Organisation internationale du Travail

▶ GB.346/PFA/3

Conseil d'administration

346e session, Genève, octobre-novembre 2022

Section du programme, du budget et de l'administration

PFA

Segment du programme, du budget et de l'administration

Date: 16 septembre 2022
Original: anglais

Troisième question à l'ordre du jour

Examen du cadre de cybersécurité de l'OIT

Objet du document

Le présent document donne des informations au sujet des conclusions d'une évaluation du niveau de maturité de la cyberrésilience et sur l'alignement des pratiques de l'OIT sur les piliers définis dans le rapport du Corps commun d'inspection intitulé *La cybersécurité dans les entités des Nations Unies* (voir le projet de décision au paragraphe 13).

Objectif stratégique pertinent: Sans objet.

Principal résultat: Résultat facilitateur C: Services d'appui efficients et utilisation efficace des ressources de l'OIT.

Incidences sur le plan des politiques: Aucune.

Incidences juridiques: Aucune.

Incidences financières: Aucune.

Suivi nécessaire: Aucun.

Unité auteur: Département de la gestion de l'information et des technologies (INFOTEC).

Documents connexes: Programme et budget pour la période biennale 2022-23.

▶ Introduction

1. En 2021, le Corps commun d'inspection (CCI) a établi un rapport présentant une vue d'ensemble des défis communs que pose la cybersécurité dans le système des Nations Unies [1]. D'après ce rapport, la position de force d'une organisation en matière de cybersécurité passe par l'adoption d'une approche globale au niveau de toute l'entité et recoupant plusieurs de ses domaines et compétences, dont les technologies de l'information et de la communication, la gestion du risque, la sûreté et la sécurité physiques, ainsi que la gestion de l'information et des connaissances au sens large. Le rapport énumère en outre dix éléments ou piliers qui concourent à améliorer la cyberrésilience des organismes du système des Nations Unies – en d'autres termes leur capacité à recenser, prévenir et détecter les cybermenaces ainsi qu'à répondre aux incidents et à redresser la situation (figure 1).

▶ Figure 1. Les piliers de la cyberrésilience définis par le CCI

2. Dans son rapport, la principale recommandation du CCI s'adresse aux chefs de secrétariat des organismes des Nations Unies; elle les invite à réexaminer leurs cadres de cybersécurité et à notifier leurs conclusions à leurs organes directeurs respectifs. Dans le droit fil des meilleures pratiques en vigueur, l'OIT a demandé à un organisme indépendant – le Centre international de calcul des Nations Unies – de procéder à cet examen et de rendre compte de ses conclusions. Le présent document donne un aperçu des principales conclusions et recommandations tirées de cet examen, lequel a revêtu la forme d'une évaluation du niveau de maturité de la cyberrésilience.

▶ Conclusions et recommandations

Le profil de maturité caractérisant la cybersécurité du Bureau

3. Le Bureau dispose d'une Unité des services de la sécurité et de l'assurance de l'information, dotée d'une équipe qui s'est étoffée depuis la nomination initiale, en 2007, d'un responsable de la sécurité informatique. Il a mis en place un système de gestion de la sécurité de

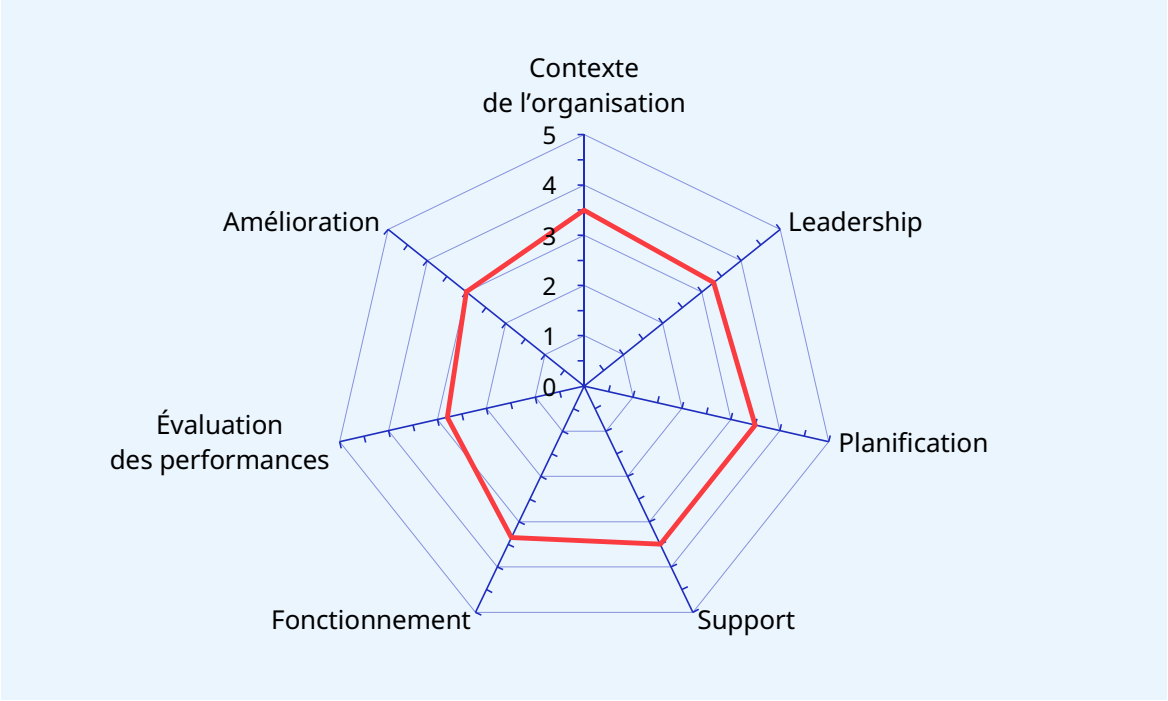
[1] Nations Unies, *La cybersécurité dans les entités des Nations Unies*, Rapport du Corps commun d'inspection, JIU/REP/2021/3, 2021.

