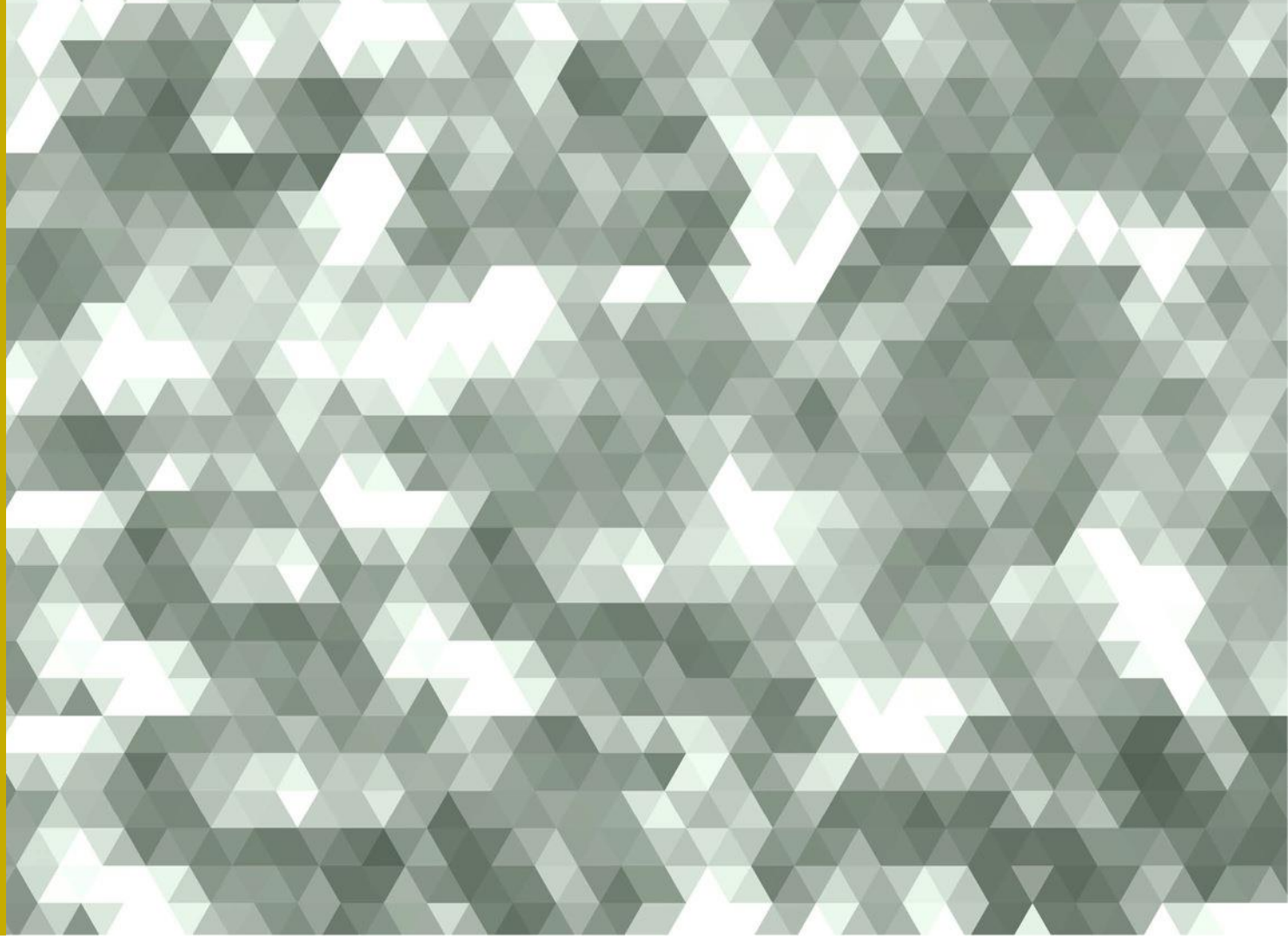

Rapport d'audit

Efficacité des contrôles informatiques au Fonds mondial

GF-OIG-15-020
11 mars 2015
Genève, Suisse

The Global Fund
Office of the Inspector General

Table des matières

I. Contexte

Au début de l'année 2015, le Bureau de l'inspecteur général a effectué un audit des contrôles de l'infrastructure, du réseau et des applications informatiques du Fonds mondial, y compris des services externalisés et sur le cloud, en vue de mesurer leur efficacité. D'importantes lacunes et faiblesses qui auraient pu être exploitées pour nuire à l'organisation ont été mises en évidence. 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 à octobre 2015 afin de permettre au Secrétariat de remédier à ces problèmes cruciaux. Cette décision a été prise conformément à la Politique pour la communication des rapports publiés par le Bureau de l'inspecteur général.

