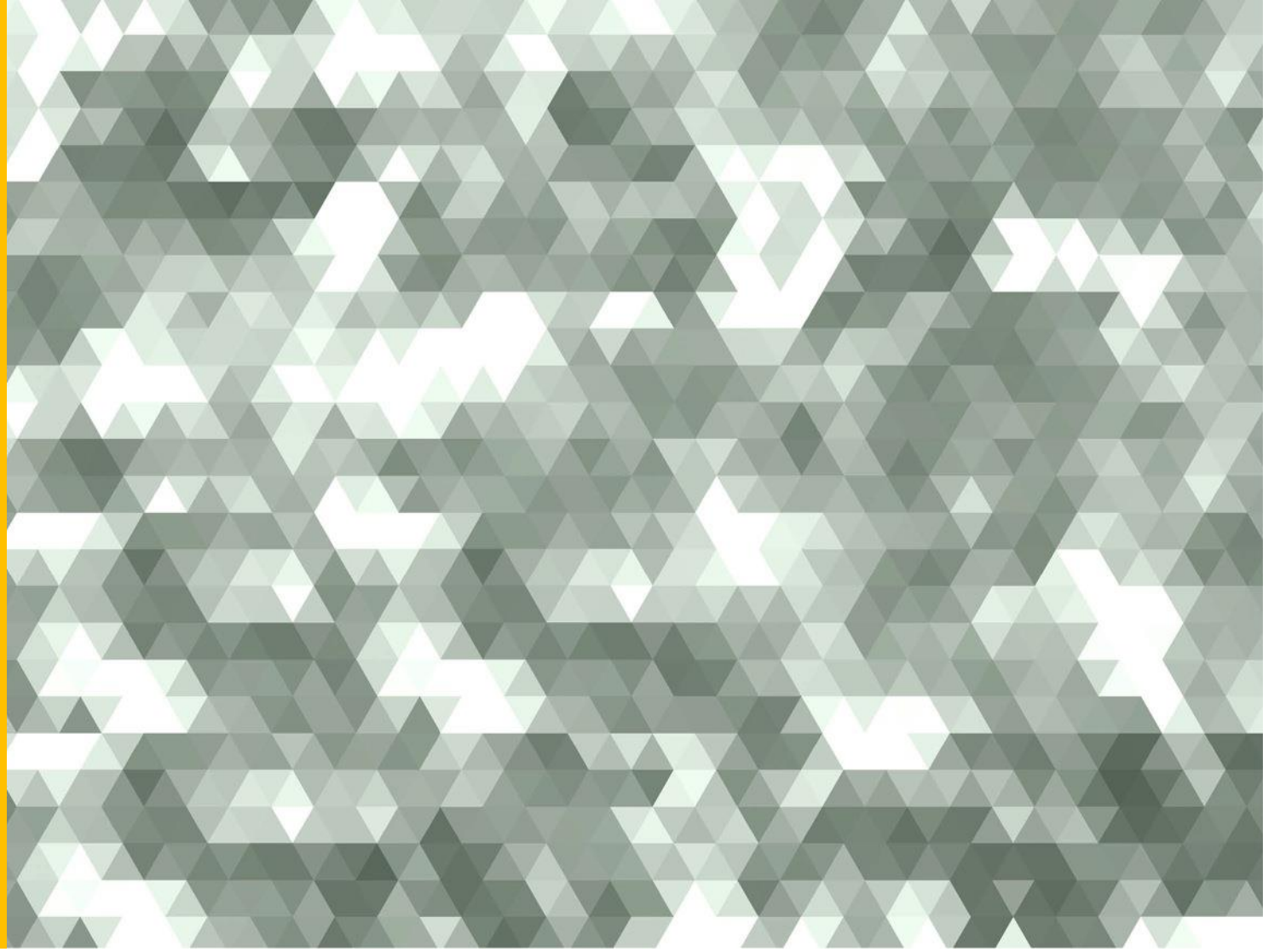


Rapport d'audit

Le cloud computing au Fonds mondial
Efficacité des contrôles informatiques

GF-OIG-17-013
28 juin 2017
Genève, Suisse

La version en langue française de ce rapport est une traduction de courtoisie, la version en langue anglaise faisant foi.

The Global Fund
Office of the Inspector General

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 viabilité du Fonds mondial en veillant à ce qu'il prenne les bonnes mesures pour accélérer la fin des épidémies de VIH, de tuberculose et de paludisme. Au travers d'audits, d'enquêtes et d'activités de consultance, le Bureau de l'Inspecteur général encourage les bonnes pratiques, limite les risques et fait état des actes répréhensibles dans un souci de transparence et d'exhaustivité.

Créé en 2005, le Bureau de l'Inspecteur général est une unité indépendante du Fonds mondial, mais qui en fait néanmoins partie intégrante. Il rend compte au Conseil d'administration par l'intermédiaire de son Comité d'audit et d'éthique, et sert les intérêts de toutes les parties prenantes du Fonds mondial. Il exerce ses activités conformément aux Normes internationales pour la pratique professionnelle de l'audit interne et aux Lignes directrices uniformes en matière d'enquête de la Conférence des enquêteurs internationaux.

Nous contacter

Le Fonds mondial est d'avis que chaque dollar compte et mène une politique de tolérance zéro vis-à-vis de la fraude, de la corruption et du gaspillage, empêchant les ressources de parvenir à ceux qui en ont besoin. Si vous soupçonnez des irrégularités ou des actes répréhensibles dans les programmes soutenus par le Fonds mondial, signalez-les au Bureau de l'Inspecteur général, aux coordonnées indiquées ci-après. Par exemple, les actes répréhensibles suivants doivent être signalés : vol d'argent ou de médicaments, utilisation de crédits du Fonds mondial ou d'autres actifs à des fins personnelles, fausse facture, organisation de formations factices, contrefaçon de médicaments, irrégularités au niveau des procédures d'appels d'offres, subornations et pots-de-vin, conflits d'intérêt, violation de droits de l'Homme, etc.

Formulaire en ligne >
Disponible en anglais, espagnol, français et russe.

Bureau de l'Inspecteur général
Le Fonds mondial
Chemin de Blandonnet 8, CH-1214
Genève, Suisse

Courriel
ispeakoutnow@theglobalfund.org

Ligne téléphonique gratuite :
+1 704 541 6918
Service disponible en anglais, arabe, chinois, espagnol, français et russe

Messagerie téléphonique 24 h/24 :
+41 22 341 5258

Télécopie – Ligne de télécopie dédiée :
+41 22 341 5257

Plus d'infos www.theglobalfund.org/oig

Rapport d'audit

Les audits du Bureau de l'Inspecteur général examinent les systèmes et les procédures du Fonds mondial et des pays, aux fins d'identifier les risques susceptibles de compromettre la capacité de l'institution à éliminer les trois épidémies, conformément à sa mission. Les audits couvrent généralement trois grands domaines : la gestion des risques, la gouvernance et le suivi stratégique. Ils visent globalement à améliorer l'efficacité du Fonds, en vue de garantir l'impact optimal des crédits qui lui sont confiés.

Rapport consultatif

Les rapports consultatifs du Bureau de l'Inspecteur général visent à poursuivre la mission et les objectifs du Fonds mondial, au moyen d'engagements à valeur ajoutée, en faisant appel aux compétences professionnelles des vérificateurs et des enquêteurs du BIG. Le Conseil d'administration, les comités ou le Secrétariat du Fonds mondial peuvent demander un rapport consultatif spécifique à tout moment. En concertation avec le demandeur, le Bureau de l'Inspecteur général peut décider de publier ce rapport.

Rapport d'enquête

Les enquêtes du Bureau de l'Inspecteur général examinent des allégations d'actes répréhensibles qui se seraient produits, ou des informations relatives à des fraudes ou des abus susceptibles d'entraver la capacité du Fonds mondial à éliminer les trois épidémies, conformément à sa mission. Le Bureau de l'Inspecteur général mène des enquêtes administratives et non pas pénales. Ses conclusions s'appuient sur des faits et les analyses y afférentes, des conclusions raisonnables pouvant parfois être tirées de faits établis.

