Rapport d'audit

Audit des

contrôles généraux des technologies de l'information du Secrétariat du Fonds mondial

GF-OIG-25-016
22 décembre 2025
Genève, Suisse

LE FONDS MONDIAL
Bureau de l'Inspecteur général

Qu’est-ce que le Bureau de l’Inspecteur général ?

Le Bureau de l’Inspecteur général (BIG) protège les actifs, les investissements, la réputation et la pérennité du Fonds mondial en veillant à ce qu’il prenne les bonnes mesures pour accélérer la fin des épidémies de sida, de tuberculose et de paludisme. Grâce à des audits, des enquêtes et des travaux consultatifs, le BIG promeut les bonnes pratiques, améliore la gestion des risques et rend compte des abus en toute exhaustivité et transparence.

Le BIG est une unité indépendante du Fonds mondial, qui en fait néanmoins partie intégrante. Il rend compte au Conseil d’administration par l’intermédiaire de son Comité de l’Audit et des Finances, et sert les intérêts de toutes les parties prenantes du Fonds mondial.

Courriel :
hotline@theglobalfund.org

Table des matières

1. Synthèse

1.1 Avis

Les contrôles généraux des technologies de l'information sont des politiques, des procédures et des activités fondatrices qui assurent l'intégrité, la confidentialité et la disponibilité des systèmes et des données informatiques. Depuis le lancement de la seconde phase de la transformation des technologies de l'information en 2019, les solutions et les systèmes informatiques ont fait l'objet d'une amélioration continue garantissant un meilleur alignement sur les principales priorités et exigences opérationnelles. De solides contrôles généraux des technologies de l'information sont essentiels pour atténuer les principaux risques dans ce domaine, notamment la perturbation des services informatiques, la perte ou la corruption de données, les menaces de cybersécurité et l'accès non autorisé à des informations confidentielles. Le présent audit du BIG complète les contrôles externes déjà réalisés à la demande de la direction des Technologies de l'information. Ces contrôles comprennent notamment les travaux de l'auditeur externe du Fonds mondial et les examens réguliers de ses certifications ISO[1].

Le Secrétariat du Fonds mondial a mis en place des procédures, des processus et des outils complets pour encadrer les domaines clés des contrôles généraux des technologies de l'information tout au long du cycle de vie des services informatiques. Ces domaines comprennent la gestion des accès, la gestion du changement, la sécurité des données, la sécurité des réseaux et les opérations informatiques. Au sein du Département des Technologies de l'information, des équipes spécialisées sont chargées de superviser, coordonner et gérer ces contrôles. En réponse à l'évolution rapide du paysage informatique et aux nouvelles menaces, le service informatique améliore continuellement la conception des contrôles généraux des technologies de l'information. Ces efforts s'appuient sur les résultats des contrôles internes et externes menés régulièrement, ainsi que sur une évaluation continue des risques. La conception des contrôles généraux des technologies de l'information est jugée **efficace** pour atténuer les principaux risques liés aux technologies de l'information.

Les contrôles généraux des technologies de l'information sont mis en œuvre et suivis de manière efficace dans la plupart des domaines. Les opérations informatiques prévoient des sauvegardes régulières des données permettant une récupération rapide. Une solide gestion des fournisseurs de services informatiques est en place pour atténuer les risques liés à l'externalisation de systèmes informatiques clés et d'activités informatiques essentielles. La résolution rapide des incidents informatiques contribue à la continuité du fonctionnement des services informatiques. Par ailleurs, des contrôles critiques pour la gestion des risques liés aux changements de système contribuent à maintenir la disponibilité et la résilience des systèmes informatiques. Le Département des Technologies de l'information met également en place de nombreux contrôles et garde-fous afin d'assurer la sécurité et la fiabilité du trafic sur le réseau tout en assurant une protection contre les menaces de cybersécurité.

De solides contrôles et procédures de sécurité des données sont en place pour plusieurs systèmes informatiques. En ce qui concerne la gestion des accès des utilisateurs, le système supprime correctement les accès à la date de fin du contrat enregistrée dans Workday. Par conséquent, la conception et l'efficacité opérationnelle des contrôles généraux des technologies de l'information

[1] Les normes ISO sont des normes mondialement reconnues dans des domaines spécifiques. En 2025, le Fonds mondial a renouvelé avec succès sa certification ISO dans trois domaines des technologies de l'information : ISO 27001 (Système de management de la sécurité de l'information), ISO 22301 (Système de management de la continuité d'activité) et ISO 20000 (Système de management des services informatiques).

destinés à préserver la confidentialité, l'intégrité et la disponibilité des données et des systèmes sont **efficaces**.

Cependant, la capacité des contrôles à atteindre leur objectif global est compromise par leur dépendance à l'égard de processus opérationnels manuels. Le départ des consultants n'est notifié aux Ressources humaines que tardivement par les départements qui les recrutent. En conséquence, le compte des consultants[2] reste actif après qu'ils ont quitté l'organisation, ce qui augmente le risque d'accès non autorisé aux données et aux systèmes. Ce problème a été soulevé par les structures de contrôle externe au cours des années précédentes. De même, les restrictions d'accès aux documents reposent sur la bonne application des étiquettes de confidentialité par les utilisateurs. Notre examen a permis de constater que plusieurs documents confidentiels sont largement accessibles sur l'intranet, car les utilisateurs n'ont pas apposé les étiquettes requises. Par conséquent, les processus opérationnels d'appui ne sont que **partiellement efficaces** pour préserver la confidentialité, l'intégrité et la disponibilité des données et des systèmes.

1.2 Principales réalisations et bonnes pratiques

Les contrôles de gestion des accès fonctionnent généralement bien tout au long du cycle de vie des comptes d'utilisateurs

Le Secrétariat du Fonds mondial a établi des contrôles de gestion des accès afin de protéger les données et les systèmes contre tout accès non autorisé par le biais de comptes d'utilisateurs. Les contrôles permettant de créer de nouveaux comptes d'utilisateurs et d'attribuer des droits d'accès sont bien conçus et efficaces. L'authentification multifacteur[3] est appliquée de manière systématique pour tous les comptes d'utilisateurs internes afin de réduire les risques d'accès non autorisés. Les droits d'accès des utilisateurs, y compris les droits des comptes privilégiés[4], font l'objet d'examens périodiques par les propriétaires des systèmes qui garantissent une séparation adéquate des tâches, en accord avec les rôles et responsabilités des utilisateurs. Les comptes des anciens employés du Fonds mondial sont rapidement désactivés lors de leur départ.