Le Bureau de l'inspecteur général a réalisé l'audit des contrôles informatiques en vue de fournir au Fonds mondial des garanties objectives, indépendantes et suffisantes en termes de conception et d'efficacité des contrôles informatiques en place pour gérer les risques majeurs ayant des répercussions sur les programmes et les opérations

Travaux précédents
Le Bureau de l'inspecteur général avait réalisé un audit de haut niveau des systèmes et procédures informatiques du Fonds mondial en avril 2014, axé sur la pertinence des contrôles, et qui avait abouti à l'identification de lacunes dans la conception des systèmes. Le Bureau de l'inspecteur général avait estimé que, dépassant la portée de cet audit de haut niveau, il conviendrait d'obtenir une garantie suffisante de l'efficacité des contrôles informatiques afin d'identifier et de gérer précisément les principaux risques ayant une incidence sur les programmes et les opérations du Fonds mondial.

Environnement technique
Le Fonds mondial utilise Active Directory de Microsoft pour l'authentification de ses utilisateurs internes et externes. Active Directory est notamment le service officiel d'identification et d'accès à l'ensemble des applications et des services cloud du Fonds mondial, à l'exception de la suite ERP et des applications Local Fund Agent CRM qui sont conservées séparément, suivent leurs propres processus et répondent à leurs propres exigences. La communication et l'authentification autonomes ERP se présentent sous la forme d'un lien dédié entre le réseau du Fonds mondial et le fournisseur ERP aux États-Unis. D'autres applications hébergées sont accessibles sur Internet.

Le Fonds mondial offre aux utilisateurs finaux diverses possibilités d'accès à distance. Les ordinateurs portables du Fonds mondial peuvent se connecter à son réseau interne via Internet, à l'aide d'un VPN.[1] Il est possible d'accéder aux courriels sur Internet et sur les dispositifs mobiles ou les ordinateurs de l'utilisateur. L'authentification pour l'accès VPN et aux courriels est assurée via un canal sécurisé à un facteur (nom d'utilisateur et mot de passe).

Le processus de travail de gestion du changement est géré à l'aide d'une solution sur le web appelée Service-Now. Un coordinateur de gestion du changement existe pour chacun de ces deux volets : infrastructure et opérations. Un catalogue complet comporte les éléments d'infrastructure et les applications concernés par les demandes de gestion du changement. Il recense les responsables et des parties responsables des éléments d'infrastructure ou d'application dans le contexte de la maintenance de l'infrastructure de la technique.

Selon la recommandation du précédent audit du Bureau de l'inspecteur général, la continuité des activités et les plans de reprise après incident ont été formalisés par le service informatique, et la mise en œuvre finale est prévue pour le deuxième trimestre de 2015. L'urgence de la mise en place de la continuité d'activité a fait l'objet d'une évaluation. En outre, une analyse d'impact de

[1] Virtual Private Network, réseau privé virtuel : configuration réseau qui permet à l'utilisateur d'accéder, en toute sécurité, à un réseau privé sur Internet.

l'interruption a été réalisée pour harmoniser la période de récupération selon l'urgence de la mise en place.

Les principaux éléments de l'infrastructure supportent et fournissent les services les plus urgents au Fonds mondial, car ils représentent le point d'entrée du réseau et le domaine d'authentification pour tous les utilisateurs de l'organisation. Certains des principaux volets de l'infrastructure sont, par nature, superflus parce qu'ils sont répartis sur tous les sites existants de l'organisation. Le principal centre de données se situe dans les locaux de l'organisation à Vernier, en Suisse, et il existe une procédure de migration des systèmes hautement prioritaires, tel qu'Exchange Email, dans chacun des centres.

II. Portée et notation

Portée

Les travaux portaient sur l'infrastructure, le réseau et les applications informatiques du Fonds mondial, y compris les services externalisés et cloud.

L'objectif de l'examen d'audit des contrôles informatiques est de 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 consistait à évaluer les contrôles informatiques dans les domaines suivants :

- **Accès aux systèmes informatiques** : l'accès de l'administrateur système et logique aux applications informatiques et aux serveurs, la sécurité, la classification, la confidentialité et la protection des données, l'accès physique aux infrastructures informatiques
- **Précision des systèmes informatiques** : précision des données
- **Agilité des systèmes informatiques** : gestion du changement et contrôles du développement du système
- **Disponibilité des systèmes informatiques** : continuité de l'activité et composants de reprises d'activité

Le Bureau de l'inspecteur général s'est basé sur la norme ISO 27001 dans sa version de 2013 pour la réalisation de cet audit des contrôles informatiques et de l'analyse de haut niveau en 2014. Cette norme mise à jour tient compte des nouvelles technologies telles que les appareils mobiles, l'informatique à distance et l'intégration de services cloud dans les environnements informatiques.

Après l'évaluation de planification initiale, il est en ressorti que certains contrôles des ressources humaines (conditions d'emploi, filtrage et recrutement), de la propriété intellectuelle (contrat de licence), de la conformité des contrats et de la gouvernance (contact avec les autorités et groupes d'intérêt particulier, réglementation des contrôles cryptographiques) n'étaient ni inclus dans les objectifs d'audits actuels ni testés.

Hors de portée

Le réseau et l'infrastructure dédiés au Bureau de l'inspecteur général, physiquement fractionnés du reste de l'organisation, ne faisaient pas partie de la portée de l'actuel audit.

