Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centrale de compensation CdC
Inspectorat interne INSP

[redacted]

Rapport N° 2013-3.8
Genève, le 24 février 2014

# Chaîne des paiements INAR

Statut du rapport: **final**

**Distribution** :

Destinataires du rapport :

- [redacted] Directeur a.i. de la CdC
- [redacted] chef de la division GETI
- [redacted] chef de la division CENT
- Contrôle fédéral des finances CDF

Copie pour connaissance à :

- [redacted] chef de la division AFac
- [redacted] cheffe de la division OAIE
- [redacted] chef a.i. de la division AVS
- [redacted] responsable RH

# Table des matières

## Sommaire


**1 Synthèse 4**

**2 Mission et périmètre 7**

**2.1 Description de la mission ..... 7**
**2.2 Bases légales ..... 7**
**2.3 Objectifs de la mission ..... 8**
**2.4 Périmètre de l'audit ..... 9**
**2.5 Démarche de l'audit ..... 9**

**3 Résultats de l'audit 11**

**3.1 Système de contrôle interne (SCI) de la sécurité de l'information ..... 11**
3.1.1 SCI de la sécurité de l'information - chaîne des paiements INAR ..... 13

**3.2 Gestion des accès aux données de paiements ..... 15**
3.2.1 Gestion des droits d'accès, des privilèges et séparation des fonctions ..... 16
3.2.2 Révocation des droits d'accès ..... 18
3.2.3 Gestion des comptes techniques ..... 20
3.2.4 Sécurité de la base de données et des serveurs de communication ..... 22

**3.3 Sécurité de l'exploitation informatique ..... 24**
3.3.1 Gestion de la sécurité de l'infrastructure ..... 24
3.3.2 Gestion des sauvegardes des données et des fichiers de paiements ..... 26
3.3.3 Gestion des incidents sur la chaîne des paiements INAR ..... 28

**3.4 Comptabilisation des paiements de rentes - Intégration des processus, procédures et contrôles comptables ..... 31**

**4 Discussion finale 34**

Annexe 1 - Tableau des recommandations et des positions ..... 35

# Glossaire

| | |
|---|---|
| ADABAS | Adaptable DAta BAse System.<br>Il s'agit d'un système transactionnel de mangement de données (base de données indexée), qui est utilisé en conjonction avec le langage de programmation Natural. L'éditeur est Software AG. |
| AFF | Administration fédérale des finances |
| BPE | Banco Popular Espanol |
| BPS | Banca Popolare di Sondrio |
| CdC | Centrale de compensation |
| CobiT | Control objectives for information and related technology |
| ERP | Enterprise Resource Planning |
| FSP&C | Projet de fonctionnalités standards de paiement et comptabilité |
| GETI | Gouvernance d'entreprise et technologies de l'information |
| INAR | Application de gestion et de paiement des rentes |
| NATURAL | Langage de programmation de 4ème génération (4GL) |
| POSIC | Politique de sécurité de l'information de la CdC |
| SCI | Système de contrôle interne |
| SFTP | Secure file transfer protocol |
| SMSI | Système de management de la sécurité de l'information |
| TPI | Trafic des paiements internationaux |

# 1 Synthèse

**Appréciation générale**

Sur la base de nos travaux d'audit, nous n'avons pas identifié d'exception majeure dans le transfert du paiement principal des rentes effectué par la chaîne des paiements INAR. En effet, nous relevons que les paiements des rentes de janvier à novembre 2013 ont été acheminés dans leur intégralité auprès de nos partenaires financiers, malgré plusieurs incidents survenus durant la période.

Nous relevons que la chaîne des paiements INAR[1] (processus applicatifs) repose sur une technologie Natural/Adabas dont les programmes n'évoluent plus à la CdC depuis plusieurs années. La perte de connaissances métiers et techniques (pertes causées en partie par le départ de personnes clés et un manque de gestion de la connaissance) n'a fait qu'accroître les difficultés des métiers (maîtrise d'ouvrage et assistance à maîtrise d'ouvrage, lors de projet) et de la GETI à respectivement définir les spécificités fonctionnelles voulues et mettre en œuvre de nouvelles fonctionnalités INAR – chaîne des paiements répondant aux besoins des utilisateurs finaux.

Des mesures ont été prises dès 2010 par la GETI (sur mandat de la Direction de la CdC) pour réaliser une analyse documentée du fonctionnement de la chaîne des paiements et produire une analyse des risques. Aujourd'hui, seules quelques mesures de mitigation des risques ont été mises en œuvre ; une grande partie d'entres elles restent encore à implémenter.

A relever l'existence d'un projet majeur : « fonctionnalités standards de paiement et comptabilité » (ci-après FSP&C[2]), qui vise à l'efficacité opérationnelle. Ce projet est doté d'une enveloppe budgétaire[3] de CHF 2'000'000.— et a pour but de moderniser le SI en offrant des fonctionnalités standards de paiement et de comptabilité. Un tel projet devait notamment permettre de répondre aux problématiques causées par l'absence d'un système de comptabilité pour tiers. Notons que le remplacement de la chaîne des paiements INAR est considéré par ce projet comme un « non-objectif », alors qu'il comprend dans ses processus applicatifs des contrôles comptables. Il n'en demeure pas moins que ce projet initié en 2011 peine à démarrer.

En outre, plusieurs faiblesses au niveau de l'environnement de contrôle du SI et plus particulièrement des activités de contrôle sur la chaîne des paiements INAR ont été relevées par notre audit. En effet, le faible niveau de maturité de l'actuel système de contrôle interne (ci-après SCI) de la sécurité des données rend la chaîne des paiements INAR plus vulnérable en cas d'incident de sécurité.

---

[1] Il s'agit essentiellement des traitements applicatifs de la chaîne des paiements.

[2] Selon la proposition de projet de juillet 2012 (document non-validé), FSP&C a pour objectif d'acquérir un ERP destiné à assurer des fonctionnalités standards de paiement et comptabilité.

[3] Le plan stratégique du SI : Symphonie attribue un budget de CHF 2'000'000.—au projet FSP&C, qui était initialement planifié de 2011 à 2013. Un total de CHF 52'015.—a été consommé sur ce projet sur la période.

Pour rappel, la responsabilité opérationnelle de l'OFIT-Genève a été transférée le 1er novembre 2011 auprès de la CdC. Le processus de transition s'est poursuivi en 2012, avec notamment la reprise du personnel de l'OFIT-Genève au 01.05.2012, afin que la CdC devienne fournisseur de prestations informatiques[4].

## Constats et recommandations principales

Nos principaux constats et recommandations en lien avec nos objectifs premiers (voir chapitre 2.3) sont décrits ci-après :

1. Nous observons que l'analyse des risques et des contrôles par le SI de la chaîne des paiements INAR (documenté par la GETI en 2010) n'a ni été actualisée ni mise en lien avec la matrice des risques et contrôles du processus d'affaire : Paiement principal des prestations AVS/AI.

2. Nous constatons que des mesures sont en place pour garantir l'intégrité et l'exactitude des paiements mais qu'elles doivent être renforcées.

3. Des mesures de sécurité (aspects techniques et organisationnels) sont appliquées aux données de paiements lors de leur traitement au sein du système INAR et de sa chaîne des paiements. Cependant, ces contrôles ne sont pas clairement documentés au sein d'un SCI de la sécurité et des lacunes en matière de gestion des accès logiques existent. Le niveau de sécurité lors de la transmission des fichiers de paiements réalisée au travers de l'infrastructure réseau doit être renforcé (ceci concerne essentiellement la sécurité des serveurs de communication);

4. Nous observons que le processus de gestion des incidents sur la chaîne des paiements doit être amélioré. Tout incident devant être renseigné dans un outil central. En outre, la procédure d'intervention en environnement de production sur les fichiers de paiements doit être documentée.

5. Nous relevons que la surveillance des processus applicatifs (Exploitation) de la chaîne des paiements INAR est documentée et fonctionne. Cependant, les procédures de surveillance d'exploitation de l'infrastructure réseau doivent encore être mises en place pour renforcer la sécurité et assurer la continuité des opérations de paiements en cas d'indisponibilité du SI.

6. La CSC ne dispose pas d'un système standard de comptabilité pour tiers (créanciers et débiteurs) où toute décision de rentes prise par les gestionnaires génère automatiquement des écritures dans un système de comptabilité auxiliaire. Les contrôles comptables sont aujourd'hui réalisés par le secteur TPI à partir de restitutions issues de la chaîne des paiements INAR. Pour rappel, INAR est une application de gestion et de paiement des rentes et non un système de comptabilité auxiliaire (créanciers et débiteurs). D'autre part, les différents retraitements manuels réalisés par le TPI sur la base des restitutions comptables rendues par la chaîne des paiements ne font pas parties intégrantes des processus standards de la GETI. Nous relevons également l'absence d'interface automatique permettant de contrôler efficacement et de faciliter (automatiser) le déversement des écritures de paiements de INAR vers le système de comptabilité principal.

[4]Le Conseil fédéral a approuvé le 28 mars 2012 une dérogation à l'ordonnance sur l'informatique dans l'administration fédérale (OIAF), selon laquelle chaque département dispose d'un seul fournisseur de prestations interne. Pour certaines prestations informatiques, la CdC devient désormais, en plus de l'OFIT, un fournisseur interne du Département des finances DFF.

Nous recommandons que les unités AVS, AFac, OAIE, CENT et la GETI réfléchissent conjointement à des mesure réalistes et motivées pour que la CSC se dote d'un système de comptabilité auxiliaire. Les résultats de cette analyse doivent mettre en lumière les besoins spécifiques non couverts ou partiellement couverts par les systèmes informatiques actuels et servir de base à l'élaboration d'un cahier des charges ayant pour cible d'homogénéiser et de simplifier le SI comptable.

En ce qui concerne la mise en œuvre de nos recommandations, nous attirons l'attention sur le fait qu'il est de la responsabilité des unités auditées de s'assurer que les moyens engagés sont proportionnels aux risques à maîtriser ou aux erreurs à corriger (principe de proportionnalité).

## Discussion finale et prises de position

Lors de l'entretien final du 18 décembre 2013, les audités ont exprimé leur intérêt ainsi que leur adhésion aux constats et recommandations .

Les positions remises par les audités figurent sous l'annexe 1 - Tableau des recommandations et des positions.

# 2 Mission et périmètre

## 2.1 Description de la mission

Il s'agit d'une mission d'audit informatique, qui consiste à s'assurer que l'ensemble des paiements des prestations de la CSC, générés à partir du module INAR et transmis vers nos partenaires financiers, restent intègres et complets tout au long du processus.

Ce contrôle s'inscrit dans le cadre de la planification 2013 des activités de l'Inspectorat interne.

