Organisation des Nations Unies pour le développement industriel

Distr. générale
20 septembre 2024
Français
Original : anglais

Conseil du développement industriel
Cinquante-deuxième session
Vienne, 25-27 novembre 2024
Point 4 f) de l'ordre du jour provisoire
Gestion générale des risques

Point sur la gestion générale des risques

Rapport du Directeur général

Par sa conclusion 2016/8, le Comité des programmes et des budgets a « invité le Directeur général à faire rapport aux prochaines sessions du Conseil du développement industriel et du Comité des programmes et des budgets sur la stratégie de l'ONUDI en matière de gestion générale des risques et à proposer des mesures globales pour faire face aux conséquences financières et administratives découlant du fait que des États Membres se retirent de l'Organisation, y compris pour inverser cette tendance au retrait ».

Le présent document actualise le rapport présenté à la quarantième session du Comité (IDB.52/9-PBC.40/9), en mettant en évidence la création du Groupe de la gestion des risques et de la conformité, nouvelle entité spécialisée relevant de la Direction des services et opérations internes, ainsi que de fonctions supplémentaires liées à la cybersécurité.

I. Introduction

1. Dans l'organigramme du Secrétariat de l'ONUDI révisé en 2024 (DGB/2024/03), l'Organisation a créé le Groupe de la gestion des risques et de la conformité. Ce nouveau groupe, coordonnateur désigné pour la gestion des risques institutionnels à l'ONUDI, prête appui au Directeur principal des services et opérations internes en poursuivant la mise au point, la coordination et l'application des dispositifs de gestion des risques institutionnels et de gestion des risques liés à la sécurité de l'information. De plus, il aide activement l'équipe de direction à promouvoir une solide culture du risque. Outre la gestion des risques et la conformité, son mandat porte sur la gouvernance de la cybersécurité.

2. Le présent document met en évidence les mesures prises par l'ONUDI pour maîtriser et réduire les risques liés à la cybersécurité.

V.24-17133 (F) 161024 171024

Merci de recycler

II. Cadre de cybersécurité et améliorations

3. Pour donner suite à la recommandation formulée par le Corps commun d'inspection dans son rapport intitulé « La cybersécurité dans les entités des Nations Unies » (JIU/REP/2021/3), l'ONUDI présente un tableau complet des mesures qu'elle a mises en œuvre en lien avec son cadre de cybersécurité. Ainsi, le document de séance IDB.52/CRP.14 présente les éléments essentiels de ce cadre et les mesures prises pour protéger l'Organisation contre les cybermenaces et garantir l'adoption de pratiques de sécurité robustes.

4. L'ONUDI a sensiblement renforcé son cadre de cybersécurité, qu'elle a adapté en tenant compte des recommandations du Commissaire aux comptes et du Corps commun d'inspection ainsi que des meilleures pratiques en vigueur dans ce secteur. Elle a créé un solide socle de cybersécurité en définissant un cadre de gouvernance et en mettant en place un système de gestion de la sécurité de l'information (conforme à la norme ISO 27001) régi par sa politique de sécurité de l'information (DGB/2023/01) ainsi que par l'instruction administrative sur le processus de gestion des risques liés à la sécurité de l'information (AI/2024/01), cette dernière décrivant le processus permettant de garantir que les risques liés à la sécurité de l'information sont recensés, évalués, maîtrisés et atténués avec efficacité, sans délai et de manière structurée.

5. Il est essentiel que l'ONUDI continue, au fil de ses progrès, d'adopter une stratégie proactive face à la cybersécurité. Il s'agit notamment de réévaluer en permanence les risques, de renforcer les capacités techniques et de favoriser une culture de la sensibilisation à la cybersécurité dans l'ensemble de l'Organisation. Ce faisant, l'ONUDI sera non seulement équipée pour faire face à l'évolution des cybermenaces et protéger ses actifs informatiques, mais aussi pour mener sa mission d'ensemble avec résilience et confiance.

