Commission d’examen des plaintes concernant la police militaire

Surveillance des contrôles internes – 2021-2022

Rapport final

Présenté par :

Samson

Version :

31 décembre 2021

Table des matières

SOMMAIRE

Depuis 2017, la Commission d'examen des plaintes concernant la police militaire (CPPM) a élaboré des mécanismes de contrôle des processus relatifs aux rapports financiers, et le processus de mise en œuvre de la Politique sur le contrôle interne est parvenu à maturité.

La portée des travaux comprenait les éléments suivants :

- Contrôles au niveau de l'entité
- Cycle de l'approvisionnement au paiement
- Frais de déplacement
- Accès des utilisateurs
- Sécurité de l'information non financière

Contrôles au niveau de l'entité

L'examen a montré que les contrôles clés au niveau de l'entité sur les rapports financiers sont pour la plupart adéquats, mais que des améliorations pourraient être apportées dans certains domaines.

Contrôles des processus opérationnels

L'examen a révélé que les contrôles internes clés sur l'information financière liés aux processus opérationnels dans le champ d'application pour l'année 2021-2022 étaient pour la plupart adéquats, mais que des améliorations pourraient être apportées dans certains domaines.

Accès des utilisateurs

Nous estimons que les contrôles relatifs aux accès des utilisateurs aux systèmes de la CPPM sont appropriés. Quelques points à améliorer ont été observés.

1. Introduction

En 2017, le Conseil du Trésor a approuvé une nouvelle Politique sur la gestion financière, laquelle remplace la Politique sur le contrôle interne (PCI). Par suite de l'établissement de cette nouvelle politique, le contrôle interne est axé sur la gestion financière. Par conséquent, la Commission d'examen des plaintes concernant la police militaire du Canada (la CPPM ou « Commission ») a pris l'initiative de consigner les principaux processus opérationnels et contrôles en place. La Commission a réalisé un examen de l'efficacité de la conception et de l'efficacité opérationnelle de ses contrôles internes et a mis en place des plans d'action de gestion adéquats visant à tirer parti des possibilités d'amélioration recensées.

La CPPM est un organisme de surveillance civile quasi judiciaire qui fonctionne sans lien de dépendance avec le gouvernement du Canada. La Commission révise et fait enquête sur les plaintes concernant la conduite d'un policier militaire et fait enquête sur les allégations d'ingérence dans des enquêtes menées par des policiers militaires. Elle formule des recommandations et présente ses conclusions directement aux hauts dirigeants de la police militaire et de la Défense nationale. En tant qu'institution fédérale, elle fait partie du portefeuille de la défense pour les fins de rapport.

Au cours de l'exercice 2019-2020, la Commission a préparé un plan de surveillance continue de ses contrôles internes afin de donner à la haute direction l'assurance de leur efficacité continue. La surveillance continue des contrôles internes de la CPPM donne aux ministères clients l'assurance que les contrôles financiers des services de la CPPM sont adéquats, en soutien à la signature de la Déclaration de responsabilité de la direction englobant les contrôles internes relatifs aux rapports financiers annuels, conformément à la Politique sur la gestion financière.

Les processus opérationnels retenus pour faire l'objet d'un suivi dans le cadre du plan de surveillance continue en raison de leur importance sont les suivants :

Contrôles clés des processus opérationnels	**Système de TI connexe**	**CIGF**	**Autre**
1. Cycle de l'approvisionnement au paiement (dépenses)	SFMC, SVP	X	
2. Frais de déplacement	HRG / SVP	X	
3. Administration de la paye	MesRHGC	X	
4. Budgétisation et prévisions	SFMC…	X	
5. Rapports financiers et clôture (clôture d'état financier, balance des comptes, présentation au Conseil du Trésor et rapport sur les états financiers)	-	X	
6. Planification des biens de TI	-	X	
Secteurs de processus non financiers			
7. Sécurité de l'information non financière			X
8. Enquêtes			X
9. Rapports annuels			X
Secteurs de CGTI			

Contrôles clés des processus opérationnels	Système de TI connexe	CIGF	Autre
10. Accès des utilisateurs (secteurs financiers)	SFMC, Phénix, SVP, HRG		X
11. Infrastructure (information non financière)			X

2. Objectif et portée

La société Samson & Associés a été mandatée pour effectuer un examen des documents, une révision structurée et des analyses d'efficacité pour les éléments visés dans le cadre du plan de surveillance continue pour l'année 2021-2022 (voir l'annexe A).

