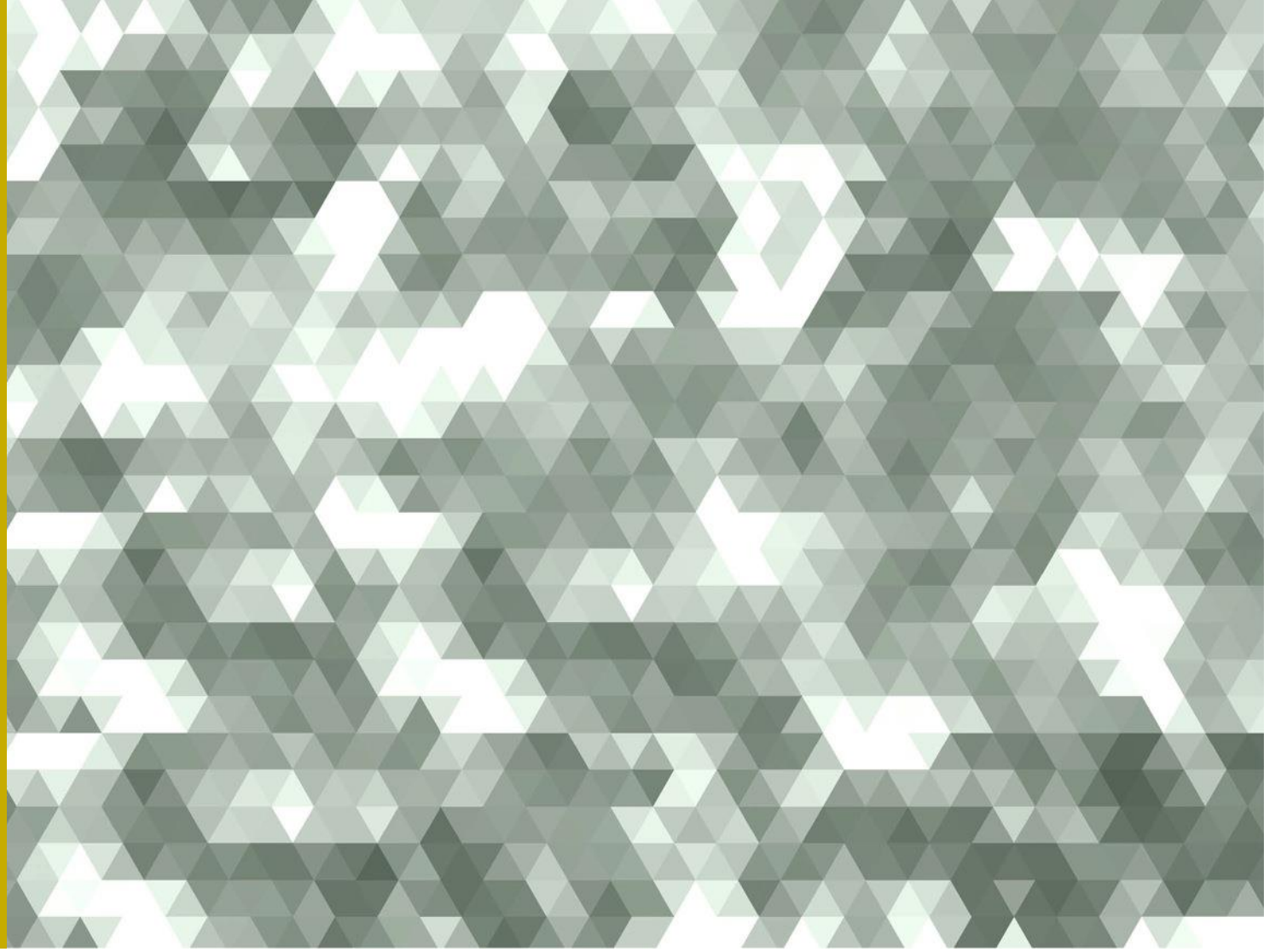

Rapport d’audit

Efficacité des contrôles informatiques au Fonds mondial

Rapport de suivi

GF-OIG-15-20b
11 novembre 2015
Genève, Suisse

The Global Fund
Office of the Inspector General

Table des matières

I. Contexte et portée

Contexte
À la fin de l'année 2014, le Bureau de l'inspecteur général a effectué un audit des contrôles applicables à l'infrastructure, au réseau et aux applications de technologie de l'information du Fonds mondial, y compris des services externalisés et cloud, en vue d'évaluer leur efficacité.