Table des matières

1. Résumé....4
   1.1. Opinion....4
   1.2. Réalisations clés et bonnes pratiques....4
   1.3. Principales difficultés et risques y afférents....4
   1.4. Notation....5
   1.5. Résumé des actions convenues de la Direction....5
2. Historique et contexte....7
   2.1. Contexte général....7
   2.2. Environnement technique des systèmes d'information....8
   2.3. Organisation des systèmes d'information au Fonds mondial....8
3. Aperçu de l'audit....9
   3.1. Objectifs....9
   3.2. Portée....9
   3.3. Correction des faiblesses identifiées précédemment....10
4. Constatations....11
   4.1. Absence de stratégie et de plan de mise en œuvre relatifs à l'adoption du cloud computing 11
   4.2. Gestion insuffisante des risques liés au cloud computing....13
   4.3. Gestion sous-optimale des prestataires de services cloud....16
   4.4. Accès aux systèmes d'information – Lacunes en matière d'accès aux données et de contrôles de sécurité des applications dans le cloud....18
   4.5. Exactitude des données informatiques – Faiblesses en matière de gestion des interfaces informatiques et des contrôles de cryptage, affectant l'exactitude des données....19
   4.6. Amélioration requise en matière de planification des reprises d'activité après incident et de tests de certaines applications cloud....21
5. Tableau des actions convenues....22

Annexe A : Classification générale des notations de l'audit....25

Annexe B : Méthodologie....26

1. Résumé

1.1. Opinion

Le cloud computing est la fourniture à la demande de ressources informatiques, d'applications à des centres de données, sur Internet, facturées à l'utilisation[1]. Le Fonds mondial a commencé à utiliser le cloud computing aux fins de se procurer des services informatiques en 2014. Environ 60 % de l'infrastructure et des applications informatiques sont actuellement gérés par des prestataires externes au moyen de techniques liées au cloud computing et à d'autres types de services externalisés et hébergés. Les activités informatiques ont ainsi gagné en souplesse, du fait d'une meilleure disponibilité des services. Cependant, l'absence d'une stratégie globale et la gestion limitée des risques y afférents ont nui à l'efficacité du déploiement des services de cloud computing. Par conséquent, la conception d'une stratégie en matière de cloud computing alignée sur les besoins du Fonds mondial et la gestion des risques y afférents nécessitent une **nette amélioration**.

Globalement, le Secrétariat a amélioré ses contrôles informatiques depuis le dernier audit du Bureau de l'Inspecteur général en 2015 (voir la section 3.3). Néanmoins, l'accès aux données dans le cloud et leur exactitude peuvent encore être améliorés. Cela dit, aucun cas majeur de perte de données ou d'interruption des services n'a été relevé depuis 2015. En conséquence, les contrôles informatiques de base sont considérés **partiellement efficaces.**

1.2. Réalisations clés et bonnes pratiques

Adoption du cloud computing : Le Fonds mondial a fait appel à des partenaires de premier plan pour ses services de cloud computing. L'externalisation de la gestion opérationnelle des services informatiques clés comporte plusieurs avantages, dont la mise à jour régulière des applications et logiciels hébergés sur serveur par les prestataires de services, la réduction des sites de gestion des données au sein du Fonds mondial, et la possibilité pour le personnel d'accéder aux données à distance via une connexion Internet.

Amélioration des contrôles informatiques : Le service informatique du Fonds mondial s'est considérablement agrandi depuis 2015, de pair avec les besoins de l'institution. Les contrôles informatiques de base se sont améliorés depuis le dernier audit du Bureau de l'Inspecteur général en 2015. Le BIG avait alors identifié des faiblesses et des lacunes importantes en matière de sécurité, qui auraient pu être exploitées à des fins malveillantes. Ces faiblesses ont depuis été largement comblées.

Plusieurs initiatives ont permis de renforcer les contrôles informatiques en matière d'accès, d'exactitude des données et de gestion des reprises d'activité après un incident. Les politiques relatives aux mots de passe ont été renforcées et un plan de reprise d'activité après incident a été établi pour les applications informatiques existantes. Des tests de pénétration et des évaluations de la vulnérabilité des applications clés ont été réalisés aux fins de garantir la mise en place de mesures de protection appropriées. De plus, une politique de réglementation de la sécurité informatique est en cours d'élaboration afin de fournir des directives sur les pratiques informatiques à risque, notamment la transmission des données.

1.3. Principales difficultés et risques y afférents

Absence d'une stratégie exhaustive en matière de cloud computing : Aucune stratégie, aucun plan de mise en œuvre n'ont été clairement établis aux fins d'adopter le cloud computing comme principal outil de prestation de services. Cette démarche visant à limiter la quantité de services fournis directement par l'infrastructure contrôlée par le Fonds mondial ou lui appartenant a fragilisé une infrastructure déjà fragmentée. Par ailleurs, le Secrétariat n'a pas évalué l'impact à

[1] https://www.ibm.com/cloud-computing/learn-more/what-is-cloud-computing

long terme du cloud computing sur l'institution. Le cloud computing au Fonds mondial a évolué naturellement, sans démarche et sans plan de déploiement clairement définis. L'absence de raisonnement clairement formulé et d'objectifs définis en matière de cloud computing compliquent l'évaluation des avancées après trois années de mise en œuvre.

Gestion limitée des risques : Dans le cadre d'une solution de cloud computing, plusieurs risques informatiques sont généralement transférés au prestataire de services. Cependant, le profil des risques informatiques évolue de telle manière que l'institution s'expose plus fortement à d'autres types de risques, tels que la gestion des données, les performances du prestataire et les risques juridiques. Par exemple, le cloud computing permet au Fonds mondial de stocker des données dans plusieurs centres, ce qui réduit les risques de perte totale en cas d'incident majeur. Parallèlement, cette réduction des risques opérationnels peut s'accompagner d'une hausse des risques juridiques, la confidentialité des données du Fonds pouvant être fragilisée si celles-ci sont stockées dans des pays ne lui accordant pas de privilèges et d'immunités et pouvant contraindre l'institution à produire des documents confidentiels. De plus, le Fonds mondial risque d'accroître excessivement sa dépendance envers certains prestataires et de se voir imposer des changements des dispositions contractuelles contraires à ses intérêts. Ces risques et d'autres risques similaires n'ont pas encore été formellement examinés, pas plus que l'impact potentiel sur les activités de l'institution n'a été évalué et, le cas échéant, donné lieu à des mesures d'atténuation clairement définies.

Lacunes en matière de gestion des prestataires de services : Le service informatique a confié la gestion de plusieurs prestataires de services à des membres de son personnel. Cependant, l'absence de cadre clair et de procédures formalisées ont entraîné des incohérences au sein de l'institution. De ce fait, les principaux aspects des résultats des prestataires ne sont pas contrôlés efficacement.

1.4. Notation

Objectif n° 1. Aucun plan de mise en œuvre, aucune stratégie n'orientent actuellement l'adoption du cloud computing au sein du Fonds mondial. La justification de l'adoption de services dans le cloud et les objectifs y afférents ne sont toujours pas définis. En conséquence, l'établissement d'une stratégie de cloud computing alignée sur les besoins institutionnels et opérationnels du Fonds mondial **nécessite une nette amélioration**.

Objectif n° 2. Les risques liés à l'adoption du cloud computing doivent être évalués et des mesures doivent être prises aux fins de les atténuer. Ainsi, la gestion des risques liés au cloud computing **nécessite une nette amélioration**.

Objectif n° 3. Le Fonds mondial a considérablement amélioré ses contrôles informatiques depuis 2015. La récupération des données et la sensibilisation aux questions de sécurité ont été renforcées. Cependant, les contrôles relatifs à l'exactitude des données et à leur accès doivent être améliorés. En conséquence, les contrôles informatiques sont considérés **partiellement efficaces.**

1.5. Résumé des actions convenues de la Direction

Le Secrétariat du Fonds mondial entend atténuer les risques identifiés par le Bureau de l'Inspecteur général au moyen des actions convenues de la Direction ci-après :

- Établissement d'une stratégie informatique dotée d'objectifs clairs soumis à l'approbation du Comité exécutif de direction.
- Amélioration des mécanismes de gouvernance informatique, au moyen d'une restructuration du Conseil de l'architecture institutionnelle (un conseil interne établi en 2016 aux fins de superviser les décisions relatives aux systèmes d'information).
- Amélioration de la gestion des risques informatiques, au moyen de l'identification des risques potentiels liés au cloud computing, d'une évaluation de leur impact et de mesures visant à les atténuer. Les risques identifiés et les mesures d'atténuation y afférentes seront intégrés dans le

registre institutionnel des risques du Fonds mondial, examiné trimestriellement par le Comité exécutif de direction.