2.1 Documents

Nous avons répertorié les principaux processus et contrôles en place sous la forme d'une description des processus opérationnels, d'une carte des processus et d'une matrice de contrôle et nous nous sommes assurés qu'ils représentent adéquatement les processus et contrôles actuels en place.

2.2 Révision structurée et essais

Nous avons effectué une révision structurée et des essais portant sur la conception et l'efficacité opérationnelle des processus suivants de la CPPM :

- Contrôles au niveau de l'entité
- Cycle de l'approvisionnement au paiement
- Frais de déplacement
- Accès des utilisateurs
- Sécurité de l'information non financière
  (Essais préliminaires uniquement – des essais complets seront effectués en 2022-2023 dans le cadre de l'examen du processus lié aux enquêtes)

La méthodologie suivante a été utilisée au cours de la mission :

1. Relever les contrôles clés à mettre à l'essai
2. Élaborer une stratégie de mise à l'essai (avec l'échantillonnage)
3. Définir les populations et prélever des échantillons
4. Réaliser une révision structurée
5. Évaluer l'efficacité de la conception
6. Évaluer l'efficacité du fonctionnement
7. Formuler la conclusion

La méthode d'échantillonnage utilisée était fondée sur l'approche adoptée par le Conseil du Trésor dans son Guide de surveillance continue du contrôle interne en matière de gestion financière. L'ampleur des mises à l'essai a été déterminée en fonction de la fréquence à laquelle un contrôle est exécuté.

3. Contrôles au niveau de l'entité

Il existe cinq éléments de contrôle interne interdépendants. Quatre de ces éléments se rapportent à la conception et au fonctionnement du système de contrôles internes. Ces éléments constituent la base et le fondement de la mise à l'essai des contrôles au niveau de l'entité. Notre examen des documents et les entretiens ont révélé que les contrôles au niveau de l'entité de la CPPM étaient pour la plupart satisfaisants :

Éléments des contrôles au niveau de l'entité	Évaluation
Environnement de contrôle	Adéquat
Évaluation des risques	Possibilité d'amélioration
Activités de contrôle et de surveillance connexe	Adéquat
Information et communication	Adéquat

3.1 Environnement de contrôle

Par ses directives et ses structures de gestion à plusieurs niveaux qui favorisent l'exercice de responsabilités appropriées dans la poursuite de ses objectifs, la CPPM démontre son engagement en faveur de l'intégrité et des valeurs éthiques. La CPPM a également adopté de bonnes pratiques de gestion, par exemple en mettant en place un comité exécutif, des processus de planification et de surveillance des opérations, des communications officielles avec les employés et des activités de surveillance. Le Comité exécutif de la CPPM est informé des activités et des enquêtes menées au sein de l'organisation. Des faits saillants lui sont présentés chaque semaine et font l'objet de discussions, au besoin. La CPPM a entrepris certaines activités de planification de la relève en procédant à une évaluation de sa main-d'œuvre. La CPPM aurait avantage à poursuivre ses activités de planification de la relève en déterminant les postes clés et les personnes qui seraient en mesure d'exercer les responsabilités associées.

De plus, la CPPM a collaboré avec Santé Canada pour élaborer une lettre d'entente interministérielle sur les Services d'aide aux employés (SAE) – services extrajudiciaires de résolution de conflit. Cette lettre d'entente permet à la CPPM de bénéficier de services d'ombudsman et de gestion informelle des conflits et d'avoir accès aux services de l'Unité de prévention du harcèlement et de la violence de Santé Canada. Un grand nombre d'employés de la CPPM ont répondu au Sondage auprès des fonctionnaires fédéraux et les résultats ont montré que, dans l'ensemble, les employés sont satisfaits de leur milieu de travail.