Les contrôles de sécurité des données sont solides dans les principaux systèmes informatiques utilisés au sein du Secrétariat

Le Département des Technologies de l'information du Fonds mondial a mis en place plusieurs contrôles pour préserver l'intégrité et la confidentialité des données, notamment des méthodes d'authentification forte qui bloquent l'accès non autorisé aux comptes d'utilisateurs. Afin de tenir compte du niveau de sensibilité variable des données, le service informatique a établi des procédures pour classer les informations en quatre catégories basées sur le risque. Un étiquetage appliqué automatiquement aux documents Microsoft Office et aux courriels Outlook régule le partage des données.

Les applications métier appliquent des restrictions d'accès aux données en fonction des rôles et des autorisations d'accès des utilisateurs. En outre, le service informatique met en œuvre une méthode

[2] Les consultants peuvent être des professionnels envoyés par des agences d'intérim, des prestataires de services de paie et/ou des consultants indépendants travaillant avec le Fonds mondial. Ils peuvent également appartenir à des prestataires de services engagés par le Fonds mondial pour effectuer un travail spécifique. Selon la nature de leur travail, le service qui les recrute peut décider de leur allouer un compte utilisateur interne pour leur permettre d'accéder plus facilement aux ressources du Fonds mondial. À la fin de leur contrat ou en cas de remplacement, de compte d'utilisateur qui leur a été attribué doit être désactivé.

[3] L'authentification multifacteur exige que les utilisateurs définissent des mots de passe forts (notamment quant à leur complexité ou leur date d'expiration) reposant sur un facteur d'authentification supplémentaire, comme un code de vérification envoyé par SMS, par appel vocal ou à travers l'application Microsoft Authenticator.

[4] Un compte privilégié est un compte d'utilisateur ou un compte système qui dispose de droits d'accès et d'autorisations supérieurs à ceux d'un compte d'utilisateur standard, ce qui permet d'y exécuter des fonctions administratives sensibles (comme gérer les droits d'accès d'autres utilisateurs).

de chiffrement conforme aux meilleures pratiques du secteur afin de garantir que les données transmises sur les réseaux et stockées dans les bases de données restent illisibles pour les personnes ou les systèmes non autorisés, préservant ainsi la confidentialité et l'intégrité des données.

Contrôles et mesures solides pour renforcer la sécurité du réseau contre les menaces de cybersécurité

Le Fonds mondial a mis en place des contrôles solides afin de protéger ses actifs contre les menaces extérieures, en particulier les cyberattaques. Ces contrôles sont appliqués systématiquement aux principaux points d'entrée, notamment les périphériques réseau, les serveurs, les terminaux et les interfaces utilisateur. Parmi les principales mesures figurent des routeurs et des pare-feu correctement configurés, une segmentation efficace du réseau, une formation régulière des utilisateurs pour les sensibiliser aux questions de cybersécurité, l'installation ou la mise à jour de logiciels antivirus et de correctifs sur les terminaux (p. ex. les ordinateurs portables et les téléphones mobiles), ainsi qu'une surveillance et une gestion continues des vulnérabilités du système et du réseau.

Des contrôles adéquats sont appliqués de manière systématique pour garantir la sécurité des changements apportés aux systèmes informatiques

Une mauvaise gestion du changement peut introduire des vulnérabilités et des problèmes opérationnels. Des contrôles adéquats sont appliqués de manière systématique pour garantir que les changements apportés aux systèmes informatiques sont sûrs et ne compromettent pas l'intégrité des données ou la disponibilité des systèmes.

Les opérations informatiques sont gérées correctement afin de garantir la disponibilité des services informatiques

Le service informatique a élaboré et mis en œuvre des procédures adéquates pour s'assurer que les contrôles des opérations informatiques sont efficaces et garantissent la disponibilité permanente des systèmes et des données informatiques. Ces procédures comprennent notamment la sauvegarde régulière des données, la centralisation des incidents informatiques et leur résolution rapide, ainsi que des processus structurés pour engager des fournisseurs de services informatiques et gérer le suivi et la fin de leur contrat.

Le système informatique du Fonds mondial fait l'objet de plusieurs évaluations indépendantes qui contribuent à son renforcement continu

Tous les trois ans, trois certifications ISO du Fonds mondial font l'objet d'un examen : ISO 27001 (Système de management de la sécurité de l'information), ISO 20000 (Système de management des services informatiques) et ISO 22301 (Système de management des services informatiques). Ces examens sont menés par un organisme de certification indépendant et fournissent des assurances quant à la conception et à l'efficacité opérationnelle des contrôles généraux des technologies de l'information décrits ci-dessus. L'auditeur externe du Fonds mondial procède chaque année à un examen des contrôles généraux des technologies de l'information ciblé sur les contrôles de gestion du changement, des opérations informatiques et de gestion des accès. Tous ces examens favorisent un environnement d'apprentissage, car ils permettent de mettre en évidence les problèmes à un stade précoce afin de les résoudre et d'améliorer les contrôles existants.

Les rapports de contrôles des systèmes et de l'organisation[5] (SOC, pour *System and Organization Controls*) de type 2 des principaux fournisseurs de services cloud du Fonds mondial – y compris les rapports concernant la sécurité et la maintenance du réseau, le système de gestion des subventions, l'application de paiement et le système de passation directe des marchés – sont examinés chaque année. Il ressort de ce contrôle supplémentaire que le Fonds mondial passe des contrats avec des fournisseurs de services appliquant des contrôles rigoureux pour garantir la disponibilité des services et préserver l'intégrité et la confidentialité des données de leurs clients, y compris celles du Fonds mondial.