D'importantes lacunes et faiblesses mises en évidence auraient pu être exploitées pour nuire à l'organisation. C'est pourquoi, à la demande de l'inspecteur général, la direction du Comité d'audit et d'éthique et le Conseil d'administration ont accepté de reporter la publication du rapport du Bureau de l'inspecteur général pour permettre au Secrétariat de remédier à ces questions cruciales. Cette décision a été prise conformément à la Politique pour la communication des rapports publiés par le Bureau de l'inspecteur général.

La direction du Comité d'audit et d'éthique et du Conseil d'administration ont demandé au Bureau de l'inspecteur général d'examiner les mesures correctives prises par le Secrétariat du Fonds mondial.

Audit de 2014
L'audit de 2014 portait sur l'infrastructure, le réseau et les applications informatiques du Fonds mondial, y compris les services externalisés et cloud. L'examen visait à donner au Conseil d'administration une garantie suffisante de l'efficacité des contrôles informatiques au niveau de l'organisation et de l'application. Plus particulièrement, cet audit visait à réaliser des contrôles informatiques dans les domaines suivants : accès aux données, précision, agilité et disponibilité des données.

Le Bureau de l'inspecteur général a sélectionné la norme ISO 27001 comme cadre d'analyse qui tient compte des nouvelles technologies, telles que les appareils mobiles, l'informatique à distance et l'intégration de services cloud dans les environnements informatiques.

L'audit a révélé que bien que le Fonds mondial eut procédé à une vaste restructuration au moyen de nouveaux projets informatiques visant à contribuer au nouveau modèle de financement et à améliorer les systèmes financiers, la sécurité informatique n'a pas été une priorité.

La notation de l'audit de 2014 était la suivante :

Risque opérationnel	**Notation**
Accès aux données	**Plan partiel pour devenir efficace**
Précision des données	**Plan complet pour devenir efficace**
Agilité des données	**Généralement efficace**
Disponibilité des données	**Plan complet pour devenir efficace**

Portée
À la suite de l'audit de 2014, le présent examen de suivi visait à évaluer les progrès du Secrétariat du Fonds mondial en matière de mise en œuvre des mesures de gestion convenues à l'issue de l'audit de 2014, en particulier concernant l'accès à, la précision et la disponibilité des données.

II. Résumé

Les faiblesses les plus importantes identifiées dans l'audit de 2014, qui étaient liées à l'amélioration de la sécurité informatique, à la gestion des accès et au contrôle des systèmes et des comptes, ont été presque totalement corrigées. Les améliorations importantes comprennent :

- le recrutement d'un responsable de la sécurité des systèmes d'information en mars 2015 ;
- l'examen approfondi des droits d'accès des utilisateurs, y compris l'accès aux bases de données et la rédaction d'un rapport d'activité complet sur les comptes privilégiés ;
- l'installation de systèmes de détection et de prévention d'intrusion, conçus pour contrôler le trafic et les données du réseau du Fonds mondial et pour réduire le risque d'activité non autorisée ou malveillante ;
- un nouvel antivirus a été installé sur la majorité des serveurs, et un processus de suivi et d'approbation des exceptions a été mis en place ;
- un renforcement des procédures de contrôle, y compris des exigences de complexité des mots de passe pour les comptes réguliers et l'expiration périodique de mots de passe pour les comptes privilégiés ; et
- l'introduction d'une nouvelle politique d'entrée/de sortie y compris pour les travailleurs occasionnels (consultants et autres comptes non-salariés), dont l'objectif est d'obtenir une unique source de données pour le personnel et les contractants et de permettre un suivi global de tous les comptes.