l'information, que des experts indépendants ont certifié conforme à la norme ISO 27001 régissant la sécurité de l'information. Ladite certification ISO est reconnue dans le monde entier comme indiquant l'alignement sur les meilleures pratiques en matière de sécurité de l'information.

4. Le Centre international de calcul des Nations Unies a utilisé à la fois la norme ISO 27001 et les piliers du CCI pour effectuer sa mission d'évaluation du degré de maturité de la cyberrésilience. Les résultats ont été établis en suivant le modèle de maturité des capacités. L'évaluation a permis de définir un niveau général de maturité de 3,58 sur 5, ce qui positionne les processus de cybersécurité de l'OIT dans la moitié supérieure du niveau 3 de maturité du modèle, lequel est classé comme «défini».

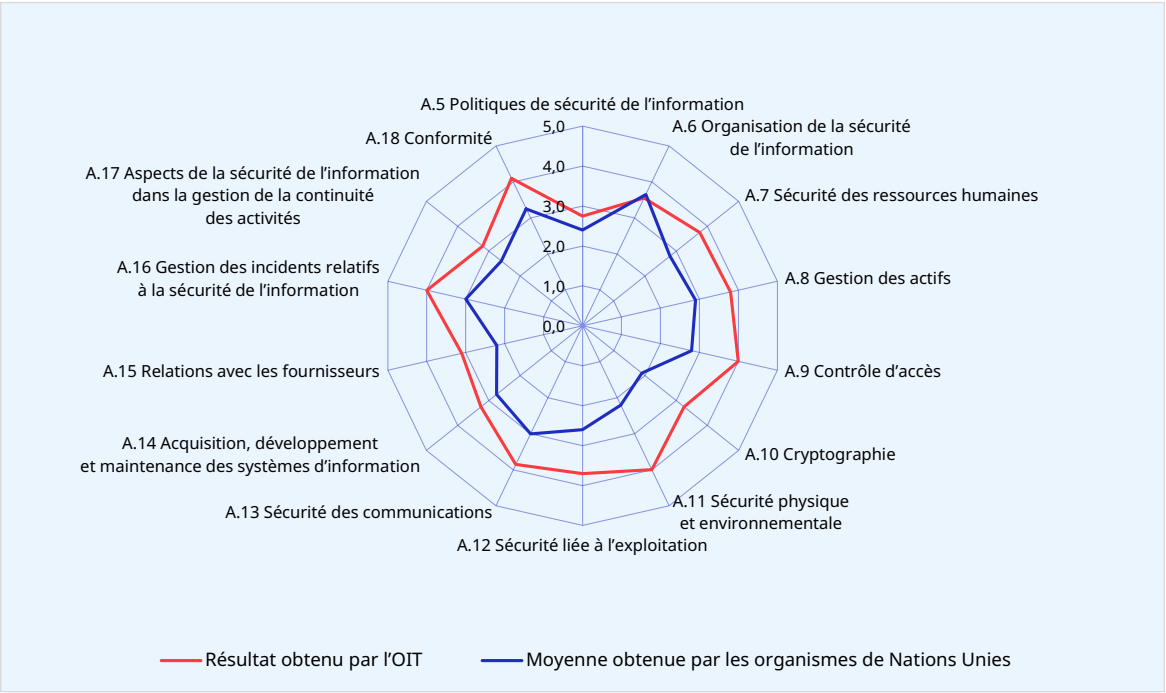
5. La figure 2 montre le niveau de maturité des grandes composantes des processus informatiques de l'OIT en fonction des domaines recensés dans la version 2013 de la norme ISO 27001 (la couleur n'est pas indicative du niveau de maturité).

▶ Figure 2. Mesure du niveau de maturité relatif à la cybersécurité de l'OIT en fonction des domaines recensés dans la norme ISO 27001



6. La figure 3 montre les conclusions établies pour l'OIT au regard des domaines de contrôle de la cybersécurité répertoriés à l'annexe A de la version 2013 de la norme ISO 27001. Une ligne symbolisant la moyenne obtenue par les autres organismes des Nations Unies soumis au même examen est représentée sur la figure et montre que l'OIT dépasse cette moyenne dans bien des domaines.