- Renforcement des spécifications en matière de sécurité des transferts de données, au moyen d'une actualisation des directives du Fonds mondial sur la gestion et la classification de l'information.
- Établissement d'une matrice de séparation des tâches pour les applications restantes ; et poursuite de l'amélioration et du test des plans de reprise de l'activité après incident.

2. Historique et contexte

2.1. Contexte général

Une entreprise adoptant le cloud computing transfère la gestion et la prestation de ses besoins informatiques (infrastructure, traitement, stockage et/ou applications) à un tiers appelé prestataire de services cloud. S'il est bien géré, le cloud computing peut comporter des avantages considérables pour l'entreprise, notamment des économies liées à une réduction des dépenses en investissements dans l'infrastructure informatique ; un assouplissement de la puissance informatique au gré de la fluctuation des volumes de données générées ; une amélioration sensible de la souplesse des activités informatiques du fait d'une plus grande disponibilité des ressources informatiques ; la délégation des responsabilités liées à la mise à jour des logiciels et de la sécurité ; une plus grande réactivité à l'évolution des besoins opérationnels ; et l'opportunité d'intégrer la gestion des données et de l'information à l'échelle de l'entreprise.

Ces avantages potentiels comportent des risques qui doivent être pleinement pris en compte. Les risques ci-après en font partie : accès non autorisé à des informations confidentielles gérées hors des frontières nationales du siège de l'institution ; vulnérabilités juridiques, des données stratégiques pouvant être stockées dans des pays n'accordant pas de privilèges et d'immunités au Fonds mondial, dépendance accrue envers le prestataire de services externe, entraînant un risque de vulnérabilité en cas de résultats médiocres ; et inefficacités financières potentielles si l'adoption du cloud computing ne permet pas de réduire les risques de redondances ou de duplications sur l'ensemble de l'écosystème dans le cloud.

Cette multiplicité de réelles opportunités pour l'institution et de risques importants souligne la nécessité d'établir une stratégie structurée et dûment pensée, définissant clairement l'état souhaité de l'infrastructure informatique ; une feuille de route structurée permettant d'y parvenir ; une procédure efficace d'analyse des compromis entre les risques et les avantages ; et une gouvernance informatique solide afin d'examiner et valider les choix stratégiques de haut niveau.

Le Fonds mondial a acquis sa première solution de cloud computing en 2014. En 2013-14, il a externalisé une grande partie de ses applications et de son infrastructure informatique à des prestataires de services externes. Le Fonds a adopté un modèle hybride[2] de cloud computing, afin de tenir compte de ses systèmes informatiques existants[3], des critères de sécurité et des capacités de personnalisation des systèmes. Le Fonds mondial utilise des clouds public et privé, ainsi que des services d'hébergement à distance plus traditionnels. Un cloud public stocke les données de plusieurs entreprises et les rend accessibles à tous les utilisateurs. Le prestataire de services prend des mesures aux fins de protéger l'accès aux données de chaque entreprise. Le Fonds mondial fait également appel à des services cloud privés, adaptés à ses besoins spécifiques. Il utilise également des centres de données virtuels, chargeant un prestataire externe de mettre en service et de maintenir en partie un équipement et des systèmes spécifiques, réservés à son utilisation.

Le Fonds mondial a adopté trois modes de prestation de services dans le cadre du cloud computing :

- *Software as a Service* (SaaS), un mode de fourniture d'applications logicielles sur Internet à la demande, généralement dans le cadre d'un abonnement souscrit auprès de prestataires externes clés. Par exemple, le département de la trésorerie du Fonds mondial utilise des services, SaaS.
- Une solution *Infrastructure as a service* permet au Secrétariat de confier le stockage et la gestion de son infrastructure informatique, notamment les serveurs, à un prestataire de services externe indépendant.
- Un *environnement à la demande* appelé « Platform as a service » (PaaS) est utilisé pour le développement, le test, la fourniture et la gestion d'applications logicielles. Le Secrétariat s'en sert pour ses applications financières et de gestion des subventions dans le cloud.

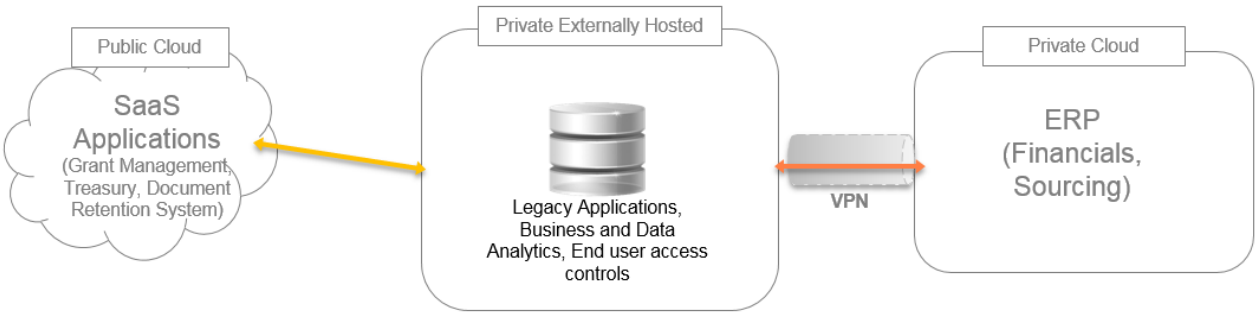
[2] Cloud hybride : mélange de services cloud, d'architectures informatiques internes dans le cloud et d'infrastructures informatiques traditionnelles, formant un modèle hybride utilisant des technologies spécifiques pour répondre à des besoins spécifiques.
[3] Un système hérité est une application ou un produit utilisé régulièrement depuis plus de 24 mois dans le système informatique, dont il est prévu de mettre à niveau la version, de migrer la plate-forme vers une nouvelle version ou d'en changer le modèle, ou de s'en séparer totalement.

2.2. Environnement technique des systèmes d'information

Le Fonds mondial utilise un service d'annuaire « Active Directory » Microsoft pour valider l'authenticité de ses utilisateurs internes et externes. Alors que la majorité des applications et services dans le cloud l'exigent pour autoriser l'accès des utilisateurs aux systèmes, d'autres applications dans le cloud telles que la suite ERP (Enterprise Resource Planning) utilisent des critères d'authentification supplémentaires et autonomes.

Le cloud computing transfère les systèmes de l'institution dans des systèmes partagés. Les utilisateurs accèdent généralement aux applications via Internet. Ainsi, la gestion et la maintenance de l'infrastructure cloud ne sont plus assurés par le Fonds mondial, mais par le prestataire de services, qui protège leur accès au moyen de critères d'authentification supplémentaires.

Le diagramme ci-après fournit un aperçu des services de cloud computing adoptés par le Fonds mondial :



La gestion des changements est assurée par une solution web prenant en charge les mises à jour et les modifications de l'infrastructure et des applications. Un Conseil de contrôle des changements établi en 2014 s'appuie sur une solution web pour gérer les incidents, la maintenance et les demandes de changement. Il se réunit chaque semaine afin d'approuver l'établissement/la modification des systèmes de l'environnement de production, d'évaluer l'état de préparation au déploiement, de garantir le respect des règles en matière de gestion des versions, et d'approuver ou de refuser les changements.

