CENTRE INTERNATIONAL DE FORMATION DE L'OIT

Conseil du Centre

75e session, Turin, 17-18 octobre 2013 **CC 75/5/4**

POUR INFORMATION

CINQUIÈME QUESTION À L'ORDRE DU JOUR

Suivi des recommandations du Chef auditeur interne pour l'année qui s'est achevée au 31 décembre 2012

Introduction

1. Lors de la 74e session du Conseil du Centre (novembre 2012), le Chef auditeur interne du Bureau international du Travail, qui est aussi l'auditeur interne du Centre, a présenté au Conseil un rapport sur les principaux résultats de l'audit interne et des missions d'enquête effectués au Centre en 2011. Sur la base d'une évaluation des risques concernant les processus métiers du Centre, le Bureau de l'audit interne (IAO) a mené un audit de la sécurité informatique en octobre et novembre 2011 et a remis son rapport final en janvier 2012.

2. Le présent document aborde les mesures de suivi prises par le Centre pour donner application aux recommandations en matière de sécurité informatique contenues dans le rapport présenté par l'IAO au Conseil en 2012.

3. L'auditeur interne n'a pas relevé de faiblesses significatives dans le système de contrôle interne du Centre dans le domaine de la sécurité informatique. Toutes les recommandations prioritaires du rapport de 2012, les recommandations restantes sur la gestion et le contrôle par le Centre des recettes générées par les activités de formation, ainsi que les réponses apportées par le Centre et les détails des actions de suivi achevées, figurent à l'annexe I.

4. Le Centre continuera à travailler avec l'auditeur interne et le tiendra informé des progrès réalisés dans l'application des recommandations encore en suspens.

Turin, le 13 septembre 2013.

Annexe I[1]

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre	Date d'achèvement
Recettes générées par les activités de formation				
1	Le Centre ne peut évidemment présumer des excédents futurs, ni s'attendre à bénéficier de fonds tombés du ciel. C'est pourquoi il est impératif qu'il budgétise correctement toutes ses activités de formation et se dote de systèmes assurant la perception intégrale et en temps utile de ses recettes.	Une circulaire concernant l'examen, l'approbation, la signature et le traitement des contrats relatifs à des activités liées à la formation a été publiée afin de donner effet aux recommandations sur l'établissement de fonctions plus centralisées dans le domaine de la mobilisation de ressources. Cette circulaire établit la méthode pour la conservation de l'historique des accords de financement, qui servira de base pour le suivi et le contrôle de la balance de ces accords. L'équipe de projet de l'examen des processus métiers (BPR) a développé et mis en œuvre un outil de budgétisation, améliorer le module relatifs aux sommes à recevoir d'Oracle afin d'enregistrer et de garder une trace des accords de financement et mis au point des rapports afin de garantir que les recettes sont perçues intégralement et dans les temps.	Achevé	15 mars 2013

[1] *Les recommandations n^os^ 5 et 6 avaient déjà été mises en œuvre en septembre 2012 et fait l'objet d'un rapport au Conseil dans le document CC 74/4/4.*

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre	Date d'achèvement
2	En 2011, le Centre a commandité un examen des processus métiers (BPR) de ses activités, lequel avait commencé au moment où l'audit a eu lieu. Le cahier des charges du BPR couvre les revenus générés par les activités de formation. De ce fait, la mise en œuvre des changements subséquents aux recommandations et conclusions de l'IAO devra être envisagée après l'achèvement du BPR.	L'équipe BPR est actuellement en train de conclure ses travaux sur les recommandations formulées par l'équipe de projet de Genève. Les outils développés à ce jour sont un outil de budgétisation, un module de garantie pour l'enregistrement et le suivi des accords de financement, un outil de facturation amélioré et une nouvelle version de MAP (un outil de planification des activités) qui ne nécessite plus de mise à jour manuelle de certaines données mais les récupère automatiquement d'Oracle. Le dernier point du BPR, l'outil de gestion des transferts de revenus à travers les années, est actuellement en test et devrait être déployé en septembre.	En cours (95%)	30 septembre 2013
3	L'IAO a examiné le flux de travail régissant le traitement des revenus générés par les activités de formation et a identifié une marge de simplification dans certains domaines, notamment en ce qui concerne le rôle des programmes techniques. Il est également imaginable que les Services financiers soient directement impliqués dans la détermination de la contribution du Centre à ses coûts fixes, ainsi que dans l'examen du rôle du Service du développement de programmes et de la coopération régionale (unité COORD) dans l'approbation de l'émission des factures.	L'intégration des fonctions de COORD et de l'ancienne unité de facturation et de contrôle des coûts au sein de la section de la gestion budgétaire et du rapport financier (BMFR) des Services financiers a simplifié et rationalisé le traitement des revenus générés par les activités de formation. L'utilisation de cours standard, qui a accéléré le processus de facturation, est une réalité depuis novembre 2012. Les Services financiers continuent à revoir périodiquement la politique de tarification et à recommander les ajustements nécessaires des éléments de coût standard de cette politique. L'émission des factures et toutes les demandes d'allocation de fonds passent désormais par l'unité BMFR.	Achevé	15 mars 2013