Notation[2]

Risque opérationnel	**Notation**	**Référence des conclusions**
Accès aux données	**Plan partiel pour devenir efficace**	1.1, 1.2, 1.3, 1.4, 1.5, 1.6
Précision des données	**Plan complet pour devenir efficace**	2.1, 2.2,
Agilité des données	**Généralement efficace**	3.1
Disponibilité des données	**Plan complet pour devenir efficace**	4.1

[2] Voir l'annexe A pour la définition des notations du Bureau de l'inspecteur général.

III. Résumé

Selon une analyse externe de 2012, l'infrastructure informatique du Fonds mondial devrait être progressivement externalisée. Depuis lors, des mesures proactives ont été prises en vue de répondre à cette recommandation. En 2013-2014, l'objectif du service informatique était de faire migrer son application et son infrastructure vers des partenaires externes, particulièrement sur le cloud.[3] Lors de cette transition, une plus grande attention a été portée sur la gestion de la migration sur le cloud et à la garantie que les services actuels répondent aux besoins opérationnels du Fonds mondial.

Au cours des dernières années, le paysage informatique du Fonds mondial a fait l'objet d'une importante transformation. En effet, ces deux dernières années, de nouveaux projets informatiques visant à soutenir la mise en œuvre du nouveau modèle de financement et des systèmes financiers améliorés ont été lancés. Les initiatives principales comprennent le projet Finance Step-Up[4] et l'outil CRM pour la gestion des subventions et d'autres fonctions.[5]

Historiquement, la sécurité informatique organisationnelle du Fonds mondial n'a pas été considérée comme une priorité, en raison des éléments d'ouverture et de transparence du modèle d'activité. Le Fonds mondial évolue vers un modèle plus sévère pour répondre aux besoins d'intégrité et de résistance, en vue d'améliorer la gestion des registres et d'assurer l'atténuation des risques. Ce modèle imposera des accès limités sur la base de la sensibilité, de la confidentialité et de la classification des données déterminées essentiellement par leurs propriétaires.

De manière générale, les contrôles informatiques internes étaient considérés comme **efficaces pour l'agilité des données** (gestion du changement et développements du système). Les contrôles de la **disponibilité des données** (continuité de l'activité et composants de reprises d'activité) **et de la précision des données** ont révélé certaines faiblesses, mais le Secrétariat dispose d'**un plan complet pour devenir efficace**.

Les contrôles relatifs à l'**accès aux données** (logiques et accès, sécurité, confidentialité et protection des données) ne sont pas adaptés et seul **un plan partiel pour devenir efficace est en place**. Parmi les conclusions critiques, on recense :

1. Accès aux données :

La plupart des contrôles informatiques internes ont été supervisés de manière partielle ou inadaptée ; cette tâche est habituellement confiée à une **fonction de sécurité du système d'information** spécialisée. En outre, le Bureau de l'inspecteur général a estimé que les politiques de sécurité informatiques étaient obsolètes et dépassées, que les employés n'étaient pas suffisamment sensibilisés aux meilleures pratiques en matière de sécurité informatique et que les systèmes de suivi et de sécurité révélaient des faiblesses.

L'absence de **matrice** formelle **de répartition des tâches au sein des applications professionnelles ERP** entraîne un risque que des fonctions incompatibles soient attribuées à un nombre limité d'utilisateurs. Cela entrave plus encore la mise en œuvre des contrôles de prévention et de détection des fonctions ainsi que la responsabilité dans les applications professionnelles ERP.

Bien que le travail ait débuté, **l'accès des utilisateurs n'a pas été contrôlé régulièrement**. Dès lors, des droits ou des autorisations ont été mal accordés (par exemple, employés ayant quitté l'organisation, mais étant toujours définis dans les applications professionnelles ou utilisateurs que le service des ressources humaines a supprimés, mais qui sont toujours considérés comme

[3] Le cloud computing est l'utilisation de l'Internet pour lancer des applications ou pour stocker des données.
[4] Finance Step Up est un projet de transformation lancé en 2014 et conçu pour réviser les processus et les systèmes financiers du Fonds mondial, pour fournir un nouveau modèle de données financières et pour doter tout le personnel du langage financier commun.
[5] CRM (Customer Relationship Management) est un projet visant à fournir une plateforme unique de gestion des subventions selon le nouveau modèle de financement axé sur l'automatisation des processus existants.

utilisateurs autorisés dans Active Directory). Il convient également de prendre en considération le risque des mouvements internes, d'un département à l'autre, sans révocation des anciens droits d'accès. En outre, la configuration des droits logiciels au serveur (« comptes de services ») **ne limite pas correctement l'accès selon les tâches requises** ; cela engendre le risque qu'un problème, qui pourrait se limiter à un système, se propage à d'autres. L'accès et l'utilisation de tels droits d'accès ne sont pas suivis de manière exhaustive et vérifiable, ce qui rend difficiles la détection d'incident et l'intervention.

Le cadre de classification des données élaboré par le service juridique pourra être mis en œuvre par les informaticiens dès que le Comité exécutif de direction l'aura transmis, revu et approuvé. Ce cadre introduit une nouvelle approche en termes d'évaluation des risques et de protection des données, qui fait l'objet d'un examen jusqu'à présent. Il s'agit également de la première étape de l'introduction de l'activité dans les processus de conservation, d'accès et de classification des données. Cela constituera une des missions du responsable de la sécurité des systèmes d'information en cours de recrutement.