2.3. Organisation des systèmes d'information au Fonds mondial

Le service informatique du Fonds mondial se compose de deux équipes principales : une équipe tournée vers les utilisateurs, et une autre chargée de relations avec les prestataires de services. L'équipe chargée des utilisateurs fournit une assistance informatique aux divisions du Fonds mondial, tandis que l'équipe dédiée aux prestataires de services se charge des services de maintenance, des services techniques et de l'intégration des données. Chaque équipe est dirigée par un responsable des partenaires informatiques, globalement chargé de gérer l'efficacité des services fournis par des prestataires de solutions dans le cloud et traditionnelles utilisés par leurs portefeuilles respectifs.

La gestion des licences logicielles incombe à l'équipe des services de maintenance de l'infrastructure technique. Le service informatique est dirigé par un responsable des systèmes d'information, chargé de la stratégie informatique et de la gouvernance y afférente. Il rend compte au directeur financier. Par ailleurs, des équipes chargées de domaines transversaux tels que la sécurité de l'information, la stratégie et l'infrastructure des systèmes d'information, la gestion des activités et des projets, rendent compte directement au responsable des systèmes d'information. En 2017, le budget total du service informatique alloué au fonctionnement et aux infrastructures s'élève à 31,3 millions de dollars US.

3. Aperçu de l'audit

3.1. Objectifs

Le présent audit vise à fournir une assurance raisonnable sur l'adéquation et l'efficacité des contrôles informatiques du Secrétariat, en particulier des services de cloud computing.

Il vise spécifiquement à déterminer si :

- le cadre et la stratégie liés aux systèmes de l'information dans le cloud sont dûment conçus, conformément aux besoins des activités et du fonctionnement de l'institution ;
- les risques liés au cloud computing sont gérés efficacement ; et
- les contrôles informatiques réalisés par le Fonds mondial et les prestataires de services cloud sont adéquats et efficaces, et offrent un niveau optimal de sécurité et de résultats.

3.2. Portée

Le présent audit comprenait :

- un examen des documents relatifs à la stratégie en matière de services cloud, et de la gestion des risques y afférents au sein du Secrétariat ;
- un examen des politiques et des procédures du Fonds mondial en matière de systèmes d'information ;
- une évaluation des mécanismes d'assurance du Secrétariat relatifs aux prestataires de services cloud ;
- des entretiens de responsables d'applications dans le cloud ;
- une validation de l'architecture informatique et des contrôles de six applications clés dans le cloud ; et
- un examen de 82 domaines de contrôle des six applications cloud sélectionnées, couvrant la sécurité de l'application, la sécurité et l'intégrité des données, l'accès des utilisateurs aux systèmes, la gestion des incidents et de la maintenance, l'établissement des systèmes, la gestion de la connaissance et la planification des reprises de l'activité après incident.

L'équipe de vérificateurs n'a pas visité les prestataires de services cloud, mais elle a examiné les certifications indépendantes fournies par des tiers des contrôles mis en œuvre par les prestataires de services.

3.3. Correction des faiblesses identifiées précédemment

Le BIG avait réalisé un audit de « l'efficacité des contrôles informatiques en 2015 (GF-OIG-15-020), centré sur l'accès, l'exactitude, l'agilité et la disponibilité en matière de données. Un audit de suivi avait été mené en novembre 2015 (GF-OIG-15-020B). Les risques identifiés lors de ces deux audits, liés aux applications informatiques existant à l'époque, ont été traités. Cependant, des risques émergents pourraient voir le jour, du fait de l'évolution de l'environnement informatique.

Précédents audits du BIG pertinents :

Audit sur l'efficacité des contrôles informatiques au Fonds mondial GF-OIG-15-020

Audit sur l'efficacité des contrôles informatiques au Fonds mondial (rapport de suivi) GF-OIG-15-020B

4. Constatations

4.1. Absence de stratégie et de plan de mise en œuvre relatifs à l'adoption du cloud computing

Le Fonds mondial a pour la première fois adopté une solution de cloud computing en 2014. Fin 2016, il avait transféré environ 60 % de ses applications et services informatiques dans le cloud. Or, aucune stratégie globale, aucun plan de mise en œuvre n'ont éclairé cette décision.

Le cloud computing a accru la disponibilité des services informatiques et réduit la charge de travail liée à la gestion d'un centre de données hébergé sur site, au Fonds mondial. La plupart des applications dans le cloud utilisent les outils de sécurité, de sauvegarde et de reprise de l'activité après incident des prestataires de services. Ceux-ci assurent la mise à jour régulière des applications et des logiciels.

En septembre 2014, le Comité exécutif de direction a adopté une stratégie en matière de technologies de l'information pour la période 2014/2016. Cependant, cette stratégie ne couvrait pas l'utilisation de services de cloud computing au sein du Fonds mondial. La mise en œuvre de la solution n'a été précédée et suivie d'aucune évaluation des besoins, analyse coût-efficacité ou analyse des risques. Aucun plan de mise en œuvre n'a été établi afin d'identifier la nature des services requis et le calendrier du déploiement des différents services dans le cloud. Ces manquements ont fragilisé une infrastructure et des services informatiques déjà fragmentés, et compliqué l'intégration des applications. Le service informatique ne possède pas actuellement de vue globale de l'architecture informatique couvrant l'ensemble des applications et des services fournis dans le cloud. Il convient d'établir un cadre d'architecture, afin d'éclairer les décisions en matière de stratégie, de conception et de planification des systèmes d'information. L'absence d'un tel cadre peut affecter la pérennité et la prise en charge des systèmes, et alourdir les coûts, du fait d'investissements inappropriés ou de coûts de maintenance accrus.

Implications à long terme du cloud computing : L'institution n'a toujours pas évalué et pris en compte les effets à long terme des services dans le cloud. L'adoption du cloud computing aura inévitablement un impact sur les ressources informatiques (nombre et compétence du personnel, et infrastructure) requises en interne. Ces implications doivent être évaluées. En matière de disponibilité des services à long terme, certaines décisions relatives aux systèmes d'information ne tiennent pas compte du cloud computing. Par exemple, suite à l'adoption du cloud computing, le Fonds mondial a continué d'acquérir des applications logicielles non compatibles avec un système dans le cloud. La continuité, la latence et la disponibilité des services risquent d'en pâtir si le serveur client de l'application non fournie dans le cloud dysfonctionne ou n'est pas disponible.

Examen visant à vérifier si le cloud computing atteint les objectifs établis : Le Fonds mondial n'a pas évalué si les avantages attendus du cloud computing avaient été obtenus depuis son adoption en 2014. Cela tient essentiellement au fait que les justifications de l'adoption du cloud computing n'ont jamais été établies. En prévision des rotations du personnel informatique, notamment du responsable des systèmes d'information, les grandes décisions relatives aux technologies de l'information doivent être documentées, afin de permettre aux successeurs de mettre en œuvre et d'évaluer efficacement les décisions dans des domaines clés tels que le retour sur investissement. L'évaluation des résultats au vu des objectifs établis permet de déterminer les domaines pouvant être corrigés en interne dans des délais raisonnables.

Les causes profondes des faiblesses en matière de stratégie et de plan de mise en œuvre de solutions dans le cloud sont dues au manque de mécanismes de gouvernance informatique au sein du Fonds mondial. L'institution ne possède pas de structures de gouvernance prévoyant l'examen et l'approbation des grandes décisions liées aux technologies de l'information. En mai 2016, le responsable des systèmes d'information a créé un Conseil de l'architecture institutionnelle afin d'améliorer la gouvernance dans ce domaine. Composé du responsable des systèmes d'information, du Bureau de la gestion des projets liés aux technologies de l'information, et des gestionnaires des partenaires informatiques, le Conseil est chargé d'approuver l'ensemble des décisions liées à ce domaine. Cependant, il n'a pas été en mesure de remplir son mandat efficacement, pour plusieurs

raisons. Les comités d'orientation du Secrétariat chargés des projets internes n'ont pas reconnu et accepté le Conseil comme organe décisionnaire des questions liées aux technologies de l'information au sein du Fonds mondial. Les responsables des processus opérationnels n'ont pas été impliqués dans la définition des rôles et responsabilités du Conseil. De plus, les procédures et les critères d'évaluation du Conseil n'ont pas été pleinement définis. Faute de procédures de gouvernance officielles, le Conseil n'a généralement pas été impliqué dans les décisions liées aux systèmes d'information. Le Comité exécutif de direction n'a pas encore examiné l'adoption du cloud computing, défini les objectifs y afférents ou évalué les avancées au regard de ces objectifs, examiné les risques inhérents à ces solutions et l'atténuation des principaux risques.