De manière générale, les activités de correction susmentionnées ont compensé les faiblesses concernant le suivi et l'accès défaillants, dont souffrait le Fonds mondial après l'audit de 2014. Malgré ces importantes améliorations, d'autres faiblesses résident dans la gestion informatique et nécessitent une attention particulière.

La plus grande faiblesse qui n'a pas été compensée concerne la disponibilité des systèmes et des données. En effet, le Fonds mondial ne dispose toujours pas de plan de reprise informatique après incident pleinement éprouvé et formalisé. Cela s'explique surtout par le fait que le service informatique a externalisé la gestion et la fourniture de tous les serveurs et des services d'application connexes. Les discussions avec cette tierce partie ont débuté, mais aucune disposition contractuelle visant la mise en place d'un plan de reprise informatique n'a été formalisée. En attendant la mise en place et l'essai d'un tel plan, il est possible que des données ou des systèmes informatiques soient inaccessibles pour une longue période en cas d'incident ou d'interruption, ce qui pourrait avoir un impact négatif sur la continuité des opérations pendant cette période. Cependant, en vue de protéger les données du Fonds mondial pendant ce temps, des arrangements provisoires ont été mis en place jusqu'en novembre 2015, lorsqu'un prestataire externe devrait fournir un service complet de sauvegarde.

En outre, il convient de traiter les lacunes suivantes avant que les améliorations ne soient pleinement efficaces :

- le Comité exécutif de direction n'a pas encore revu ni approuvé plusieurs politiques en matière d'accès, de classification des données, de cryptage ou d'approche générale de sécurité informatique du Fonds mondial ;
- la question des exceptions identifiées lors de l'examen des droits d'accès n'a pas encore été pleinement résolue, de même que les rapports d'activités pour les comptes privilégiés ne sont pas contrôlés régulièrement ;
- l'efficacité de l'antivirus est encore limitée, car quatre serveurs ne sont pas encore protégés ;
- il est toujours nécessaire d'installer un logiciel d'authentification des systèmes nécessitant un haut niveau de sécurité ; et

- tous les consultants ne sont pas encore intégrés dans le module des ressources humaines du système du Fonds mondial, limitant ainsi l'efficacité de la nouvelle approche d'entrée et de sortie.

De manière générale, sur la base des données de notre examen de suivi, le Bureau de l'inspecteur général est d'avis que Fonds mondial a corrigé les principales faiblesses identifiées dans l'audit précédent. Cependant, des efforts supplémentaires sont nécessaires pour mettre pleinement en œuvre les mesures de gestion convenues dans le rapport d'audit de 2014. La section III du rapport contient de plus amples informations sur les mesures individuelles.

III. Statut des mesures de gestion convenues

01 Accès aux données

Mesure de gestion convenue 1.1. : Examens périodiques des droits d'accès des utilisateurs et des fonctions des applications

<table>
<tr><td colspan="2">Le Secrétariat du Fonds mondial améliorera les processus en place concernant l'accès aux données, notamment en :

▪ Effectuant un examen complet des accès des utilisateurs à toutes les données du Fonds mondial en vue de déterminer si des inadéquations et des lacunes existent toujours malgré les contrôles de cohérence entre les sites de stockage des données. Cela comprend un examen systématique des actuelles fonctions et autorisations des utilisateurs en vue de s'assurer qu'ils en bénéficiaient sur une base du « besoin d'en connaître ». Il convient de réaliser une analyse pour les utilisateurs dont l'affectation au sein du Secrétariat a changé, surtout lorsqu'ils bénéficient de droits non révoqués émanant de leur précédente fonction.

▪ Effectuer un examen de tous les comptes de service dans Active Directory pour s'assurer qu'ils sont toujours utilisés et que les serveurs et propriétaires de l'application sur lesquels ils travaillent sont clairement identifiés. Cela comprend la limitation de l'accès à ces comptes par le biais d'objets de stratégie de groupe de sorte qu'aucune connexion interactive ne soit permise et que les autorisations d'accès au fichier de connexion se limitent uniquement aux systèmes requis.