1.3 Principaux problèmes et risques

Le manque de consistance dans la classification des données sur SharePoint[6] permet un accès non autorisé à des données personnelles et confidentielles

Un volume important d'informations stockées dans des dossiers SharePoint n'est pas protégé de manière adéquate. Actuellement, tout employé ou consultant disposant d'un compte interne au Fonds mondial peut accéder à des documents dont l'accès devrait être restreint, notamment des informations personnelles identifiables (qui permettent d'identifier directement un individu), les coordonnées de parties prenantes externes, des données sur la santé du personnel et des communications confidentielles.

Le non-respect par les utilisateurs des protocoles de classification des données et des contrôles techniques disponibles, l'automatisation insuffisante des contrôles d'accès (en particulier pour les fichiers PDF), l'inconsistance des pratiques de restriction des données dans les différents services et l'absence de contrôle de la conformité sont à l'origine du problème. Pour y remédier, le Département des Technologies de l'information a mené une formation sur la classification des données en vue d'en renforcer la protection. En coordination avec d'autres départements et divisions, le Département des Technologies de l'information prend des mesures pour réguler les accès dans SharePoint.

Les départements ne préviennent pas les Ressources humaines du départ de leurs consultants, ce qui conduit à un maintien prolongé de leurs accès aux systèmes au-delà de la date de fin de contrat

Les normes de sécurité informatique telles que la norme ISO 27001 exigent la désactivation immédiate des comptes d'utilisateurs lors du départ d'un employé ou d'un consultant afin d'empêcher tout accès non autorisé et de réduire le risque d'exploitation d'un compte dormant. Le BIG a constaté que 23 % des comptes de consultants dont le contrat a pris fin entre janvier et juin 2025 ont été désactivés avec un retard allant de 14 à 68 jours. Huit consultants ont accédé à leur compte après leur date officielle de départ.

Ce problème récurrent, déjà mis en évidence par l'auditeur externe du Fonds mondial, découle d'une coordination insuffisante entre les responsables des services recruteurs et le Département des Ressources humaines. Si aucune faille de sécurité n'a été signalée à ce jour, la désactivation en temps utile des comptes est essentielle pour protéger les systèmes et les données.

[5] Un rapport de contrôles des systèmes et de l'organisation (SOC) de type 2 est un audit indépendant qui examine le fonctionnement des contrôles internes d'un organisme de services sur une période définie selon les critères de services de confiance (sécurité, disponibilité, intégrité du traitement, confidentialité et respect de la vie privée).
[6] Microsoft SharePoint est une plateforme en ligne qui permet au personnel du Fonds mondial de créer, stocker, organiser, partager et gérer des informations et des documents.

1.4 Objectifs, notations et champ

L'objectif général de l'audit était de fournir au Conseil d'administration du Fonds mondial une assurance raisonnable quant à la conception et à l'efficacité des contrôles généraux des technologies de l'information en place pour garantir la confidentialité, l'intégrité et la disponibilité des principaux systèmes et données du Fonds mondial. L'audit a en particulier évalué les éléments suivants :

<table>
<tr><th>Objectifs</th><th colspan="2">Notations</th><th>Champ</th></tr>
<tr><td>Conception appropriée des contrôles généraux des technologies de l'information pour faire face aux principaux risques liés aux technologies de l'information</td><td colspan="2">Efficace</td><td rowspan="3">Période d'audit
Janvier 2024 à juin 2025

Exclusion du champ
Les systèmes informatiques de Microsoft Office (dont Outlook, MS Office et Teams) n'entrent pas dans le champ direct de l'audit. Cependant, notre examen de la gestion des accès des utilisateurs a porté indirectement sur ces applications, car elles reposent sur un mécanisme d'authentification commun à la plupart des applications et systèmes du Fonds mondial, y compris ceux qui ont été sélectionnés dans le cadre de nos tests.</td></tr>
<tr><td rowspan="2">Efficacité opérationnelle des contrôles généraux des technologies de l'information destinés à préserver la confidentialité, l'intégrité et la disponibilité des données et des systèmes</td><td>Conception et efficacité opérationnelle des contrôles généraux des technologies de l'information</td><td>Efficace</td></tr>
<tr><td>Processus opérationnels d'appui</td><td>Partiellement efficace</td></tr>
</table>

Le BIG a interrogé les parties prenantes concernées, notamment au sein du Département des Technologies de l'information et du Département des Ressources humaines, ainsi que les propriétaires des systèmes, et a procédé à des vérifications des processus de contrôle. Nous avons étudié les politiques, les procédures, les mécanismes de gouvernance et la documentation connexe, et nous avons testé les principales activités afin d'évaluer la conception et la mise en œuvre des contrôles. Nous nous sommes appuyés sur les examens d'autres structures de contrôle externe (notamment l'audit externe du Fonds mondial et les examens des certifications ISO), conformément aux normes internationales d'audit interne (norme 9.5 Coordination et utilisation d'autres travaux).

L'**Annexe A** du présent rapport fournit des détails sur la classification générale des notations d'audit.

2. Environnement et contexte

2.1 Vue d'ensemble des contrôles généraux des technologies de l'information au Fonds mondial

Le Secrétariat du Fonds mondial opère dans un environnement des technologies de l'information très automatisé. Pour protéger les systèmes et les données informatiques, le Département des Technologies de l'information a conçu et mis en œuvre plusieurs contrôles préventifs et de détection, communément appelés contrôles généraux des technologies de l'information. Ces contrôles sont conçus pour assurer la confidentialité, l'intégrité et la disponibilité des systèmes et des données informatiques.

Les contrôles généraux des technologies de l'information sont classés en cinq catégories principales[7] :

- **Contrôles de gestion des accès :** veiller à ce que seuls les utilisateurs autorisés puissent accéder à certains systèmes et à certaines données afin de prévenir les accès non autorisés et les violations de données.
- **Opérations informatiques :** maintenir la fiabilité, la performance et la sécurité des systèmes informatiques grâce aux contrôles de routine, à la maintenance et à la gestion des incidents.
- **Gestion du changement :** s'assurer que les changements apportés aux systèmes et aux applications sont correctement contrôlés, autorisés, testés et documentés avant leur déploiement afin de minimiser le risque de perturbations ou de vulnérabilités.
- **Contrôles de sécurité des données :** protéger les informations tout au long de leur cycle de vie, depuis leur création et leur stockage jusqu'à leur transmission et leur élimination.
- **Contrôles de sécurité des réseaux :** défendre l'infrastructure de l'organisation contre les cybermenaces.