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre	Date d'achèvement
4	Les différents systèmes informatiques utilisés au Centre en rapport avec la gestion des coûts des activités de formation, comme par exemple les services de restauration et de gestion hôtelière, ne sont pas intégrés avec le module de gestion financière Oracle, ce qui entraîne des retards dans la collecte de toutes les informations sur les coûts de chaque activité, et allonge donc le temps nécessaire à l'émission d'une facture. L'absence de systèmes intégrés induit également un risque de duplication des efforts et d'erreurs d'encodage parce que la base de données servant principalement à générer des informations sur la participation aux activités de formation n'est pas reliée au système de gestion financière Oracle.	Dans le cadre de la réalisation du BPR, un outil visant à accélérer l'émission des factures relatives aux cours ouverts sur la base de l'extraction automatique d'informations depuis MAP a été développé. Cette intégration a atténué le risque d'erreurs d'encodage et duplication des efforts. En outre, si un budget a été calculé et téléchargé dans Oracle, les données contenues dans MAP sont automatiquement mises à jour et tiennent compte de toutes les transactions concernant l'activité en question, ce qui résulte en une intégration réelle des données entre MAP et Oracle. Le logiciel de gestion des services hôteliers et de restauration (SoftSolutions) et Oracle ERP sont deux systèmes différents au niveau de la portée et des données qu'ils contiennent. SoftSolutions est un logiciel de gestion hôtelière, tandis qu'Oracle est le système de gestion financière du Centre. Aucune alimentation directe n'est possible entre les deux systèmes, les activités basées sur Oracle ne commençant qu'après vérification et validation des données fournies par SoftSolutions. En l'absence d'alimentation directe, un rapport basé sur la feuille de données résumées de l'activité produite par SoftSolutions afin de réduire le temps et les efforts nécessaires pour collecter les données et encoder les données requises dans Oracle, ce qui accélère les processus de clôture des activités et de facturation.	Achevé	31 août 2013

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre
Sécurité informatique			
1	*Classification des actifs* Mener une classification, dresser l'inventaire et assigner les actifs informatiques aux processus métiers correspondants et évaluer l'impact sur la perte de confidentialité, l'intégrité et la disponibilité de ces actifs sur la base des exigences opérationnelles, légales et réglementaires.	Un inventaire des actifs informatiques a été dressé et une politique de gestion de ces actifs a été publiée dans le cadre de la politique relative à l'utilisation des technologies de l'information. Les Services des technologies de l'information et de la communication (ICTS) ont mené une analyse de l'impact de la défaillance de composants (CFIA), qui a servi pour l'évaluation de l'impact sur la perte de confidentialité, l'intégrité et la disponibilité des actifs.	Achevé
2	*Évaluation des risques informatiques* Officialiser une méthodologie de gestion des risques englobant tous les aspects relatifs à la sécurité, comme la confidentialité, l'intégrité et la disponibilité. Mener l'analyse des risques au niveau du Centre, en étendant celle déjà réalisée pour le plan de continuité du service des systèmes informatiques.	En 2012, la section ICTS a adopté un plan stratégique 2012-15, qui aborde l'évaluation et la gestion des risques informatiques. Un cadre de gouvernance des technologies de l'information et de la communication (TIC) a été mise en place dans le cadre de cette stratégie, et la Direction du Centre dirige le Comité de gouvernance des TIC. Un registre énumérant les risques potentiels liés aux technologies de l'information et établissant les stratégies qui permettent de les atténuer, est également tenu. Le chef de la section ICTS est membre du Comité de gestion des risques. Les principaux risques informatiques sont intégrés dans le registre des risques du Centre. La section ICTS a également mené une analyse de l'impact de la défaillance de composants (CFIA) et une analyse de l'impact sur les opérations (BIA) et tient à jour et améliore en permanence son plan de continuité du service.	Achevé