## 2.2 Bases légales

Nous avons effectué notre contrôle en vertu de l'article 11 de la *Loi fédérale du 28 juin 1967 sur le Contrôle fédéral des finances* (LCF) (RS 614.0).

Les bases légales sur lesquelles nous nous sommes appuyés pour nos travaux d'audit sont présentées ci-après :

- Loi fédérale sur l'assurance-vieillesse et survivants (LAVS) (RS 831.10) ;
- Loi fédérale du 19 juin 1992 sur la protection des données (LPD) (RS 235.1) ;
- Ordonnance relative à la loi fédérale sur la protection des données (OLPD) (RS 235.11) ;
- Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale (OIAF) (RS 172.010.58) ;
- Ordonnance du 4 juillet 2007 concernant la protection des informations (OPrI) ;

Nous nous sommes également appuyés sur les directives et règlements suivants :

- Les Directives du CI concernant la sécurité informatique dans l'administration fédérale ;
- Le règlement maison « Lignes directrices de la sécurité de l'information à la CdC – Politique de sécurité de l'information de la CdC » datant du 1er août 2012.

## 2.3 Objectifs de la mission

Notre audit a pour objectif principal de réviser le processus informatisé de la chaîne des paiements INAR afin de s'assurer de l'intégrité[5], de l'intégralité, de la confidentialité et de la disponibilité des données de paiements des prestations de la Caisse suisse de compensation (CSC) auprès de ses bénéficiaires.

L'objectif de la mission est de vérifier :

- L'existence et l'efficacité d'un système de gestion des risques concernant la chaîne des paiements INAR ;
- L'existence de mesures garantissant l'intégrité et l'exactitude des paiements par un système de contrôle interne informatique efficace ;
- L'existence et l'efficacité des mesures de sécurité (aspects techniques et organisationnels) appliquées aux données de paiements lors de leur traitement au sein du système INAR et lors de leur transmission au travers de l'infrastructure réseaux ;
- Que les processus de gestion des incidents et de gestion des changements sur la chaîne des paiements sont définis, connus et améliorés en continu;
- Que les processus d'exploitation de la chaîne des paiements sont efficaces et que des procédures adéquates sont en place afin d'assurer la continuité des opérations de paiements.

Cet audit a pour objectif de s'assurer que la CSC gère sa chaîne de paiements (processus critique de l'entreprise selon l'analyse des risques de l'inspectorat) de manière adéquate et conforme aux lois, dans le but de respecter son mandat de prestation. Une défaillance sur le processus des paiements causerait des pertes financières et d'image considérables.

Ces objectifs ont été communiqués aux audités lors de la séance d'ouverture d'audit tenue le 6 septembre 2013 en présence de [redacted]

[5] L'intégrité des données désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. L'intégrité des données comprend quatre éléments, l'intégralité, la précision, l'exactitude/authenticité et la validité.

## 2.4 Périmètre de l'audit

Le périmètre de cet audit a porté sur les volets suivants :

- La sécurité applicative INAR et la sécurité de l'infrastructure réseaux en lien avec le flux des paiements des rentes AVS/AI ;
- La gestion de l'exploitation ainsi que la sécurité de la chaîne batch des paiements (il s'agit du traitement mensuel automatisé) ;
- La gestion des changements sur la chaîne des paiements ;
- Le système de contrôle interne informatique, les contrôles d'application (contrôles automatiques sur les processus applicatifs), ainsi que les contrôles manuels dépendant du système informatique (par exemple, les listes issues de INAR contrôlées par le TPI) permettant de s'assurer de l'exactitude et de l'exhaustivité des paiements ;
- Les sauvegardes de données ;
- La continuité des paiements de rentes.

Nous soulignons que les systèmes d'information autres que INAR – par exemple GEDO, les bases Lotus Notes, Corres, Helios, ainsi que tout autre système informatique (par exemple, un serveur) n'ayant pas été inventorié[6] ou se trouvant en amont de la chaîne des paiements INAR – ne font pas l'objet du périmètre de l'audit.

## 2.5 Démarche de l'audit

Notre audit a débuté le 6 septembre 2013. Les démarches suivantes ont été suivies pour sa réalisation :

- Entretiens avec les personnes clés ;
- Prise de connaissance de l'environnement informatique, des systèmes de trafic des paiements (cartographie des architectures, diagrammes de flux de données, etc.) ;
- Prise de connaissance des processus et procédures informatiques et métiers ;
- Tests de cheminement – suivi d'une opération de paiement de rente mensuelle et des travaux de contrôles effectués par la GETI et le TPI ;
- Tests de contrôle - test des contrôles en place.

[6] A la date de notre audit, la cartographie des systèmes informatiques ainsi que l'inventaire des actifs étaient en cours de réalisation par la GETI.

Les opérations de contrôle que nous avons effectuées sont mentionnées dans le programme de contrôle qui fait partie de nos notes de travail.

Notre audit s'est déroulé selon les normes de la profession. Nous avons utilisé le CobiT, qui est la référence reconnue dans le domaine.

# 3 Résultats de l'audit

## 3.1 Système de contrôle interne (SCI) de la sécurité de l'information

**Exigences**

La loi du 7 octobre 2005 sur les finances de la Confédération (LFC) prescrit explicitement la mise en place, l'utilisation et la supervision d'un système de contrôle interne (SCI) au sein de l'administration fédérale.

Le SCI vise en particulier à protéger la fortune de la Confédération, à assurer la régularité de la tenue et de l'établissement des comptes (y compris du traitement des données) et à garantir la fiabilité des rapports.

En application de la LFC, chaque unité administrative est tenue de disposer d'un système de contrôle interne (SCI)[7] qui :

> *2. inclut une analyse écrite des risques financiers auxquels l'unité administrative est exposée, qu'ils soient généraux ou qu'ils découlent de processus particuliers;*
>
> *3. décrit les mesures de contrôle d'ordre réglementaire, organisationnel ou technique permettant de gérer ces risques (réglementation appropriée des compétences, fondée sur la séparation des fonctions et incluant un plan relatif aux autorisations d'accès aux systèmes de traitement des données financières);*
>
> *5. définit les prestations qui doivent être fournies par les prestataires principaux de l'unité administrative, en particulier pour les prestations du secteur des technologies de l'information (TI);*
>
> *6. englobe tout ce qui touche aux données financières, c'est à dire non seulement le traitement des données proprement dit, mais aussi les éventuels systèmes en amont et les interfaces faisant partie intégrante du traitement des données financières.*

Le SCI est un élément clé de la politique de gestion des risques de la Confédération. Selon « le Guide d'application des prescriptions légales relatives au système de contrôle interne des processus avec incidences financières dans l'administration fédérale »[8] : *une gestion des risques et un système de contrôle consolidés garantissent à l'unité administrative (UA) de pouvoir reconnaître les nouveaux risques et de gérer ceux qui ont été identifiés. C'est pourquoi il est dans l'intérêt de l'UA de mettre en place un système de contrôle global, axé sur tous les risques opérationnels. Dans le cadre de la gestion des risques, chaque UA doit prévoir des mesures appropriés pour éviter, diminuer et financer les risques. Les mesures planifiées doivent réduire la probabilité de survenance des risques ou leurs éventuelles conséquences.*

---

[7] Se référer aux directives et instructions relatives à la gestion budgétaire et comptable de la Confédération : http://www.accounting.admin.ch/handbuch_hh/grundsatz_rf/00442/index.html?lang=fr

[8] Lien vers le guide : http://intranet.accounting.admin.ch/handbuch_hh/grundsatz_rf/00442/index.html?lang=fr&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ae2IZn4Z2qZpnO2Yuq2Z6gpJCDd319fmym162epYbg2c_JjKbNoKSn6A--

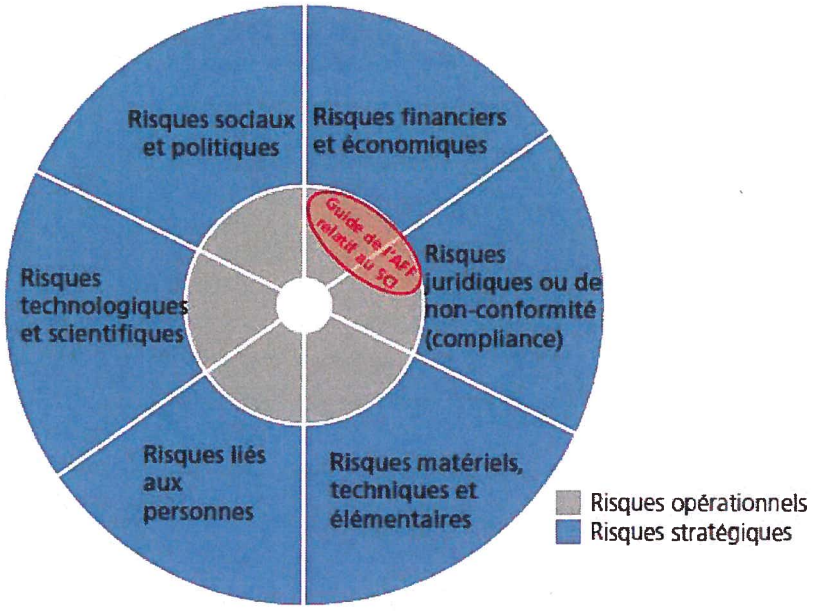


Figure 1 : Risques aux sein de la Confédération.
Source : Guide d'application des prescriptions légales relatives au SCI des processus avec incidences financières dans l'administration fédérale

*Les systèmes d'information liés aux finances et communications jugés importants pour la présentation des comptes (y compris le système de comptabilité) se composent des procédures et de la documentation mises en place pour déclencher des transactions à incidences financières, pour les enregistrer, les traiter et les consigner dans un rapport.*

La directive émise par l'OFAS sur la révision des caisses de compensation AVS, valables dès le 1er janvier 2004 (Etat au 1er janvier 2013) demande aux réviseurs lors de la révision principale de contrôler l'existence et l'efficience d'un système de contrôle interne (CM 2102 *Organisation pratique de la Caisse de compensation*). L'analyse porte notamment sur la garantie de la sécurité et de la protection des données.

**Méthode**

D'un point de vue méthodologique, l'établissement du SCI de la sécurité de l'information suit le concept COSO pour la réalisation du SCI de l'entreprise. Communément, le SCI de la sécurité de l'information s'appuie sur des normes professionnelles reconnues (ISO/CEI 27001 et ISO/CEI 27002) pour la sélection des contrôles informatiques clés permettant d'atteindre les objectifs de SCI de l'entreprise.

Une démarche d'analyse des risques dans le cadre d'un SCI doit prendre en considération l'impact du SI sur les processus d'affaires et proposer des contrôles proportionnels à la gravité de chaque risque identifié. Cette démarche doit notamment prendre en compte les contrôles automatiques des applications par rapport aux contrôles manuels, afin d'optimiser les processus et de réduire les risques résiduels.