2.2 Vue d'ensemble des principaux systèmes informatiques du Fonds mondial couverts par les contrôles généraux des technologies de l'information

L'environnement informatique du Fonds mondial comprend l'infrastructure informatique, les applications, les plateformes et les terminaux tels que les ordinateurs portables et les téléphones mobiles. L'ensemble de ces éléments soutient les opérations quotidiennes et permet la bonne marche des fonctions essentielles de l'organisation.

La plupart des systèmes informatiques du Fonds mondial sont basés sur le cloud[8], et les risques associés sont gérés par une supervision structurée des fournisseurs et de solides processus de gestion des services informatiques. Au sein de l'écosystème informatique, les applications[9] sont regroupées en trois catégories principales, en fonction de leur objectif et de leur fonctionnalité :

[7] Bien qu'il s'agisse d'un élément essentiel des contrôles généraux des technologies de l'information, nous n'évoquons pas ici les contrôles du cycle de vie du développement logiciel. En effet, dans la plupart des cas, le Fonds mondial ne développe pas ses propres logiciels, mais exploite plutôt des systèmes, des plateformes et des applications fournis par le biais de services cloud.
[8] Un système informatique basé sur le cloud est un ensemble intégré de matériel informatique, de logiciels et de ressources réseau hébergés sur des serveurs distants et diffusés sur Internet pour fournir des services de calcul, de stockage et d'application sans dépendre d'une infrastructure sur site.
[9] Ce tableau ne répertorie pas l'intégralité des systèmes et applications du Fonds mondial.

Business application	Office application	IT Management Application
• GOS (Grant) • Kyriba (Payments) • Oracle Fusion (Finance) • Wambo (procurement) • Workday (HR) • Tableau (Data reporting) • TeamMate + (OIG) • TMS (Admin travel) • CMS/CSS (Case Mgt)	• Adobe Sign • Microsoft Teams • Office 365 - Exchange Online – GF • Office 365 - SharePoint Sites – GF • Outlook • SharePoint • MS Office Suite (Word, Excel, PowerPoint) • www.theglobalfund.org	• Active Directory • ADFS (SSO) • Azure Subscription • CyberArk Endpoint Privilege Manager • EnCase • MIM (Microsoft Identity Manager) • ProofPoint • ServiceNow

2.3 Examen des contrôles généraux des technologies de l'information

Ces derniers mois, le Secrétariat du Fonds mondial a fait l'objet de plusieurs examens indépendants visant à évaluer la conception et l'efficacité de ses contrôles généraux des technologies de l'information. Ces examens jouent un rôle déterminant pour le renforcement du cadre de contrôle interne de l'organisation et la fiabilité de son environnement informatique. Il s'agit principalement des examens suivants :

- **Certifications ISO.** Le Fonds mondial est titulaire de trois certifications ISO, valables jusqu'en 2028 :
  - ISO 27001 : Système de management de la sécurité de l'information
  - ISO 22301 : Système de management de la continuité d'activité
  - ISO 20000 : Système de management des services informatiques

  Ces certifications fournissent une assurance sur l'adéquation et l'efficacité des contrôles et des activités liés à ces trois domaines. Un examen de surveillance est réalisé chaque année par un organisme de certification indépendant et un processus de recertification complet a lieu tous les trois ans.

- **Examen des contrôles généraux des technologies de l'information par l'auditeur externe.** Dans le cadre de l'audit de l'état financier annuel, l'auditeur externe KPMG examine les contrôles généraux des technologies de l'information en appui des principales applications et infrastructures financières. Le rapport 2024 a conclu que les contrôles informatiques pertinents étaient conçus de manière adéquate et fonctionnaient efficacement, à quelques exceptions près. L'examen portait sur des domaines tels que la gestion des accès des utilisateurs, le contrôle des changements et les opérations informatiques.

- **Programme de sécurité des clients de SWIFT[10].** Le Fonds mondial fait l'objet d'évaluations annuelles dans le cadre du programme de sécurité des clients de SWIFT, qui garantit que les institutions utilisant le réseau SWIFT se conforment à un socle de contrôles obligatoires en matière de cybersécurité. Ces évaluations portent sur différents domaines, notamment la sécurité de l'authentification, les restrictions d'accès, la détection des incidents et l'intégrité des systèmes liés aux environnements associés à SWIFT.

[10] SWIFT est un réseau de messagerie sécurisé utilisé par les institutions financières pour envoyer et recevoir des informations sur les transactions financières, par exemple les transferts de fonds internationaux. Pour réaliser ses paiements, le Fonds mondial emploie KYRIBA, un logiciel certifié par SWIFT.

Chacun des examens mentionnés ci-dessus présente un objectif, un champ, des priorités et une approche distincts en fonction du niveau d'assurance qu'il entend fournir. L'audit du BIG a complété ces activités d'assurance existantes en ciblant les domaines des contrôles généraux des technologies de l'information pour lesquels des tests supplémentaires pouvaient être envisagés. Une approche basée sur les risques a été appliquée afin d'assurer une couverture complète tout en évitant les doubles emplois.

3. Constats

3.1 Les contrôles généraux des technologies de l'information sont solides et bien mis en œuvre dans des domaines essentiels tels que la sécurité des réseaux, les opérations informatiques et la gestion du changement

Le Secrétariat du Fonds mondial a établi et mis en œuvre de manière efficace des contrôles des opérations informatiques et des processus de gestion du changement sécurisés afin de garantir la disponibilité continue des services informatiques. De solides contrôles de sécurité du réseau sont en place pour assurer une protection contre les menaces de cybersécurité.