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre
3	*Contrôle de l'accès* Formaliser le processus de contrôle de l'accès (y compris l'accès à distance), en définissant le flux de travail pour la gestion des comptes et des profils et pour l'octroi, le maintien et le retrait des droits d'accès. Renforcer la politique en matière de mots de passe (longueur, complexité, expiration) pour toutes les applications et tous les systèmes. Mener avec les acteurs appropriés un examen régulier des utilisateurs et des droits d'accès. Les informations sensibles ne doivent pas être accessibles via l'Internet, sauf sous contrôle strict, et toutes les données doivent être envoyées sous forme cryptée.	Un catalogue des services proposés par la section ICTS, qui aborde les procédures formelles pour l'octroi, la modification et le retrait des droits d'accès aux systèmes informatiques, a été préparé. La politique en matière de mots de passe a été intégrée dans la politique sur l'utilisation des technologies de l'information. La section ICTS est en pleine migration du domaine de Novell vers Microsoft. Après l'achèvement du projet en 2013, ICTS pourra mettre en œuvre une politique renforcée en matière de mots de passe pour toutes les applications et tous les systèmes. ICTS coordonne et examine régulièrement avec les Services des ressources humaines (HRS) les changements au niveau du personnel et les droits d'accès correspondants. Les comptes d'utilisateurs et les droits qui y sont liés sont revus chaque mois. La section ICTS a entamé le travail d'identification des systèmes qui imposent des contrôles cryptographiques supplémentaires. Outre la fourniture de moyens de communication cryptés et d'échange de documents par connexion sécurisée, elle est également en train de mettre en place une solution pour le codage des ordinateurs portables et des disques partagés.	En cours (95%)

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre
4	*Cadre de politique de sécurité* Il y aurait lieu de formaliser un cadre de politique de contrôle de l'accès et de sécurité, y compris pour les politiques et procédures manquantes en matière de sécurité informatique, comme la gestion des incidents, la gestion des connexions, le contrôle de l'accès, la sécurité du réseau, l'enlèvement du matériel, la gestion du changement, etc. Définir et mettre en œuvre un plan de formation et de sensibilisation des utilisateurs à la sécurité informatique.	Une circulaire sur la politique en matière de sécurité informatique couvrant tous les domaines définis dans la norme ISO/IEC 27001 a été adoptée. Les contrôles techniques et administratifs plus spécifiques sont détaillés dans la politique sur l'utilisation des technologies de l'information. Une politique de gestion des connexions et des procédures de gestion du changement ont été publiées en 2012. La section ICTS a organisé la première session de sensibilisation à la sécurité informatique mi-2013. Cette formation est incluse dans le programme de développement du personnel du Centre et doit être suivie par tous les fonctionnaires.	Achevé

N°	Recommandation	Réponse du Centre	Statut de mise en œuvre
5	*Développement des indicateurs de performance clés pour les technologies de l'information* Identifier les indicateurs de performance clés avec les intervenants correspondants (Formation, Administration, Direction) afin de mesurer les performances et l'efficacité de l'offre informatique (applications, systèmes, services). Ces indicateurs peuvent être centrés sur les principaux domaines de risque et sur les prestations (opérations, projets, sécurité, investissements, personnel, etc.). Défini les modalités pour la collecte des informations nécessaires pour produire ces indicateurs et les outils de mesure correspondants. Établir un tableau de bord pour le rapport des performances et la mise en exergue des problèmes éventuels.	Les indicateurs clés ont été identifiés pour les processus et opérations critiques. La métrique utilisée est basée sur: - le catalogue des services et la cible pour le niveau de service; - la norme ISO 27001; - l'analyse de l'impact de la défaillance de composants; - le processus de gestion des risques; - le rapport sur le statut du projet; - la gestion du changement; - la gestion des incidents; - la politique de sécurité informatique; - la mesure de la sécurité. Un tableau de bord a été mis en place, qui examine régulièrement les performances et donne l'alerte en cas de problèmes ou incidents nécessitant une action.	Achevé
	Sécurité du système Définir le rôle de responsable de la sécurité et lui confier la responsabilité formelle de la gestion et du contrôle de la sécurité informatique.	Comme indiqué dans le plan stratégique ICTS 2012-15, le chef de la section fait fonction de responsable de la sécurité informatique et rapporte directement à la Direction du Centre.	Achevé