L'analyse des risques du SI doit non seulement prendre en considération les contrôles de sécurité de l'information en relation avec les processus métier mais également considérer les risques et contrôles liés à la fonction informatique comme le développement, la maintenance des applications, la gestion de l'exploitation et la sécurité informatique.

### 3.1.1 SCI de la sécurité de l'information - chaîne des paiements INAR

**Contexte**

Le SCI du processus d'affaire « Paiement principal des prestations AVS/AI » a été documenté et date du 22 avril 2008.

Une analyse des risques et des contrôles envers le processus informatique de la chaîne des paiements INAR a été réalisée en 2010 par la GETI sur mandat de la direction de la CdC. Cette analyse a été réalisée suite à plusieurs incidents sur la chaîne des paiements INAR. Elle avait notamment pour objectif de répondre aux multiples incertitudes quant à la pérennité et l'évolutivité de l'application ainsi que de faire des propositions détaillées pour réduire ou supprimer les risques.

**Constats de l'Inspectorat**

Nous relevons que la « matrice des risques/de contrôle » pour le processus d'affaire « Paiement principal des prestations AVS/AI » (sous l'unité administrative CdC/CENT) n'a pas été mise à jour depuis le 22 avril 2008. En outre, les risques et les mesures de sécurité en matière de protection des données de paiements ne sont pas documentés et centralisés dans une matrice des risques et de contrôles. Il s'agit des contrôles automatiques INAR et de sa chaîne des paiements qui couvrent les risques liés à un manque d'intégrité, d'exhaustivité ou d'exactitude des données de paiements. A titre d'exemple, les vérifications automatiques exercées sur la chaîne des paiements, qui doivent permettre d'assurer la complétude et l'exactitude des fichiers de paiements en fin de chaîne, ne sont pas décrites au sein d'un document de référence.

Nous observons qu'une autre analyse des risques et des contrôles du système informatique de la chaîne des paiements INAR, réalisée en 2010 par la GETI, n'a à ce jour ni été actualisée ni mise en lien avec la « matrice des risques/de contrôle » du processus d'affaire « Paiement principal des prestations AVS/AI ». En outre, nous relevons que les données de paiements (y compris les données comptables) traitées, ainsi que les spécificités fonctionnelles de la chaîne des paiements ne sont pas pleinement et formellement décrites.

De manière générale, nous relevons l'absence d'un SCI de la sécurité de l'information documenté et centralisé pour les processus clés de la GETI. Notons que ces processus sont en cours de description dans le cadre du projet de système de management de la qualité (SMQ).

**Risques**

En l'absence d'un SCI à jour prenant en compte le SCI de la sécurité de l'information, la CdC n'est pas à même de savoir si tous les risques ont bien été identifiés et si toutes les mesures de contrôles sont bien en place sur la chaîne des paiements. Toute défaillance de sécurité du SI de la chaîne des paiements risque d'affecter la confidentialité et l'intégrité des données de paiements ainsi que la continuité de paiements des rentes.

**Recommandations de l'Inspectorat**

1. Au vu de nos constats, nous recommandons à la GETI de documenter son système de contrôle interne de la sécurité de l'information et de l'intégrer au projet général du SCI de la CdC. Pour ce faire, nous recommandons à la GETI de se coordonner avec le(s) responsable(s) du SCI de l'institution, de définir les responsabilités et d'attribuer les ressources nécessaires pour l'accomplissement de cette tâche. Un des résultats attendus de cette coordination est l'intégration des contrôles nécessaires à la sécurité de l'information dans le système de contrôle des processus métiers clés, tels que le « Paiement principal des prestations AVS/AI ».

   *La mise en place du SCI de la sécurité de l'information constitue un pré-requis aux traitements des recommandations de sécurité du SI présentées dans ce rapport.*

## 3.2 Gestion des accès aux données de paiements

**Cadre normatif**

Gestion des biens

Selon la norme ISO/IEC 27002 (chapitre 7), le propriétaire[9] des données est responsable de la validation des droits d'accès à ses données. Aussi, afin de mener au mieux sa mission, celui-ci doit identifier les données les plus critiques et les plus sensibles pour l'institution afin de déterminer leur besoin de sécurisation. Cette identification s'inscrit dans le cadre du processus de classification des données[10] présenté au chapitre 7.4 du document : « Lignes directrices de la sécurité de l'information à la CdC – Politique de sécurité de l'information de la CdC » (ci-après, POSIC).

Sécurité des données

Selon la norme ISO/IEC 27002 (chapitre 11), l'accès à l'information, aux moyens de traitement de l'information et aux processus métiers doit être contrôlé sur la base des exigences d'exploitation et de sécurité. Afin de garantir la sécurité des données, l'entreprise doit donc être à même de maîtriser l'accès à ses informations.

La POSIC de l'institution se base sur la norme ISO/IEC 27002 et décrit notamment les domaines/sous-domaines prioritaires suivants en matière de sécurité de l'information :

- Le « Contrôle des accès » (chapitre 7.7 de la POSIC),
- La sécurité des « échanges d'information » avec des entités externes (chapitre 7.6 de la POSIC).

[9] Le propriétaire des données est la personne responsable de l'intégrité des données.

[10] Selon CobiT, un système de classification doit être basé sur les dimensions critiques et sensibles des données (par ex. publiques, confidentielles, secrètes) qui s'appliquent à toute l'entreprise. Ce système doit comprendre les détails sur la propriété des données, la définition des niveaux de sécurité et des contrôles de protection appropriés, une brève description des règles de conservation et de destruction des données, et de leurs dimensions critiques et sensibles. Il doit être utilisé comme base pour les contrôles, comme les contrôles d'accès, d'archivage ou de cryptage.

### 3.2.1 Gestion des droits d'accès, des privilèges et séparation des fonctions

**Contexte**

Un contrôle d'accès envers un système dont la sécurité logique se base sur une définition par rôle permet aux personnes responsables (par exemple, au propriétaire des données) d'attribuer des droits d'accès aux utilisateurs sur la base d'un modèle organisationnel. Les utilisateurs doivent se voir assigner des rôles au sein du système informatique (tels que : gestionnaire AVS, comptable, etc.), sur la base d'une analyse du fonctionnement et des besoins opérationnels des services de la CdC. Les rôles attribués aux utilisateurs doivent se fonder sur leurs compétences et leurs responsabilités au sein de l'organisation. De cette manière, les privilèges attribués aux utilisateurs sont restreints aux seules fonctions nécessaires à la réalisation de leur travail.

**Constats de l'Inspectorat**

Nous relevons que la GETI ne dispose pas d'une procédure pour la gestion des groupes utilisateurs, des profils standards pour l'octroi des droits d'accès à l'application INAR ainsi qu'à ses fonctionnalités de paiements. En l'absence d'un tel référentiel, le service utilisateur attribue ou modifie les droits d'accès du compte utilisateur sur la base d'une demande métier (mandat informatique) en réalisant une copie des droits d'accès d'un compte utilisateur préexistant (héritage). En procédant de la sorte, l'utilisateur peut cumuler des droits d'accès qui ne sont pas en adéquation avec sa fonction et ses responsabilités. Dès lors, les principes de séparation des fonctions incompatibles et de moindre privilège ne sont plus garantis.
A relever qu'en l'absence d'un tel référentiel documenté et validé par les métiers, il nous est difficile de contrôler que le principe de séparation des fonctions est respecté pour INAR et sa chaîne des paiements.
Sur la base de nos travaux, nous observons tout de même que :

- Plusieurs utilisateurs disposent d'identifiants multiples (par exemple : EMD2, EMD3 ou APH, APH1, APHX) ;
- Trois comptes appartenant à l'exploitation (GETI) ont des accès en production au menu comptabilité CSC. Selon le métier (TPI), ces utilisateurs ne peuvent pas faire grand-chose avec ce menu. Le métier est néanmoins surpris d'apprendre qu'ils y ont accès ;
- Cinq comptes ont accès au menu cotisants à l'assurance facultative, alors qu'ils ne font pas partie de l'organisation de l'AFac selon l'organigramme de la CdC ;
- Deux comptes ont accès au menu AI prestation alors qu'ils ne se trouvent pas dans l'organisation de l'OAIE selon l'organigramme de la CdC.

D'autre part, nous constatons un manque de maîtrise de la part de la GETI envers le composant de sécurité : Natural Security. Ce dernier permet de gérer les accès aux environnements Natural dont l'application INAR fait partie. Actuellement, aucune règle de sécurité ne décrit les concepts de sécurité appliqués au système Natural Security, son fonctionnement, le(s) responsable(s) de ce système, les domaines d'application, les exigences et conformités de sécurité pour la gestion des comptes (personnes, groupes de personnes, administrateurs, terminaux, librairies), les accès aux fichiers et aux utilitaires systèmes.

L'inspectorat avait déjà relevé, dans son rapport d'audit sur la « gestion des accès informatique » datant du 30 août 2011, l'absence de profils standards métiers aux applications.

**Risque**

Une telle situation génère un risque d'accès indus susceptibles de mettre en péril la confidentialité ainsi que l'intégrité des données de paiements.

**Recommandations de l'Inspectorat:**

Nous recommandons que les actions suivantes soient déployées en coordination avec le responsable des données INAR et la GETI (notamment le responsable de la sécurité du SI) :

2. Définir puis mettre en œuvre un processus d'approbation des droits d'accès en regard des exigences en matière de sécurité des données de paiements des rentes.

3. Créer des profils d'accès standards qui correspondent aux rôles définis au sein de l'organisation. Dans le cas présent, il est nécessaire de connaître l'existant et donc de documenter les droits d'accès gérés par Natural Security, soit :
    - Les groupes ;
    - Les utilisateurs faisant partie de ces groupes et leurs autorisations (écritures, lectures, suppression) ;
    - Les droits d'accès aux librairies et aux programmes, ainsi que la description des programmes (les opérations qu'ils permettent de faire).

    Il sera ainsi plus aisé pour les métiers de déterminer si les principes de séparation des fonctions et de moindres privilèges sont effectivement respectés.

4. Documenter les concepts de sécurité appliqués au système Natural Security, son fonctionnement, le(s) responsable(s) de ce système, les domaines d'application, les exigences et conformités de sécurité pour la gestion des comptes, les accès aux fichiers et l'accès aux utilitaires systèmes.

### 3.2.2 Révocation des droits d'accès

**Exigences**

La POSIC dicte (au chapitre 7.7) les mesures de contrôle suivantes à prendre en matière de gestion des comptes utilisateurs :

- « Etant donné leurs risques plus importants, les droits d'accès privilégiés sont rigoureusement limités et contrôlés » ;
- « Le processus de gestion des accès des utilisateurs est formalisé, en particulier [..] la désactivation de l'utilisateur et de ses droits lorsqu'il quitte la CdC » ;
- « La validité des droits d'accès en vigueur doit être contrôlée périodiquement ».