▶ Figure 3. Évaluation du niveau de maturité de la cybersécurité à l'OIT au regard des domaines de contrôle pertinents répertoriés à l'annexe A de la norme ISO 27001



7. L'évaluation du niveau de maturité de la cyberrésilience a montré que les multiples contrôles de sécurité prévus par la norme ISO 27001 ont déjà été mis en œuvre et concordent avec les recommandations que le CCI a formulées dans son rapport. Cette évaluation a en outre mis en évidence des possibilités d'améliorer encore les contrôles de cybersécurité.

8. La figure 4 illustre le degré de confomité actuel de l'OIT pour chaque contrôle de cybersécurité. Les contrôles de cybersécurité considérés comme «conformes» respectent la norme ISO 27001 relative aux bonnes pratiques du secteur. Ceux qui sont évalués comme étant «partiellement conformes» sont, dans une certaine mesure, en adéquation avec la norme ISO 27001, mais risquent de révéler une non-conformité mineure lors d'un audit de certification. Il y aurait lieu de mettre en place un plan d'atténuation visant à obtenir la certification et à la conserver. Les contrôles de cybersécurité qualifiés de «non conformes» s'écartent par trop de la norme ISO 27001 et se verraient frappés de non-conformité grave lors d'un audit de certification; ils appellent par là même une action prioritaire. Aucun des contrôles de cybersécurité en vigueur à l'OIT n'a été jugé comme relevant de cette catégorie.

9. La conformité avec les dix piliers de la cyberrésilience définis par le CCI est détaillée à l'annexe I.

▶ Figure 4. Contrôles de cybersécurité répertoriés à l'annexe A de la norme ISO 27001: degré de conformité de l'OIT

Politiques de sécurité de l'information	Organisation de la sécurité de l'information	Sécurité des ressources humaines	Gestion des actifs	Contrôle d'accès	Cryptographie	Sécurité physique et environnementale	Sécurité liée à l'exploitation	Sécurité des communications	Acquisition, développement et maintenance des systèmes d'information	Relations avec les fournisseurs	Gestion des incidents relatifs à la sécurité de l'information	Gestion de la continuité des activités	Conformité
A5.1 Orientation de la direction en matière de sécurité de l'information	A6.1 Organisation interne	A7. Avant l'embauche	A8.1 Responsabilité relative aux actifs	A9.1 Exigences métier en matière de contrôle d'accès	A10.1 Mesures cryptographiques	A11.1 Zones sécurisées	A12.1 Procédures et responsabilités liées à l'exploitation	A13.1 Gestion de la sécurité des réseaux	A14.1 Exigences de sécurité applicables aux systèmes d'information	A15.1 Sécurité de l'information dans les relations avec les fournisseurs	A16.1 Gestion des incidents relatifs à la sécurité de l'information	A17.1 Continuité de la sécurité de l'information	A18.1 Respect des obligations juridiques et contractuelles
	A6.2 Appareils mobiles et télétravail	A7.2 Pendant la durée du contrat	A8.2 Classification de l'information	A9.2 Gestion de l'accès utilisateur		A11.2 Matériels	A12.2 Protection contre les logiciels malveillants	A13.2 Transfert de l'information	A14.2 Sécurité des processus de développement et d'assistance technique	A15.2 Gestion de la prestation de services des fournisseurs		A17.2 Redondances	A18.2 Examens relatifs à la sécurité de l'information
		A7.3 Rupture, terme ou modification du contrat de travail	A8.3 Manipulation des supports	A9.3 Responsabilités des utilisateurs			A12.3 Sauvegarde		A14.3 Données de test				
				A9.4 Contrôle d'accès au système et aux applications			A12.4 Journalisation et surveillance						
							A12.5 Maîtrise des logiciels en exploitation						
							A12.6 Gestion des vulnérabilités						
							A12.7 Audit des systèmes d'information						

Contrôles conformes — Contrôles partiellement conformes — Contrôles non conformes — Contrôles non applicables

10. Si l'évaluation a généré des résultats plutôt positifs, elle a aussi donné lieu à une liste de recommandations que le Bureau pourrait suivre s'il souhaite améliorer encore sa cyberrésilience (annexe II). Comme la mise en œuvre de ces recommandations reviendrait à réaffecter des ressources du Bureau, il est proposé de mettre l'accent sur les recommandations susceptibles de générer le meilleur retour sur investissement.

11. Le Bureau propose d'actualiser son plan de communication en matière de cybersécurité afin d'y incorporer les recommandations qui pourraient favoriser l'établissement d'une feuille de route cohérente pour améliorer la cyberrésilience.

12. Chaque recommandation fera l'objet d'un examen approfondi afin de chiffrer les actions envisagées et leurs effets potentiels. Les propositions et l'estimation des coûts seront ensuite soumises, aux fins de hiérarchisation et d'orientation, au Comité de gouvernance des technologies de l'information, qui se compose de hauts fonctionnaires représentatifs des trois portefeuilles du Bureau. Compte tenu des décisions prises par le Bureau à la lumière de ces éléments d'orientation, il est proposé d'intégrer les rapports de situation dans les documents fournissant des mises à jour sur la stratégie de l'Organisation en matière de technologies de l'information, lesquels sont présentés tous les ans au Conseil d'administration.