Les politiques de mots de passe ne sont pas assez restrictives et ne correspondent pas aux meilleures pratiques. L'analyse des **politiques en matière de mots de passe du domaine a révélé des paramètres incohérents en termes de complexité, d'expiration, de longueur et d'historique.** En outre, les auditeurs ont remarqué des mots de passe qui n'expiraient pas pour des comptes administratifs nommés et des utilisateurs standard.

Les services à distance, y compris l'accès à distance Virtual Private Network, sont **accessibles à l'aide d'un nom d'utilisateur et d'un mot de passe.** Or, il est recommandé d'utiliser une authentification multifacteur, réduisant le risque de vols d'identifiants par des utilisateurs malveillants. Une authentification multifacteur repose sur un objet en votre possession (téléphone, token) en complément de quelque chose que vous connaissez (identifiant, mot de passe) afin d'accéder aux ressources.

2. Précision des données :

Aucune solution antivirus ne contrôlait les serveurs de l'organisation, ce qui représente un grand risque d'infection de logiciels malveillants.

Après avoir effectué une évaluation de la vulnérabilité à l'aide de l'outil recommandé par Microsoft, le Bureau de l'inspecteur général a mis en évidence 31 des 50 serveurs d'infrastructure Microsoft testés qui n'ont pas été mis à jour lors du dernier correctif de sécurité. Cela représente un **« haut risque » selon l'outil de classification Microsoft**.

La procédure d'accès des utilisateurs internes suit deux processus de travail distincts. Les membres du personnel à temps plein sont identifiés à l'aide d'un identifiant employé et appliquent la politique standard des ressources humaines dans les systèmes du Fonds mondial. Les contractants, ou les travailleurs occasionnels sur le fournisseur ERP, suivent une procédure d'accès parallèle qui n'est pas gérée par les ressources humaines, mais directement par les services informatiques et des achats. Cela signifie donc que les données ne sont pas harmonisées pour les deux types d'employés.

3. Disponibilité des données :

Selon une recommandation du Bureau de l'inspecteur général en 2013, un plan de continuité de l'activité a été élaboré, dont le délai initialement prévu était le 31 octobre 2014. Le service informatique l'a révisé et, à l'heure actuelle, aucun exercice de gestion des catastrophes n'a eu lieu. Un exercice de reprise de l'activité axé sur la priorité des applications est prévu pour le troisième trimestre de 2015. Cependant, le plan de reprise d'activité n'a été testé que partiellement sur la plateforme ERP. L'exercice s'est avéré fructueux pour la suite ERP qui a été rétablie en un jour, conformément aux conditions de l'accord de services cloud gérés. Le plan de continuité de l'activité

pour d'autres ressources et systèmes informatiques repose sur l'infrastructure Data Protection Manager.

Au moment de l'audit, toutes les données devant être protégées avaient migré vers l'infrastructure Data Protection Manager.[6] On remarque cependant que la base de données SharePoint 2007 n'était pas comprise dans Data Protection Manager, car elle entraînait des échecs répétés de toute la sauvegarde en raison de sa taille.[7] Une sauvegarde distincte a été mise en place pour cette base de données, mais elle s'est avérée inefficace et a échoué lors de la période d'audit.

[6] DPM, Data Protection Manager, est une solution de sauvegarde centralisée de Microsoft

[7] Une base de données SharePoint 2007 est utilisée comme référentiel de données dans l'ancien environnement Intranet du Fonds mondial. Le cycle de vie du produit a pris fin et n'est plus supporté.

IV. Résultats et mesures convenues

01 Accès aux données

1.1	Examens périodiques des droits d'accès des utilisateurs et des fonctions des applications

Les droits d'accès des utilisateurs ne sont pas correctement gérés. Aucun examen régulier de l'utilisateur, fondé sur des vérifications de cohérence, n'est réalisé pour les sites de stockage des données du Fonds mondial.

Un modèle de gestion d'identité fédérée est utilisé au Fonds mondial pour créer, supprimer et gérer automatiquement les utilisateurs et les droits sur les systèmes du Fonds mondial. Un tel modèle convient pour insérer de nouveaux utilisateurs et droits d'accès émanant de l'appartenance à un groupe. Les autorisations peuvent être révoquées dans le cadre du processus de résiliation, lorsqu'un utilisateur est supprimé d'Active Directory. [8,9]

- L'efficacité du modèle est plus limitée si un utilisateur final change simplement de service ou de centre de coûts que s'il quitte l'organisation. Dans le premier cas, ses identifiants ne changent pas et son appartenance à l'ancien service n'est pas toujours supprimée par le propriétaire du groupe.

- Un autre facteur aggravant est le fait qu'aucun examen formel des droits d'accès des utilisateurs n'ait été réalisé depuis la suppression du poste de responsable de la sécurité des systèmes d'information en 2012.