**Constats de l'Inspectorat**

Nous constatons que les mesures de contrôles prescrites par la POSIC quant à la révocation des comptes utilisateurs et de leurs droits accès à INAR ainsi qu'aux systèmes par lesquels les données de paiements véhiculent ne sont pas respectées. En effet, nous observons les faiblesses suivantes :

- Un total de 181 comptes utilisateurs sont présents dans le système Natural Security[11], alors que les propriétaires de ces comptes restent introuvables dans l'organigramme de la CdC (ils ont potentiellement quitté la CdC). Il s'agit d'utilisateurs internes et d'utilisateurs temporaires. Dix de ces comptes ont des accès de type administration.

- Un total de 7 comptes utilisateurs sont présents sur le serveur Mercure (serveur permettant notamment l'envoi des fichiers de paiements aux partenaires financiers), alors que leurs propriétaires ont quitté l'institution. Un total de 30 comptes ont accès à ce serveur, ce qui paraît très élevé au vu de la sensibilité des données qu'il héberge. Ces accès « permanent » devraient être limités aux seuls utilisateurs habilités qui se connectent périodiquement pour exercer leurs tâches. D'autant plus qu'entre mai et septembre, seuls 11 de ces comptes se sont effectivement connectés au serveur.

Nos constats présentés ci-dessus découlent du fait que le processus de gestion des habilitations (surveillance ainsi que désactivation ou suppression des droits d'accès lors d'absence, de départ et de mutation de collaborateurs) est inefficace.

L'inspectorat avait déjà relevé, dans son rapport d'audit sur la « gestion des accès informatique » datant du 30 août 2011, l'absence de contrôle périodique des états des accès.

**Risque**

Une telle situation génère un risque d'accès indus susceptibles de mettre en péril la confidentialité ainsi que l'intégrité des données de paiements.

[11] Natural Security gère notamment la sécurité des accès à INAR.

**Recommandations de l'Inspectorat:**

Nous recommandons que les actions suivantes soient déployées par les responsable des données de paiements et le responsable de sécurité en coordination avec les unités, services concernés :

5. Dans un premier temps, désactiver ou supprimer les comptes utilisateurs de Natural Security et de Mercure dont le propriétaire a quitté la CdC.
   Dans un deuxième temps, nous recommandons la mise en œuvre d'un processus efficace de revue périodique des droits d'accès (recommandation émanant de l'audit de gestion des accès du 30 août 2011). Nous insistons sur le fait que ce processus de revue doit permettre de confirmer que les droits d'accès existants dans les systèmes sont conformes aux besoins des collaborateurs et respectent la POSIC.

6. En sus d'une revue périodique des droits d'accès utilisateurs, nous préconisons le paramétrage d'une désactivation automatique lorsque des personnes externes ou internes se voient octroyer des droits d'accès de type temporaire à INAR.

7. Les RH doivent s'assurer que toute mutation (changement de poste d'un collaborateur) ainsi que les départs des collaborateurs sont bien communiqués à la GETI. Une confirmation de la GETI doit parvenir au RH, une fois le travail effectué.

### 3.2.3 Gestion des comptes techniques

**Contexte**

Une gestion inappropriée des privilèges d'administration d'un système peut constituer une source importante de défaillance et de vulnérabilité. Il convient donc de s'assurer :

- Que les comptes utilisateurs permettant d'exploiter et d'administrer le système possèdent leur propre identifiant, c'est-à-dire un compte spécifique et différent du compte d'administration système par défaut;
- Que les mots de passe des comptes restent nominatifs et qu'ils ne soient pas communiqués.

Selon la norme ISO/IEC 27002 un identifiant unique et exclusif doit être accordé afin de vérifier l'identité déclarée par l'utilisateur et de pouvoir suivre les opérations effectuées sous sa responsabilité. Des mesures doivent être mises en place pour garantir l'imputabilité.

**Constats de l'Inspectorat**

Nous relevons les faiblesses suivantes :

- Le compte de test : FORM01 est présent dans Natural Security et accède aux librairies[12] INAR de production. Ce compte dispose de droits d'accès en administration à Natural Security.
- Les comptes techniques Y31 et Y23 sont présents et accèdent aux librairies INAR de production. Ils disposent également de droits d'accès en administration.
- L'utilisation par le service d'exploitation (GETI) de comptes techniques de type générique tels que :
    - « root » et « prod » pour administrer le serveur Mercure ;
    - « DBA » pour administrer la base de données ADABAS.

L'utilisation de ces comptes sensibles s'effectue en l'absence d'une procédure dictant les mesures de sécurité à prendre, notamment en matière de gestion et de communication du mot de passe.

**Risque**

Cette situation ne permet pas de garantir que les données de paiements des rentes sont sécurisées de manière permanente. Un risque d'accès indus aux données confidentielles et/ou critiques, ainsi que des lacunes en matière de traçabilité existent.

[12] Les librairies Natural contiennent les programmes sources ainsi que des objets réalisant des fonctions particulières lorsqu'ils sont appelés par l'utilisateur.

**Recommandations de l'Inspectorat:**

Afin de garantir la sécurité des accès aux données (en terme de confidentialité, de traçabilité des activités et de respect du principe de séparations des tâches), nous recommandons que:

8. Des identifiants uniques et nominatifs soient attribués aux collaborateurs de la GETI qui exercent des travaux d'administration sur la base de données ou d'intégration sur les serveurs de production. Par mesures de sécurité, le compte de tests doit être supprimé de l'environnement de production. Les tests doivent se faire dans un environnement dédié.

9. Les mots de passe des comptes techniques ayant des droits d'accès privilégiés ne doivent pas être communiqués entre collaborateurs. Le mot de passe du compte d'administration doit respecter les contraintes fixées par la POSIC. D'autre part, l'intervention en environnement de production par le biais d'un compte technique doit être limitée au temps de l'intervention ; les droits d'accès accordés à l'utilisateur doivent automatiquement être révoqués après les travaux.

10. L'utilisation des comptes d'administration des systèmes de la base de données (de type technique) doit faire l'objet d'une surveillance permanente en environnement de production.

### 3.2.4 Sécurité de la base de données et des serveurs de communication

**Exigences**

Selon CobiT, le besoin de maintenir l'intégrité de l'information et de protéger les actifs informatiques exige un processus de gestion de la sécurité efficace. Celui-ci doit permettre de réduire au maximum les conséquences de failles et d'incidents de sécurité.

**Constats de l'Inspectorat**

Nous relevons qu'il n'existe ni une procédure de sécurité pour les donnés de paiements contenues dans ADABAS (base de données pour INAR), ni une procédure de sécurité envers les serveurs Edifact et Mercure en charge de stocker et communiquer les fichiers de paiements.

D'un point de vue technique, nous constatons les faiblesses suivantes :

- Les collaborateurs habilités du service 321 utilisent le protocole non sécurisé « telnet » pour se connecter au serveur Mercure, afin de transmettre le troisième jour ouvrable du mois les fichiers de paiements à l'UBS. Un manuel a été rédigé par le TPI afin de décrire de manière détaillée la procédure de contrôle à suivre. La procédure de communication des fichiers de paiements à l'UBS n'étant pas automatisée, un risque résiduel subsiste dans l'éventualité d'une erreur humaine ou technique.

  D'autre part, même si le serveur renvoie le message « transfert des données vers UBS - transfert ok », il est toujours possible qu'un message d'erreur soit affiché plus bas sur l'écran. Charge à l'utilisateur d'y être attentif.

- Le serveur Edifact n'envoit aucun message d'alerte lors de la purge des fichiers de paiements ou lors de la réception à double des fichiers. Des journaux d'activités (fichiers logs) sur l'exécution des divers scripts sont générés.

- Aucune politique de mots de passe (password policy) n'est activée sur le serveur Mercure. Une alerte est certes générée dans le cas où le mot de passe créé par l'utilisateur a un faible niveau de sécurité, mais elle peut être outrepassée par l'utilisateur.

- Le compte technique du serveur Edifact nommé par défaut : « edifact » est utilisé par la solution ConnectDirect de l'éditeur du logiciel (Sterling Software) pour établir la connexion avec le serveur Mercure. Ce compte est utilisé conjointement à une clé cryptée en lieu et place d'un mot de passe. A savoir que la nature de cette clé est méconnue par la GETI, celle-ci étant créé et gérée par la solution ConnectDirect.

- Le contrat Edifact passé avec le prestataire de service Compudata ne prend pas en compte les exigences de sécurité logique, de gestion des changements et de continuité en conformité avec la POSIC.

  Le niveau de maîtrise de la GETI quant à l'administration du serveur Edifact est très faible, la gestion du serveur ayant été déléguée auprès du prestataire. Il est pourtant du ressort de la GETI de s'assurer que le niveau de sécurité de ce serveur est conforme à la POSIC de la CdC.

## Risque

Une telle situation génère un risque d'accès indus susceptibles de mettre en péril la confidentialité ainsi que l'intégrité des données de paiements. En outre, le risque de non délivrance ou de délivrance erronée des fichiers de paiements auprès des intermédiaires financiers subsiste.

## Recommandations de l'Inspectorat:

11. Nous recommandons qu'une procédure de gestion de la sécurité des bases de données et serveurs soit documentée et qu'elle couvre notamment les aspects suivants :
    - Gestion des mots de passe ;
    - Gestion des comptes et profils – par exemple les comptes d'exploitation, d'administration et de sécurité ;
    - Ségrégation des environnements et accès aux bases de données (environnement de développement, d'assurance qualité et de production) ;
    - Stockage des mots de passe ;
    - Gestion des scripts d'exploitation ;
    - Gestion des protocoles de communication (seule l'utilisation du SSH (protocole version 2)) devrait être autorisé pour la connexion avec les serveurs; Les transferts entre serveurs ainsi qu'entre serveurs et clients doivent se faire par le biais un protocole sécurisé, par exemple sftp ;
    - La communication des paramètres de connexion.

Au vu de nos constats, nous recommandons également à la GETI de s'assurer que la sécurité du serveur Edifact respecte la POSIC. Il s'agit entre autre de vérifier que :

12. Les connexions des utilisateurs au serveur Mercure s'établissent pas le biais d'un protocole sécurisé ;

13. Tous les traitements des purges des fichiers de paiements sur les serveurs soient sous alertes. Il en va de même des contrôles de réception de fichiers à double ;

14. La politique de mot de passe sur le serveur Edifact soit activée, et ce en conformité avec la POSIC ;

15. Les logs systèmes sont conservés suffisamment de temps dans le cas où ils devraient être exploités, par exemple lors d'une enquête liée à un incident de sécurité. La conservation des logs devant elle-même suivre une politique de conservation[13] des données.