Action convenue de la Direction n° 1 : Comme le prévoit le plan de transition du responsable des systèmes d'information, le Secrétariat établit une stratégie relative aux systèmes d'information, tenant compte du cloud computing. La stratégie définit les modes d'organisation et de fonctionnement du service informatique. Elle définit les objectifs pratiques en matière de qualité, d'exploitabilité et d'acceptance des services informatiques. Elle est soumise à l'approbation du Comité exécutif de direction.

Titulaire : Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Date cible : 31 décembre 2017

Action convenue de la Direction n° 2 : Le Secrétariat améliore les mécanismes de gouvernance des systèmes d'information au terme d'une refonte du Conseil de l'architecture institutionnelle. L'organisation, la portée, le mandat, notamment la composition, les procédures et les critères en matière de décision du conseil seront mieux définis dans le cadre de la stratégie relative aux systèmes d'information.

Titulaire : Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Date cible : 31 décembre 2017

4.2. Gestion insuffisante des risques liés au cloud computing

Le cloud computing permet aux entreprises d'externaliser la gestion de certains risques liés aux systèmes d'information à des tiers. Il les expose cependant à d'autres types de risques, liés aux données, aux fournisseurs et aux questions juridiques par exemple, qui doivent être atténués au moyen de mesures volontaristes. Le Fonds mondial doit évaluer les risques potentiels liés au cloud computing et prendre des mesures aux fins de les atténuer.

Le Secrétariat a confié la responsabilité de la gestion quotidienne de certains risques opérationnels liés aux systèmes d'information à des prestataires de services dans le cloud. Ces responsabilités varient selon les prestataires, en fonction des contrats et de la nature des services, mais incluent généralement des dispositions de sauvegarde et de reprise de l'activité après incident, la gestion continue des services, la mise à niveau des logiciels et le déploiement des applications. Cependant, la responsabilité de ces risques incombe en dernier lieu au Fonds mondial, qui doit les atténuer au moyen de mesures de gestion des fournisseurs, de gestion des résultats et de garantie des contrôles. Le cloud computing modifie également le profil des risques institutionnels et peut comporter des risques liés aux données, aux fournisseurs et aux questions juridiques que le Fonds mondial n'a pas encore évalués.

Risques liés à la gestion des données : Le cloud computing fragilise la protection des données de l'institution, puisque celle-ci contrôle moins la manière dont les prestataires de services traitent les données. La protection des données est par ailleurs compliquée du fait des nombreux transferts de données entre les systèmes et les sites. En conséquence, le Fonds mondial doit définir la nature et le type de données (selon les barèmes de classification des données) stockées dans le cloud et les critères minimaux de sécurité requis pour leur transfert. Le Fonds mondial n'a pas encore déterminé le type de données pouvant être stockées dans le cloud et les contrôles y afférents. De ce fait, des informations confidentielles pourraient être stockées dans le cloud, sans qu'elles soient protégées par des contrôles appropriés.

Si les interfaces des systèmes et des applications clés ont été documentées, dans le cas d'une application clé, les spécifications de sécurité y afférentes n'ont pas été définies et documentées. Aucun critère de protection minimal n'est actuellement défini en matière de transfert des données dans le cloud. En conséquence, des critères de sécurité différents ont été adoptés par chaque responsable de système, ce qui accroît l'exposition de l'institution aux risques d'incohérence et de qualité insuffisante des données. Lorsque des données sont transférées d'un site ou d'un système dans un autre, elles risquent d'être interceptées. Ce risque augmente dans les environnements cloud partagés, des données stratégiques ou confidentielles étant alors davantage exposées à des accès non autorisés.

Risques liés aux fournisseurs : Le Fonds mondial n'a pas encore évalué les risques liés aux prestataires de services dans le cloud, afin de déterminer le niveau de risque y afférent et les ressources requises aux fins de gérer ces fournisseurs. Ce point, allié à l'absence de mesures institutionnelles visant à atténuer les risques liés au cloud computing, a ouvert la voie à des pratiques de gestion des relations avec les prestataires de services incohérentes selon les gestionnaires des partenaires informatiques du Fonds mondial. Par exemple, les niveaux d'assurance relatifs aux contrôles des fournisseurs varient selon les responsables de systèmes au Fonds mondial. Celui-ci n'a pas évalué les contrôles des fournisseurs de services informatiques ou obtenu de certification externe indépendante pour trois des six applications clés dans le cloud depuis 2014. Or, selon les pratiques standard du secteur, ces certifications doivent être renouvelées tous les deux ans au minimum. Ces applications gèrent des données de référence sur les subventions et servent de fondement à la gestion des connaissances au sein du Secrétariat.

Lorsque des certifications tierces ont été obtenues, les conclusions des rapports ne sont pas dûment suivies d'effets. Par exemple, un examen indépendant d'une des applications clés (utilisée par la quasi-totalité du personnel du Fonds mondial et plus de 400 maîtres d'œuvre des subventions en mai 2017) fait état de faiblesses majeures des contrôles appliqués par le fournisseur. Cependant, rien n'indique que le Fonds mondial a déterminé leur impact sur les services fournis par le prestataire et les mesures d'atténuation potentiellement requises.

Risques liés aux questions juridiques : Les prestataires de services cloud stockent les données sur plusieurs sites aux fins de minimiser les risques de perte totale en cas d'incident ou d'infraction. De ce fait, le Fonds mondial encourt le risque d'être sommé de divulguer des informations dans des pays ne lui accordant pas de privilèges et d'immunités. Or, l'institution n'a pas évalué la probabilité et l'impact de ce risque. Le service informatique a en partie atténué ce risque, en imposant dans les contrats signés avec certains prestataires le stockage des données de l'institution en Suisse et aux États-Unis uniquement. Néanmoins, l'institution reste exposée au risque, du fait des modalités de stockage et d'hébergement des données de deux applications majeures. Le contrat actuel relatif à ces deux applications autorise le prestataire à transférer les données dans des pays n'accordant pas de privilèges et d'immunités au Fonds mondial sans l'autorisation du Secrétariat.

Le service informatique produit un rapport mensuel des risques, incorporé dans un registre institutionnel des risques tenu à jour par le département de la gestion des risques. Comme indiqué dans un rapport d'audit du BIG sur la gestion des risques[4], les faiblesses du département des risques en matière de compétences ont affecté la capacité du personnel à garantir l'identification des risques liés aux systèmes d'information et à prendre des mesures d'atténuation appropriées avant l'adoption de solutions de cloud computing.

Le Fonds mondial a initié une procédure d'établissement d'une politique sur la réglementation de la sécurité informatique, aux fins de fournir des orientations sur les risques liés aux systèmes d'information, notamment à la transmission des données. Un projet de politique a été préparé en janvier 2017 et est en cours d'examen par le service informatique. Une fois finalisée, la politique définira et prescrira une série de mesures visant à atténuer les risques liés aux systèmes d'information, notamment ceux externalisés à des prestataires de solutions de cloud computing.

Action convenue de la Direction n° 3 : Le Secrétariat améliore la gestion des risques liés aux systèmes d'information. À ces fins, il identifie les risques potentiels liés au cloud computing, évalue leur impact et prend des mesures visant à les atténuer.

Les risques identifiés sont atténués au moyen des mesures ci-après :

- l'application, par le département chargé des achats, des procédures existantes, aux fins de s'assurer que les départements juridique et informatique examinent l'ensemble des contrats futurs relatifs aux services de cloud computing ;
- un examen de la faisabilité d'une modification des deux contrats, aux fins de combler les faiblesses identifiées et de prendre des mesures alternatives visant à combler les faiblesses si le résultat des négociations contractuelles n'est pas favorable ;
- l'utilisation d'outils tels que le Conseil de l'architecture institutionnelle afin de garantir l'établissement d'un plan de reprise de l'activité après incident pour les deux applications identifiées par l'examen. Le plan est testé par le service informatique du Fonds mondial, en coordination avec les prestataires de services cloud. Les tests de reprise de l'activité après incident, réalisés semestriellement, prémunissent le Secrétariat des pertes de données et garantissent l'accès aux données conformément aux niveaux de services convenus ;
- un examen, biennal au minimum, des certifications tierces relatives aux trois applications identifiées, et le suivi des conclusions susceptibles d'exposer le Fonds mondial à un risque ; et
- une amélioration des procédures de suivi des activités des utilisateurs, au moyen d'une identification de trois exceptions d'activités maximum visées par le suivi. La mise en œuvre d'un mécanisme d'alerte visant à signaler les exceptions relatives aux fonctions stratégiques. Ce mécanisme sera déployé progressivement sur les applications cloud identifiées.