S'agissant de la plateforme ERP[10], le Bureau de l'inspecteur général a relevé que des utilisateurs supprimés dans Active Directory, principalement des consultants ou des contractants ayant quitté l'organisation, existaient toujours et bénéficiaient toujours de tous leurs droits et accès dans le système du prestataire ERP. Néanmoins le risque entraîné par l'accès indu de ces utilisateurs est largement atténué, car l'accès à la suite E-Business est uniquement possible via une connexion sur un ordinateur du Fonds mondial, ce qui est habituellement impossible pour les consultants et contractants qui ont quitté l'organisation.

- L'accès aux comptes de service n'est pas limité aux systèmes sur lesquels ils fonctionnent. Par exemple, un compte de service pour une application ou un groupe de serveurs donné doit disposer d'une restriction d'accès à ces systèmes.[11] Pour les comptes de services privilégiés, tels que ceux bénéficiant de droits d'administration de domaine, une description détaillée de leur utilisation ainsi que la possibilité d'identifier le propriétaire de leur application doit être utilisée dans Active Directory comme attribut (l'attribut « gestionnaire » est une possibilité).

Dans de nombreux systèmes, y compris les contrôleurs de domaine, aucun agent DELL Secure Works n'est installé pour le contrôle des utilisateurs.[12,13]

- La piste d'audit pour l'utilisation des comptes administratifs et privilégiés ne dispose pas d'informations suffisantes et aucun contrôle n'existe pour compenser le manque de suivi.

[8] Federated Identity Management permet aux utilisateurs précédemment authentifiés dans l'environnement du Fonds mondial, d'accéder aux services cloud.
[9] Service Microsoft directory permet l'identification et l'authentification des utilisateurs et des ordinateurs.
[10] Une solution intégrée pour applications et logiciel professionnel comprenant divers modules
[11] Comptes fonctionnels exécutant une tâche, un service ou une tâche planifiée anonymement sur un serveur ou un poste de travail. De manière générale, les comptes de service ne sont pas liés à des utilisateurs nommés, mais à des applications
[12] Un serveur d'authentification Windows
[13] Un agent est un programme informatique qui agit pour le compte d'un utilisateur ou d'un programme et qui, généralement, extrait des informations pour les insérer dans ou les extraire d'un système de gestion centralisé.

Mesures de gestion convenues

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 bénéficient 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.

- Effectuant 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 privilégié.

Propriétaire : Responsable des systèmes d'information
Date limite : 31 décembre 2015

1.2	Matrice de répartition des tâches pour la plateforme ERP et contrôle des accès des utilisateurs

La matrice de répartition des tâches pour l'application ERP n'est pas formalisée et les contrôles visant à évaluer les fonctions et responsabilités incompatibles dans l'environnement ERP ne sont pas effectués.

La matrice de répartition des tâches pour la suite d'applications ERP n'est pas suffisamment formalisée dans les différentes fonctions du service des finances. Les utilisateurs qui bénéficient de plus de droits que la lecture seule ont accès à de nombreux modules. L'analyse du Bureau de l'inspecteur général a relevé que, en pratique, les propriétaires accordaient les autorisations selon le « besoin d'en connaître », en fonction du poste de l'utilisateur au Fonds mondial, mais il n'existe pas de répartition claire de la matrice des tâches au sein de la division Finances, informatique, achats et administration.

Sans matrice de responsabilité claire, le risque lié aux responsabilités pouvant engendrer d'éventuels conflits entre les modules de la solution ERP accessibles aux employés du service des finances reste présent.

Mesures de gestion convenues

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 d'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

1.3	Politiques, fonction de sécurité informatique et sensibilisation des utilisateurs.

La fonction de sécurité du système d'information n'existe pas au sein de l'organisation, la politique de sécurité informatique n'est pas mise à jour régulièrement et aucune formation de sensibilisation des employés à la sécurité informatique n'est organisée.

- Il n'existe aucune fonction de sécurité représentée par un responsable de la sécurité des systèmes d'information, car ce poste a été supprimé après 2012. Les questions de sécurité informatique ont été déléguées à l'équipe de services de maintenance et d'infrastructure technique. Un poste de responsable de la sécurité des systèmes d'information a récemment été recréé au sein de l'organisation.

- Le Bureau de l'inspecteur général a observé que l'actuelle politique informatique est bien communiquée et est disponible en ligne pour les utilisateurs au sein de l'organisation. Cependant, son contenu est obsolète et ses informations ne reflètent pas nécessairement la situation actuelle de l'organisation, en particulier s'agissant de la protection des données, de l'utilisation personnelle et raisonnable de ressources, d'une politique en matière de rangement du bureau, des formations régulières de sensibilisation à la sécurité informatique, d'une politique de mots de passe ou d'une classification de sécurité.

- À l'heure actuelle, le Fonds mondial ne propose aucun document ni aucune formation de ses employés sur la sensibilisation à la sécurité informatique, alors que la sensibilisation à la sécurité est l'un des principaux objectifs de la gestion informatique cette année.

Mesures de gestion convenues

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 élaborera, en collaboration avec les ressources humaines, une série de séances de formation sur la sensibilisation à 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 : 31 décembre 2015

1.4	Classification, protection et confidentialité des données.

Il n'existe aucune politique de classification des données pour évaluer et formaliser le niveau de confidentialité et de protection nécessaire pour chaque type de données.