▶ Projet de décision

13. **Le Conseil d'administration prend note des informations figurant dans le document GB.346/PFA/3 et demande au Bureau de tenir compte de ses orientations pour donner suite aux recommandations issues de l'examen du cadre de cybersécurité de l'OIT.**

▶ Annexe I

Conformité avec les piliers du CCI

Pilier 1 – Mobilisation des organes délibérants et directeurs

Orientations formulées par le CCI

- Les organes directeurs devraient formuler des orientations stratégiques de haut niveau, notamment au moyen d'une déclaration expresse d'appétence pour le risque.
- Les entités devraient mettre au point un mécanisme de communication d'informations pour recueillir et diffuser des indicateurs de cybersécurité pertinents auprès des organes directeurs, et prévoir des protocoles de remontée de l'information à suivre en cas d'attaque.

Conclusions

Dans son rapport, le CCI cite plusieurs exemples d'organismes du système des Nations Unies ayant apporté des améliorations institutionnelles aux cadres relatifs à la cybersécurité sur la base de recommandations de contrôle. Il a par ailleurs été constaté que les organes directeurs étaient mobilisés au sein du Bureau.

- Le poste de responsable de la sécurité informatique a initialement été créé sur recommandation du Conseil d'administration.
- Le Conseil d'administration est informé des cyberrisques par plusieurs moyens, notamment:
  - o des rapports sur les audits relatifs à la sécurité de l'information établis par le Bureau de l'audit interne et du contrôle;
  - o des rapports établis par le Comité consultatif de contrôle indépendant (sur la base des informations communiquées par le responsable de la sécurité de l'information);
  - o des rapports ponctuels sur les atteintes à la cybersécurité présentés au Comité de gouvernance des technologies de l'information par le responsable des systèmes d'information et, le cas échéant, au Conseil d'administration.

L'Unité des services de la sécurité et de l'assurance de l'information a en outre établi un ensemble d'indicateurs clés de risque, bien que celui-ci ne soit pas exhaustif. Le cadre de gestion des risques du Bureau mentionne la notion d'appétence pour le risque en des termes généraux. Le registre des risques stratégiques qui figure dans le Programme et budget pour la période biennale 2022-23 mentionne expressément les risques de cyberattaques contre les systèmes de l'OIT (événement à risque 8). Toutefois, les bases de référence de tolérance aux risques de cybersécurité définies pour guider les équipes opérationnelles gagneraient à être plus claires.

Recommandations

- Le Comité de gouvernance des technologies de l'information devrait préciser les niveaux de risque de cybersécurité acceptables sur la base des orientations du Conseil d'administration.
- Le Comité de gouvernance des technologies de l'information devrait être informé sur une base annuelle des problèmes, évolutions, risques et possibilités communs en matière de

sécurité de l'information, sur la base d'une analyse des tendances dans ce domaine, de rapports d'audit, des registres des risques, des évaluations des risques de sécurité de l'information, des enquêtes menées et des données incidentes.

Pilier 2 – Incorporation de la cybersécurité dans la gestion du risque institutionnel

Orientations formulées par le CCI

- Il convient de mettre davantage l'accent sur l'élaboration de mesures d'atténuation des risques efficaces et concrètes, qui devront s'accompagner d'une solide planification de la continuité des opérations.
- Les spécialistes de la cybersécurité devraient participer pleinement à la conception, à la mise en œuvre et au suivi des processus internes de gestion des risques.

Conclusions

Dans son rapport, le CCI affirme que l'incorporation formelle de la cybersécurité dans le cadre de gestion des risques d'une entité contribue à faire de cette question l'une des priorités de l'entité concernée. Le Bureau a instauré un système de gestion des risques institutionnels piloté par le responsable principal de la gestion des risques, qui relève du Trésorier et contrôleur des finances. Ce système comporte un registre des risques stratégiques qui inclut un risque relatif aux perturbations causées par les cyberattaques. Les risques de sécurité de l'information sont également pris en compte au niveau opérationnel, car le Département de la gestion de l'information et des technologies (INFOTEC) et l'Unité des services de la sécurité et de l'assurance de l'information contribuent au registre des risques. Ces risques sont en outre souvent mentionnés dans les registres des risques des bureaux de pays. Toutefois, la gestion du risque institutionnel comporte certaines limites.

- Les risques relatifs à la sécurité de l'information pourraient être davantage précisés dans le cadre du système de gestion du risque institutionnel.
- La cohérence des opérations de gestion des risques entre le siège et certains projet financés par les fonds alloués à la coopération pour le développement est limitée. Certaines responsabilités de gestion des risques sont déléguées. La gestion des risques de sécurité de l'information n'est pas homogène d'un projet de coopération pour le développement à l'autre.