▪ Établissant une liste complète de tous les systèmes de production soumis à l'examen (y compris les serveurs et les dispositifs gérés par les fournisseurs, mais pas les systèmes d'essai et de développement) et en garantissant qu'ils sont inclus dans la solution de suivi DELL Secure Works ou dans une solution équivalente et adaptée. Le Secrétariat s'assurera que les rapports prédéfinis puissent générer un rapport d'activité complet et inviolable pour tout compte bénéficiant de droits.</td></tr>
<tr><td>Propriétaire : Responsable des systèmes d'information</td><td>Date limite : 31 décembre 2015</td></tr>
<tr><td colspan="2">Statut : Partiellement réalisé</td></tr>
</table>

Le Secrétariat du Fonds mondial a mis en œuvre certaines améliorations de l'accès aux données, en particulier :

- L'examen de l'accès utilisateur à toutes les bases de données du Fonds mondial a bien été réalisé. Les propriétaires d'applications ont fait l'objet d'un entretien et d'une enquête. Sur la base des informations fournies, tous les accès aux bases de données ont été modifiés en conséquence. Les accès aux bases de données sont uniquement accordés via la politique de groupe qui définit la sécurité des utilisateurs et les politiques de mise en réseau à l'échelle des machines. L'accès, même en lecture seule, a été réduit autant que possible. L'accès aux différentes pages web de SharePoint est contrôlé via Active Directory, mais les autorisations peuvent être contournées et adaptées individuellement par le supérieur hiérarchique/les administrateurs de site de l'équipe pour répondre au besoin de l'utilisateur.

- Les comptes de services sont reliés aux objets de stratégie de groupe. Aucun utilisateur ne peut se connecter au compte de service, car les comptes de service servent uniquement à connecter un logiciel à une base de données. Néanmoins, il existe toujours une liste d'exceptions. Elle contient les comptes de service pour lesquels les utilisateurs et/ou les fonctions n'ont pas été clairement identifiés et les comptes de base de données avec un accès direct à la base de données. Selon le service informatique, la liste devrait être réduite avant la fin de l'année. Cependant, cette liste

d'exception d'accès direct existera toujours, servira à des fins précises et sera contrôlée par le biais d'un rapport sur les exceptions.

- Le service informatique a dressé une liste de tous les serveurs en vue de sélectionner ceux contenant des données sensibles qui devraient être insérées dans l'outil de suivi Dell Secureworks. Parmi les 158 serveurs de production, 53 ont été intégrés dans l'outil de suivi. Les serveurs sélectionnés contiennent des données plus sensibles selon les recommandations de Dell. Des rapports prédéfinis, permettant la création d'un rapport d'activité complet et inviolable de tous les comptes privilégiés, adaptés aux particularités du Fonds mondial, sont disponibles, mais ne sont pas régulièrement suivis. Un employé spécialisé a été engagé pour exécuter cette tâche à compter d'octobre 2015.

Mesure de gestion convenue 1.2. : Matrice de répartition des tâches pour la plateforme ERP et contrôle des accès des utilisateurs.

Le service des processus et des systèmes financiers formalisera la répartition de la matrice de responsabilité des tâches et réalisera un examen officiel auprès des utilisateurs bénéficiant de droits d'accès dans plus d'un module en vue d'évaluer des éventuels conflits. Un processus formalisé d'approbation et de suivi des exceptions sera également développé. Le service informatique mettra en place les contrôles de prévention et de détection requis en vue d'une évaluation continue de l'application établie selon la matrice de responsabilité et la demande d'approbation du service financier pour toute exception identifiée.	
Propriétaire : Responsable de la sécurité des systèmes d'information et responsable, systèmes financiers et processus	**Date limite :** 30 juin 2015
Statut : Réalisé	

Le service des finances a formalisé la matrice de répartition des tâches en juin 2015. Chaque responsable du service des finances a apporté son soutien à l'élaboration du document, mais le directeur financier n'a pas encore officiellement approuvé ce dernier. Le service informatique a mis à jour les profils utilisateur sur la base de cette analyse et a élaboré un outil de suivi des exceptions des profils utilisateurs sur la base des fonctions et responsabilités affectées. L'outil est disponible depuis la fin juin 2015. Le service des finances devrait transmettre un rapport tous les mois afin de formuler des observations sur les exceptions ou de mettre à jour les bons profils utilisateurs.