6. Dans le rapport du Commissaire aux comptes sur les comptes de l'ONUDI pour l'année financière allant du 1er janvier au 31 décembre 2023 (IDB.52/4-PBC.40/4), présenté à la quarantième session du Comité des programmes et des budgets, le Commissaire aux comptes a validé les progrès de l'ONUDI en matière de cybersécurité en classant les cinq recommandations concernant la création d'une fonction consacrée à la cybersécurité, la mise au point d'un système de gestion de la sécurité de l'information et la mise en œuvre d'un processus de gestion de la vulnérabilité. Les faiblesses techniques critiques recensées par le Commissaire aux comptes ont également été relevées et corrigées, et un test de pénétration de la sécurité mené en 2023 par l'ONUDI avec le concours de sociétés extérieures spécialisées a révélé de nouveaux problèmes, qui ont été pris en compte dans le plan de travail de la Division des services de transformation numérique, d'innovation et d'optimisation des activités de coopération technique. Une évaluation des risques liés à la sécurité de l'information menée en 2023 a également permis de recenser les actifs et les risques les plus importants, et donné lieu à un plan complet de traitement des risques liés à la sécurité de l'information pour 2023-2024, qui prévoit 35 activités, dont 15 sont achevées et les autres en cours d'exécution. Un tableau complet de ces activités est présenté à l'annexe du présent document. Les résultats décrits confirment l'efficacité de la fonction de cybersécurité de l'ONUDI pour recenser et maîtriser les risques de manière proactive, ainsi que pour renforcer la sécurité et la résilience de l'Organisation.

7. Le présent document est complété par le document de séance IDB.52/CRP.14, qui décrit les processus contribuant à améliorer la cyberrésilience de l'Organisation.

III. Mesure à prendre par le Conseil

8. Le Conseil est invité à prendre note des informations figurant dans le présent document.

Annexe

État d'avancement des activités prévues dans le plan de traitement des risques liés à la sécurité de l'information pour 2023-2024

Activités terminées

1. Effectuer des tests de pénétration : un prestataire extérieur a été engagé pour effectuer des tests de pénétration approfondis afin de simuler des attaques perpétrées par une personne ayant accès au réseau interne. Cela a permis de parfaire les contrôles et d'inscrire de nouvelles activités dans le plan de traitement des risques.

2. Appliquer une méthode d'authentification moderne dans Exchange Online : une méthode d'authentification moderne a été appliquée dans Exchange Online afin d'améliorer la sécurité des échanges de courrier électronique.

3. Mettre hors service le système de partage de fichiers xFiles : l'ancien système de partage de fichiers de l'ONUDI a été mis hors service et une solution de partage moderne de Microsoft 365 (OneDrive) a été mise en œuvre, qui permet de réduire la surface d'attaque.

4. Améliorer l'authentification dans Microsoft Teams : une authentification multifactorielle a été appliquée dans Teams afin d'atténuer les risques de vol de données d'identification.

5. Améliorer les politiques relatives aux mots de passe : de nouvelles procédures ont été élaborées et mises en œuvre concernant les règles en matière de mots de passe, l'octroi de droits et le contrôle de la conformité.

6. Améliorer l'authentification, l'expérience utilisateur et la sécurité : l'authentification unique a été transférée dans Azure AD de Microsoft 365, ce qui a permis d'améliorer le contrôle, la résilience et la disponibilité.

7. Appliquer l'authentification multifactorielle dans les systèmes en nuage : l'authentification multifactorielle a été activée pour tous les services utilisant l'authentification dans le nuage afin de renforcer la sécurité.

8. Outil et processus de gestion de la vulnérabilité : un outil de gestion de la vulnérabilité a été mis en place pour les ressources critiques telles que les systèmes publics, les serveurs critiques et les postes de travail des administrateurs. Un processus et une procédure supplémentaires ont également été élaborés, conformément aux recommandations du Commissaire aux comptes et aux meilleures pratiques en vigueur.

9. Améliorer le contrôle de la conformité : le contrôle de la conformité des principaux contrôles de cybersécurité a été amélioré pour les faire cadrer avec les données de référence minimales des Nations Unies et les meilleures pratiques de Microsoft.

10. Améliorer la sécurité des systèmes Microsoft 365 : l'authentification unique Seamless SSO a été appliquée dans certains systèmes Microsoft 365 de manière à améliorer l'expérience utilisateur et la sécurité.

11. Assurer une formation spécialisée en interne pour les administrateurs de ressources informatiques : une formation interdisciplinaire a été délivrée en interne aux administrateurs et des cours spécialisés dispensés aux utilisateurs à privilèges.

12. Revoir le stockage des fichiers dans les bureaux hors Siège : on a procédé à un examen des autorisations et examiné la possibilité de transférer dans Teams les fichiers partagés des bureaux hors Siège pour renforcer la sécurité.

13. Améliorer les processus et les politiques de sécurité : les processus et les politiques régissant les droits d'accès, la séparation des tâches et les configurations sécurisées ont été améliorés afin de coller davantage aux pratiques courantes.