Titulaire : Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Date cible : 30 septembre 2018

[4] Procédures du Fonds mondial relatives à la gestion des risques GF-OIG-17-010

Action convenue de la Direction n° 4 : Le service informatique produit actuellement un rapport mensuel sur les risques, fondé sur un indicateur de risque, incorporé dans le registre institutionnel des risques du Fonds mondial, tenu à jour par le département de la gestion des risques. Le service informatique actualise le rapport mensuel au vu des risques potentiels relatifs au cloud computing. En collaboration avec le département de la gestion des risques, il les intègre dûment dans le registre institutionnel des risques. Le Comité exécutif de direction examine et approuve trimestriellement le registre institutionnel des risques.

Titulaire : Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Date cible : 30 septembre 2017

4.3. Gestion sous-optimale des prestataires de services cloud

Le service informatique du Fonds mondial a assigné des membres de son équipe à la gestion de divers services cloud fournis par des prestataires de premier plan. La gestion des fournisseurs est axée sur la disponibilité des services et la résolution des incidents. Cependant, tel qu'il est conçu, l'accord de niveau de service relatif à la plateforme de gestion des subventions ne permet pas un suivi efficace. La gestion des résultats relatifs à certains aspects fondamentaux d'un contrat avec un fournisseur portant sur la détection et la suppression des virus est insuffisante.

Les six applications visées par l'examen sont couvertes par des contrats. Le Secrétariat se réunit régulièrement avec les prestataires de services afin de discuter de la gestion des services et des incidents, et de garantir la disponibilité et la fourniture des services.

Gestion des résultats des prestataires de services cloud : Le Fonds mondial n'a pas défini de cadre régissant la gestion des prestataires de services. En conséquence, les gestionnaires des partenaires informatiques adoptent des pratiques divergentes. Par exemple, la fréquence d'examen des résultats, les réunions d'examen des contrats et les voies de recours en cas d'identification d'une faiblesse ne sont pas définies. De ce fait, les gestionnaires des partenaires informatiques ont parfois dû résoudre les faiblesses identifiées au cas par cas. Cela affecte l'efficacité du suivi et la gestion des connaissances au sein du service informatique.

Les résultats des prestataires de trois applications sur six ne sont pas examinés au regard des accords de niveau de service. Ainsi, l'accord de niveau de service d'un fournisseur couvre les obligations en matière de sécurité telles que la détection et la suppression des virus, ou l'efficacité du filtre des courriers indésirables, sans que la conformité à ces dispositions soit périodiquement évaluée.

Le niveau de maturité de gestion institutionnelle des prestataires de services informatiques peut être amélioré. Le service informatique n'a pas réalisé d'évaluation des risques liés aux prestataires de services cloud, afin de déterminer leurs points forts et leurs points faibles, et les contrôles de gestion des résultats requis. Les négociations du service informatique avec les prestataires sont centrées sur le prix et la prestation de services, sans définir d'objectifs communs, la gestion des risques ou l'assistance liée à la fourniture des services.

Gestion des contrats : Certaines dispositions des contrats établis avec les prestataires de services peuvent être améliorées aux fins de garantir une disponibilité continue et sécurisée des données sur l'ensemble des applications. Par exemple, le contrat et l'accord de niveau de service relatifs à la plateforme de gestion des subventions ne définissent pas clairement les niveaux de disponibilité des services et de sécurité requis. En particulier, un des accords de niveau de service ne précise pas dans quel délai les services doivent être restaurés suite à une interruption. L'accord indique simplement que le prestataire doit fournir une assistance raisonnable aux fins de restaurer les services.

Le contrat relatif à deux des six applications ne contient pas de dispositions contraignant le prestataire à signaler les risques importants susceptibles d'affecter la fourniture ou la sécurité des services, conformément aux pratiques du secteur. L'inclusion d'une clause relative à la divulgation des risques, une pratique courante dans l'industrie informatique, oblige le prestataire de services à signaler volontairement les risques connus ou probables affectant sa capacité à fournir les services convenus.

Le contrôle et le suivi des principales dispositions contractuelles des prestataires de services cloud comportent des incohérences. Bien que les obligations contractuelles du système de gestion de la trésorerie et du système ERP soient dûment gérées, ce n'est pas le cas du prestataire de services de deux autres applications clés. En particulier, la conformité en matière de stockage des données, de reprise de l'activité après incident et de sauvegarde des applications n'est pas vérifiée. Le BIG note que le Fonds mondial a fait appel à des acteurs expérimentés de premier plan pour ses services de

cloud computing. En conséquence, sa marge de manœuvre en matière de négociation des contrats pourrait être limitée. Cependant, le Secrétariat doit examiner la possibilité d'utiliser des dispositions contractuelles plus favorables, négociées entre des organismes apparentés aux Nations Unies et le prestataire de services sélectionné pour deux des six applications visées par notre examen.

Action convenue de la Direction : Voir l'action n° 3

4.4. Accès aux systèmes d'information – Lacunes en matière d'accès aux données et de contrôles de sécurité des applications dans le cloud

Le Fonds mondial a amélioré ses pratiques en matière de gestion des mots de passe et réalisé des vérifications de sécurité indépendantes de son système ERP et de son application de gestion de la trésorerie. Cependant, la gestion des droits d'accès des utilisateurs et le contrôle des activités dans le cloud doivent être améliorés.

L'institution a accru la sensibilité aux questions de sécurité informatique et intensifié les formations y afférentes. De nouvelles politiques relatives à la sécurité de l'information et aux mots de passe doivent être déployées. Dans le cadre d'un « programme de sensibilisation à la sécurité de l'information », une formation en ligne sur la sécurité des mots de passe et des courriels a été assignée à l'ensemble du personnel du Fonds.

Gestion des droits d'accès des utilisateurs : Deux des six applications dans le cloud clés ne possèdent pas de matrice de séparation des tâches définissant les droits d'accès[5] des utilisateurs. En conséquence, le service informatique ne peut pas pleinement examiner la pertinence des rôles et responsabilités assignés aux utilisateurs des applications. Sans matrice, les responsabilités allouées aux différents modules des applications risquent d'entrer en conflit. À mesure que l'utilisation de plateformes dans le cloud continue de croître, l'attribution de droits d'accès inappropriés à des fonctions spécifiques des applications risque d'entraîner des pertes de données ou des fuites d'information stratégique suite à une enfreinte aux privilèges des utilisateurs.

Lorsqu'une matrice de séparation des tâches a été préparée, rien n'indique qu'elle est régulièrement examinée par le service informatique et les responsables de processus opérationnels. La responsabilité des droits d'accès des utilisateurs sur la plateforme de conservation de la documentation est confiée aux responsables des sites. Une attestation annuelle des responsables de site définit la gestion de la matrice. Cependant, l'attestation ne comprend pas d'examen du bien-fondé des rôles et responsabilités attribués aux utilisateurs.

Suivi des activités sur les ordinateurs : Les prestataires de services cloud mettent régulièrement à jour les antivirus et les pare-feu des applications. Cependant, le service informatique ne suit pas étroitement les activités des utilisateurs sur les applications dans le cloud afin de détecter les activités non autorisées ou malveillantes dans les plus brefs délais. Les systèmes du Fonds mondial possèdent une fonctionnalité de piste d'audit (journaux des ordinateurs et traçabilité des activités) afin de faciliter le suivi des activités sur les ordinateurs. Or, le service informatique utilise cette fonctionnalité à la demande des départements uniquement, et ne surveille pas activement les activités anormales telles que les niveaux élevés ou inhabituels de connexions à des applications spécifiques. Pourtant, un journal détaillé et exhaustif des activités sur les ordinateurs alerterait les informaticiens et les aiderait à réagir en cas d'incident. Il pourrait servir à contrôler la manière dont les données confidentielles sont utilisées et partagées, et à détecter les utilisations inappropriées des données. L'absence de ces contrôles pourrait affecter la capacité du Fonds mondial à identifier les fuites de données et à détecter à temps les activités non autorisées ou malveillantes sur les ordinateurs.

