UNION POSTALE UNIVERSELLE

Téléphone +41 31 327 17 17
Télécopie +41 31 327 17 38
www.bdo.ch

BDO SA
Hodlerstrasse 5
3001 Berne

Pour le Conseil d'administration

DE L'UNION POSTALE UNIVERSELLE (UPU)

Berne

Rapport du service d'audit interne 04.2020
Rapport du service d'audit interne pour 2020

15 septembre 2020
2122 0573/1-2
HIM/BIT

Numéro de rapport	04.2020
Période d'audit	Janvier à septembre 2020
Diffusion du projet de rapport	14 septembre 2020
Date du rapport	15 septembre 2020
Diffusion du rapport	Directeur général Comité interne d'audit Direction générale Vérificateur externe

Table des matières

1. Rapport annuel d'activité

Fonction d'audit interne

La charte de révision interne établit que «le réviseur interne élabore un rapport annuel, en vue de sa présentation, dans son intégralité, à la prochaine session du Conseil d'administration, accompagné des observations appropriées du Directeur général».

Attribution du mandat d'audit interne

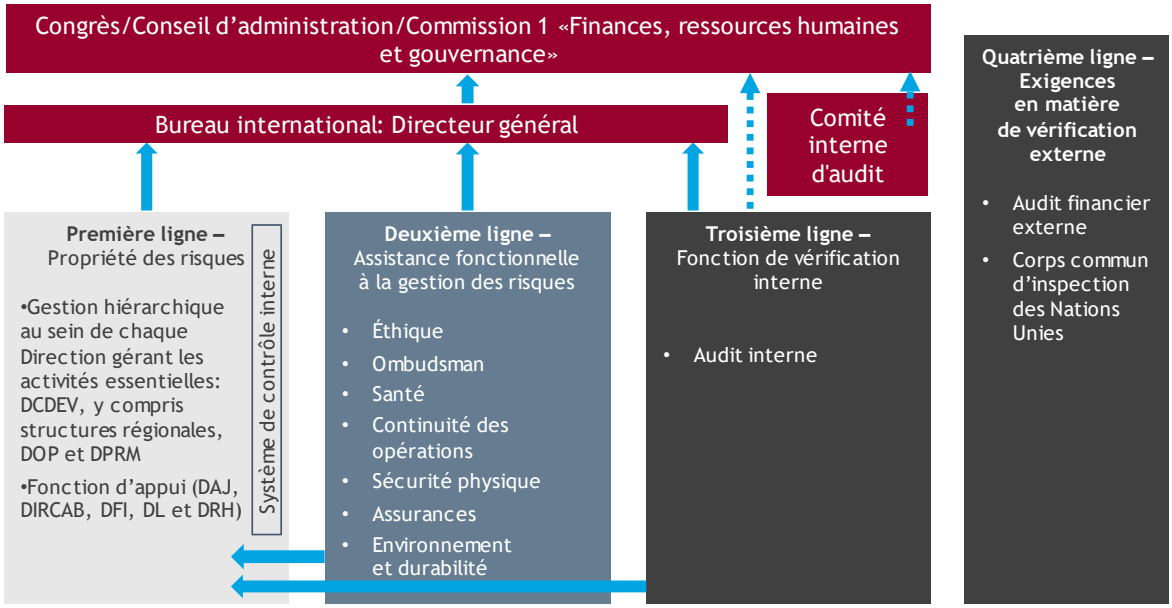
À la suite de l'appel d'offres intitulé «Audit interne de l'Union postale universelle», BDO a été sélectionné pour assurer l'audit interne pour une période de six ans allant de 2018 à 2023.

Afin d'obtenir une compréhension de l'environnement de l'UPU dans ses différents secteurs d'activité, BDO a acquis des connaissances sur la base de la documentation de l'organisation. En outre, des réunions avec le vérificateur extérieur, le Contrôle fédéral des finances, ont eu lieu pour obtenir une meilleure compréhension de l'organisation. Sur cette base, l'évaluation des risques, la planification d'audit pour 2018 et le plan de rotation pour les années 2018 à 2023 ont été établis. En consultation avec l'UPU, le plan d'audit a été ajusté en raison de la pandémie de COVID-19. Cela signifie que l'audit de la gestion de la continuité des opérations est réalisé en 2020 au lieu de 2021. À l'inverse, l'audit de l'organisation du Bureau international sera reporté de 2020 à 2021.

L'audit interne comme élément du cadre élargi de gestion des risques de l'UPU

La charte susmentionnée stipule que «la révision interne se définit, à l'UPU, comme une fonction indépendante apportant au Directeur général et, à travers lui, aux organes directeurs l'assurance que l'organisation est gérée de manière efficace».

L'audit interne fait partie du cadre élargi de gestion des risques, qui s'appuie sur le concept de «lignes de défense». Le cadre de l'UPU est présenté ci-dessous:



Évaluation des risques et planification de l'audit pour 2020

D'après les normes de The Institute of Internal Auditors, l'audit interne évalue les risques de l'organisation au niveau de la planification. L'évaluation des risques et la planification d'audit ont été élaborés sur la base de la stratégie 2017–2020 présentée en 2016 lors du Congrès d'Istanbul, de l'évaluation des risques de 2017, des connaissances rassemblées au moyen du processus de transfert ainsi que des éventuelles attentes spécifiques du Bureau international.