Recommandation

- La gestion des risques de sécurité de l'information devrait être mieux intégrée au système de gestion du risque institutionnel, et les pratiques de gestion du risque devraient être appliquées à la gestion de la sécurité de l'information afin de faciliter l'allocation des ressources en fonction des priorités de manière à obtenir les meilleurs résultats.

  Cette recommandation est de nouveau formulée au titre du pilier 9.

Pilier 3 – Parti à tirer de la convergence entre sécurité physique et cybersécurité

Orientations formulées par le CCI

- Intégrer les cadres de gestion de la sûreté et de la sécurité physiques et de la cybersécurité dans l'architecture institutionnelle.

- Renforcer les capacités en matière de cybersécurité au sein de la fonction de sûreté et de sécurité physiques.

Conclusions

Dans son rapport, le CCI fait observer que la frontière entre sécurité physique et cybersécurité est floue. En effet, les systèmes d'information et de communication sont de plus en plus utilisés pour garantir la sécurité physique, et les incidents de sécurité sont parfois dans le même temps des atteintes à la sécurité physique et des atteintes à la cybersécurité. Ceci étant, au sein du Bureau, la sphère physique et la sphère «cyber» demeurent généralement traitées comme deux sphères distinctes.

- La sécurité physique est gérée par le Département de l'administration et des services internes (INTSERV), conformément aux politiques du système de gestion de la sécurité des Nations Unies.
- La cybersécurité est gérée par l'Unité des services de la sécurité et de l'assurance de l'information, conformément à la norme ISO 27001.

Chaque équipe réalise de multiples contrôles dans le domaine qui relève de sa compétence, et INTSERV collabore avec INFOTEC dans le cadre des contrôles de la gestion de l'identité et de l'accès. Une lacune a toutefois été constatée, qui résulte du fait que les deux domaines se recoupent et du faible niveau d'expertise en matière de cybersécurité au sein de l'équipe d'INTSERV: la conformité du réseau des dispositifs de l'Internet des objets [1] aux normes de cybersécurité n'a pas été évaluée.

Recommandation

- Une évaluation des risques et un test de sécurité du réseau de l'Internet des objets devraient être réalisés.

Pilier 4 – Élaboration de cadres réglementaires pour le respect des règles et la responsabilisation

Orientations formulées par le CCI

- Mettre au point un mode d'expression et des messages simples, non techniques et engageants qui visent à faire comprendre de manière concrète les conséquences que peut avoir un cybercomportement à risque.

[1] Réseau opérationnel composé des capteurs et des dispositifs permettant d'automatiser et de gérer certaines des opérations quotidiennes de gestion des biens et des installations de l'OIT.

- Renforcer la responsabilisation individuelle en cas d'incidents causés par une mauvaise hygiène informatique. Trouver des moyens équilibrés de gérer la non-conformité qui soient proportionnés à la gravité de l'infraction, afin d'encourager les individus à assumer la responsabilité de leurs pratiques à risque.

Conclusions

Dans son rapport, le CCI note que des références à la cybersécurité devraient être incluses dans les documents de stratégie, d'orientation générale, de procédure et d'orientation technique. C'est le cas à l'OIT, comme relevé pendant l'évaluation du niveau de maturité de la cyberrésilience.

- L'Unité des services de la sécurité et de l'assurance de l'information se réfère à la norme ISO 27001 dans le cadre du système de gestion de la sécurité de l'information mis en œuvre.
- La série de documents relatifs au système de gestion de la sécurité de l'information couvre toute une gamme de domaines de contrôle technique. Toutefois, certains documents pourraient être revus plus souvent, et des parties prenantes interrogées semblent éprouver des difficultés à comprendre les documents. Les membres du personnel n'ont pas tous également conscience de la valeur des données et de la gravité des atteintes à la cybersécurité. De ce fait, la mise en œuvre des contrôles de cybersécurité et des processus de cybersécurité à l'échelle de l'Organisation n'est pas cohérente. De surcroît, il a été avancé que les recommandations issues des évaluations de la sécurité de l'information n'étaient pas toujours appliquées avec la même rigueur que les recommandations d'audit.
- Les procédures disciplinaires normalisées utilisées par les ressources humaines dans le système des Nations Unies pour sanctionner les membres du personnel qui enfreignent les politiques et les normes sont suivies à l'OIT. Toutefois, les activités de sensibilisation ont été menées de manière irrégulière pendant la pandémie. Ces activités devront reprendre sur une base régulière pour permettre une meilleure compréhension des responsabilités individuelles.
- Certains responsables de systèmes, y compris dans le cadre de projets de coopération pour le développement, choisissent de ne pas se conformer aux politiques et normes de sécurité de l'information mises en place par l'Unité des services de la sécurité et de l'assurance de l'information.
- L'OIT dispose d'un certain nombre de mécanismes de gestion et de traitement de signalements de manquements graves, ainsi que d'un cadre pour la protection des lanceurs d'alerte, mais les signalements relatifs à la cybersécurité ne sont généralement pas couverts. L'OIT a également une capacité de suivi et de traitement des incidents, mais celle-ci est principalement axée sur les atteintes à la sécurité liées à la technologie.