Les contrôles de sécurité du réseau sont solides, mais la formation de sensibilisation à la sécurité peut être améliorée

L'audit le plus récent (mars 2025) pour la certification ISO 27001 a révélé que les contrôles et les outils de surveillance sont suffisants pour atténuer et gérer les risques liés aux points d'entrée que les cyberattaquants externes cherchent à exploiter. Il s'agit notamment d'une configuration appropriée des périphériques réseau (tels que les pare-feu et les routeurs), d'une segmentation correcte du réseau, d'un processus adapté de gestion des correctifs, d'une surveillance des vulnérabilités et de mécanismes de remédiation, ainsi que d'une formation régulière des utilisateurs à la sécurité.

Au cours de l'audit, le BIG a vérifié que tous les terminaux disposaient de signatures antivirus à jour les protégeant des attaques de cybersécurité de plus en plus sophistiquées. Le BIG a également noté que des correctifs de sécurité[11], en particulier pour Microsoft Windows, étaient régulièrement appliqués aux terminaux afin de maintenir l'intégrité du système.

Si l'audit du BIG et l'examen de la certification ISO 27001 établissent tous deux que le service informatique dispense régulièrement des formations de sensibilisation à la sécurité, il est possible d'améliorer ce processus. Les politiques les plus importantes en matière de technologies de l'information ne sont pas systématiquement communiquées aux nouveaux arrivants. Bien que le service informatique ait élaboré une présentation décrivant les politiques et réglementations en la matière, le Département des Ressources humaines, qui assure l'intégration des nouvelles recrues, ne l'a pas incluse dans son processus d'accueil. En outre, alors que les nouveaux membres du personnel sont tenus de suivre les cours de formation obligatoires existants dès leur arrivée, les nouveaux consultants disposant d'un compte d'utilisateur du Fonds mondial ne sont quant à eux pas systématiquement inscrits à ces sessions dans le cadre de leur intégration. Cela contribue au manque de connaissances des risques liés à la cybersécurité parmi ces groupes. La vague suivante de formations obligatoires pouvant avoir lieu plusieurs mois après l'intégration, une période prolongée de vulnérabilité est créée.

Malgré de solides contrôles de la sécurité du réseau, des cyberattaquants externes peuvent encore réussir à percer les défenses du réseau d'une organisation. Pour atténuer ce risque, le service informatique a conçu et mis en œuvre un protocole complet de gestion des incidents. Celui-ci a démontré son efficacité en réduisant de manière significative l'impact des attaques d'hameçonnage.

[11] Un correctif est une mise à jour logicielle destinée à résoudre un problème ou à améliorer un programme.

Les contrôles de la gestion du changement[12] sont bien conçus et mis en œuvre de manière efficace

Les examens des certifications ISO 27001 (Système de management de la sécurité de l'information) et ISO 20000 (Système de management des services informatiques) réalisés en mars 2025, ainsi que l'audit externe mené en 2024, ont permis de constater que les processus et procédures de gestion du changement du Fonds mondial pour les systèmes importants sont appropriés et efficaces. Plus particulièrement, des contrôles sont en place pour atténuer les principaux risques tout au long du cycle de vie de la gestion du changement, depuis l'introduction des demandes de changement jusqu'aux examens postérieurs à leur mise en œuvre.

Les contrôles des opérations informatiques sont bien conçus et mis en œuvre de manière efficace afin de garantir la disponibilité permanente des systèmes et des données

Les contrôles des opérations informatiques englobent les activités quotidiennes qui contribuent à maintenir la fiabilité des systèmes informatiques, à garantir l'intégrité des données et à favoriser une reprise rapide à la suite de perturbations, tout en minimisant les risques d'interruption des services. Le service informatique a mis au point des procédures spécifiques pour chaque catégorie d'activité opérationnelle. Ces activités font l'objet d'un suivi mensuel sous la forme de rapports et de réunions auxquels participent la haute direction du Département des Technologies de l'information (y compris son directeur et les cadres supérieurs concernés), ainsi que les responsables opérationnels pertinents.

Les examens de recertification ISO 27001 (Système de management de la sécurité de l'information) et ISO 20000 (Système de management des services informatiques) ont confirmé l'adéquation et l'efficacité de la mise en œuvre de la procédure de gestion des incidents. La majorité des incidents sont résolus dans les délais fixés, ce qui contribue à un taux de disponibilité élevé (au moins 99 %) des systèmes informatiques du Fonds mondial.

L'organisation emploie des mécanismes de sauvegarde en temps réel pour Microsoft Azure et les applications appartenant au Fonds mondial. Par ailleurs, un système de sauvegarde immuable[13] est en place pour atténuer les risques associés à la perte de données et aux attaques de rançongiciel[14]. La certification ISO 22301 (Système de management de la continuité des activités), réalisée en mars 2025, apporte une assurance forte sur l'efficacité de ces pratiques de sauvegarde et de restauration.

L'environnement informatique du Fonds mondial repose fortement sur des prestataires de services tiers : les principaux systèmes informatiques sont basés sur le cloud et certaines activités informatiques clés sont externalisées. Cette dépendance à l'égard de prestataires de services externes présente des risques inhérents, car les défaillances de ces fournisseurs pourraient perturber considérablement les services informatiques. Pour atténuer ces risques, le Département des Technologies de l'information a mis en place une fonction dédiée à la gestion des fournisseurs de services informatiques, soutenue par des procédures et des outils opérationnels exhaustifs. L'audit du BIG a révélé que ce processus de gestion des fournisseurs est bien conçu, qu'il emploie des outils innovants (comme le portail de gestion des fournisseurs), et qu'il est géré efficacement tout au long du cycle de vie des fournisseurs. Pour évaluer les risques liés aux fournisseurs, le

[12] Un changement est l'ajout, la modification ou la suppression de tout élément susceptible d'affecter les services informatiques. La gestion du changement est le processus qui contrôle le cycle de vie de tous les changements, permettant ainsi d'apporter des évolutions bénéfiques en perturbant le moins possible les services informatiques.
[13] Une sauvegarde immuable est un type particulier de sauvegarde qui ne peut pas être modifiée, supprimée ou altérée une fois qu'elle a été créée, et ce pendant une période déterminée.
[14] Une attaque de rançongiciel (ou *ransomware*) est un type de cyberattaque durant laquelle un logiciel malveillant infecte un ordinateur ou un réseau et verrouille ou crypte les fichiers et les données de la victime, les rendant inaccessibles jusqu'au paiement de la rançon demandée.