16. Le contrat Edifact passé avec le prestataire de service Compudata prenne en compte les exigences de sécurité en conformité avec la POSIC.

[13] Selon l'ordonnance 780.11 sur la surveillance de la correspondance par poste télécommunication (disponible sous http://www.admin.ch/opc/fr/classified-compilation/20002506/) les procès-verbaux de journalisation doivent être conservés durant une année sous une forme permettant de déterminer quelles données ont été consultées.

## 3.3 Sécurité de l'exploitation informatique

### 3.3.1 Gestion de la sécurité de l'infrastructure

**Exigences**

Selon CobiT, des techniques de sécurité et des procédures de gestion associées doivent être mises en place pour autoriser et contrôler les flux d'informations entre réseaux. Les données sensibles doivent donc circuler sur des circuits sûrs, dotés de contrôles qui garantissent la confidentialité et l'intégrité du contenu.

**Constats de l'Inspectorat**

Nous relevons les faiblesses suivantes concernant les communications des fichiers de paiements :

- Les serveurs Edifact et Mercure ne disposent pas d'un environnement de test. En l'absence d'un tel environnement, la CdC ne peut pas tester les changements[14] effectués sur ses systèmes de communication avant le lancement de la chaîne des paiements en production.
- La procédure de gestion des clés de chiffrement des fichiers de paiements et des communications entre les serveurs et les établissements financiers n'est pas documentée. Il s'agit par exemple de : la méthode de génération des clés, la communication des clés publiques, la protection de la clé privée, les accès à la clé privée, les changements, etc.
- Il n'existe pas de contrôle d'intégrité sur les fichiers de paiements depuis leur génération par INAR (le Host) jusqu'à leur communication auprès des instituts financiers. Un tel contrôle pourrait s'exécuter par exemple à l'aide d'une fonction de hachage, appelée en anglais *checksum* [15]
- Le réseau qui achemine les fichiers de paiements INAR (depuis le Host) vers le serveur Mercure est faiblement sécurisé. En effet, le transferts des fichiers de paiements s'effectue par le bais du protocole FTP non chiffré. Le protocole sécurisé SFTP est par contre utilisé pour les connexions entre le serveurs Mercure et les institutions financières.

[14] Par exemple, la mise à jour du système, les modifications des programmes de conversion au format EDIFACT, les scripts de lancement de la chaîne des paiements en production.
[15] Exemple de checksum permettant de contrôler l'intégrité d'un fichier : MD5, SHA1.

**Risque**

La sécurité de l'infrastructure réseau et les modalité d'envoi des fichiers de paiements ne sont pas adaptées au niveau de confidentialité des données de paiements, afin de les protéger des accès indus et de tout mauvais usage.

**Recommandations de l'Inspectorat:**

Nous recommandons à la GETI de renforcer les mesures de protection des actifs d'information que sont les données de paiements au travers des mesures suivantes :

17. Mise en place d'un environnement de test pour les serveurs de communication ;

18. Formalisation de la procédure de gestion des clés de chiffrement[16] ;

19. Mise en place d'un contrôle d'intégrité des fichiers de paiements depuis leur génération jusqu'à leur acheminement ;

20. Soumission à l'OFIT du besoin de sécuriser la connexion réseaux acheminant en sortie du mainframe les fichiers de paiements vers les serveurs de communication gérés par la GETI.

21. Enfin, nous sommes d'avis que des tests d'intrusions sur l'infrastructure IT doivent être réalisés, dans le but d'identifier d'éventuelles vulnérabilités réseaux.

[16] Selon CobiT les objectifs de contrôle en matière de gestion des clés de chiffrement sont de s'assurer de l'existence : des politiques et des procédures pour gérer la génération, la modification, la révocation, la destruction, la distribution, la certification, le stockage, l'entrée, l'utilisation et l'archivage de clés de chiffrement afin de garantir leur protection contre toute modification ou divulgation non autorisée.

### 3.3.2 Gestion des sauvegardes des données et des fichiers de paiements

#### Exigences

Selon CobiT, la division des SI doit définir et mettre en place des procédures pour la sauvegarde et la restauration des systèmes, des applications, des données et de la documentation conformes aux exigences des métiers et au plan de continuité.

#### Constats de l'Inspectorat

Nous relevons les faiblesses suivantes en matière de gestion de la continuité des opérations systèmes :

- L'absence de procédure de sauvegarde documentée pour :
  - Les fichiers de paiement en sortie de la chaîne de paiements INAR ;
  - Les serveurs Edifact et Mercure. Les fichiers de paiements sont conservés une année sur le serveur Mercure et un mois sur le serveur Edifact.

  D'autre part, la politique de conservation des sauvegardes n'est pas documentée.
- Les serveurs Mercure et Edifact ne sont pas redondants ;
- Les lignes réseaux acheminant les fichiers de paiements auprès des institutions financière ne sont pas redondantes. En outre, le réseau n'est pas « surveillé » par le biais d'un outil adéquat.

En outre, le rapport Ernst&Young sur la révision principale de l'exercice 2012 de la CSC relève le point suivant : « *en cas de sinistre majeur des systèmes peu avant la date de paiement, la CdC ne serait pas en mesure d'effectuer le versement des rentes étant donné qu'il n'existe pas un second robot capable de déclencher les rentes* ».

#### Risque

L'infrastructure réseau ainsi que les données de paiements sont indisponibles et ne peuvent pas être aisément restaurées de manière exacte et exhaustive afin de transmettre les fichiers de paiements à temps aux institutions financières.

#### Recommandations de l'Inspectorat:

Nous recommandons à la GETI la mise en œuvre des actions suivantes :

22. Documenter les procédures de sauvegarde et les procédures de restauration, en conformité avec les exigences métiers, légales et de sécurité. La politique de durée de rétention des fichiers de paiements doit être documentée et harmonisée ;

23. S'assurer que les infrastructures soient dédoublées et/ou que des procédures et contrôle correctifs répondant aux risques encourus soient en place, afin d'assurer la continuité des opérations de la chaîne des paiements en cas d'indisponibilité de l'un de ses composants. Ces contrôles doivent être mis en place dans le cadre du plan de secours informatique (PSI) et du plan de continuité d'activité (PCA).

### 3.3.3 Gestion des incidents sur la chaîne des paiements INAR

#### Exigences

Selon CobiT, le processus de gestion des incidents doit permettre à l'entreprise de s'assurer :

- Qu'un incident informatique n'a qu'un impact minimum sur les processus d'affaires ;
- Que les transactions métiers automatisées et les échanges d'informations restent intègres et fiables ;
- Que l'intégrité de l'information et les conséquences d'éventuelles failles et incidents de sécurité sont réduites au minimum.

#### Faits

Depuis le début de l'année 2013, un total de neuf incidents sur la chaîne des paiements INAR ont été dénombrés. Six de ces incidents sont de nature informatique (sous la responsabilité directe de la GETI).

#### Constats de l'Inspectorat

Durant notre mission d'audit, deux incidents[17] sont survenus dans le processus de la chaîne des paiements des rentes, sans toutefois impacter la délivrance de la prestation. Il s'agit des incidents suivants :

- **Paiement principal des rentes d'octobre 2013** : suite à un problème technique de connexion avec la BPE empêchant l'envoi automatique des fichiers de paiements, la GETI a dû procéder le 1 octobre 2013 à un envoi manuel des fichiers à destination de la BPE. Il apparaît que cet incident est récurrent avec la BPE. La GETI réalise actuellement des travaux d'analyses en coordination avec l'OFIT et la BPE pour identifier la cause réelle de l'évènement et proposer une résolution définitive du problème.

- **Paiement principal des rentes de novembre 2013 :** le 6 novembre 2013, l'UBS a rejeté l'ensemble du fichier des paiements des rentes car deux codes BIC étaient erronés. La raison exacte de ce rejet en bloc était encore méconnue par le métier (état au 01.12.2013), l'UBS ayant traité les fichiers même en cas de problème de codes BIC par le passé.
  A la demande du chef de service 321 et sous la supervision de ce dernier et de l'inspectorat, les deux numéros BIC ont été corrigés par la GETI sur la base d'une copie du fichier de paiement, en environnement de production. Après correction, le fichier des paiements a été transmis par le service 321 à l'UBS, qui a confirmé sa bonne réception. L'incident a été documenté.
  En date du 8 novembre 2013, la correction des numéros BIC à la source - c'est-à-dire dans GEDO - a été exécutée. Aucune mesure spécifique n'a été prise pour introduire dans le système de nouvelles règles concernant ces comptes BIC.

[17] La norme ISO 20000 définit un incident comme "*any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service*".

Il sied de préciser qu'au cours de l'audit d'autres incidents de sécurité ont été identifiés. Le responsable de la sécurité a informé l'Inspectorat en août 2013 qu'un incident de sécurité portant sur les fichiers de quittances PostFinance avait été identifié. A ce jour, l'Inspectorat n'a pas reçu le rapport lié à cet incident. Lors de l'audit, l'Inspectorat a relevé que les fichiers de confirmation Postfinance étaient déposés sur un répertoire non sécurisé du disque réseau (fichiers accessibles par tous les utilisateurs paramétrés dans le système, c'est-à-dire par presque tous les collaborateurs de la CdC). A ce sujet, l'Inspectorat a transmis une note à l'intention de la direction en date du 4 octobre 2013.

Nous relevons qu'il n'existe pas de procédure documentée de sécurité lorsque la GETI intervient en urgence sur les fichiers de données de paiements en environnement de production (dans le cas présent il s'agit du serveur Mercure).

Bien que la plupart des rapports d'incidents soient documentés, nous observons que les incidents sur la chaîne des paiements ne sont pas systématiquement renseignés et centralisés dans l'outil de gestion des incidents : Remedy.

Nous ne disposons pas d'une assurance raisonnable quant à l'exhaustivité des incidents survenus entre 2012 et 2013, ceux-ci devant normalement être renseignés dans l'outil de gestion des incidents. Cependant, sur la base des informations fournies par la GETI et le métier (les collaborateurs du secteur TPI et de l'unité Prestations AVS), nous n'avons pas identifié d'incident critique causé par la chaîne des paiements INAR ayant eu pour conséquence la non délivrance de la prestation ou la délivrance de prestations erronées.

## Risque

Des risques subsistent quant à la bonne délivrance de la prestation, notamment lorsque les clients subissent les conséquences d'incidents qui auraient pu être évités où que ces incidents ne sont pas traités de manière adéquate et dans des délais raisonnables. Un gaspillage de ressources existe lorsqu'il faut trouver à chaque fois une nouvelle solution de contournement sur un incident au lieu de corriger le problème à son origine.