Mesure de gestion convenue 1.3. : Politiques, fonction de sécurité informatique et sensibilisation des utilisateurs

Le Secrétariat du Fonds mondial améliorera les processus en place concernant la sécurité informatique, notamment par le biais des mesures suivantes : ▪ La procédure de recrutement d'un responsable de la sécurité des systèmes d'information sera menée à bien. Cette procédure a débuté au cours de l'audit, lorsque l'annonce du poste a été diffusée. Un candidat a déjà été sélectionné et commencera en mars. En vue d'améliorer la fonction de sécurité au sein de l'organisation, des documents liés à la sécurité seront régulièrement mis à jour. ▪ Le service informatique développera, en collaboration avec les ressources humaines, une série de séances de formation visant à la sensibilisation sur la sécurité de l'information et les proposera au Comité exécutif de direction pour approbation et mise en œuvre.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 30 juin 2015
Statut : Partiellement réalisé	

À la suite du recrutement d'un responsable de la sécurité des systèmes d'information en mars, le service informatique a mis à jour une série de politiques informatiques. Le service informatique

considère que la politique d'accès de l'utilisateur du Fonds mondial est en vigueur, cependant elle n'a pas été publiée sur l'intranet ni approuvée par Comité exécutif de direction.

Le responsable de la sécurité des systèmes d'information a élaboré un plan et une feuille route visant à sensibiliser davantage les utilisateurs sur la sécurité informatique, mais aucun accord formel n'a été requis auprès du Comité exécutif de direction et le programme n'a pas encore été déployé. Aucune information sur la sécurité informatique n'a été publiée sur l'intranet et aucune séance de formation n'a été organisée avec les utilisateurs standard de l'organisation, en vue de mieux les sensibiliser à la sécurité informatique.

Mesure de gestion convenue 1.4. : Classification, protection et confidentialité des données

S'agissant du projet de classification des données, les informaticiens apporteront leur contribution aux principes directeurs en cours de finalisation par le service juridique. Le projet de gestion de documents SharePoint 2013 mettra également en œuvre un cadre permettant la classification des documents. Le projet consiste actuellement à faire migrer les documents juridiques vers la plateforme. Une classification sous la forme de métadonnées ajoutées aux sites (actuellement les termes en projet public, interne, confidentiel et à accès limité) sera activée. Dans le cadre de ce projet, le service informatique envisage de doter les documents et sites SharePoint d'une icône qui représente leur classification. Le responsable des systèmes d'information proposera au Comité exécutif de direction, pour décision, une analyse d'évaluation des risques de cryptage des données pour les données du Fonds mondial stockées sur des ordinateurs portables ou des médias externes.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 30 septembre 2015
Statut : Non achevé	

Le service informatique a mis à jour la politique de classification des données, qui définit les catégories de classification (public, interne, confidentiel et hautement confidentiel) et fournit un cadre de classification selon la confidentialité de certains types de documents et d'informations. Le service juridique a communiqué ce cadre à chaque département et a requis un retour d'information. Il envisage également de transmettre cette politique au Comité exécutif de direction à la fin 2015. Aucune mise en œuvre de la classification des données ne sera réalisée sur Share Point avant que le Comité exécutif de direction n'approuve la politique de classification des données.

Le responsable des systèmes d'information a réalisé une évaluation concernant le cryptage des données et des dispositifs pour le Secrétariat, mais cette analyse n'a pas été approuvée par les propriétaires de données. Cette décision sur le cryptage des données n'a pas encore été transmise pour approbation au Comité exécutif de direction.