La planification d'audit pour 2020 a été approuvée par le Directeur général.

2. Audit interne pour 2020 – Principales observations

Pour 2020, nous avons produit quatre rapports d'audit, trois prévus dans le plan d'audit, l'un concernant le suivi d'audit et un audit supplémentaire sera effectué au quatrième trimestre de 2020.

Une note de planification a été établie pour chacune de ces missions d'audit. Ces missions d'audit interne ont pour principaux objectifs:

- d'examiner la couverture des risques identifiés;
- d'examiner l'organisation du domaine faisant l'objet de l'audit;
- d'identifier les mesures et les réponses de la Direction générale relatives aux facteurs de risque et de les examiner;
- d'identifier des domaines pouvant être améliorés dans le cadre des mesures et des réponses de la Direction générale.

Toutes les recommandations émises dans nos rapports ont été présentées à la Direction générale afin d'obtenir ses commentaires. Celle-ci a accepté nos recommandations.

Tous les rapports d'audit interne ont été présentés au Comité interne d'audit.

Les conclusions de ces audits n'ont pas pour but de souligner les éléments du système de contrôle interne qui fonctionnent bien, mais plutôt d'attirer l'attention de la Direction générale sur les éventuelles faiblesses en la matière.

Les conclusions et les recommandations découlant des audits internes entrepris ont fait l'objet de discussions avec les équipes d'encadrement concernées. Celles-ci sont d'accord avec ces conclusions et ont établi des plans d'action visant à renforcer les réponses de la Direction générale aux facteurs de risque.

Rapport de l'audit interne de juin 2019 – Communication du Bureau international

Cet audit visait à évaluer l'organisation et les contrôles internes relatifs à la communication interne en place au sein du Bureau international. Nous avons évalué/examiné les processus/domaines suivants:

- Canaux de communication.
- Communication aux membres du personnel.

Nos principales observations sont les suivantes:

1. *Repenser et simplifier le processus d'approbation et de publication*

   Le processus d'approbation d'une communication de service peut prendre jusqu'à cinq jours. Dans certains cas, cela ne permet pas aux employés d'être informés à temps.

   Nous recommandons de repenser et de simplifier le processus d'approbation afin de pourvoir réagir plus vite en temps de crise. Cela permettrait d'assurer que la communication du jour arrive dans les délais.

Une communication de service a été publiée sur l'intranet du Bureau international à propos des délais d'approbation et de publication des communications de service. Le délai est de cinq jours pour une communication non urgente et de trois jours pour une communication urgente.

2. *Changements aux instructions administratives*

Les changements apportés aux instructions administratives ne sont pas systématiquement communiqués aux membres du personnel.

Nous recommandons de communiquer systématiquement toutes les modifications.

3. *Compte rendu écrit des réunions périodiques*

Aucun document n'est produit après une réunion périodique. Si des membres du personnel étaient en mission ou ne pouvaient pas être présents, aucun résumé des informations communiquées n'est disponible.

Nous recommandons d'établir un protocole pour les réunions périodiques selon lequel tous les membres du personnel doivent avoir connaissance des informations importantes qui y sont présentées.

Dans l'avenir, il devra toujours y avoir un résumé des points abordés afin que les membres absents puissent également être au courant de ce qui a été discuté. Le résumé de la réunion périodique du 19 décembre 2019 a été envoyé à BDO.

Rapport de l'audit interne de février 2020 – Communication avec les Pays-membres

Cet audit visait à évaluer l'organisation et les contrôles internes relatifs à la communication avec les Pays-membres.

Nous avons évalué/examiné les processus/domaines suivants:

- Communication relative à la préparation du Congrès.
- Système de vote.
- Incidence de la pandémie de COVID-19 sur le 27e Congrès.

Nos principales observations sont les suivantes:

4. *Étendre le délai de soumission d'une proposition*

Les Pays-membres ont été informés que le délai du 10 juin devrait être respecté même si une extension pourrait être envisagée.

Nous recommandons d'étendre le délai du 10 juin pour la soumission par les Pays-membres de leurs propositions afin de permettre à ces derniers d'apporter des modifications aux documents déjà soumis.

5. *Clarifier la situation réelle dans le Règlement général de l'Union*

Le Règlement général de l'Union ne comprend pas de règles sur la responsabilité et sur ce qui se passe quand un Congrès ne peut avoir lieu en raison d'un cas de force majeure.

Nous recommandons de clarifier dans le Règlement général ce qui se produit lorsqu'un Congrès ne peut avoir lieu et doit être reporté. Actuellement, seul un changement géographique est réglementé, le Conseil d'administration faisant autorité sous certaines conditions. Nous recommandons également de clarifier les incidences du report avec le Vérificateur extérieur.

Rapport de l'audit interne de mars 2020 – Cybersécurité

Cet audit visait à évaluer l'état de vigilance des employés et leur comportement face aux attaques informatiques par hameçonnage ainsi que les processus internes relatifs aux incidents de cybersécurité.