3.2 Évaluation des risques

L'évaluation des risques consiste à cerner et à analyser les risques (tant internes qu'externes) pertinents pouvant avoir une incidence sur l'atteinte des objectifs opérationnels, y compris ceux liés à la gestion financière. Dans le cadre de notre examen, nous nous attendions à ce que la CPPM dispose d'un processus de détermination, d'analyse et de gestion des risques liés à ses activités.

La CPPM dispose d'une fonction de gestion des risques chargée d'élaborer le plan ministériel de l'entité et d'effectuer une évaluation des risques pour déterminer les principaux domaines tels que la sécurité et l'information. Nous avons toutefois constaté dans le cadre de notre examen que bien qu'une évaluation des menaces ait été effectuée, la CPPM aurait avantage à élargir la portée de son processus d'évaluation pour y inclure le risque de fraude dans l'ensemble de l'organisation. Ainsi, la CPPM devrait étudier la possibilité d'élargir son protocole actuel de signalement des actes répréhensibles pour y inclure explicitement le risque de fraude. De plus, si une évaluation des risques de fraude est intégrée au processus, les communications sur la

divulgation d'actes répréhensibles à l'ensemble du personnel devraient comprendre des efforts de sensibilisation à la détection et au signalement de fraudes.

> **Recommandation 1 :** Nous recommandons à la CPPM d'améliorer son processus d'évaluation des menaces afin d'y inclure le risque de fraude et de s'assurer que les employés sont conscients des risques de fraude, de la façon de les détecter et des protocoles de signalement.

3.3 Activités de contrôle et surveillance connexe

Les activités de contrôle sont des mesures prévues par les politiques et les procédures pour aider à assurer l'application des directives de la direction qui visent à atténuer les risques. Des activités de contrôle sont exécutées à tous les niveaux de l'entité, et ce, à différentes étapes des processus opérationnels, et visent également l'environnement technologique. Elles peuvent avoir trait à la prévention ou à la détection, ainsi qu'englober une gamme d'activités manuelles et automatisées.

Le suivi de la qualité du rendement des contrôles internes de l'entité au fil du temps est une fonction connexe aux activités de contrôle. La surveillance active s'effectue au moyen d'activités de surveillance continue, d'évaluations distinctes ou d'une combinaison des deux.

Depuis 2019, la CPPM a adopté un cadre de contrôle rigoureux et un plan de surveillance continue des contrôles internes de l'information financière. En conséquence, les activités de contrôle et de surveillance connexe sont considérées comme adéquates et suffisantes. Un processus de suivi des contrôles internes sera réalisé en 2022 pour veiller à ce que les recommandations soient prises en compte et mises en œuvre.

3.4 Information et communication

L'objectif de cette composante des contrôles au niveau de l'entité est de garantir que l'information pertinente est relevée, puis consignée et communiquée pour que les personnes concernées puissent s'acquitter de leurs responsabilités en temps opportun. Les systèmes d'information produisent des rapports qui contiennent des renseignements opérationnels et financiers et des renseignements liés à la conformité, ce qui permet d'exploiter et de contrôler les processus de l'organisation. De façon plus générale, des communications adéquates sont également nécessaires, c'est-à-dire que les personnes doivent comprendre leur rôle dans le système de contrôle interne et la manière dont leurs activités s'inscrivent dans le travail des autres. Elles doivent disposer d'un moyen de transmettre l'information importante aux échelons supérieurs de l'organisation.

Comme nous l'avons indiqué précédemment (section 3.1), la CPPM a adopté plusieurs pratiques qui ont permis de mieux consigner et communiquer les renseignements nécessaires dans l'ensemble de l'organisation. La CPPM est une petite organisation, mais elle a adopté de nombreuses pratiques bien établies. La recommandation 1 formulée précédemment contribuera à améliorer la façon dont les renseignements clés sont communiqués.