À la suite de l'audit de haut niveau du Bureau de l'inspecteur général en avril 2014, les services informatique et juridique ont lancé un projet commun relatif à la classification des données et les responsabilités en matière de conception du cadre et de la politique ont été clairement définies. La date limite de finalisation du projet a été fixée au 1er octobre 2014.

Actuellement, des projets de politique de classification de l'information du Fonds mondial, les directives sur la gestion de l'information et la politique de protection des données sont en cours d'examen. La version provisoire du cadre de classification des données établi par le service juridique définit quatre catégories de classification : *public, interne, confidentiel et à accès limité*. Toutefois, la classification des données du Fonds mondial selon les catégories susmentionnées n'a pas été mise en œuvre et les systèmes informatiques n'appliquent ni ne prennent en compte de telles classifications.

Le Fonds mondial ne met pas en œuvre un cryptage matériel pour protéger contre la perte ou le vol les données de l'organisation stockées localement sur des ordinateurs portables ou d'autres supports externes. Cela limite également les garanties que peut offrir le Fonds mondial en termes de gestion des informations confidentielles. De plus, ces données englobent les informations sur les employés et sur les partenaires commerciaux et techniques, ainsi que sur les maîtres d'œuvre et les bénéficiaires. Toute personne ayant un accès physique aux serveurs, aux postes de travail ou aux ordinateurs portables peut accéder aux données. Le responsable des systèmes d'information estime que le manque de perfectionnement au niveau des processus et des utilisateurs du Fonds mondial suppose que le cryptage sera complexe et aboutira probablement à une perte des données.

Mesures de gestion convenues

S'agissant du projet de classification des données, les informaticiens apporteront leur contribution aux principes directeurs que le service juridique finalise. 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 diffusion restreinte*) 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

1.5	Les politiques de mots de passe en vigueur ne sont pas assez efficaces.

L'analyse des politiques de mots de passe en vigueur a révélé des faiblesses et des incohérences. La politique d'expiration des mots de passe pouvait être ignorée manuellement pour certains comptes utilisateurs.

Les politiques de mots de passe mises en œuvre dans les domaines d'authentification ne répondent pas aux exigences fixées par l'actuelle politique de sécurité du Fonds mondial. Des paramètres incohérents ont été observés en ce qui concerne l'historique, la durée de vie des mots de passe, les exigences de complexité et la politique d'expiration.

Mesures de gestion convenues

Le Secrétariat du Fonds mondial améliorera les processus en place concernant l'accès aux systèmes, notamment en :

- prenant immédiatement des mesures visant s'assurer que tous les comptes utilisateurs nommés, indépendamment de leur rôle 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

1.6	Accès au réseau de technologie d'information du Fonds mondial

L'accès aux services à distance, y compris l'accès à distance au réseau du Fonds mondial via Virtual Private Network, repose une authentification à un facteur.

De manière générale, un nom d'utilisateur et un mot de passe servent à contrôler l'accès à des systèmes à accès limité. Or, même si des mots de passe complexes sont utilisés, cette authentification comporte des faiblesses inhérentes importantes. Il est recommandé de remplacer l'authentification à un facteur par une authentification multifacteur. Une authentification multifacteur consiste en un accès aux ressources qui repose sur un objet en votre possession (téléphone, token) en complément de quelque chose que vous connaissez (identifiant, mot de passe). Un avantage remarquable de l'authentification multifacteur est qu'elle résiste aux attaques communes qui consistent à obtenir le mot de passe à partir d'un ordinateur infecté ou lorsqu'il est transmis de l'ordinateur à l'application destinataire.

À l'heure actuelle, l'accès VPN au réseau de l'organisation et l'accès à d'autres services à distance, tel que webmail, repose sur un système d'authentification à un facteur.

Outre l'accès à distance aux systèmes, le Fonds mondial ne contrôle, actuellement, pas suffisamment l'accès à son réseau filaire. Bien que l'accès sans fil au réseau de l'organisation soit suffisamment contrôlé à l'aide de certificats de cryptage, il est tout de même possible de connecter un ordinateur externe au réseau filaire institutionnel et d'obtenir une adresse IP au niveau de l'ordinateur du client.[14]

Le réseau du Fonds mondial est basé sur des commutateurs réseau qui se trouvent à chaque étage ainsi que dans les centres de données. Ces systèmes complexes peuvent être configurés et gérés comme des ordinateurs serveurs. L'interface de configuration est accessible à l'aide d'un protocole Telecommunication Network (Telnet) non sécurisé.[15,16] En effet, Telnet envoie toutes les données, y compris les mots de passe, en texte clair sur le réseau. Une personne ayant accès au réseau physique entre un administrateur et le commutateur peut aisément obtenir les mots de passe et altérer la configuration.