Nous avons évalué le comportement des employés sur la base des réponses à un courriel d'hameçonnage que nous avons créé et diffusé. L'évaluation a été réalisée en trois phases:

- Création du courrier électronique d'hameçonnage.
- Vérification de la fonctionnalité.
- Exécution de l'attaque par hameçonnage.

Nos principales observations sont les suivantes:

6. *Développer la promotion des processus existants au sein du service informatique et la formation en la matière*

   À 9 h 23 et à 9 h 24, trois participants (membres du service informatique) ont envoyé des alertes électroniques à tous les employés du Bureau international. Ces courriers électroniques ont été envoyés séparément. La réaction a semblé non coordonnée, deux courriers électroniques ayant été envoyés à une minute d'intervalle, dans un style et une formulation différents. Une telle réaction est généralement susceptible d'augmenter la confusion chez les employés alors qu'ils sont censés recevoir une aide.

   L'une des alertes comprenait la transmission du message d'hameçonnage avec un lien pleinement fonctionnel.

   Nous recommandons que le processus décrit dans le document IS-DOC-A16-021 (Procédure de gestion des incidents) de l'équipe en charge de la sécurité des informations (InfoSec) fasse l'objet d'une formation en interne et, si nécessaire, soit complété par un processus spécialisé pour les attaques par hameçonnage ou les piratages. Simultanément, le personnel informatique ainsi que les autres employés devraient être formés de manière à savoir clairement quel service, équipe ou point de contact devrait informer sur ces attaques et à quel service, équipe ou point de contact signaler ces attaques.

   Si un message d'alerte est envoyé à tous les employés, nous recommandons d'y joindre une capture d'écran du courriel d'hameçonnage plutôt que de faire suivre le message lui-même. Le message devrait indiquer quoi faire si un employé a déjà cliqué sur le lien et ce que va faire le service informatique pour régler la situation.

   Outre ces recommandations de procédure, le service informatique peut également procéder à des interventions techniques pour prévenir la propagation d'une attaque après sa détection. Nous recommandons de bloquer immédiatement tous les systèmes impliqués dans un hameçonnage (expéditeur du courrier électronique, adresse IP, domaines des liens intégrés, etc.) comme mesures d'urgence afin d'empêcher la transmission de données sensibles aux pirates informatiques.

7. *Formation de sensibilisation à la cybersécurité pour tous les employés*

   Dix pour cent de tous les employés ont soumis des données.

   Nous recommandons la mise à disposition d'informations sur l'intranet ainsi qu'une formation pour tous les employés afin d'accroître la sensibilisation, à intervalles réguliers.

8. *Hausse du nombre d'évaluations des attaques par hameçonnage*

   Cinq pour cent de tous les employés déjà formés ont malgré tout transmis des données. Cela représente plus de 10% de tous les employés. L'effet positif d'une campagne de sensibilisation peut dont être reconnu.

   Nous recommandons après une formation de sensibilisation de tous les employés et la formation des membres du service informatique en matière de processus corrects de démarrer une nouvelle campagne en matière d'hameçonnage afin de rendre le succès visible.

9. *Les équipes de responsables devraient connaître les processus*

   Nous avons constaté que toutes les équipes responsables concernées par les documents relatifs aux politiques pour la certification ISO27001 sont entièrement formées. En outre, les informations ne sont pas encore partagées avec tous les employés.

   Nous recommandons la formation des équipes responsables par rapport aux documents réf.1 ainsi que le partage d'informations avec tous les employés afin d'accroître la connaissance et la sensibilisation du plus grand nombre possible.

10. *Mettre à jour les documents existants*

    L'instruction administrative (PER) nº 23.Rev 4 de mai 2009 ne reflète pas complètement la situation actuelle. Plus précisément, elle ne contient toujours pas de renseignements sur les points de contact.

    Nous recommandons de mettre à jour et de compléter le document avec les points de contact nécessaires.

Rapport de l'audit interne de mai 2020 – Suivi des recommandations

Conformément aux bonnes pratiques, un audit a spécifiquement porté sur le suivi des recommandations formulées par l'audit interne durant la période 2011–2019. Cet examen a montré que 12 des 23 recommandations de l'audit étaient appliquées en mars 2019, 1 était achevée et les 10 restantes étaient en cours de mise en œuvre.

3. Remarques finales

À la suite des décisions de la Commission 2 «Finances et administration» du Conseil d'administration prises en novembre 2014, les Pays-membres peuvent demander la consultation des rapports d'audit interne au Bureau international, conformément aux termes de la circulaire du Bureau international 61 du 11 mai 2015.

Par le biais des déclarations ci-après, l'auditeur interne BDO confirme qu'il se conforme et s'est conformé aux prescriptions en matière d'indépendance durant la période d'audit. Nous confirmons que nous avons reçu un soutien et la coopération sans réserve des personnes qui ont participé à cet audit et nous tenons à les remercier.

Berne, le 15 septembre 2020

BDO SA

Matthias Hildebrandt
Partenaire, Swiss CPA

Thomas Bigler
Responsable principal, Swiss CPA
Vérificateur en chef