4. Résultats – Processus opérationnels

Principaux processus financiers	Évaluation de l'efficacité de la conception et du fonctionnement	Principales lacunes en matière de contrôle	Nombre de contrôles clés
Cycle de l'approvisionnement au paiement	Possibilités d'amélioration	2	11
Frais de déplacement	Possibilités d'amélioration	2	8
Sécurité de l'information non financière*	Possibilités d'amélioration	-	-

*La majorité de l'information non financière pour laquelle des protocoles de sécurité sont requis concerne les enquêtes. Le processus relatif aux enquêtes sera évalué en 2022-2023 et il est prévu que des essais de fonctionnement détaillés soient effectués à cette occasion. Samson & Associés s'est concentré sur les essais relatifs à l'efficacité de la conception en 2021-2022.

En 2021-2022, notre examen a porté essentiellement sur l'efficacité de la conception et sur l'obtention d'une bonne compréhension des protocoles d'accès des utilisateurs et de gestion des documents du système de gestion de l'information (Documentum).

4.1 Cycle de l'approvisionnement au paiement

La portée des contrôles du processus opérationnel relatif au cycle de l'approvisionnement au paiement commence par le fait de remplir un formulaire d'achat local de la CPPM. Le formulaire est acheminé pour approbation à l'autorité responsable en vertu de l'article 32 de la LGFP et l'engagement est enregistré dans le SFMC. Pour s'assurer que les engagements sont conservés et mis à jour en temps opportun, la CPPM tient à jour une feuille de suivi répertoriant tous les engagements enregistrés. Cette feuille de calcul est mise à jour lorsque les factures sont reçues et consignées en rapport avec les engagements. Nous avons constaté que dans 2 cas sur 15, la feuille de calcul n'a pas été mise à jour.

> **Recommandation 2 :** Nous recommandons que la CPPM s'assure que les engagements sont mis à jour à la réception des factures pour garantir l'exactitude des fonds non grevés et le déblocage des fonds non utilisés.

Un contrat ou un bon de commande est créé pour l'achat. Après la réception des biens ou la prestation des services, les factures sont reçues dans la boîte de réception des finances et envoyées à l'autorité déléguée appropriée pour examen et certification des factures conformément aux exigences de l'article 34 de la LGFP. La facture est ensuite renvoyée aux Services financiers aux fins de paiement. Lorsque les Services financiers reçoivent la facture, un contrôle de la qualité est effectué pour s'assurer que le paiement est approprié en vertu des exigences de l'article 33 de la LGFP. Une fois le paiement approuvé, il est lancé par le biais du Système normalisé de paiement (SNP).

Le fournisseur envoie si nécessaire des modifications au fichier principal des fournisseurs. La demande est reçue et vérifiée par l'agent d'approvisionnement ou le commis aux finances qui saisit la modification dans le SFMC avec l'accès de sécurité ZZZZ. Toutes les modifications saisies sont examinées et approuvées par un agent des finances conformément à l'article 33 de la LGFP.

Au cours de nos vérifications, nous avons constaté que l'accès permettant d'ajouter ou de supprimer des fournisseurs du fichier principal des fournisseurs est accordé à tous les utilisateurs des Services financiers. Ainsi, il n'y a pas de séparation des tâches entre les utilisateurs ayant accès aux fonctions d'ajout ou de suppression de fournisseurs dans le fichier principal et ceux ayant accès au traitement des comptes créditeurs. Des contrôles compensatoires sont en place pour, étant donné que la CPPM est une très petite organisation, où les modifications apportées au fichier principal des fournisseurs sont effectuées par deux personnes.

L'accès trop étendu aux systèmes augmente le risque relatif à la séparation des tâches lorsque des personnes ont accès à plusieurs fonctions dans le SFMC.

> **Recommandation 3 :** Nous recommandons que des contrôles de surveillance soient mis en place pour veiller à la gestion du risque détecté en ce qui concerne la de séparation des tâches. Par exemple, un système de notifications pourrait être mis en place pour gérer ce risque.

4.2 Voyages

La portée des contrôles pour le processus opérationnel des dépenses de voyages englobe la détermination du besoin d'effectuer un déplacement, l'approbation des demandes de déplacement conformément au pouvoir d'engagement des dépenses en vertu de l'article 32 de la LGFP, de certifier les demandes de remboursement de frais de déplacement (article 34 de la LGFP) et de traiter les demandes de paiement (article 33 de la LGFP).

