Organisation de Coopération et de Développement Économiques

C(2024)81/PART2/ADD6

À usage officiel **Français - Or. Anglais**

4 novembre 2024

CONSEIL

Conseil

AUDIT DE PERFORMANCE 2023 : DÉCENTRALISATION – PHASE 2 – LA SÉCURITÉ NUMÉRIQUE AU NIVEAU DES DIRECTIONS

Synthèse

JT03554606

NAJWYŻSZA IZBA KONTROLI
COUR DES COMPTES DE LA POLOGNE

Synthèse du rapport de l'Auditeur externe

DÉCENTRALISATION – PHASE 2
LA SÉCURITÉ NUMÉRIQUE À L'ÉCHELLE DES DIRECTIONS

1. Cet audit de performance avait pour objectif d'évaluer si la sécurité numérique était bien protégée dans le cadre de la gestion décentralisée de l'Organisation en vérifiant si les politiques et mesures de contrôle correspondantes étaient appliquées de façon cohérente à l'échelle des Directions et des autres composantes de l'Organisation et si ces Directions et autres composantes auto-évaluaient dûment leur maturité dans ce domaine.

2. Pour réaliser une évaluation globale et équilibrée, l'Auditeur externe a pris en compte les résultats de ses audits antérieurs ayant un rapport avec le thème de l'audit actuel, dont l'audit consacré aux systèmes de gestion des risques (2022) et la première phase de l'audit sur la décentralisation de l'OCDE (2023).

3. Compte tenu des résultats des audits susmentionnés et de ceux de procédures d'audit complémentaires, l'Auditeur externe a décidé de s'intéresser plus particulièrement à la mise en œuvre des politiques, des lignes directrices et de la documentation opérationnelle relatives à la sécurité numérique dans les Directions de substance décentralisées, aux conséquences que l'acquisition de logiciels par ces Directions induit pour la sécurité informatique de l'ensemble de l'Organisation, et à l'Auto-évaluation que les Directions font de leur niveau de maturité pour ce qui est de la sécurité numérique.

4. Pour atteindre l'objectif général visé, le travail d'audit a principalement consisté en : l'examen des politiques, des lignes directrices et de la documentation opérationnelle pertinentes ; l'analyse des applications informatiques citées ; la prise de renseignements auprès du personnel chargé de veiller à la sécurité numérique au sein des Directions ; et la vérification par échantillonnage de certaines solutions informatiques. L'Auditeur externe s'est avant tout préoccupé de savoir si les Directions procédaient, en concertation avec EXD/DKI, à une évaluation des risques liés aux applications qu'elles utilisaient, ces applications étant intégrées au cadre de sécurité numérique de l'Organisation. L'Auditeur externe a aussi examiné les Auto-évaluations effectuées par l'ensemble des Directions pour 2023.

Évaluation générale

5. **Les récentes initiatives menées par l'OCDE dans le domaine de la sécurité numérique contribuent à renforcer cette sécurité à l'échelle des Directions et des autres composantes de l'Organisation. Les produits et services numériques, y compris les services cloud, font l'objet d'une évaluation des risques afin d'éviter tout recours à des solutions informatiques susceptibles de représenter une menace pour l'Organisation. L'exercice d'Auto-évaluation qui a été mis en place permet généralement aux parties concernées de procéder à une analyse détaillée des divers aspects de la sécurité numérique auxquels les Directions décentralisées sont chargées de veiller.**

6. **Les politiques, les lignes directrices et la documentation opérationnelle mises en œuvre aux côtés de l'exercice d'Auto-évaluation pourraient, à condition que leur potentiel soit pleinement exploité, offrir une certaine marge d'action pour surveiller la sécurité numérique, détecter et résoudre les problèmes et apporter les améliorations requises. Elles constitueraient ainsi, au sein d'une panoplie plus large d'outils, des instruments utiles à l'appui de la gestion des risques numériques au sein de l'Organisation décentralisée.**

7. **Les applications nouvellement acquises sur lesquelles a porté notre analyse ont été sélectionnées conformément à des besoins confirmés, ont été acceptées à l'issue d'une procédure régulière et devaient faire l'objet d'une évaluation des risques avant leur déploiement ainsi que durant leur phase d'utilisation. De plus, les contrats examinés comportaient des clauses relatives à la sécurité numérique. Ces constats**

montrent que les mesures de précaution idoines ont été appliquées, et qu'elles ont fait l'objet d'un suivi.