Mesure de gestion convenue 1.5. : Les politiques de mots de passe en vigueur ne sont pas assez efficaces

Le Secrétariat du Fonds mondial améliorera les processus en place concernant l'accès aux systèmes, notamment en : ▪ Prenant immédiatement des mesures visant à s'assurer que tous les comptes utilisateurs nommés, indépendamment de leurs fonction et poste dans l'organisation, disposent d'un mot de passe qui expire et que tous les mots de passe administratifs locaux sont renforcés ; ▪ Effectuant une révision de la politique de sécurité informatique et des pratiques et de la configuration requise pour les mots de passe, en estimant le niveau souhaité d'identité et de sécurité pour toutes les fonctions et les systèmes informatiques, en proposant au Comité exécutif de direction, pour approbation, une nouvelle politique de sécurité informatique prenant tous ces éléments en considération.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 31 décembre 2015
Statut : Partiellement réalisé	

Tous les comptes privilégiés disposent maintenant d'une date d'expiration et la complexité des mots de passe a été renforcée. Les mots de passe des comptes normaux ont également été réinitialisés et la complexité accrue.

La politique de sécurité informatique a été mise à jour et deux nouvelles sous-politiques ont été ajoutées : la politique d'accès des utilisateurs et la politique de protection des mots de passe qui décrit

la complexité des mots de passe. Les politiques n'ont pas été transmises pour approbation au Comité exécutif de direction, mais devraient l'être au quatrième trimestre de 2015.

Mesure de gestion convenue 1.6. : Accès au réseau de technologie d'information du Fonds mondial

Dans le cadre de ses fonctions et responsabilités, le responsable de la sécurité des systèmes d'information évaluera les risques et les contrôles de sécurité de l'infrastructure et proposera des mesures d'atténuation adaptées. En outre, il proposera au responsable des systèmes d'information des solutions pour une authentification multifacteur du VPN et un contrôle d'accès amélioré au réseau filaire du Fonds mondial. Le protocole Telnet sera supprimé au deuxième trimestre 2015, quand une nouvelle solution sera disponible.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 30 septembre 2015
Statut : Partiellement réalisé	

Le responsable de la sécurité des systèmes d'information a effectué une évaluation des risques et les deux facteurs d'exigences d'authentification ont uniquement été identifiés pour la gestion de trésorerie et seront déployés dans les prochains mois. Aucune exigence générale pour une authentification à deux facteurs n'a été identifiée à ce stade, mais le service informatique continue de travailler avec différents prestataires pour s'assurer que l'infrastructure répond aux normes en cas de poursuite de déploiement. S'agissant de la sécurité de la connexion filaire, le protocole Telnet a été remplacé par une solution permettant un réseau de communication et une authentification cryptés en août 2015.

02 Précision des données

Mesure de gestion convenue 2.1. : Procédure d'entrée pour les employés à temps complet et les contractants

Une procédure sera mise en œuvre pour passer au crible tous les employés du Fonds mondial (internes et externes) en vue de s'assurer que les documents d'activité probants sur les utilisateurs (au sein du Secrétariat du Fonds mondial) sont complets et appropriés. Un projet visant à faire du GFS la source unique de données utilisateurs sera lancé en collaboration avec l'équipe de services généraux (RH) de l'informatique.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 31 décembre 2015
Statut : Partiellement réalisé	

Une politique d'entrée/de sortie y compris des travailleurs occasionnels a été formalisée en août 2015. Sur la base de cette politique, toutes les données sur les employés et les travailleurs occasionnels seront conservées dans le module GFS qui fait partie de la plateforme ERP. Lorsqu'un nouvel employé ou un nouveau travailleur occasionnel travaille au Fonds mondial, les ressources humaines et les autres services concernés complètent une fiche dans le GFS qui applique automatiquement le changement d'emploi. Les anciens droits d'accès sont automatiquement désactivés lorsque le nouvel emploi est activé. Toutes les données sur l'employé sont conservées dans un dossier du GFS et toutes les modifications de l'historique y sont conservées.