Une demande de voyage est créée par un organisateur de voyage au nom de l'employé à l'aide de l'outil de réservation en ligne du portail des Services de voyage partagés (SVP). La demande est acheminée à l'autorité déléguée appropriée conformément à l'article 32 de la LGFP pour approbation et l'employé peut entreprendre

les préparatifs de voyage une fois le déplacement approuvé. Après le voyage, l'employé fournit tous les reçus recueillis pendant le voyage à l'organisateur de voyage. L'organisateur de voyage crée alors une demande de remboursement de frais de déplacement à laquelle sont joints l'ensemble des reçus à titre de pièces justificatives. La demande de remboursement de frais de déplacement est acheminée à l'autorité déléguée pour approbation conformément à l'article 34 de la LGFP. L'organisateur de voyage sélectionne la personne chargée de l'approbation de la demande de voyage et de la demande de remboursement de frais de déplacement à partir d'un menu déroulant du SVP. La demande est ensuite acheminée vers le processeur qui effectue un contrôle d'assurance de la qualité de la demande avant d'approuver le paiement conformément à l'article 33 de la LGFP. Une fois le paiement approuvé, il est lancé par le biais du SNP.

Au cours de nos essais sur l'accès des utilisateurs du SVP, nous avons constaté que des personnes avaient accès à des fonctionnalités non nécessaires dans le cadre de leurs fonctions :

- cinq utilisateurs sur 9 ne devraient plus avoir accès à l'approbation des demandes de voyage dans le SVP en vertu des exigences de l'article 32 de la LGFP;
- cinq utilisateurs sur 9 ne devraient plus avoir accès à l'approbation des demandes de remboursement de frais de déplacement dans le SVP en vertu des exigences de l'article 34 de la LGFP.

L'existence d'autorisations d'accès inadéquates augmente le risque d'accès non autorisé au SVP, ce qui pourrait entraîner une corruption accidentelle ou intentionnelle des données, mettant ainsi à risque l'intégrité des renseignements de l'organisation.

> **Recommandation 4 :** Nous recommandons que l'accès logique au SVP soit retiré systématiquement dès qu'un employé quitte la Commission ou qu'il change de rôle et n'a plus besoin d'y accéder dans le cadre de ses fonctions. De plus, nous recommandons de procéder à un examen périodique des accès afin de détecter toute anomalie et de la corriger en temps opportun.

4.2 Sécurité de l'information non financière

Comme indiqué précédemment, la composante de l'examen portant sur les mécanismes de traitement sécuritaire et approprié des dossiers d'enquête par le biais de vérification de dossiers spécifiques sera réalisée dans le cadre du processus d'enquête en 2022-2023. En 2021-2022, nous avons mis l'accent sur l'efficacité de la conception (compréhension de l'environnement et de l'approche de contrôle) pour d'autres documents.

En raison de la propagation de la COVID-19 qui a obligé le personnel de la CPPM à travailler à distance, l'organisation a adopté une approche virtuelle. Pour ce faire, elle a eu recours aux systèmes existants (Documentum et lecteur partagé) et a récemment adopté Office 365.

Nous avons examiné les documents dont dispose la CPPM et, à part les dossiers d'enquête, très peu de renseignements protégés sont gérés sur ses systèmes organisationnels.

Les pratiques de gestion de la documentation de la CPPM font appel à la plateforme Documentum et sont appuyées par une documentation claire et des normes d'accès définies pour les utilisateurs. Cependant, le lecteur partagé et Teams ne disposent pas du même niveau de contrôle de la gestion des documents.

Au moment de notre examen, les dossiers physiques n'avaient pas encore tous été transférés sous forme numérique pour être accessibles sur le lecteur partagé, Teams ou Documentum. La CPPM doit adopter un processus d'assurance de la qualité pour veiller à ce que la numérisation des dossiers soit complète et exacte.

> **Recommandation 5 :** Nous recommandons que des pratiques et des protocoles de gestion de l'information soient mis en place pour tous les systèmes électroniques de gestion de l'information, que ce soit par le biais de Documentum, du lecteur partagé ou de Teams.