8. L'Auditeur externe constate néanmoins l'existence de plusieurs lacunes qui, s'il n'y était pas remédié, seraient susceptibles d'accroître les risques pesant sur la sécurité numérique à l'échelle des Directions. Certains ajustements sont nécessaires face aux lacunes constatées au niveau de l'évaluation des risques liés aux services cloud ainsi qu'au niveau du traitement des Auto-évaluations de sécurité numérique.

9. Bien que tous les logiciels utilisés au sein des Directions soient censés faire l'objet d'une évaluation des risques, cette évaluation, dans les faits, n'est pas systématique en ce qui concerne les services cloud. L'audit a révélé en effet que trois Directions et autres composantes de l'Organisation sur les cinq examinées n'avaient pas présenté de demande d'évaluation des risques en matière de sécurité numérique en préalable au déploiement de huit de ces services (sur 16 étudiés dans le cadre de l'audit), alors même qu'elles étaient tenues de le faire par la Politique de l'OCDE sur la sécurité dans le cadre de la conception et de l'exécution des projets et par la Politique de l'OCDE en matière d'utilisation des services cloud.

10. À cet égard, **il est recommandé de continuer de sensibiliser les dirigeants de l'Organisation et les autres membres du personnel à la sécurité numérique s'agissant du respect par les Directions de la procédure d'Évaluation des risques associés aux solutions numériques, de la procédure d'Évaluation des demandes relatives à l'utilisation des services cloud et des nouvelles mesures de sécurité relatives aux achats de solutions informatiques déployées en dehors du réseau et/ou des locaux de l'OCDE.**

11. Par ailleurs, même si les résultats de l'exercice d'Auto-évaluation sont communiqués à la hiérarchie centrale[1], celle-ci est insuffisamment informée des mesures correctives éventuellement prises par les Directions lorsque les objectifs fixés n'ont pas été atteints. Dans le cadre des procédures actuelles, les Directions sont encouragées à communiquer des commentaires ou des plans d'action à cet effet à la hiérarchie centrale, mais aucun texte ne les y oblige. Il s'en est suivi que les informations sur les lacunes et sur les mesures proposées pour améliorer la sécurité numérique qu'elles ont communiquées par le cadre de l'Auto-évaluation et adressées à la hiérarchie centrale n'étaient pas complètes.

12. À cet égard, **il est recommandé qu'au sein des Lignes directrices de l'OCDE en matière de technologies de l'information, la Procédure d'affirmation sur la sécurité numérique précise qu'il relève de la responsabilité des Directions et des autres composantes de l'Organisation de présenter, quand le niveau de maturité attendu n'est pas atteint, des plans d'action pertinents prévoyant des mesures pour remédier aux lacunes.**

13. Toutes les Directions ont préparé des Auto-évaluations pour 2023 qui indiquaient leur niveau de maturité en matière de sécurité numérique. Cependant, une des Auto-évaluations n'a pas été soumise au Cabinet du Secrétaire général. En effet, elle a été effectuée par une unité organisationnelle distincte hébergée par la Direction de la coopération pour le développement, laquelle ne l'a pas incluse dans l'Auto-évaluation qu'elle a soumise.

14. À cet égard, **il est recommandé de faire en sorte que toutes les Auto-évaluations préparées par les composantes de l'Organisation soient soumises à la hiérarchie centrale.**

[1] EXD et SGE.

15. En outre, les instructions relatives aux Auto-évaluations comportent une incohérence quant au niveau souhaité d'identification des informations sensibles et quant au degré de protection correspondant. Plus précisément, le niveau souhaité d'identification est inférieur au degré de protection des informations sensibles, ce qui est susceptible de nuire à leur bonne interprétation par les Directions.

16. À cet égard, **il est recommandé d'étudier la possibilité de fixer l'objectif de l'énoncé n° 7 (« *Les informations sensibles, notamment les données personnelles, gérées par la Direction/le Programme ont été inventoriées* ») à un niveau au moins égal à l'objectif de l'énoncé n° 8 (« *Des mesures de sécurité appropriées sont appliquées aux informations sensibles, et notamment aux données personnelles, gérées par la Direction/le Programme* »).**