Mesures de gestion convenues

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

[14] Adresse IP : numéro d'identification unique attribué de manière statique ou dynamique et caractérisant un équipement dans un réseau basé sur le protocole Internet (IP)
[15] Telnet est un protocole qui imite une interface de ligne de commande sur des systèmes à distance. Bien que globalement dépassé, il est toujours utilisé pour gérer les périphériques réseau tels que les commutateurs ou les routeurs.
[16] Un commutateur est un appareil qui relie des ordinateurs et d'autres équipements sur un réseau. À la différence d'une plateforme qui diffuse des paquets d'informations à tous les hôtes connectés, un commutateur peut filtrer la communication selon les ports.

02 Précision des données

2.1	Politique d'entrée et précision des données des utilisateurs

La procédure d'entrée pour les contractants et les employés à temps plein est exécutée selon différents processus informatiques et est gérée par différents services.

L'entrée d'employés à temps plein au Fonds mondial est gérée par le service des ressources humaines et celle des consultants par le service des achats. Chaque procédure utilise des systèmes et des processus informatiques différents pour fournir des ressources et des accès.

Le GFS sert actuelle à conserver les données du personnel permanent alors les fiches des contractants sont créées à l'aide d'une procédure distincte (formulaire d'application Service-Now[17]) dans Active Directory.

Par conséquent, cela peut entraîner des anomalies dans les données. Par exemple, certains consultants n'avaient pas de registre pour un supérieur hiérarchique responsable dans Active Directory au moment de l'audit. Les registres suivants contenaient des erreurs en termes d'affectation des noms d'utilisateur : Active Directory, GFS basé sur ERP et la base de données KABA (contrôle de l'accès physique au bâtiment).

Des incohérences dans la gestion des utilisateurs peuvent aboutir à des contractants non gérés ou à du personnel permanent toujours identifié comme « travailleur occasionnel » alors qu'il est devenu employé à temps plein, ou encore à la conservation d'un accès physique alors que la personne a quitté l'organisation. Consolider les documents d'activité probants dans le GFS et unifier les procédures pour les contractants en ajoutant une date d'expiration correspondant au terme de leur contrat pourrait améliorer la procédure de gestion des utilisateurs.

Mesures de gestion convenues

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

[17] Un des prestataires de services cloud du Fonds mondial

2.2	Contrôle des serveurs, des solutions antivirus et évaluation de la vulnérabilité.

Aucun système de détection d'intrusion (IDS) ou de prévention des intrusions (IPS) n'est en place aux limites du périmètre réseau de l'organisation. Certains serveurs ne sont pas contrôlés par une solution antivirus.[18,19]

Après avoir évalué les solutions anti-malware et interrogé l'ingénieur réseau, le Bureau de l'inspecteur général a remarqué qu'aucune solution IDS/IPS n'était en place aux limites du périmètre réseau de l'organisation. De tels systèmes sont conçus pour contrôler et détecter des activités malveillantes sur le réseau, pour créer un journal et un rapport sur ces activités, et enfin pour les bloquer ou les éviter. Une activité malveillante comprend notamment un trafic réseau créé par un virus ou un logiciel néfaste similaire.

Selon le journal d'activité de la solution antivirus de l'organisation, de nombreux serveurs ne sont actuellement pas surveillés. Des contrôles de cohérence effectués grâce aux résultats d'Active Directory ont révélé que certains serveurs n'étaient pas protégés contre les virus puisqu'aucun antivirus n'était installé. Le service informatique a indiqué qu'il s'agissait d'un choix délibéré fondé sur la recommandation du fournisseur de logiciel qui conseillait d'arrêter le scan antivirus dans certains cas. Néanmoins, ces exceptions ne sont pas identifiées ou documentées et il n'existe dès lors aucune information de vérification à cet égard.

Les évaluations de la vulnérabilité effectuées sur un éventail limité de 50 serveurs Windows choisis au hasard ont abouti à une notation « *à haut risque* » (selon le classement Microsoft) pour 31 serveurs, principalement en raison de correctifs de sécurité non appliqués.[20]

Mesures de gestion convenues

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

[18] Un IPS, ou système de prévention des intrusions, est une solution de sécurité réseau. Contrairement à l'IDS, il tentera de bloquer/d'arrêter automatiquement l'activité malveillante.
[19] Un IDS, ou système de détection d'intrusion, est un dispositif ou un logiciel qui contrôle les activités malveillantes ou les violations de politique sur un réseau ou sur un système hôte. Il crée des journaux, des alertes et des rapports sur ces activités.
[20] Un correctif de sécurité ou hotfix est une mise à jour de code qui corrige les faiblesses d'un système d'exploitation ou d'une application.

03 Agilité des données

3.1	Gestion du changement et contrôles du développement de système

Les contrôles de la gestion du changement et du développement de système se sont avérés efficaces, mais des améliorations sont nécessaires en matière de suivi des demandes en matière de gestion du changement.

Les liens entre l'infrastructure et les opérations ne sont pas perceptibles dans le système de demandes en matière de gestion du changement. Par exemple, si un prérequis existe au niveau de l'infrastructure, il ne se reflète pas nécessairement dans la demande de changement opérationnel.

Un processus de travail distinct est nécessaire pour les prestataires de services cloud qui gèrent leur propre processus de demande de changement, en particulier pour la plateforme ERP ou pour le fournisseur du centre de données virtuelles (VDC). [21, 22] Les changements apportés exclusivement via ces plateformes ne sont pas toujours identifiables dans l'outil Service Now. Il est possible d'ajouter manuellement toutes les demandes de changement dans Service Now, bien que cela ne soit actuellement pas effectué régulièrement.