14. Optimiser les processus de sécurité de l'information : les meilleures pratiques en vigueur en matière de sécurité de l'information ont été adoptées et adaptées afin d'optimiser les conditions de sécurité dans l'Organisation.

15. Examen de la sécurité de Teams : un examen des paramètres de sécurité et des autorisations de Teams a été effectué.

Activités en cours

16. Examiner les comptes en fonction des principes du besoin d'en connaître et du moindre privilège : les comptes à privilèges, les comptes de service et les droits d'accès au partage de fichiers font l'objet d'un examen constant et des mesures telles que le service du mot de passe pour administrateur local sont en cours d'application.

17. Mettre en œuvre Credential Guard : la fonction de sécurité Credential Guard est en cours de mise en œuvre sur les serveurs et les terminaux, le but étant de renforcer la sécurité et de réduire le risque de divulgation des données d'identification.

18. Mettre en œuvre dans l'ensemble de l'ONUDI les politiques les plus récentes en matière de mots de passe : les politiques relatives aux mots de passe et les accès privilégiés sont mis à jour en fonction des procédures actualisées en la matière.

19. Améliorer la gestion des correctifs : des mesures sont en cours pour perfectionner les processus de gestion des correctifs et de résolution des problèmes.

20. Améliorer la sécurité du système SAP : des mesures sont mises en œuvre pour donner suite aux constatations issues des audits et améliorer l'hygiène informatique dans le système SAP.

21. Améliorer le pare-feu : des améliorations sont en cours, notamment la mise en œuvre d'un modèle de sécurité Zero Trust et un examen complet de l'architecture et de la gestion du pare-feu et des politiques de sécurité.

22. Remplacer l'outil de gestion des mots de passe pour les administrateurs de ressources informatiques : l'outil obsolète de gestion des mots de passe pour les administrateurs est en cours de remplacement.

23. Évaluation de la maturité du modèle Zero Trust : une évaluation complète de la maturité du modèle Zero Trust est en cours afin d'orienter les améliorations futures.

24. Mettre hors service et remplacer les systèmes existants : des mesures sont en cours pour mettre hors service et remplacer les systèmes existants afin de réduire la surface d'attaque.

25. Améliorer les interventions en cas d'atteinte à la sécurité : les processus et les outils d'intervention en cas d'atteinte à la sécurité sont en train d'être renforcés au moyen de ressources internes et externes.

26. Examen des principaux contrôles de SAP : le contrôle de la conformité des principaux contrôles de SAP et des processus correspondants est en cours, conformément aux recommandations du Commissaire aux comptes.

27. Séparation des tâches dans la fonction informatique pour le progiciel de gestion intégré : la séparation des tâches dans la fonction informatique pour SAP est en train d'être améliorée, tant que les ressources le permettent, conformément aux recommandations du Commissaire aux comptes.

28. Comptes personnalisés pour les administrateurs : la mise en œuvre de comptes personnalisés et séparés pour les administrateurs de différents systèmes informatiques progresse.

29. Expérimenter l'authentification sans mot de passe : de nouvelles méthodes d'authentification sans mot de passe destinées à renforcer la sécurité tout en simplifiant l'accès sont en cours d'évaluation et d'expérimentation.

30. Passer en revue les fournisseurs d'accès à Internet dans les bureaux hors Siège : la qualité des services Internet dans les bureaux hors Siège et la bande passante qu'ils utilisent sont en cours d'examen.

31. Renforcer la coopération avec les partenaires extérieurs : les possibilités de collaboration avec des partenaires extérieurs sont actuellement à l'examen, le but étant de répondre aux besoins en matière de connaissances spécialisées et de sécurité.

32. Élaborer un plan de mise en application d'un modèle de sécurité Zero Trust : le plan de mise en application d'un modèle de sécurité Zero Trust cadrant avec les priorités de l'Organisation et les profils de risques est en cours d'élaboration.

33. Authentification multifactorielle pour tous les services accessibles au public : l'authentification multifactorielle pour tous les accès externes et privilégiés est en cours de mise en œuvre.

34. Améliorer la gestion et la découverte des actifs : des mesures sont en cours pour améliorer les outils de gestion et de découverte des actifs, notamment en développant l'inventaire des serveurs et en perfectionnant le déploiement des correctifs.

35. Envisager d'aménager un site de reprise des activités après un sinistre : un site secondaire de reprise après sinistre et de sauvegarde des données permettant d'assurer la continuité des activités est en cours d'aménagement.