Cependant, le personnel externe (les consultants) n'est pas encore intégré dans le module du GFS et des employés qui ont quitté le Fonds mondial, mais restent dans Active Directory ne sont pas non plus inclus dans le module pour faire l'objet d'un suivi.

Mesure de gestion convenue 2.2. : Contrôle des serveurs, des solutions antivirus et évaluation de la vulnérabilité

La mise en œuvre immédiate de mesures concernant les agents antivirus manquants sera étudiée et exécutée, et concernera en priorité les serveurs ayant une fonction de production et/ou un accès à Internet. Des exceptions selon les recommandations de Microsoft pour la base de données et les serveurs hôtes virtuels seront répertoriées. Des systèmes de prévention et de détection d'intrusion seront mis en place. Dans le cadre de ses fonctions et responsabilités, le nouveau responsable de la sécurité des systèmes d'information évaluera les solutions chiffrées pour le contrôle et la protection des centres de données et de l'infrastructure réseau de l'organisation et les proposera au responsable des systèmes d'information.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 30 juin 2015
Statut : Partiellement réalisé	

La solution Microsoft End Point Security a été installée sur tous les serveurs en septembre 2015 pour remplacer la solution Trend Micro. Cependant, il convient de travailler encore sur quatre serveurs pour que l'antivirus soit pleinement efficace.

Le responsable de la sécurité des systèmes d'information a communiqué au responsable des systèmes d'information des solutions chiffrées pour le contrôle et la protection du système du réseau. Parmi les trois systèmes de protection/détection d'intrusion proposés, un système a été sélectionné et, après avoir fait l'objet d'un essai en juillet, il a été mis en œuvre en septembre.

03 Agilité des données

Mesure de gestion convenue 3.1. : Gestion du changement et contrôles du développement de système

En guise de contrôle compensateur, les références des demandes des tiers en matière de gestion du changement doivent être insérées dans le champ prévu à cet effet de l'outil Service Now.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 30 juin 2015
Statut : Réalisé	

Un dispositif servant à insérer manuellement les références de tiers dans l'outil Service Now est maintenant en place.

04 Disponibilité des données

Mesure de gestion convenue 4.1. : Plan de continuité d'activité

Le responsable des systèmes d'information finalisera et signera les documents d'analyse des incidences et le plan de continuité d'activité. Toutes les données du Fonds mondial seront sauvegardées de manière fiable et les tests complets de reprise d'activité après incident seront réalisés comme programmé, la continuité d'activité en cas d'indisponibilité imprévue des bureaux du Secrétariat sera prise en compte.	
Propriétaire : Responsable des systèmes d'information	**Date limite :** 30 septembre 2015
Statut : Non achevé	

Une analyse d'incidence a été formalisée et signée par le responsable des systèmes d'information. L'analyse d'incidence n'inclut pas de section consacrée à la portée minimale des ressources (remplacement) (bâtiments, personnel, informatique/données, personnel et prestataires de service externes) qui doivent être disponibles en cas de crise afin d'aboutir au niveau de récupération désiré.

Le Bureau de l'inspecteur général a estimé que le plan de reprise informatique n'a pas été formalisé ou pleinement éprouvé. Cela s'explique surtout par le fait que le service informatique a externalisé la gestion et la mise à disposition de tous les serveurs et de services d'application connexes. Les discussions avec cette tierce partie ont débuté, mais aucune disposition contractuelle visant la mise en place d'un plan de reprise informatique n'a été établie. Cependant, en vue de protéger les données du Fonds mondial pendant ce temps, des arrangements provisoires ont été mis en place jusqu'en novembre 2015, lorsqu'un prestataire externe devrait fournir un service complet de sauvegarde.

Nous avons également remarqué que la stratégie informatique, y compris l'actuelle stratégie de disponibilité des données, n'a jamais fait l'objet de discussion au sein du Comité exécutif de direction.