Recommandations

- Un programme devrait être mis en place à l'échelle de l'Organisation pour renforcer la culture de la sécurité de l'information de l'OIT. Un tel programme devrait prévoir:
  - o les mesures que peuvent prendre les directeurs pour établir des modèles de bonnes pratiques en matière de cybersécurité;

- une communication ciblée reposant sur un mode d'expression non technique et engageant, permettant aux individus de comprendre facilement quelles peuvent être les conséquences d'un cybercomportement à risque;
- des activités de sensibilisation à la sécurité de l'information adaptées aux fonctions;
- des contrôles de la responsabilisation établissant clairement les responsabilités individuelles dans la préservation d'une bonne hygiène informatique.

Cette recommandation est également valable pour les piliers 6, 7 et 8, compte tenu des conclusions formulées au titre de ces piliers.

- Des directives et listes de contrôle fondées sur les risques en matière de sécurité devraient être élaborées pour aider les responsables des projets de coopération pour le développement à comprendre comment protéger leurs données et leurs systèmes au regard de l'appétence pour le risque convenue. Des points de vérification relatifs à la sécurité devraient être intégrés (et des bases de référence minimales en matière de sécurité, formalisées) dans les cadres d'acquisition, de développement et de maintenance des systèmes.

Cette recommandation est également valable pour le pilier 7, compte tenu des conclusions formulées au titre de ce pilier.

Pilier 5 – Mise à profit des contributions des mécanismes de contrôle

Orientations formulées par le CCI

- Élaborer des procédures pour faire en sorte que les connaissances et l'expérience des spécialistes de la cybersécurité au sein d'une organisation puissent systématiquement éclairer et alimenter le travail de la fonction de contrôle.

Conclusions

Le rapport du CCI comporte plusieurs exemples d'améliorations de la cybersécurité apportées sur la base de recommandations de contrôle, lesquels démontrent l'utilité de celles-ci. Le Bureau maintient des fonctions de contrôle, notamment celles décrites ci-après.

- Le contrôle opérationnel est effectué au moyen du suivi des indicateurs clés de risque, des enquêtes et des rapports sur les incidents de l'Unité des services de la sécurité et de l'assurance de l'information, et par la mise en œuvre du cadre de gestion des risques.
- Le contrôle stratégique est effectué au moyen des analyses de gestion du Comité de gouvernance des technologies de l'information, de l'examen du plan de travail de l'Unité des services de la sécurité et de l'assurance de l'information réalisé par le directeur des systèmes d'information, et de l'examen de la stratégie en matière de technologies de l'information et des rapports d'audit, d'évaluation et de contrôle auquel procède le Conseil d'administration. Si l'Unité des services de la sécurité et de l'assurance de l'information contribue souvent à ces fonctions de contrôle stratégique, il n'existe aucune procédure opérationnelle documentée permettant de garantir sa participation cohérente et efficace aux examens.

- Les audits indépendants sont réalisés par:
  - o des auditeurs externes – un auditeur indépendant est sollicité pour faciliter l'obtention de la certification ISO 27001 pour le système de gestion de la sécurité de l'information. Toutefois, la sécurité de l'information en ce qui concerne les systèmes d'information et de communication non gérés par l'Unité des services de la sécurité et de l'assurance de l'information ne relève pas du champ des audits;
  - o des auditeurs internes – le Bureau de l'audit interne et du contrôle réalise chaque année deux à trois audits de la sécurité de l'information. Les domaines d'audit sont sélectionnés sur la base d'une approche fondée sur l'analyse des risques. Par ailleurs, des tests de pénétration sont effectués conjointement par le Bureau de l'audit interne et du contrôle et des consultants extérieurs. Le dernier en date a été réalisé en 2019, et un autre est prévu pour 2022.

Recommandation

- Il conviendrait de mettre au point des indicateurs clés de performance supplémentaires pour mesurer l'efficacité des contrôles de cybersécurité et de la gestion des activités de résolution des problèmes, et d'en assurer le suivi.

Pilier 6 – Établissement d'une culture de la cybersécurité du sommet à la base

Orientations formulées par le CCI

- Faire en sorte que l'équipe de direction soit consciente des conséquences que peuvent avoir l'inaction et une mauvaise hygiène informatique, ainsi que des risques associés.
- Instaurer progressivement une culture dans laquelle la survenance d'un incident serait considérée non pas comme un échec, mais comme un point de départ pour résoudre un problème commun et mieux protéger l'entité concernée.

Conclusions

Dans son rapport, le CCI constate que la prise de conscience et la responsabilisation de la direction exécutive est un point de départ, et que la direction doit encourager la prise en compte des erreurs et des vulnérabilités.

L'équipe de direction du Bureau est tenue informée des risques et des problèmes de cybersécurité par divers canaux d'information (voir pilier 5). La création de l'Unité des services de la sécurité et de l'assurance de l'information, l'appui en faveur de la certification du système de gestion de la sécurité de l'information, et l'approbation des politiques, normes et procédures relatives à la cybersécurité attestent de la mobilisation de la direction sur cette question.