Département des Technologies de l'information s'appuie également sur les rapports d'audit SOC 2, qui fournissent une assurance indépendante sur la conception et l'efficacité opérationnelle des contrôles effectués par les fournisseurs de services informatiques lorsqu'ils fournissent des services à leurs clients.

La conception des contrôles généraux des technologies de l'information est jugée appropriée pour atténuer les principaux risques liés aux technologies de l'information. Par conséquent, aucune mesure de gestion n'est nécessaire.

3.2 Si les contrôles de sécurité des données sont bien conçus, l'application non systématique des exigences en matière de classification des données accroît le risque d'atteinte à la vie privée et à la confidentialité des données.

Bien que les contrôles de sécurité des données du Fonds mondial soient conçus de manière adéquate, le BIG a relevé des lacunes de mise en œuvre dans l'application des protocoles sur les sites SharePoint, qui ont permis un accès non autorisé à des informations confidentielles et privées.

Les données sont l'un des atouts les plus précieux de tout système informatique. Elles doivent être protégées contre tout accès non autorisé afin que leur confidentialité et leur intégrité soient préservées. Pour atteindre cet objectif, le Secrétariat du Fonds mondial a conçu et mis en œuvre une série de contrôles de sécurité des données dans l'ensemble de son environnement informatique.

Les contrôles sont conçus de manière efficace pour réduire le risque de compromission de la confidentialité et de l'intégrité des données

La protection des données commence par la prévention de l'accès non autorisé aux comptes d'utilisateurs. Pour atténuer ce risque, le Département des Technologies de l'information a mis en œuvre une série de contrôles, notamment de robustes mécanismes d'authentification et une gestion et un suivi complets des accès liés aux comptes d'utilisateurs, comme indiqué à la section 3.3. Par ailleurs, les contrôles de sécurité du réseau ont été renforcés pour protéger les terminaux (tels que les ordinateurs portables et les téléphones mobiles) contre les accès externes non autorisés. Ces mesures contribuent à protéger à la fois les appareils et les données qu'ils contiennent (voir section 3.1).

Certains types de données de l'organisation sont particulièrement sensibles. La divulgation non autorisée de données personnelles, financières ou relatives aux ressources humaines peut entraîner d'importants risques opérationnels et juridiques, ainsi que pour la réputation. Afin d'atténuer ces risques, le service informatique, sous la supervision et l'orientation du Conseil de gouvernance des données, a établi des règles de classification des données qui classent les informations en quatre groupes fondés sur le risque : Public (risque faible ou nul), Restreint (risque modéré), Confidentiel (risque élevé) et Hautement confidentiel (risque très élevé). Une classification automatisée a été mise en œuvre pour les documents Microsoft Office et les courriels Outlook, les documents confidentiels devant être étiquetés de manière appropriée pour en contrôler l'accès et le partage. Le service informatique a mis en place une formation obligatoire sur la protection des données, qui met l'accent sur la classification des données, afin de familiariser le personnel avec ces contrôles.

Un niveau de protection supplémentaire a été créé afin que les données au repos (p. ex. les données stockées dans une base de données) et les données en mouvement (p. ex. les données transmises

par courrier électronique ou entre appareils) ne puissent être consultées que par des personnes autorisées. Pour ce faire, les données sont cryptées, ce qui les rend illisibles pour les personnes ou les systèmes non autorisés, afin d'en préserver la confidentialité et l'intégrité. L'audit de la certification ISO 27001 a confirmé que le Département des Technologies de l'information a défini des procédures adéquates pour gérer le processus de chiffrement et qu'il applique des méthodes de chiffrement conformes aux meilleures pratiques du secteur.

Le manque de consistance dans l'application de la classification des données sur SharePoint a permis un accès à des données personnelles et confidentielles

Si les règles de classification et de restriction des données sont appliquées de manière efficace dans les applications et plateformes informatiques du Fonds mondial (comme Workday, le système de gestion des subventions ou le système de gestion financière des subventions), de tels contrôles n'ont pas été appliqués de manière consistante aux informations stockées dans les dossiers SharePoint. En raison de la nature des plateformes de partage de documents, il incombe au personnel d'appliquer une classification appropriée à leurs documents. Le BIG a toutefois constaté que des employés et des consultants du Fonds mondial pouvaient accéder à des documents sensibles depuis des comptes d'utilisateurs internes. Il s'agit notamment des catégories suivantes de documents, dont l'accès aurait dû être restreint afin de préserver la vie privée et la confidentialité :

- Des **informations personnelles identifiables du personnel**, telles que l'adresse du domicile, la nationalité, l'état civil et les renseignements figurant sur le passeport, que l'on trouve souvent dans les passeports téléchargés et les formulaires de demande de visa.
- Des **coordonnées**, y compris celles de hauts fonctionnaires externes.
- Des **informations sensibles à caractère personnel**, telles que des informations sur la santé des employés et des consultants.
- Des **communications confidentielles**, notamment des notes de service du Fonds mondial et des lettres adressées à la direction par des fonctionnaires dans les pays.

Les facteurs ayant contribué à l'accès non autorisé à des informations sensibles conservées sur SharePoint sont les suivants :

- Un manque de fonctionnalités permettant d'appliquer les protocoles de classification des données : si des fonctionnalités de classification des données sont activées pour les documents Microsoft Office et les messages Outlook, elles ne s'étendent pas aux fichiers PDF, le format le plus utilisé pour les documents sensibles sur SharePoint.
- Un manque de consistance des pratiques en matière de restriction des données : certains départements ou groupes d'utilisateurs ont créé de manière proactive des dossiers dont l'accès est restreint pour les données confidentielles, ce qui n'est pas le cas de tous. La formation obligatoire récemment mise en place sur la protection des données vise à remédier à ce manque de consistance, mais elle n'est efficace que si chaque membre du personnel suit les procédures qui y sont décrites.
- Absence de contrôle du respect des politiques par les groupes d'utilisateurs : malgré les efforts de sensibilisation menés à travers la formation obligatoire, il n'existe actuellement aucun mécanisme permettant de contrôler le respect des politiques de classification des données et de contrôle des accès.