Annexe A Catégorie générale de notation de l'audit

Très efficace	**Aucun problème important n'a été relevé.** Les procédures de contrôles internes, de gouvernance et de gestion des risques étaient adaptées, appropriées et efficaces pour garantir l'atteinte des objectifs.
Généralement efficace	**Certains problèmes importants ont été remarqués, mais ne sont pas déterminants pour l'atteinte générale de l'objectif stratégique dans l'environnement ayant fait l'objet de l'audit.** De manière générale, des procédures de contrôles internes, de gouvernance et de gestion des risques étaient adaptées, appropriées et efficaces. Cependant, cela peut encore être amélioré.
Plan complet pour devenir efficace	**Plusieurs problèmes importants et/ou un problème significatif ont été remarqués. Toutefois, un plan SMART (spécifiques, mesurables, réalisables, réalistes et limitées dans le temps) était en place pour les traiter** lorsque le mandat d'audit a été communiqué. S'il est mis en œuvre, ce plan devrait garantir des procédures de contrôles internes, de gouvernance et de gestion des risques adéquates, appropriées et efficaces.
Plan partiel pour devenir efficace	**Plusieurs problèmes importants et/ou un problème significatif ont été remarqués. Toutefois, un plan partiel SMART était en place pour les traiter** lorsque le mandat d'audit a été communiqué. S'il est mis en œuvre, ce plan devrait améliorer les procédures de contrôles internes, de gouvernance et de gestion des risques.
Inefficace	**Plusieurs problèmes importants et/ou un problème significatif ont été remarqués.** Les procédures de contrôles internes, de gouvernance et de gestion des risques étaient inadaptées, inappropriées ou inefficaces. Elles ne garantissaient pas l'atteinte des objectifs. **Aucun plan visant à traiter ces problèmes n'était en place** lorsque le mandat d'audit a été communiqué.

Annexe B : Méthodologie

Le Bureau de l'inspecteur général réalise ses audits conformément à la définition globale de l'Institute of Internal Auditors' (IIA) de l'audit interne, des normes internationales pour la pratique professionnelle de la vérification interne et du code de conduite. Ces normes permettent de garantir la qualité et le professionnalisme des travaux du Bureau de l'inspecteur général.

Les principes et les modalités de l'approche d'audit du Bureau de l'inspecteur général sont décrits dans sa charte, son manuel d'audit, son code de conduite et dans les mandats spécifiques à chaque engagement. Ils permettent à nos auditeurs de fournir un travail de qualité et d'œuvrer de manière efficace. Ils sont également un moyen de garantir l'indépendance des auditeurs du Bureau de l'inspecteur général et l'intégrité de leur travail. Le manuel d'audit du Bureau de l'inspecteur général contient des instructions détaillées sur la réalisation de ses audits, conformément aux normes appropriées et au niveau de qualité attendue.

La portée des audits du Bureau de l'inspecteur général peut être spécifique ou plus large, selon le contexte, et couvre la gestion des risques, la gouvernance et les contrôles internes. Les audits servent à tester et à évaluer les systèmes de contrôle et de supervision en vue de déterminer si le risque est cerné de manière adaptée. Un test détaillé est réalisé auprès du Fonds mondial et des bénéficiaires de subventions, et vise à fournir des évaluations spécifiques des différents domaines d'activité de l'organisation. D'autres sources d'information, telles que le travail d'autres auditeurs/fournisseurs de garantie, sont également utilisées pour étayer les conclusions.

De manière générale, les audits du Bureau de l'inspecteur général contiennent une évaluation des programmes, des activités, des systèmes de gestion et des procédures des entités et institutions chargées de gérer les financements du Fonds mondial, en vue d'évaluer s'ils répondent aux exigences d'économie, d'efficience et d'efficacité lors de l'utilisation de ces ressources. Ces dernières peuvent inclure un examen des entrées (moyens financiers, humains, matériels, organisationnels ou réglementaires nécessaires à la mise en œuvre du programme), des produits (du programme), des résultats (impacts immédiats du programme sur les bénéficiaires) et des impacts (changements à long terme dans la société, attribuables 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.