Action convenue de la Direction n° 5 : Au regard de la matrice de séparation des tâches des applications sélectionnées, le Secrétariat réalise un examen des utilisateurs finaux bénéficiant de droits d'accès à deux modules ou plus, aux fins d'évaluer les conflits potentiels. Il établit également une procédure officielle d'approbation et de suivi des exceptions.

Titulaire : Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Date cible : 30 juin 2018

---

[5] La gestion des comptes utilisateurs, en particulier ceux bénéficiant de privilèges d'accès spéciaux, est essentielle à la protection contre les accès non autorisés et les utilisations abusives. Les comptes doivent être attribués aux personnes autorisées uniquement, et fournir le niveau minimum d'accès aux applications, aux ordinateurs et aux réseaux. (https://www.itgovernance.co.uk/access-control-and-administrative-privilege)

4.5. Exactitude des données informatiques – Faiblesses en matière de gestion des interfaces informatiques et des contrôles de cryptage, affectant l'exactitude des données

L'adoption du cloud computing et la nature fragmentée de l'architecture des systèmes d'information ont entraîné la création de multiples interfaces qui doivent être identifiées et dont le niveau de sécurité doit être évalué.

Le cloud computing entraîne le transfert de données sur une multitude d'applications et de systèmes. À ces fins, il convient d'identifier toutes les interfaces des systèmes et des applications, de manière à garantir l'établissement de contrôles de sécurité appropriés. Le responsable de la sécurité des systèmes d'information a lancé des tests de pénétration dans les départements et sur les applications clés au troisième trimestre 2016. L'institution dirige elle-même ces tests aux fins d'identifier les vulnérabilités potentielles de son infrastructure et des systèmes d'information susceptibles d'être exploitées par des tiers, et prend des mesures volontaristes visant à combler les faiblesses relevées. Une feuille de route des tests de pénétration a été ébauchée pour la période 2016/2017, couvrant trois applications clés et domaines fonctionnels. Il s'agit de l'application de gestion des subventions, du système de conservation de la documentation, et des interfaces relatives aux ressources humaines. Les tests de pénétration sont menés par un acteur externe indépendant, chargé d'analyser les systèmes et/ou les réseaux. Si les prestataires de services cloud n'autorisent pas le client à réaliser de test de pénétration, celui-ci utilise des portails de confiance pertinents.

Interfaces des systèmes d'information et contrôles de rapprochement : Les applications utilisées au sein du Fonds mondial possèdent des interfaces variées. Or, le service informatique n'a pas clairement documenté toutes ces interfaces et établi de contrôles de rapprochement afin de garantir la cohérence des données entre les applications. Par ailleurs, certaines interfaces pourraient être automatisées. Par exemple, un audit du BIG de la gestion de la trésorerie du Fonds mondial avait relevé l'absence d'interface automatisée entre les plateformes de négoce en ligne et hors ligne du système de gestion de la trésorerie[6]. L'absence de liste exhaustive et définie des interfaces et des contrôles de rapprochement favorise l'incohérence des données entre les applications. Les prises de décisions pourraient alors être fondées sur des données incorrectes.

Contrôles de cryptage des données : Le service informatique n'a pas garanti de contrôles des cryptages cohérents des transferts de données pour l'ensemble des interfaces. Chaque gestionnaire des partenaires informatiques est libre de choisir l'outil de cryptage des données utilisé lors des transferts de données sur des applications dans le cloud. De ce fait, des niveaux insuffisants de cryptage peuvent parfois être utilisés pour une même information sur les différents systèmes. Or, le maillon le plus faible définit le niveau d'efficacité du cryptage des données en circulation.

Les contrôles de cryptage des données menés par les prestataires de services cloud doivent être certifiés par des acteurs indépendants au moyen d'examens ISO 27001[7]. Or, le Fonds mondial n'a pas obtenu ces certifications depuis 2014 pour les trois principales applications utilisées. Ces certifications doivent pourtant être renouvelées tous les deux ans au minimum, conformément aux pratiques du secteur. Eu égard à la plateforme de gestion des subventions dont la certification[8] a été obtenue, le Secrétariat n'a pris aucune mesure, malgré les faiblesses importantes en matière de contrôles relevées dans le rapport. Le Secrétariat établit actuellement une politique en matière de réglementation de la sécurité des systèmes d'information, afin de fournir des orientations sur la transmission des données et les contrôles y afférents.

Action convenue de la Direction n° 6 : Parallèlement à l'action convenue de la Direction n° 3, le Secrétariat :

[6] GF-OIG-17-001 Gestion de la trésorerie du Fonds mondial

[7] Publiée par l'Organisme international de normalisation, la norme ISO 27001 cible les systèmes de gestion de la sécurité de l'information. Les examens SOC 2 (Service Organization Control) vérifient les contrôles réalisés par un prestataire de services portant sur la gouvernance, les risques, la conformité, la vérification approfondie et la supervision, relatifs à la sécurité, la disponibilité ou l'intégrité de traitement des systèmes ou de la confidentialité des processus des systèmes d'information. Les rapports SOC 3 évaluent le niveau de fiabilité des systèmes des prestataires de services en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité.

[8] La certification des prestataires est un examen indépendant des contrôles de sécurité informatique, fourni sous la forme d'un rapport SSAE16 ou SOC 2.

1. en collaboration avec les responsables des données, s'appuie sur les documents de référence actuels du Fonds mondial relatifs à la classification et la gestion de l'information, afin de garantir l'établissement de spécifications de sécurité applicables aux transferts de données et aux interfaces des applications dans le cloud identifiées dans le cadre de l'examen et des contrôles de rapprochement. Un niveau approprié de sécurité de l'information est mis en œuvre afin de respecter les obligations documentées ; et

2. réalise une analyse de faisabilité et du rapport coût-efficacité de l'automatisation des interfaces manuelles stratégiques des applications identifiées.

Titulaire : Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Date cible : 30 septembre 2018

4.6. Amélioration requise en matière de planification des reprises d'activité après incident et de tests de certaines applications cloud

Le Secrétariat a sensiblement amélioré ses plans de reprise de l'activité après incident, même si certains domaines peuvent encore gagner en efficacité. Suite au rapport d'audit du BIG des contrôles informatiques du Secrétariat en 2015, un plan de reprise de l'activité après incident avait été établi pour les applications clés alors utilisées. Cependant, des plans similaires doivent encore être définis pour les applications acquises après l'audit de 2015.

Les plans de reprise de l'activité après incident établis par le Secrétariat peuvent être améliorés. En collaboration avec les prestataires de services cloud, le Secrétariat a défini et testé des plans de reprise de l'activité après incident pour les applications de gestion de la trésorerie, de gestion des subventions et ERP. Les plans n'établissent pas d'ordre de priorité de récupération des données au regard du système de classification. Rien n'indique que des engagements applicables aux partenaires commerciaux ont été intégrés dans le plan de reprise de l'activité après incident relatif à l'application de gestion des subventions.