Le service informatique a commencé à collaborer avec plusieurs équipes du Secrétariat du Fonds mondial pour restreindre et nettoyer les fichiers sensibles et à caractère personnel, mais certains de ces documents étaient encore accessibles sur SharePoint au moment de la rédaction du présent

rapport. Bien que le Fonds mondial ne soit pas soumis à des réglementations spécifiques en matière de confidentialité des données en raison des privilèges et immunités qui lui sont accordés, les politiques informatiques internes – notamment le règlement sur l'approbation des utilisateurs de technologies et le manuel de l'employé – soulignent l'importance de la protection de la confidentialité des données. L'absence d'une protection adéquate des données personnelles peut exposer l'organisation à des risques pour sa réputation ou de nature juridique, notamment en cas d'utilisation abusive de ces informations.

Mesure de gestion convenue n° 1

Le Secrétariat prendra les mesures suivantes pour traiter les différents points identifiés par le BIG :

1. Sensibilisation et formation. Un cours spécifique sur la protection des données et de l'information sera créé et ajouté dans iLearn (en collaboration avec les Ressources humaines). Ce cours sera obligatoire pour tous les employés et consultants et proposé régulièrement. Les contenus seront actualisés autant que nécessaire.
2. La direction des Technologies de l'information et la direction des Questions d'éthique et des Risques élaboreront un plan visant à établir un contrôle approprié du respect des politiques afin d'atténuer davantage ce risque. Ce plan prévoira des conséquences adaptées en cas de non-respect.
3. La direction des Technologies de l'information, en coordination avec les divisions/départements du Secrétariat du Fonds mondial, lancera une campagne de nettoyage sur l'intranet « Engage » du Fonds mondial afin de restreindre l'accès aux données personnelles accessibles relevées au cours de l'audit.

TITULAIRE : Direction des Technologies de l'information et Direction des Questions d'éthique et des Risques

DATE CIBLE : mars 2026

3.3 Les contrôles de gestion des accès sont bien gérés tout au long du cycle de vie des comptes d'utilisateurs, sauf lors de l'intégration des consultants

Dans l'ensemble, les contrôles de gestion des accès au sein du Secrétariat du Fonds mondial sont bien conçus et mis en œuvre de manière efficace tout au long du cycle de vie des comptes d'utilisateurs. Cependant, les comptes des consultants ne sont pas désactivés immédiatement après leur départ, ce qui augmente le risque d'accès non autorisé aux systèmes et aux données du Fonds mondial. Par ailleurs, il conviendrait de renforcer les méthodes d'authentification des utilisateurs externes qui accèdent aux systèmes du Fonds mondial.

Les contrôles de gestion des accès sont essentiels pour garantir que l'accès aux systèmes et aux données se limite aux utilisateurs autorisés. Compte tenu de leur importance, les contrôles des accès sont systématiquement inclus dans le champ des examens menés par les structures de contrôle externe du Fonds mondial en matière de technologies de l'information, y compris l'examen de la certification ISO 27001 et les audits externes.

Des procédures adéquates sont en place pour gérer efficacement les contrôles des accès, de la création à la clôture des comptes d'utilisateurs

Le service informatique a mis en place des processus et des procédures solides pour gérer efficacement l'intégration des nouveaux employés et consultants. Les droits d'accès sont accordés en fonction des besoins des utilisateurs, selon le principe du moindre privilège[15].

Le service informatique a mis en œuvre une méthode d'authentification solide pour vérifier l'identité d'un utilisateur avant de lui accorder l'accès. Ce processus comprend notamment l'authentification multifacteur, qui exige que les utilisateurs définissent des mots de passe forts conformes aux meilleures pratiques (notamment quant à leur complexité ou leur date d'expiration) reposant sur un facteur d'authentification supplémentaire.

Pour faire face aux risques liés aux droits d'accès, les responsables opérationnels, tels que les équipes chargées des Achats et des Finances, mènent un processus de certification annuel afin d'examiner et de valider les droits d'accès des utilisateurs pour leurs applications métier respectives (comme Wambo ou le système de gestion financière des subventions). L'auditeur externe, KPMG, a confirmé que ce contrôle de détection est exécuté comme prévu, à quelques exceptions près.

La phase finale du cycle de vie des comptes d'utilisateurs implique la désactivation ou la suppression des comptes du système des Ressources humaines (Workday) et du gestionnaire d'identité de Microsoft à la suite du départ des employés ou des consultants. Le BIG a constaté que les comptes d'utilisateurs des anciens employés du Fonds mondial sont rapidement désactivés.

La désactivation régulièrement tardive des comptes d'utilisateurs internes dans les principaux systèmes informatiques augmente le risque d'accès non autorisé aux données et aux systèmes du Fonds mondial

Malgré les bonnes pratiques mentionnées ci-dessus, certains consultants ont conservé un accès à leur compte d'utilisateur au-delà de leur période contractuelle, ce qui augmente les risques d'accès résiduels. Les normes de sécurité informatique telles que la certification ISO 27001[16] exigent la

[15] Le principe du moindre privilège est un concept de sécurité de l'information selon lequel un utilisateur ou une entité ne doit avoir accès qu'aux données, ressources et applications nécessaires à l'accomplissement de la tâche requise.
[16] Contrôle AC-2 : Gestion des comptes (NIST 800 – 53) et Annexe A.5.18 Droits d'accès (ISO / IEC 27001)

désactivation immédiate des comptes d'utilisateurs lorsque les employés ou les consultants quittent l'organisation. Ce contrôle est essentiel pour empêcher tout accès non autorisé, non seulement par d'anciens membres du personnel, mais aussi par des cyberattaquants externes qui pourraient exploiter des comptes dormants[17] pour compromettre la sécurité du système.