Cela signifie que les changements dans un système peuvent avoir une incidence négative et imprévue sur d'autres systèmes, détectée uniquement lorsque le changement est opéré. En outre, puisque ces modifications ne sont pas enregistrées dans une base de données centrale, il peut être plus difficile d'identifier l'origine d'un problème.

Mesures de gestion convenues

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

[21] Les prestataires de services externes dont les systèmes sont situés sur le cloud font confiance aux utilisateurs authentifiés du Fonds mondial et leur accordent l'accès à leurs plateformes de service.
[22] Un fournisseur de service d'hébergement administré du Fonds mondial

04 Disponibilité des données

4.1	Analyse des incidences et plan de continuité d'activité

Toutes les données du Fonds mondial ne font pas l'objet d'une sauvegarde fiable puisque le projet de gestion du plan de reprise n'a pas encore été finalisé.

À la suite de l'audit du Bureau de l'inspecteur général d'avril 2014, le service informatique a reconnu que la reprise informatique après incident devait devenir une priorité pour le Fonds mondial. Un projet visant la mise en œuvre d'un plan complet de reprise après incident a été présenté au Comité d'audit et d'éthique en octobre 2014 et fixait la réalisation d'un test complet de reprise pour le deuxième trimestre 2015. Toutefois, au moment de l'audit, le Bureau de l'inspecteur général a relevé ce qui suit :

- L'analyse des incidences sur les activités ainsi que la création du plan de continuité d'activité (PCA) n'ont pas été signées par le responsable des systèmes d'information. [23, 24]
- Au moment de l'audit, toutes les données devant être protégées avaient migré vers l'infrastructure Data Protection Manager.[25] On remarque cependant que la base de données SharePoint 2007 n'était pas comprise dans Data Protection Manager, car elle entraînait des échecs répétés de toute la sauvegarde en raison de sa taille. [26] Une sauvegarde distincte a été mise en place pour cette base de données, mais elle s'est avérée inefficace et a échoué au moment de l'audit.
- Le nombre de connexions VPN disponibles en cas de reprise complète après sinistre ne permet pas l'accès simultané de tous les employés du Secrétariat. En cas de reprise complète après incident, le nombre maximal de connexions VPN disponibles est actuellement limité à 242. En outre, le plan de continuité d'activité considère que tous les utilisateurs pourront continuer à travailler sur leur ordinateur portable, peu importe leur fonction. Cependant, cela suppose que sans contrôle d'accès hiérarchisé, l'accès aux utilisateurs clés pourrait ne pas être disponible en temps opportun.

Mesures de gestion convenues

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

[23] Analyse des incidences sur les activités : évaluation et classification des applications et des éléments d'une infrastructure qui, au final, définiront un niveau de menace.
[24] PCA, plan de continuité d'activité
[25] DPM, Data Protection Manager, est une solution de sauvegarde centralisée de Microsoft
[26] Une base de données SharePoint 2007 est utilisée comme référentiel de données dans l'ancien environnement Intranet du Fonds mondial. Le cycle de vie du produit a pris fin et n'est plus supporté.

V. Tableau des mesures convenues

N°	Catégorie	Mesure de gestion convenue	Propriétaire/date
1.1	Examens périodiques des droits d'accès des utilisateurs et des fonctions des applications	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 privilégié.	**Propriétaire :** Responsable des systèmes d'information **Date limite :** 31 décembre 2015
1.2	Matrice de répartition des tâches pour la plateforme ERP et	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	**Propriétaire :** Responsable des systèmes d'information gestionnaire, systèmes

	contrôle des accès des utilisateurs.	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.	financiers et processus **Date limite :** 30 juin 2015
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 : En achevant le processus de recrutement d'un responsable de la sécurité des systèmes d'information qui a débuté au cours de l'audit avec la diffusion de l'annonce. Un candidat a déjà été sélectionné et commencera en mars. S'agissant de l'amélioration la fonction de sécurité au sein de l'organisation, les documents liés à la sécurité seront régulièrement mis à jour. En veillant à ce que le service informatique élabore, en collaboration avec les RH, une série de séances de formation sur la sensibilisation à la sécurité de l'information et les propose au Comité exécutif de direction pour approbation et mise en œuvre.	**Propriétaire :** Responsable des systèmes d'information **Date limite :** 31 décembre 2015
1.4	Classification, protection des données et confidentialité	S'agissant du projet de classification des données, les informaticiens apporteront leur contribution aux principes directeurs que le service juridique finalise. 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

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
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
2.1	Politique d'entrée et précision des données des utilisateurs	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.	**Propriétaires :** Responsable des systèmes d'information **Date limite :** 31 décembre 2015
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.	**Propriétaire :** Responsable des systèmes d'information **Date limite :** 30 juin 2015

		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.	
3.1	Gestion des modifications et contrôles du développement du 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
4.1	Analyse des incidences et 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

VI. 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.

VII. 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.