Malgré la mise en place de l'Unité des services de la sécurité et de l'assurance de l'information et d'équipes d'appui (par exemple dans les domaines de la gestion du risque institutionnel, de la continuité des activités, de la gouvernance informatique et de l'audit interne et du contrôle), des difficultés continuent de se poser au sein du Bureau et affaiblissent son dispositif de cybersécurité.

De surcroît, même si la direction est aussi favorable aux moyens non monétaires de faire évoluer la culture et les comportements grâce à des campagnes de simulation d'hameçonnage et prend une part active aux initiatives relatives à la cybersécurité (audits externes, par exemple), il lui est toujours possible d'aller plus loin, en participant de manière visible à d'autres programmes de sensibilisation.

Recommandations

- Un examen global des ressources allouées à la sécurité de l'information et des responsabilités y relatives dans l'Organisation devrait être réalisé en vue d'améliorer la mise en conformité avec les contrôles de sécurité existants et de garantir une plus grande cohérence entre la sécurité de l'information et la gestion des risques.

  Cette recommandation est également valable pour le pilier 9, compte tenu des conclusions formulées au titre de ce pilier.

- Un programme devrait être mis en place à l'échelle de l'Organisation pour renforcer la culture de la sécurité de l'information de l'OIT, comme recommandé au titre du pilier 4.

Pilier 7 – Adoption d'une démarche à l'échelle de l'entité

Orientations formulées par le CCI

- Décentraliser et déléguer des responsabilités au profit des responsables intermédiaires.
- Définir les cyberresponsabilités propres à chaque rôle et organiser des formations et des activités de sensibilisation à la cybersécurité adaptées aux fonctions.

Conclusions

Dans son rapport, le CCI rappelle qu'il est de plus en plus admis que la cybersécurité est davantage qu'une question d'informatique. Au sein du Bureau, l'Unité des services de la sécurité et de l'assurance de l'information et INFOTEC ne sont pas les seuls à avoir des responsabilités en matière de sécurité de l'information, même si la décentralisation des responsabilités comporte certaines limites.

- Les questions de cybersécurité ne sont pas intégrées aux processus de travail des équipes. Ainsi:
  - l'intégration des contrôles de cybersécurité aux procédures de gestion des programmes et des projets est limitée, de sorte que les contrôle de sécurité sont menés de manière incohérente d'un projet ou d'une équipe à l'autre;
  - les processus relatifs à la cybersécurité sont mis en œuvre de manière hétérogène par les bureaux de pays.
- Une formation minimale à la cybersécurité tenant compte des différents rôles est dispensée à l'ensemble du personnel.

Recommandations

- Un programme devrait être mis en place à l'échelle de l'Organisation pour renforcer la culture de la sécurité de l'information de l'OIT, comme recommandé au titre du pilier 4.
- Des directives et listes de contrôle fondées sur les risques en matière de sécurité devraient être élaborées pour aider les responsables des projets de coopération pour le développement, comme recommandé au titre du pilier 4.

Pilier 8 – Importance du personnel en tant que première ligne de défense

Orientations formulées par le CCI

- Veiller à ce que chaque membre du personnel acquière les compétences numériques de base et donner aux utilisateurs les moyens de contribuer activement à améliorer la cyberrésilience.
- Mettre au point un programme de formation et de sensibilisation assorti d'objectifs clairement définis pour chaque catégorie de parties prenantes, selon les risques que ces objectifs présentent pour l'entité.

Conclusions

L'importance du «facteur humain» s'agissant de la cybersécurité est de mieux en mieux comprise, et le fait que les utilisateurs finals sont de plus en plus pris pour cibles est globalement reconnu. Conscient que les utilisateurs doivent être suffisamment vigilants pour constituer la première ligne de défense, le Bureau fait obligation à tout le personnel de suivre une formation de base comportant un volet sur la sécurité de l'information. D'autres activités de communication et de sensibilisation ponctuelles (par exemple des campagnes de simulation d'hameçonnage, mentionnées dans les conclusions relatives au pilier 6, et la diffusion d'alertes en cas de menace) contribuent à rendre les utilisateurs plus vigilants.

Certaines limites peuvent toutefois réduire les niveaux actuels de vigilance.

- Le taux d'achèvement de la formation de base est élevé, mais cela ne suffit pas à garantir un changement des comportements.
- Tout le personnel ne bénéficie pas d'une formation régulière et d'une formation adaptée aux fonctions (voir piliers 4 et 7).

Recommandation

- Un programme devrait être mis en place à l'échelle de l'Organisation pour renforcer la culture de la sécurité de l'information de l'OIT, comme recommandé au titre du pilier 4.

Pilier 9 – Affectation optimale de ressources financières à la cybersécurité

Orientations formulées par le CCI

- Déterminer comment allouer les ressources consacrées à la cybersécurité le plus utilement possible.
- Relier les investissements en matière de cybersécurité aux exigences opérationnelles et aux pratiques saines de gestion des risques afin d'éviter un afflux ou une insuffisance de ressources dans des domaines clés.