Le BIG a observé que 50 des 217 comptes de consultants (23 %) dont les contrats ont pris fin entre janvier et juin 2025 ont été désactivés avec un retard (allant de 14 à 68 jours) à la suite de leur départ. Une analyse plus approfondie a révélé que huit de ces consultants avaient accédé à leur compte après leur départ officiel. Ce problème a déjà été soulevé par l'auditeur externe KPMG, ce qui met en évidence une faiblesse récurrente des contrôles dans le processus de départ des consultants.

Cette situation peut s'expliquer par une coordination insuffisante entre les services recruteurs et les Ressources humaines au moment de notifier la fin d'un contrat. Ce problème se pose surtout pour les consultants qui quittent l'organisation avant la date officielle d'expiration de leur bon de commande, soit parce qu'ils ont été licenciés prématurément, soit parce qu'ils ont été remplacés par d'autres consultants de la même entreprise.

Bien qu'aucun incident lié à un accès non autorisé résultant d'une désactivation tardive d'un compte ne soit survenu au Fonds mondial, il est déjà arrivé que des insuffisances similaires en matière de contrôle aient conduit, dans d'autres secteurs, à des violations importantes affectant l'intégrité des données et la disponibilité des systèmes.

Il conviendrait de renforcer les méthodes d'authentification des utilisateurs externes afin de réduire le risque de compromission des comptes

Lors de l'examen des comptes d'utilisateurs externes, le BIG a constaté que leurs mots de passe ne sont pas configurés de manière à expirer, ce qui va à l'encontre des meilleures pratiques en matière de sécurité des mots de passe.

Le BIG reconnaît par ailleurs que, conformément à la décision du Comité exécutif de direction d'approuver l'activation de l'authentification multifacteur pour les utilisateurs externes à haut risque en 2022, tous les utilisateurs externes ne sont pas tenus d'authentifier leur accès aux systèmes informatiques du Fonds mondial au moyen de plusieurs facteurs.

Dans le contexte du Fonds mondial, l'impact potentiel de la compromission d'un compte d'utilisateur externe, par exemple dans le système de gestion des subventions, est généralement plus faible que celui des utilisateurs internes, car les parties prenantes externes ne bénéficient que d'un accès limité aux données du système global.

Mesure de gestion convenue n° 2
Une ressource pédagogique spécifique (appelée « Journey ») portant sur le processus de désactivation des employés et des consultants sera créée et ajoutée à Workday (le système d'information sur les ressources humaines). Elle sera obligatoire et ciblera les responsables concernés. Elle sera dispensée de la manière suivante : 1) en formation initiale, 2) à chaque intégration d'un nouveau consultant, 3) en rappel annuel.
TITULAIRE : Direction des Ressources humaines
DATE CIBLE : mars 2026

[17] Les comptes dormants sont des comptes actifs qui n'ont pas été utilisés pendant une période prolongée.

Annex A. Classification des notations d'audit et méthodologie

Efficace	Absence de problème ou problèmes mineurs constatés. Les processus de contrôle interne, de gouvernance et de gestion des risques sont conçus de façon adéquate, régulièrement mis en œuvre de façon appropriée et efficace pour fournir l'assurance raisonnable que les objectifs seront atteints.
Partiellement efficace	Problèmes d'importance modérée constatés. Les processus de contrôle interne, de gouvernance et de gestion des risques sont conçus de façon adéquate et généralement mis en œuvre de façon appropriée, mais un ou un petit nombre de problèmes ont été identifiés qui sont susceptibles de présenter un risque modéré pour la réalisation des objectifs.
Nécessite une nette amélioration	Un problème ou un petit nombre de problèmes significatifs constatés. Les processus de contrôle interne, de gouvernance et de gestion des risques présentent quelques problèmes au niveau de leur conception ou de leur efficacité opérationnelle. Ces problèmes sont tels que l'on ne peut pas encore avoir l'assurance raisonnable que les objectifs seront probablement atteints tant qu'ils ne seront pas résolus.
Inefficace	Plusieurs problèmes significatifs et/ou un (des) problème(s) grave(s) constaté(s). Les processus de contrôle interne, de gouvernance et de gestion des risques ne sont pas conçus de façon adéquate et/ou ne sont généralement pas efficaces. Ces problèmes sont de telle nature que la réalisation des objectifs est gravement compromise.

Le BIG réalise ses audits conformément à la définition de l'audit interne du Global Institute of Internal Auditors, aux normes internationales de pratique professionnelle d'audit interne et au code d'éthique. Ces normes permettent de garantir la qualité et le professionnalisme des travaux du BIG. Les principes et les modalités de l'approche d'audit du BIG sont décrits dans son acte constitutif, son manuel d'audit, son code de conduite et les mandats spécifiques à chaque engagement. Ces documents garantissent également l'indépendance des auditeurs du BIG ainsi que l'intégrité de leurs travaux.

Le champ des audits du BIG peut être spécifique ou étendu, en fonction du contexte, et couvre la gestion du risque, la gouvernance et les contrôles internes. Les audits testent et évaluent les systèmes de contrôle et de supervision pour déterminer si les risques sont gérés de façon appropriée. Des tests détaillés servent à établir des évaluations spécifiques de ces différents domaines. D'autres sources de preuves, telles que les travaux d'autres auditeurs/fournisseurs de contrôles externes, servent également à étayer les conclusions.

Les audits du BIG comprennent habituellement un examen des programmes, des opérations, des systèmes et des procédures de gestion des organes et des institutions qui gèrent les financements du Fonds mondial afin d'évaluer s'ils utilisent ces ressources de façon efficiente, efficace et économiquement rentable. Ils peuvent inclure un examen des intrants (moyens financiers, humains, matériels, organisationnels ou réglementaires nécessaires à la mise en œuvre du programme), des produits (produits fournis par le programme), des résultats (effets immédiats du programme sur les

bénéficiaires) et des impacts (modifications à long terme dans la société que l'on peut attribuer au soutien du Fonds mondial).

Les audits couvrent un vaste éventail de thèmes et se concentrent particulièrement sur les questions liées à l'impact des investissements, à la gestion de la chaîne d'approvisionnement, à la gestion du changement et aux contrôles financiers et fiduciaires clés du Fonds mondial.