d'audit a constaté que des droits d'accès incompatibles avaient été octroyés à certains utilisateurs en ayant recours à deux méthodes différentes : - Un seul rôle au sein de la sécurité se voit confier des transactions incompatibles dans SAP. - Des utilisateurs différents se voient confier plusieurs rôles incompatibles sur le plan de la sécurité. Certains pouvoirs financiers peuvent être exercés par des utilisateurs à l'égard de leurs propres fournisseurs. L'équipe d'audit a découvert que les pouvoirs financiers suivants pouvaient être exercés par les utilisateurs à l'égard de leurs propres fournisseurs : - Bien que le flux de travail établi pour les déplacements est conçu pour éviter que les utilisateurs exercent les pouvoirs prévus aux articles 32 et 34 à l'égard de leurs propres fournisseurs, ces pouvoirs peuvent être exercés par les utilisateurs qui bénéficient d'un droit d'accès direct au module FI (voir l'observation 1.1). - Le pouvoir de payer (article 33) ainsi que les activités appuyant la vérification des comptes peuvent	Cette lacune, sur le plan de la séparation des droits d'accès incompatibles et de la capacité des utilisateurs d'exercer des pouvoirs financiers à l'égard de leurs propres dépenses, risque d'inciter à des gestes inappropriés et à la dissimulation des erreurs.	Le DPF devrait examiner les rôles relatifs à la sécurité et les accès des postes affectés à la vérification des comptes afin de s'assurer qu'aucun droit d'accès incompatible n'est octroyé. La portée de l'examen devrait englober notamment toute question relative aux droits incompatibles et le risque que la situation actuelle représente. Lorsque les exigences opérationnelles requièrent des droits d'accès incompatibles, il faut instaurer des contrôles manuels compensatoires pour repérer les utilisateurs qui exercent leurs PSDF à l'égard de leurs propres fournisseurs. Les mesures de contrôle	La nécessité de créer une exception pour les déplacements et les bons de commande a été analysée. Cette exception a été considérée comme représentant un faible risque et jugée indispensable au bon fonctionnement du processus opérationnel. La DGDPF convient qu'il faut établir des mesures d'atténuation officielles. Mesure : La DGDPF déterminera, consignera et mettra en œuvre des mesures d'atténuation et des activités de surveillance pour s'assurer de repérer les droits d'accès incompatibles qui ont été utilisés. Date d'achèvement : 31 mars 2016

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
aussi être exercés par des utilisateurs à l'égard de leurs fournisseurs.		critiques, en matière de droits d'accès, devraient être mises à l'épreuve périodiquement afin de vérifier qu'elles fonctionnent conformément aux attentes.	
3.2. Limite des rôles de nature délicate Nous avons examiné les droits d'accès des différentes fonctions critiques touchant la vérification des comptes dans SAP et avons relevé quelques incohérences. Les droits d'accès pour débloquer les transactions à risque élevé ou pour procéder à la vérification des comptes fondée sur l'échantillonnage de transactions à risque faible ont été octroyés à de nombreux employés provenant de groupes et de catégories de classification différents (ex. : services administratifs, agents financiers, commis). L'examen de la documentation n'a pas permis d'établir un ensemble de critères commun appuyant la pertinence des droits d'accès accordés.	L'omission de restreindre les droits d'accès aux personnes appropriées nuit au processus vérification des comptes dont dépendent les agents financiers lors du traitement des paiements puisqu'aucune autre vérification des comptes n'est effectuée avant l'émission des paiements.	Le DPF devrait établir des critères clairs pour l'octroi des droits d'accès aux postes qui font la vérification des comptes, en tenant compte des exigences opérationnelles et des compétences, et s'assurer que ces droits sont accordés en conséquence. Ceux-ci devraient être soumis à une révision périodique pour s'assurer qu'ils demeurent appropriés.	La DGDPF est d'accord avec cette recommandation. Mesure : La DGDPF évaluera la définition des agents financiers et la consignera aux fins d'assurance de la qualité. Les droits d'accès seront octroyés en conséquence ou, au besoin, on consignera des mesures d'atténuation adaptées aux exigences opérationnelles. Date d'achèvement : 31 mars 2016

Observations	Incidence	Recommandation	Réponse de la direction et plan d'action
3.3. Droits d'accès excessifs accordés à l'équipe de l'OSSI de SAP Les employés du groupe de l'OSSI de SAP (environ 80 employés) ont obtenu l'accès à l'environnement de production de SAP pour la quasi-totalité des transactions soumises à nos tests d'audit, y compris les transactions qui permettent de contourner le flux de travail des approbations. L'équipe d'audit a été informée qu'il s'agissait là d'une situation temporaire, conçue pour permettre aux équipes techniques de résoudre des problèm es liés à l'environnement de production dans la première année de mise en œuvre du système.	L'équipe de l'OSSI de SAP a actuellement le droit d'accéder au traitement des paiements, depuis la première inscription jusqu'à la vérification des comptes, ce qui pourrait donner lieu à un usage inapproprié de cet accès. L'examen n'a pas indiqué qu'il y avait un processus de surveillance ou des contrôles compensatoires qui avaient été établis.	Le DPF devrait appliquer des mesures pour s'assurer que les droits d'accès temporaires ne sont pas utilisés de manière inappropriée pendant la période de mise en œuvre et que les droits accordés en trop sont supprimés une fois l'environnement de production stabilisé.	La DGDPF est d'accord avec cette recommandation. Mesure : Les droits d'accès seront supprimés après l'exécution des activités critiques de fin d'exercice. Entre-temps, on peut avoir accès aux pistes de vérification aux fins de surveillance. Date d'achèvement : 30 septembre 2015