Deux des six applications ne possèdent toujours pas de plan de reprise de l'activité après incident. Conformément au contrat établi avec le prestataire de services, le Secrétariat est responsable de la récupération de ses données en cas d'incident. Le contrat stipule que le prestataire n'est pas spécialiste de la récupération après sinistre et que le Secrétariat doit prendre des mesures aux fins de récupérer ses données en cas de défaillance du système. Or le Fonds mondial ne possède actuellement pas d'outil de sauvegarde des données pour ces deux applications hébergées dans le cloud, et aucun plan ne prévoit la récupération des données en cas de défaillance du système. Les applications stockent la majorité des documents stratégiques du Fonds mondial et servent d'outil principal de gestion de la connaissance. Certains documents sont des accords de subventions, des rapports sur les résultats des subventions, des contrats avec des prestataires de services et des communications électroniques avec diverses parties prenantes. En décembre 2014, le risque lié à cette situation s'est concrétisé sous la forme d'un incident majeur de stockage dans le système de conservation de la documentation. Suite à cela, l'accès aux documents et courriels a été interrompu, parfois pendant plus d'une semaine. Les dispositions relatives à la reprise de l'activité après incident ont été sensiblement améliorées depuis cet événement, des tests de récupération après sinistre étant réalisés régulièrement sur les applications hébergées dans un cloud privé.

Action convenue de la Direction : Voir l'action n° 3.

5. Tableau des actions convenues

Action convenue de la Direction	Date cible	Titulaire
1. Comme le prévoit le plan de transition du responsable des systèmes d'information, le Secrétariat établit une stratégie relative aux systèmes d'information, tenant compte du cloud computing. La stratégie définit les modes d'organisation et de fonctionnement du service informatique. Elle définit les objectifs pratiques en matière de qualité, d'exploitabilité et d'acceptance des services informatiques. Elle est soumise à l'approbation du Comité exécutif de direction.	31 décembre 2017	Directeur du département chargé des finances, de l'informatique, des achats et de l'administration
2. Le Secrétariat améliore les mécanismes de gouvernance des systèmes d'information au terme d'une refonte du Conseil de l'architecture institutionnelle. L'organisation, la portée, le mandat, notamment la composition, les procédures et les critères en matière de décision du conseil seront mieux définis dans le cadre de la stratégie relative aux systèmes d'information.	31 décembre 2017	Directeur du département chargé des finances, de l'informatique, des achats et de l'administration
3. Le Secrétariat améliore la gestion des risques liés aux systèmes d'information. À ces fins, il identifie les risques potentiels liés au cloud computing, évalue leur impact et prend des mesures visant à les atténuer. Les risques identifiés sont atténués au moyen des mesures ci-après : o l'application, par le département chargé des achats, des procédures existantes, aux fins de s'assurer que les départements juridique et informatique examinent l'ensemble des contrats relatifs aux services de cloud computing ; o un examen de la faisabilité d'une modification des deux contrats, aux fins de combler les faiblesses identifiées et de prendre des mesures alternatives visant à combler les faiblesses si le résultat des négociations contractuelles n'est pas favorable ; o l'utilisation d'outils tels que le Conseil de l'architecture institutionnelle afin de garantir l'établissement d'un plan de reprise de l'activité après incident pour les deux applications identifiées par l'examen. Le plan est testé par le service informatique du Fonds mondial, en coordination avec les prestataires de services cloud. Les tests de reprise de l'activité après incident, réalisés semestriellement, prémunissent le	30 septembre 2018	Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Action convenue de la Direction	Date cible	Titulaire
Secrétariat des pertes de données et garantissent l'accès aux données conformément aux niveaux de services convenus ; o un examen, biennal au minimum, des certifications tierces relatives aux trois applications identifiées, et le suivi des conclusions susceptibles d'exposer le Fonds mondial à un risque ; et o une amélioration des procédures de suivi des activités des utilisateurs, au moyen d'une identification de trois exceptions d'activités maximum visées par le suivi. La mise en œuvre d'un mécanisme d'alerte visant à signaler les exceptions relatives aux fonctions stratégiques. Ce mécanisme sera déployé progressivement sur les applications cloud identifiées.		
4. Le service informatique produit actuellement un rapport mensuel sur les risques, fondé sur un indicateur de risque, incorporé dans le registre institutionnel des risques du Fonds mondial, tenu à jour par le département de la gestion des risques. Le service informatique actualise le rapport mensuel au vu des risques potentiels relatifs au cloud computing. En collaboration avec le département de la gestion des risques, il les intègre dûment dans le registre institutionnel des risques. Le Comité exécutif de direction examine et approuve trimestriellement le registre institutionnel des risques.	30 septembre 2017	Directeur du département chargé des finances, de l'informatique, des achats et de l'administration
5. Au regard de la matrice de séparation des tâches des applications sélectionnées, le Secrétariat réalise un examen des utilisateurs finaux bénéficiant de droits d'accès à deux modules ou plus, aux fins d'évaluer les conflits potentiels. Il établit également une procédure officielle d'approbation et de suivi des exceptions.	30 juin 2018	Directeur du département chargé des finances, de l'informatique, des achats et de l'administration
6. **Parallèlement à l'action convenue de la Direction n° 3,** le Secrétariat : 1. en collaboration avec les responsables des données, s'appuie sur les documents de référence actuels du Fonds mondial relatifs à la classification et la gestion de l'information, afin de garantir l'établissement de spécifications de sécurité applicables aux transferts de données et aux interfaces des applications dans le cloud identifiées dans le cadre de l'examen et des contrôles de rapprochement. Un niveau approprié de	30 septembre 2018	Directeur du département chargé des finances, de l'informatique, des achats et de l'administration

Action convenue de la Direction	Date cible	Titulaire
sécurité de l'information est mis en œuvre afin de respecter les obligations documentées ; et 2. réalise une analyse de faisabilité et du rapport coût-efficacité de l'automatisation des interfaces manuelles stratégiques des applications identifiées.		

Annexe A : Classification générale des notations de l'audit

Efficace	**Aucun problème ou peu de problèmes mineurs relevés**. Les procédures de contrôles internes, de gouvernance et de gestion des risques sont conçues comme il convient, bien appliquées en permanence et efficaces pour donner une garantie raisonnable que les objectifs seront atteints.
Partiellement efficace	**Problèmes modérés relevés**. Les procédures de contrôles internes, de gouvernance et de gestion des risques sont conçues comme il convient et généralement bien appliquées, mais un problème ou un nombre restreint de problèmes ont été identifiés et sont susceptibles de faire courir un risque modéré pour la concrétisation des objectifs.
Nécessite une nette amélioration	**Un problème majeur ou un petit nombre de problèmes majeurs relevés**. Les pratiques en matière de contrôles internes, de gouvernance et de gestion des risques présentent quelques faiblesses de conception ou d'efficacité opérationnelle, à tel point que tant qu'elles ne sont pas corrigées, on ne peut raisonnablement garantir que les objectifs sont susceptibles d'être atteints.
Inefficace	**Plusieurs problèmes majeurs et/ou un ou plusieurs problèmes fondamentaux relevés.** Les procédures de contrôles internes, de gouvernance et de gestion des risques ne sont pas conçues comme il se doit et/ou ne sont pas globalement efficaces. La nature de ces problèmes est telle que la concrétisation des objectifs est gravement compromise**.**

Annexe B : Méthodologie

Le Bureau de l'Inspecteur général réalise ses audits conformément à la définition mondiale de l'audit interne de l'Institute of Internal Auditors (IIA), 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 Bureau de l'Inspecteur général.

Les principes et les détails de la méthode d'audit du Bureau de l'Inspecteur général sont décrits dans sa Charte, son Manuel d'audit, son Code de conduite et le mandat spécifique de chaque mission. Ils aident nos vérificateurs à fournir des travaux professionnels de qualité élevée et à intervenir de façon efficiente et efficace. Ils garantissent également l'indépendance des auditeurs du BIG ainsi que l'intégrité de leurs travaux. Le Manuel d'audit du BIG contient des instructions détaillées pour la réalisation de ses audits, dans le respect des normes appropriées et de la qualité attendue.

La portée des audits du BIG peut-être spécifique ou étendue, 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 sont réalisés dans l'ensemble du Fonds mondial ainsi que chez les récipiendaires des subventions et servent à établir des évaluations spécifiques des différents domaines des activités de l'organisation. D'autres sources de preuves, telles que les travaux d'autres auditeurs/fournisseurs d'assurances, 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 crédits 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 portent sur un large éventail de sujets et mettent en particulier l'accent sur les problèmes liés à l'impact des investissements, à la gestion de la chaîne des achats et des stocks, à la gestion des évolutions et aux principaux contrôles financiers et fiduciaires du Fonds mondial.