## Recommandations de l'Inspectorat:

24. Nous recommandons que tous les incidents de la chaîne des paiements soient systématiquement enregistrés, classifiés, priorisés, et communiqués (procédure d'escalade d'un incident) à qui de droit (avec copie à la Direction et à l'Inspectorat) selon une procédure documentée. Le responsable de la sécurité du SI doit immédiatement être alerté lorsqu'un incident de sécurité survient, afin que les mesures corrective nécessaires soient mises en place en conformité à la POSIC.
25. Nous recommandons également la mise en place d'une procédure documentée de sécurité lorsque la GETI intervient en urgence sur les fichiers de données de paiements. Cette procédure d'urgence doit contenir : le mode opératoire pour l'annonce de l'incident auprès des parties concernée et responsables des données – ouverture du ticket d'incident, l'accord du responsable des données pour intervention sur les fichiers de paiements, les modalités de sécurité appliquées, le canal de communication utilisé, les collaborateurs de la GETI habilités à intervenir sur les fichiers de paiements, le contrôle quant à l'intégrité des fichiers corrigés (si correction il y a), les responsabilités des parties impliquées (du côté de la GETI, du métier et de l'institution financière).

26. Nous recommandons qu'un contrôle de plausibilité sur les paiements BIC soit réalisée afin de notamment éviter tout incident lors de l'exécution de la chaîne des paiements.

## 3.4 Comptabilisation des paiements de rentes - Intégration des processus, procédures et contrôles comptables

### Contexte

Toutes les décisions de paiements des rentes effectuées pendant le mois par les gestionnaires AVS, AI et AFac sont traitées à la fin du dernier jour du mois par la chaîne des paiements INAR afin de produire les fichiers de paiements des rentes et des restitutions comptables. Les fichiers de paiements sont communiqués automatiquement auprès des partenaires financiers (exception faite pour UBS[18]). Le premier jour ouvrable du mois, le service 322 effectue ses contrôles mensuels sur la base de différents états de contrôles comptables produits par la chaîne des paiements INAR (fichiers plats). Les contrôles ainsi réalisés sont manuels[19] (faits à l'aide d'Excel) et visent à :

- S'assurer qu'aucun incident n'a eu lieu sur la chaîne des paiements ;
- Produire une récapitulation des paiements par intermédiaire ;
- Contrôler des écritures INAR, les paiements et récapitulation pour la comptabilité principale (HELIOS). Il s'agit notamment de vérifier le nombre et le montant des rentes versées (intégralité) ainsi que leur continuité[20].
- Récapituler les prestations AVS/AI CH/ETR et virer les retours aux fonds dus AVS/AI CH/ETR
- Réconcilier[21] (mensuellement) les Prestations et Paiements INAR

Une fois que le service 322 annonce formellement que ses travaux de contrôles sont terminés, le service 321 procède aux siens en se basant sur les états de contrôles issus de la chaîne des paiements ainsi que du fichier de récapitulation et pièces comptables fournis par le service 322. Des étapes de contrôle et de validations manuelles se suivent tout au long du processus des paiements mensuels, tels que : confirmation de réception des fichiers de paiements par nos partenaires financiers, contrôle des erreurs et rejets de paiements, traitement des ordres de paiements, demande de fonds, libération des paiements.

Le TPI effectue ses contrôles entre les 1er et le 4ème jours ouvrables, après que les fichiers de paiements aient été transmis auprès de nos partenaires financiers. Dès le 5ème jour ouvrable du mois, les partenaires financiers exécutent le paiement des prestations.

---

[18] Le 3ème jour ouvrable du mois, le transfert du fichier UBS est exécuté manuellement par le TPI.
[19] Une procédure documente l'ensemble des tâches à exécuter par le TPI.
[20] Selon les collaborateurs du TPI, les cas d'exceptions identifiés dans les états de contrôles de la chaîne des paiements (par exemple, la liste « Décomptes non équilibrés ») n'ont pas nécessité une relance de la chaîne des paiements ces sept dernières années.
[21] Cette réconciliation est établie afin de justifier l'écart entre les prestations octroyées et les paiements comptabilisés dans INAR. Cet écart se vérifie au moyen de plusieurs écritures INAR.

**Constats de l'Inspectorat**

Nous relevons les faiblesses suivantes :

- L'absence d'un système de comptabilité pour tiers (créanciers et débiteurs) où toute décision de rentes prise par les gestionnaires générait automatiquement des écritures en comptabilités auxiliaires. Les contrôles comptables sont réalisés par le secteur TPI à partir de listes issues de la chaîne des paiements INAR, qui est une application de gestion et de paiements des rentes et non un système de comptabilité auxiliaire. Les contrôles sont réalisés après que les fichiers de paiements aient été transmis auprès des partenaires financiers (sauf pour l'UBS).

  Il ressort des différents travaux effectués par le secteur TPI que la chaîne de paiements INAR n'est pas à même de fournir des listes de contrôles exploitables en l'état pour la réalisation des contrôles comptables. Les (re-)traitements réalisés par le métier à l'aide d'Excel (macros) sont hors de contrôle des processus standards de sécurité informatique que doit garantir la GETI. En outre, un risque inhérent subsiste dans le fait que les connaissances sur le fonctionnement des macros Excel sont aujourd'hui centralisées auprès d' un seul collaborateur du TPI.

  De plus, une grande partie des listes de vérification comptables fournies par la chaîne des paiements INAR à l'intention du secteur TPI sont inutilisées par le métier. A titre d'exemple, seules 12 des 60 listes communiquées par la GETI et enregistrées sur le répertoire BLN : « Listes CENT sur Eole » sont réellement utilisées par le service 322.

- L'absence d'interface automatique sécurisée permettant le déversement et le contrôle automatique des écritures de paiements vers le système de comptabilité principale Helios. En effet, aujourd'hui des pièces comptables mensuelles sont générées par la chaîne des paiements INAR sous un format « .csv [22]» - celles-ci devant être reprises et contrôlées par le TPI avant d'être imputées « manuellement » [23]dans la comptabilité générale Helios.

- L'absence d'une solution informatique intégrée pour le cash management et le trafic des paiements (avec PostFinance, UBS, BPE, BPS).

Nous avons été informés que le projet FSP&C initialisé en 2011 vise à acquérir un progiciel commercial de type ERP afin que les processus et procédures de paiements et de comptabilité soient intégrés et conformes aux bonnes pratiques en la matière. Aujourd'hui, l'organisation de ce projet n'est pas clarifiée, les ressources et compétences nécessaires pour mener à terme ce projet ne sont pas toutes identifiées et les responsabilités ne sont pas clairement documentées dans la proposition de projet Hermès(document qui n'a jamais été validé). Ce projet a commencé en 2011 et a été gelé en 2012. Actuellement aucune date de (re-)démarrage n'est planifiée, néanmoins le projet figure dans le portefeuille des projets et a été qualifié comme indispensable lors de la Commission Informatique du 10 décembre 2013.

Notons que le document *Planification stratégique de l'informatique* datant de 2008 (document validé par la Cominf) avait déjà identifié pour les programmes IT-CSC des potentiels de développements pour les problématiques suivantes :

---

[22] Un fichier Comma-separated values (.csv) est un fichier texte.

[23] Il s'agit d'un contrôle manuel dépendant de l'informatique. En effet, dans le cas présent l'utilisation d'un fichier XML permet d'importer les pièces comptable dans Helios pour comptabilisation.

*« L'organisation des activités de paiement et de comptabilisation n'est pas maîtrisée. Il n'y a ni documentation ni processus explicites. Ces opérations ne sont donc pas optimisées.*

*Les données provenant des applications en amont des paiements sont parfois incomplètes ou erronées, en particulier les adresses de paiement IBAN-BIC[24]. Les activités de paiement et de comptabilisation impliquent des saisies multiples des mêmes données dans des applications informatiques différentes, engendrant pertes de temps, risques d'erreurs et non-traçabilité des opérations ».*

**Risque**

L'absence d'un outil informatique comptable approprié aux besoins du métier pour la réalisation de leurs opération et contrôles comptables entraîne des redondances dans le traitement des données et des contrôles, qui rendent le travail inefficient.

Cette situation engendre également des risques d'erreurs (paiements indus, paiements à double) dues aux saisies multiples et manuelles et des risques liés aux problématiques des droits d'accès (modifications non autorisée) ainsi que la difficulté de tracer des opérations effectuées.

En outre, la confiance des utilisateurs envers l'efficacité des systèmes informatiques diminue, ce qui dégrade l'image de la GETI.

**Recommandations de l'Inspectorat:**

Nous recommandons aux unités AVS, AFac, OAIE et CENT en partenariat avec la GETI de prendre les mesures suivantes :

27. Evaluer sur la base des besoins métiers les possibilités (organisationnelles et techniques) d'intégrer les activités opérationnelles et de contrôles comptables (réalisées à ce jour manuellement par le TPI sur la base d'états de la chaîne des paiements INAR) au sein d'une solution de comptabilité auxiliaire. Dans ce cadre, il s'agit d'identifier les données comptables et de prioriser les besoins et fonctionnalités comptables jusqu'alors utilisées dans INAR et sa chaîne des paiements, afin de les désimbriquer, puis d'introduire un système dédié pour la comptabilité auxiliaire des tiers. Les résultats de l'analyse doivent mettre en lumière les besoins spécifiques non couverts ou partiellement couverts par les systèmes informatiques actuels et servir de base à l'élaboration d'un cahier des charges ayant pour cible d'homogénéiser et de simplifier le SI comptable et financier.

    Disposer d'une solution de comptabilité auxiliaire permettra au service 321 d'avoir une approche centralisée et multi-banque procurant une vision d'ensemble de tous les états de comptes et des flux de paiements. Une telle solution permettra d'éviter bon nombre de traitements aujourd'hui manuels et simplifierait les procédures tout en offrant un niveau de sécurité élevé dans le traitement et les échanges avec les partenaires financiers.

[24] Le 6 novembre 2013, l'UBS a rejeté l'ensemble du fichier des paiements des rentes car deux codes BIC étaient erronés. Pour plus de détail, veuillez vous reporter à l'observation numéro 3.3.3 du rapport.

28. A court terme, faire un recensement des listes utiles pour le secteur TPI et ne fournir que celles répondants aux besoins métiers ;

La mise en œuvre des recommandations mentionnées ci-dessus doit s'inscrire dans une approche méthodique et pragmatique en répondant aux besoins métiers et en se conformant à la stratégie des SI.

# 4 Discussion finale

Les recommandations qui figurent dans le présent rapport ont fait l'objet d'un entretien final avec [redacted] Directeur a.i. de la CdC, [redacted] cheffe de la division OAIE, [redacted] chef de la division GETI, [redacted] chef a.i. de la division CENT, [redacted] chef de la section Prestation (AFac), [redacted] cheffe a.i. de la section Processus d'affaires et support (CENT), [redacted] Responsable de la sécurité de l'information (GE-TI), en date du 18 décembre 2013.