Recommandation 6 : Nous recommandons que la CPPM adopte un processus d'assurance de la qualité pour son initiative de numérisation afin de s'assurer que les principaux dossiers physiques sont numérisés de manière à préserver l'intégrité des documents.

CONCLUSION – CONTRÔLES DES PROCESSUS OPÉRATIONNELS

L'examen a révélé que les contrôles internes clés sur les processus opérationnels fonctionnent en général de manière efficace.

5. RÉSULTATS RELATIFS AUX CGTI

2021-2022	SECTEURS VISÉS PAR LES CONTRÔLES	CONTRÔLES COURANTS	SFMC	MESRHGC (congé et heures supp)	DOCUMENTUM	SNP (FOURNISSEURS)	HRG (VOYAGES)
Gestion des TI	3	Exclu de la portée de l'examen en 2021-2022					
Sécurité des TI (accès des utilisateurs)	6	Possibilité d'amélioration	Forts	Forts	Forts	Forts	Forts
Développement d'applications et gestion du changement	4	Exclu de la portée de l'examen en 2021-2022					
Opérations informatiques et réseau	1	Exclu de la portée de l'examen en 2021-2022					

Remarque : Annexe B

5.1 Contrôle d'accès des utilisateurs : arrivée et départ

Les principaux contrôles d'accès des utilisateurs sont effectués au moment où les employés arrivent dans une organisation et lorsqu'ils la quittent. C'est à l'arrivée que la majorité des accès utilisateurs sont attribués, approuvés et mis en œuvre, et au départ que les mesures nécessaires sont prises pour supprimer les accès. Nous avons effectué une vérification de 12 accès utilisateurs dans le cadre de notre examen.

À la CPPM, un formulaire est utilisé pour consigner ces deux étapes. Il n'y avait pas nécessairement de processus dûment établi il y a plus de cinq ans, mais le processus correspondant est en place depuis plus de deux ans.

Nous avons constaté que les contrôles à l'arrivée sont adéquats. Les quelques employés pour lesquels aucun formulaire d'arrivée ne figurait dans les documents étaient en poste à la CPPM depuis de nombreuses années et leurs accès étaient appropriés.

Cependant, nous avons relevé des cas d'employés qui avaient quitté la CPPM, mais dont les comptes systèmes étaient toujours actifs :

- Cinq utilisateurs de HRG
- Deux utilisateurs du SFMC

Nous n'avons pas été en mesure de confirmer si l'accès au réseau de ces employés avait été supprimé en temps opportun, mais ils n'avaient plus d'accès au réseau au moment où nous avons mené notre vérification.

Bien que la composante de l'accès des utilisateurs soit importante, nous n'avons pas connaissance d'une utilisation abusive de l'accès au système par ces employés et, dans la plupart des cas, le risque lié à l'application spécifique est limité en raison d'un accès nécessaire au réseau (qui semble avoir été supprimé). Il est à noter que le processus de départ de la CPPM comporte un certain nombre d'interventions manuelles nécessaires pour informer les personnes concernées afin qu'elles suppriment les accès en temps opportun.

> **Recommandation 7 :** Nous recommandons que le processus de départ soit normalisé de manière à assurer la suppression en temps opportun de tous les accès aux applications et au réseau au moment du départ. Les opérations de suppression des accès des utilisateurs (applications et accès au réseau) devraient être consignées pour attester du moment de la suppression.

5.2 Examen continu de l'accès des utilisateurs

Un responsable des processus opérationnels a été désigné pour chacun des systèmes de l'organisation. En plus de l'approbation de l'accès utilisateur au moment de l'embauche (contractuel), un examen régulier de l'accès utilisateur doit être effectué pour s'assurer que les accès sont toujours nécessaires et appropriés.

Bien qu'un examen annuel périodique dûment consigné des accès semble en place pour la plupart des applications (contrôles compensatoires), nous n'avons pas trouvé de documentation pour l'examen des accès au réseau.

> **Recommandation 8 :** Nous recommandons que l'examen continu des accès des utilisateurs soit consigné pour consultation ultérieure.

CONCLUSION SUR LES CONTRÔLES D'ACCÈS DES UTILISATEURS

Nous estimons que les contrôles d'accès des utilisateurs aux systèmes visés par le présent examen sont généralement appropriés.