Conclusions

Dans son rapport, le CCI note que, malgré l'augmentation des ressources allouées à la cybersécurité, le sentiment que les moyens ne sont pas suffisants continue de faire obstacle à la prise en charge de tous les aspects de la cyberrésilience. Il ressort d'échanges avec l'équipe de direction du BIT que l'inadéquation des ressources compromet les progrès concernant certaines activités et contribue de ce fait à affaiblir la cybersécurité dans plusieurs domaines, tels que la gestion des actifs, la gestion des vulnérabilités, la gouvernance des projets de

coopération pour le développement, la gouvernance des données et le suivi de certains aspects de la gestion de la sécurité de l'information.

Recommandations

- Un examen global des ressources allouées à la sécurité de l'information et des responsabilités y relatives dans l'Organisation devrait être réalisé, comme recommandé au titre du pilier 4.
- La gestion des risques de sécurité de l'information devrait être mieux intégrée au système de gestion du risque institutionnel, et les pratiques de gestion du risque devraient être appliquées à la gestion de la sécurité de l'information afin de faciliter l'allocation des ressources en fonction des priorités de manière à obtenir les meilleurs résultats, comme recommandé au titre du pilier 2.

Pilier 10 – Investissement dans des ressources humaines spécialisées

Orientations formulées par le CCI

- Conserver les capacités internes spécialisées en cybersécurité [2].

Conclusions

De nombreux organismes des Nations Unies se sont dotés de capacités en ressources humaines spécialisées dans le domaine de la cybersécurité. C'est le cas de l'OIT.

- Le Bureau a nommé un responsable de la sécurité de l'information à temps plein qui dirige les spécialistes de la cybersécurité de l'Unité des services de la sécurité et de l'assurance de l'information. Les responsabilités de ces spécialistes ont évolué au fil du temps et incluent à la fois des opérations de sécurité et la gouvernance de la cybersécurité.
- L'Unité des services de la sécurité et de l'assurance de l'information fait aussi appel à des spécialistes extérieurs de la cybersécurité, qui fournissent des services supplémentaires dans le domaine de la sécurité de l'information, notamment en matière de renseignements sur les menaces, de suivi de la sécurité, de gestion des incidents et de test de la pénétration [3].

Dans son rapport, le CCI souligne qu'il est important de garantir que les considérations de cybersécurité peuvent être exprimées et entendues par les décideurs compétents, sans restriction, indépendamment de l'entité organisationnelle responsable de la cybersécurité – qu'il s'agisse ou non du département de l'information et de la communication.

Le responsable de la sécurité de l'information et l'Unité des services de la sécurité et de l'assurance de l'information ont toute latitude pour communiquer aux décideurs compétents leurs avis sur les questions de cybersécurité. Ceci étant, il est sans doute possible de faire en sorte que les aspects relatifs à la cybersécurité soient plus utilement pris en compte dans d'autres cadres institutionnels, tels que ceux ayant trait à la gestion du risque institutionnel, à la gestion de l'information et des connaissances, à la sûreté et à la sécurité physiques, et au contrôle.

[2] Il faudrait prévenir les conflits d'intérêts lorsque l'équipe chargée du contrôle est distincte et indépendante de l'équipe chargée de fournir des services de cybersécurité.

[3] Une entreprise extérieure gère le centre d'exploitation du réseau et le centre de sécurité pour le compte du Bureau.

▶ Annexe II

Feuille de route pour une meilleure cyberrésilience

Pilier du CCI	Recommandation
1	Le Comité de gouvernance des technologies de l'information devrait préciser les niveaux de risque de cybersécurité acceptables sur la base des orientations du Conseil d'administration.
1	Le Comité de gouvernance des technologies de l'information devrait être informé sur une base annuelle des problèmes, évolutions, risques et possibilités communs en matière de sécurité de l'information, sur la base d'une analyse des tendances dans ce domaine, de rapports d'audit, des registres des risques, des évaluations des risques de sécurité de l'information, des enquêtes menées et des données incidentes.
2, 9	La gestion des risques de sécurité de l'information devrait être mieux intégrée au système de gestion du risque institutionnel, et les pratiques de gestion du risque devraient être appliquées à la gestion de la sécurité de l'information afin de faciliter l'allocation des ressources en fonction des priorités de manière à obtenir les meilleurs résultats.
3	Une évaluation des risques et un test de sécurité du réseau de l'Internet des objets devraient être réalisés.
4, 6, 7, 8	Un programme devrait être mis en place à l'échelle de l'Organisation pour renforcer la culture de la sécurité de l'information de l'OIT.
4, 7	Des directives et listes de contrôle fondées sur les risques en matière de sécurité devraient être élaborées pour aider les responsables des projets de coopération pour le développement à comprendre comment protéger leurs données et leurs systèmes.
5	Il conviendrait de mettre au point des indicateurs clés de performance supplémentaires pour mesurer l'efficacité des contrôles de cybersécurité et de la gestion des activités de résolution des problèmes et d'en assurer le suivi.
6, 9	Un examen global des ressources allouées à la sécurité de l'information et des responsabilités y relatives dans l'Organisation devrait être réalisé.