L'Inspectorat interne remercie toutes les parties qui ont été auditées de leur collaboration.

Responsable de l'Inspectorat interne: [redacted]

Responsable de la mission: [redacted]

## Annexe 1 - Tableau des recommandations et des positions

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| 1. | Au vu de nos constats, nous recommandons à la GETI de documenter son système de contrôle interne de la sécurité de l'information et de l'intégrer au projet général du SCI de la CdC. Pour ce faire, nous recommandons à la GETI de se coordonner avec le(s) responsable(s) du SCI de l'institution, de définir les responsabilités et d'attribuer les ressources nécessaires pour l'accomplissement de cette tâche. Un des résultats attendus de cette coordination est l'intégration des contrôles nécessaires à la sécurité de l'information dans le système de contrôle des processus métiers clés, tels que le « Paiement principal des prestations AVS/AI ». | GETI | Coordination avec le(s) responsable(s) du SCI de l'institution afin de définir les responsabilités et d'attribuer les ressources nécessaires pour documenter le SCI GETI.<br><br>Le calendrier des activités spécifiques pour documenter le SCI GETI y compris pour le domaine sécurité de l'information seront déterminées après la fin de l'étape décrite ci-dessus.<br><br>La CdC dispose de l'outil MEGA qui sera être utilisé pour documenter les risques et contrôles. | 30.04.2014 | [redacted] |
| | | AVS | Les Unités AVS, AFac et OAIE ont discuté ensemble et se sont mis d'accord sur une prise de position commune.<br>Les Unités sont à disposition de la GETI. En ce qui concerne les processus métier, le groupe qualité AVS travaille depuis quelques mois à la mise en place du SCI y relatif. | | [redacted] |
| | | AFac | | | [redacted] |
| | | OAIE | | | [redacted] |
| | | CENT | Le TPI est disposé de fournir son soutien quant aux éventuels aspects relevant de la coordination. | | [redacted] |
| 2. | Définir puis mettre en œuvre un processus d'approbation des droits d'accès en regard des exigences en matière de sécurité des données de paiements des rentes. | GETI | a. L'analyse des droits d'accès va être traitée dans le cadre du projet de revue des droits d'accès actuellement en cours de réalisation par le groupe Risques et sécurité d'entreprise (RSE).<br>L'acquisition d'un outil de revue des droits d'accès tel que Brainwave est actuellement étudiée. | 31.12.2014 | [redacted] |
| | | | b. La mise en œuvre d'un processus d'approbation va être adressée par le projet PSM (Plateforme Service Management) actuellement en cours d'initialisation. | Processus d'appel d'offre OMC | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | | | | en cours. | |
| | | AVS | Les Unités AVS, AFac et OAIE ont discuté ensemble et se sont mis d'accord sur une prise de position commune. | - | [redacted] |
| | | AFac | | | [redacted] |
| | | OAIE | Les trois Unités susmentionnées ne sont pas concernées par ce point. | | [redacted] |
| | | CENT | Le TPI s'aligne sur la position de la GETI. | | [redacted] |
| 3. | Créer des profils d'accès standards qui correspondent aux rôles définis au sein de l'organisation. Dans le cas présent, il est nécessaire de connaître l'existant et donc de documenter les droits d'accès gérés par Natural Security, soit :<br>o Les groupes ;<br>o Les utilisateurs faisant partie de ces groupes et leurs autorisations (écritures, lectures, suppression) ;<br>o Les droits d'accès aux librairies et aux programmes, ainsi que la description des programmes (les opérations qu'ils permettent de faire).<br>Il sera ainsi plus aisé pour les métiers de déterminer si les principes de séparation des fonctions et de moindres privilèges sont effectivement respectés. | GETI | Se référer à la prise de position 2 a. | 31.12.2014 | [redacted] |
| | | AVS | Les Unités AVS, AFac et OAIE ont discuté ensemble et se sont mis d'accord sur une prise de position commune. | | [redacted] |
| | | AFac | | | [redacted] |
| | | OAIE | Les accès métiers à INAR sont gérés par le profil GEDO par le biais duquel les dossiers sont attribués. Toutefois, s'il s'agit des accès à la chaîne de paiements, les Unités métier ne sont pas concernées. En effet, les Unités métiers n'ont pas de droit d'accès sur les données de paiement de la CENT.<br>Les Unités métier sont en attente de la liste relative aux droits d'accès. Dès réception de ladite liste, celle-ci fera l'objet d'une analyse approfondie et d'une mise à jour. | | [redacted] |
| | | CENT | Le TPI souhaiterait obtenir une liste des droits d'accès en usage à ce jour. | | [redacted] |
| 4. | Documenter les concepts de sécurité appliqués au système Natural Security, son fonctionnement, le(s) responsable(s) de ce système, les domaines d'application, les exigences et conformités de sécurité pour la | GETI | Collecte et agrégation des informations relatives au concept de sécurité relative à la couche sécuritaire Natural Security. | 30.06.2014 | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | gestion des comptes, les accès aux fichiers et l'accès aux utilitaires systèmes. | | | | |
| 5. | Dans un premier temps, désactiver ou supprimer les comptes utilisateurs de Natural Security et de Mercure dont le propriétaire a quitté la CdC.<br><br>Dans un deuxième temps, nous recommandons la mise en œuvre d'un processus efficace de revue périodique des droits d'accès (recommandation émanant de l'audit de gestion des accès du 30 août 2011). Nous insistons sur le fait que ce processus de revue doit permettre de confirmer que les droits d'accès existants dans les systèmes sont conformes aux besoins des collaborateurs et respectent la POSIC. | GETI | Nettoyage des comptes utilisateurs relatifs à la couche sécuritaire Natural Security et du serveur Mercure. La condition préalable au nettoyage des comptes utilisateurs est l'obtention d'une liste provenant des ressources humaines. | 30.03.2014 | [redacted] |
| | | | La deuxième partie de la recommandation concernant la mise en œuvre d'un processus efficace de revue périodique des droits d'accès sera considérée dans la documentation du SCI. Se référer à la recommandation 1. | 30.04.2014 | [redacted] |
| 5. | Dans un deuxième temps, nous recommandons la mise en œuvre d'un processus efficace de revue périodique des droits d'accès (recommandation émanant de l'audit de gestion des accès du 30 août 2011). Nous insistons sur le fait que ce processus de revue doit permettre de confirmer que les droits d'accès existants dans les systèmes sont conformes aux besoins des collaborateurs et respectent la POSIC. | AVS<br>AFac<br>OAIE | Les Unités AVS, AFac et OAIE ont discuté ensemble et se sont mis d'accord sur une prise de position commune.<br>Les Unités sont à disposition de la CENT. | Voir position à la recommandation 1 | [redacted] |
| | | CENT | Le TPI est disposé de procéder à une revue périodique des droits d'accès dans la mesure où la liste y relative lui est transmise. | | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| 6. | En sus d'une revue périodique des droits d'accès utilisateurs, nous préconisons le paramétrage d'une désactivation automatique lorsque des personnes externes ou internes se voient octroyer des droits d'accès de type temporaire à INAR. | GETI | Evaluation technique d'une solution automatisée pour désactiver les comptes utilisateurs relatifs aux personnes externes ou internes ayant des droits d'accès de type temporaire à INAR. | 30.06.2014 | [redacted] |
| 7. | Les RH doivent s'assurer que toute mutation (changement de poste d'un collaborateur) ainsi que les départs des collaborateurs sont bien communiqués à la GETI. Une confirmation de la GETI doit parvenir au RH, une fois le travail effectué. | RH | Nous sommes d'accord avec la recommandation.<br>Les départs sont d'ores et déjà annoncés par la base mandat de LN. Le changement de poste d'un collaborateur n'est pour l'instant pas annoncé à la GETI. Un processus et un support informatique doit être défini en collaboration avec la GETI. | 30.9.2014 | [redacted] |
| | | GETI | Le contrôle relatif au processus de mutation / suppression sera considéré dans la documentation du SCI. Se référer à la recommandation 1.<br><br>Note : Le maintient « sain » de comptes utilisateurs sur les serveurs dépend de la communication effective et complète entre les RH et le service aux utilisateurs. | 30.04.2014 | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| 8. | Des identifiants uniques et nominatifs soient attribués aux collaborateurs qui exercent des travaux d'administration sur la base de données ou d'intégration sur les serveurs de production. Par mesures de sécurité, le compte de tests doit être supprimé de l'environnement de production. Les tests doivent se faire dans un environnement dédié. | GETI | Analyse des comptes génériques et des comptes de type test et nettoyage des comptes inutiles.<br><br>Note : L'utilisation de comptes techniques « root » et « prod » sont là pour minimiser le nombre d'acteurs et de comptes sur le serveur Mercure et veiller à limiter au strict minimum la diffusion de droits sur le Filesystem. Par ailleurs, le compte « root » est une obligation sur les systèmes Linux et ne doit pas être employé pour l'exécution ou la gestion du serveur de manière permanente. Le compte « prod » joue ce rôle. | 30.03.2014 | [redacted] |
| 9. | Les mots de passe des comptes techniques ayant des droits d'accès privilégiés ne doivent pas être communiqués entre collaborateurs. Le mot de passe du compte d'administration doit respecter les contraintes fixées par la POSIC. D'autre part, l'intervention en environnement de production par le biais d'un compte technique doit être limitée au temps de l'intervention ; les droits d'accès accordés à l'utilisateur doivent automatiquement être révoqués après les travaux. | GETI | Les comptes techniques ne sont en principe utilisés que lors d'une activité ponctuelle sur le serveur. Les mots de passe des comptes techniques ne sont connus que des exploitants du serveur. Ces mots de passe et comptes sont conservés sur une base KeyPass cryptée et n'ont accès à cette dernière que les administrateurs système de la GETI. Vérification des mots de passe des comptes techniques afin de s'assurer de l'alignement avec la POSIC. | 30.03.2014 | [redacted] |
| 10. | L'utilisation des comptes d'administration des systèmes de la base de données (de type technique) doit faire l'objet d'une surveillance permanente en environnement de production. | GETI | De la même manière que les comptes techniques sur les serveurs, les comptes d'administration des bases de données sont eux aussi enregistrés dans une base cryptée KeyPass dont l'accès est limité au service exploitation. Evaluation d'un mécanisme de surveillance en environnement de production. | 30.04.2014 | [redacted] |