Annexe A : Plan de surveillance continue :

Secteurs de contrôle clés	Risques	Exercices financiers					Remarques
		2020-2021	2021-2022	2022-2023	2023-2024	2024-2025	
Contrôles au niveau de l'entité	Modéré	x					
Contrôles de processus opérationnels							
Cycle de l'approvisionnement au paiement (dépenses[1])	**MODÉRÉ**	X		X		X	Remarque 1
Planification des biens de TI	**MODÉRÉ**		X		X		
Frais de déplacement	**MODÉRÉ**	X		X		X	
Administration de la paye	**MODÉRÉ**		X		X		
Budgétisation et prévisions	**MODÉRÉ**		X		X		
Rapports financiers	**FAIBLE**			X			
Secteurs de processus non financiers							
Sécurité de l'information non financière	**MODÉRÉ**	X					
Enquêtes	**MODÉRÉ**		X				
Rapport annuel	**FAIBLE**			X			
Secteurs de CGTI							
Accès des utilisateurs (secteurs financiers)		X		X		X	
Infrastructure (information non financière)			X		X		

[1] La mise à l'essai comprendra le cycle de paiements pour les dépenses de fonctionnement et d'immobilisations.

Recommandations	Cote de risque	Plan d'action de gestion
Contrôles au niveau de l'entité		
Recommandation 1 : Nous recommandons à la CPPM d'améliorer son processus d'évaluation des menaces afin d'y inclure le risque de fraude et de s'assurer que les employés sont conscients des risques de fraude, de la façon de les détecter et des protocoles de signalement.	**Modéré**	La CPPM intégrera le risque de fraude au cours de sa prochaine évaluation cyclique des menaces et des risques en 2025 ou en cas de changement important apporté aux bureaux de la CPPM avant cette date. Dans l'intervalle, la CPPM mettra à jour son plan de communication en matière de sensibilisation à la sécurité, plus particulièrement l'article à paraître en mars à l'occasion du Mois de la prévention de la fraude, pour y incorporer des indications sur les personnes avec lesquelles les employés doivent communiquer en cas de fraude au travail et sur les stratégies de détection de la fraude.
Contrôles des processus opérationnels		
Recommandation 2 : Nous recommandons que la CPPM s'assure que les engagements sont mis à jour à la réception des factures pour garantir l'exactitude des fonds non utilisés et le déblocage des fonds non utilisés.	**Faible**	L'équipe des finances mettra en place des procédures opérationnelles normalisées pour veiller à ce que les engagements soient tenus à jour, à la fois dans notre feuille de calcul répertoriant les engagements et dans le SFMC. Ces procédures préciseront le calendrier à suivre ainsi que les personnes/postes responsables de la saisie, de l'examen et de l'approbation des données. Nous effectuerons également un examen semestriel des engagements afin de vérifier leur exactitude et leur exhaustivité. Nous prévoyons de mettre en œuvre ce processus à temps pour le début de l'exercice 2022-2023.
Recommandation 3 : Nous recommandons que des contrôles de surveillance soient mis en place pour veiller à la gestion du risque détecté en ce qui concerne la de séparation des tâches. Par exemple, un système de notifications pourrait être mis en place pour gérer ce risque.	**Modéré**	La CPPM s'attaquera au risque relatif à la séparation des tâches en réexaminant nos accès au SFMC et en demandant conseil au service d'assistance du SFMC pour limiter l'accès aux changements de fournisseurs. Une option à privilégier serait de créer des accès distincts pour les fonctions « créer » et « approuver », à assigner aux personnes chargées de l'approbation en vertu de l'article 33 (approuver exclusivement) et les autres utilisateurs des finances

Recommandations	Cote de risque	Plan d'action de gestion
		(créer/modifier exclusivement). La demande de changement a été soumise au SFMC avec un délai proposé de 6 mois (septembre 2022).
Recommandation 4 : Nous recommandons que l'accès logique au SVP soit supprimé systématiquement dès qu'un employé quitte la Commission ou qu'il change de rôle et n'a plus besoin d'y accéder dans le cadre de ses fonctions. De plus, nous recommandons de procéder à un examen périodique des accès afin de détecter toute anomalie et de la corriger en temps opportun.	**Modéré**	Les RH enverront désormais un courriel de fin d'emploi à la boîte de réception des finances lorsqu'un employé quitte la CPPM. Ce courriel déclenchera alors la suspension des comptes par le coordonnateur des voyages dans le portail des voyages. Nous recommandons également qu'à la fin de chaque exercice financier, les RH envoient un rapport de tous les employés ayant quitté leur emploi au cours de cet exercice, ce qui permettra au coordonnateur de vérifier que tous les départs ont bien été traités dans le système.
Recommandation 5 : Nous recommandons que des pratiques et des protocoles de gestion de l'information soient mis en place pour tous les systèmes électroniques de gestion de l'information, que ce soit par le biais de Documentum, du lecteur partagé ou de Teams.	**Modéré**	La CPPM dispose actuellement de pratiques et de protocoles d'information bien établis pour son système d'information ministériel Documentum. La CPPM travaille à consigner les procédures de gestion et de conservation des documents sur la plateforme Microsoft Teams et mettra en place une politique, un protocole et des formulaires au cours de l'exercice 2022-2023. Comme la CPPM travaille actuellement à la mise hors service des lecteurs partagés, la question de la gestion des renseignements qui y figurent sera abordée dans le cadre du processus de mise hors service des lecteurs partagés d'ici la fin de l'exercice 2023-2024.
Recommandation 6 : Nous recommandons que la CPPM adopte un processus d'assurance de la qualité pour son initiative de numérisation afin de s'assurer que les principaux dossiers physiques sont numérisés de manière à préserver l'intégrité des documents.	**Faible**	En 2017, la CPPM a adopté et consigné un processus d'assurance de la qualité pour son initiative de numérisation pour veiller à ce que les documents physiques soient numérisés de manière à garantir l'intégrité des documents. Cependant, on craint que le processus n'ait pas été suivi correctement dans le passé et que certains dossiers physiques soient actuellement conservés comme copies de sécurité des dossiers numérisés.

Recommandations	Cote de risque	Plan d'action de gestion
		La CPPM mettra en place d'ici la fin de 2022-2023 un plan pour réaliser la procédure d'assurance de la qualité des documents physiques ayant été numérisés de manière à garantir l'intégrité des documents et à les supprimer en temps opportun, conformément au Calendrier de conservation et d'élimination des documents. De plus, la CPPM est sur le point d'approuver une version révisée de la Politique en matière de disposition de l'information et des données de la CPPM. Une fois approuvée, la CPPM, par l'intermédiaire de son service juridique, mènera un processus de vérification l'an prochain avant la destruction des dossiers déjà numérisés afin de déterminer les documents clés qui doivent être conservés pour consultation ultérieure.
Accès des utilisateurs		
Recommandation 7 : Nous recommandons que le processus de départ soit normalisé de manière à assurer la suppression en temps opportun de tous les accès aux applications et au réseau au moment du départ. Les opérations de suppression des accès des utilisateurs (applications et accès au réseau) devraient être consignées pour attester du moment de la suppression.	**Modéré**	La CPPM modifiera ses formulaires de départ pour y inclure des champs supplémentaires concernant les accès liés à la TI pour s'assurer que les accès sont retirés au départ des employés. En ce qui concerne les accès spécifiques au sein de l'équipe des finances, un document distinct sera créé pour le suivi des accès (modifications et désactivation, le cas échéant).
Recommandation 8 : Nous recommandons que l'examen continu des accès des utilisateurs soit consigné pour consultation future.	**Faible**	La CPPM est dans la phase finale de l'élaboration d'une nouvelle Politique de sécurité informatique comportant de nouvelles mesures pour le contrôle des accès. La politique définira officiellement les rôles et les responsabilités de la TI et des gestionnaires en ce qui concerne l'attribution des accès et les notifications en cas de changement de profil d'emploi ou d'accès. La politique exigera également la tenue d'un registre des changements d'accès par le biais de procédures et de formulaires normalisés.