| 11. | Nous recommandons qu'une procédure de gestion de la sécurité des bases de données | GETI | Collecter l'information existante relative à la gestion de la sécurité des bases de données et des serveurs. Rédaction d'une procédure dans les domaines qui | 30.09.2014 | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | et serveurs soit documentée et qu'elle couvre notamment les aspects suivants :<br>• Gestion des mots de passe ;<br>• Gestion des comptes et profils – par exemple les comptes d'exploitation, d'administration et de sécurité ;<br>• Ségrégation des environnements et accès aux bases de données (environnement de développement, d'assurance qualité et de production) ;<br>• Stockage des mots de passe ;<br>• Gestion des scripts d'exploitation ;<br>• Gestion des protocoles de communication (seule l'utilisation du SSH (protocole ver-sion 2)) devrait être autorisé pour la connexion avec les serveurs; Les transferts en-tre serveurs ainsi qu'entre serveurs et clients doivent se faire par le biais un protocole sécurisé, par exemple sftp ;<br>• La communication des paramètres de connexion. | | seront considérés comme importants après la collecte d'information. | | |
| 12. | Les connexions des utilisateurs au serveur Mercure s'établissent par le biais d'un protocole sécurisé. | GETI | Evaluation technique afin de trouver une solution pour sécuriser le serveur Mercure. | 30.09.2014 | [redacted] |
| 13. | Tous les traitements des purges des fichiers de paiements sur les serveurs soient sous alertes. Il en va de même des contrôles de réception de fichiers à double. | GETI | Analyse des fichiers et de leurs utilisations afin d'évaluer leurs utilisations des besoins. | 31.12.2014 | [redacted] |
| | | CENT | Ce point relève de la sécurité informatique. De ce fait, le TPI attend la transmission du mandat en vue de le valider si nécessaire et se tient à disposition pour d'éventuelles questions. | A convenir (GETI) | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | | | | | |
| 14. | La politique de mot de passe sur le serveur Edifact soit activée, et ce en conformité avec la POSIC. | GETI | La consolidation des serveurs Mercure et Edifact sera effective durant le premier trimestre 2014. Ce point devient caduque. | 31.12.2014 | [redacted] |
| 15. | Les logs systèmes sont conservés suffisamment de temps dans le cas où ils devraient être exploités, par exemple lors d'une enquête liée à un incident de sécurité. La conservation des logs devant elle-même suivre une politique de conservation des données. | GETI | Evaluation des besoins de traçabilité des logs systèmes du serveur Edifact. Estimation de la faisabilité technique et évaluation de l'impact sur l'utilisation ressource du système. | 30.06.2014 | [redacted] |
| 16. | Le contrat Edifact passé avec le prestataire de service Compudata prenne en compte les exigences de sécurité en conformité avec la POSIC. | GETI | Revue détaillée de notre relation contractuelle avec Compudata initiée en 2013. Lors de la rédaction de la nouvelle mouture du contrat, les exigences de la POSIC seront prises en compte. | 30.06.2014 | [redacted] |
| 17. | Mise en place d'un environnement de test pour les serveurs de communication. | GETI | La mise en place d'un environnement de test complet est à évaluer et à valider avec le client en considérant l'aspect coût et délai.<br><br>Note : UBS ne met pas à disposition un environnement de test. | Point de situation lors de la prochaine commission INAR, le 4.03.2014 | [redacted] |
| 18. | Formalisation de la procédure de gestion des clés de chiffrement. | GETI | Evaluation du travail nécessaire pour la réalisation avec le soutien de l'équipe qualité et sécurité. | 30.09.2014 | [redacted] |
| 19. | Mise en place d'un contrôle d'intégrité des fichiers de paiements depuis leur génération jusqu'à leur acheminement. | GETI | Evaluation du travail nécessaire pour la réalisation avec le soutien de l'équipe exploitation. | 31.12.2014 | [redacted] |
| | | CENT | Ce point relève de la sécurité informatique. De ce fait, le TPI attend la transmission du mandat en vue de le valider si nécessaire et se tient à disposition | A convenir (GETI) | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | | | pour d'éventuelles questions. | | |
| 20. | Soumission à l'OFIT du besoin de sécuriser la connexion réseaux acheminant en sortie du mainframe les fichiers de paiements vers les serveurs de communication gérés par la GETI. | GETI | Il s'agit ici d'un contrôle technique dont la mise en place devrait être réalisée par l'OFIT. Le besoins doit être exprimé conjointement par la GETI et la CSC. | 30.06.2014 | [redacted] |
| 21. | Nous sommes d'avis que des tests d'intrusions sur l'infrastructure IT doivent être réalisés, dans le but d'identifier d'éventuelles vulnérabilités réseaux. | GETI | L'OFIT est notre prestataire de service d'infrastructure IT. Pour la partie de notre infrastructure IT gérée par Berne, les tests d'intrusions sont effectués par l'unité Governance de l'OFIT. Une collaboration avec l'unité Governance de l'OFIT a été initiée afin que le groupe RSE effectue également des tests d'intrusions sur l'infrastructure IT gérée par la CdC. Une planification des missions après avoir clarifié les rôles et responsabilités des deux parties prenante sera préparée. | 30.04.2014 | [redacted] |
| 22. | Documenter les procédures de sauvegarde et les procédures de restauration, en conformité avec les exigences métiers, légales et de sécurité. La politique de durée de rétention des fichiers de paiements doit être documentée et harmonisée. | GETI | Une refonte de la documentation sur la sauvegarde et la restauration des données sera menée suite à la mise en production de Mercure2; après avoir de part et d'autre établi des règles sur la conservation des données et leur support de conservation et peut être une externalisation de celles-ci. | 30.09.2014 | [redacted] |
| 23. | S'assurer que les infrastructures soient dédoublées et/ou que des procédures et contrôle correctifs répondant aux risques encourus soient en place, afin d'assurer la | GETI | Lorsque le serveur Mercure2 ( virtuel) sera mis en production, l'infrastructure de virtualisation et la sauvegarde associée permettront de relever le niveau de sécurité de ce serveur et sa haute disponibilité. Un cluster de 12 machines ESX permettra une redondance en cas de problème hardware. | 30.06.2014 | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | continuité des opérations de la chaîne des paiements en cas d'indisponibilité de l'un de ses composants. Ces contrôles doivent être mis en place dans le cadre du plan de secours informatique (PSI) et du plan de continuité d'activité (PCA). | | Un dédoublement des salles serveurs, dont une salle serait hébergée en dehors du bâtiment de la CDC permettrait d'autant plus la sécurisation de l'infrastructure terminale de la chaîne des paiements. Les projets DRP et BCM sont en cours et adresseront les points concernant le PSI et PCA. | 30.06.2015 appel d'offre OMC en cours | [redacted] |
| | | OAIE<br>AF | *Sans position de la part de l'audité* | - | - |
| 24. | Nous recommandons que tous les incidents de la chaîne des paiements soient systématiquement enregistrés, classifiés, priorisés, et communiqués (procédure d'escalade d'un incident) à qui de droit (avec copie à la Direction et à l'Inspectorat) selon une procédure documentée. Le responsable de la sécurité du SI doit immédiatement être alerté lorsqu'un incident de sécurité survient, afin que les mesures corrective nécessaires soient mises en place en conformité à la POSIC. | GETI | La procédure actuelle de gestion des événements et incidents sera présentée au métier lors de la prochaine commission INAR. La priorisation des incidents et événements actuellement utilisée dans la chaîne des paiements sera également présentée. Des éventuels ajustements seront à évaluer. | 04.03.2014 | [redacted] |
| | | CENT | Un processus d'escalation métier est en cours de finalisation. Le processus sera présenté à la GETI en vue de définir les interfaces et de délimiter les responsabilités. Le processus d'escalation convenu en 2009, s'est avéré inefficace. Le TPI insiste sur la nécessité d'une collaboration constructive afin d'assurer la communication systématique des incidents techniques. | 30.04.2014 | [redacted] |
| 25. | Nous recommandons également la mise en place d'une procédure documentée de sécurité lorsque la GETI intervient en urgence sur les fichiers de données de paiements. Cette procédure d'urgence doit contenir : le mode opératoire pour l'annonce de l'incident auprès des parties concernée et responsables des données – ouverture du ticket d'incident, l'accord du responsable des données pour intervention sur les fichiers de paiements, les modalités de sécurité appliquées, le canal de | GETI | Voir position à la recommandation 24 | Voir position à la recommandation 24 | Voir position à la recommandation 24 |
| | | OAIE | L'OAIE n' pas de remarques particulières et s'associe à la prise de position de l'AVS et de l'Afac. | - | - |
| | | CENT | Le TPI est disposé à fournir son soutien, dans la mesure où les ressources nécessaires auront été engagées, quant aux éventuels aspects relevant de la coordination. | Dès octobre 2014 - à convenir (GETI) | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | communication utilisé, les collaborateurs de la GETI habilités à intervenir sur les fichiers de paiements, le contrôle quant à l'intégrité des fichiers corrigés (si correction il y a), les responsabilités des parties impliquées (du côté de la GETI, du métier et de l'institution financière). | | | | |
| 26. | Nous recommandons qu'un contrôle de plausibilité sur les paiements BIC soit réalisée afin de notamment éviter tout incident lors de l'exécution de la chaîne des paiements. | GETI | Evaluation de ces développements notamment dans le cadre du périmètre des projets FSPC (étude) et la refonte des adresses. | A prioriser en commission informatique | [redacted] |
| | | AVS | Les Unités AVS et OAIE ont discuté ensemble et se sont mis d'accord sur une prise de position commune.<br>Les plausibilités existantes de saisie sont gérées par GEDO. Dans le projet de refonte des adresses, il faudra prévoir également des plausibilités de saisie des adresses. Toutefois, les plausibilités sur les paiements ne concerne pas nos Unités.<br>Une séance de la Commission informatique aura lieu le 11 février 2014 pendant laquelle il est prévu de discuter et de prendre une décision relative au portefeuille des projets. Par conséquent, la planification de la mise en œuvre ne pourra se faire qu'après ladite séance. | 11 février 2014 | [redacted] |
| | | OAIE | | | [redacted] |
| 27. | Evaluer sur la base des besoins métiers les possibilités (organisationnelles et techniques) d'intégrer les activités opérationnelles et de contrôles comptables (réalisées à ce jour manuellement par le TPI sur la base d'états de la chaîne des paiements INAR) au sein d'une solution de comptabilité auxiliaire. Dans ce cadre, il s'agit d'identifier les données comptables et de prioriser les besoins | GETI | Evaluation de ces développements dans le cadre du périmètre du projet FSPC (étude). | A prioriser en commission informatique | [redacted] |
| | | CENT | En ce qui concerne le projet FSPC, la première étape semble correspondre à l'ISO 20022. Il serait pertinent de restreindre le périmètre dudit projet au format de paiement ISO 20022, et dans un deuxième temps, à l'outil d'analyse relatif aux paiements effectués, tel qu'il a déjà été développé par M. Minck et que la GETI a repris. | A convenir (GETI) | [redacted] |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | et fonctionnalités comptables jusqu'alors utilisées dans INAR et sa chaîne des paiements, afin de les désimbriquer, puis d'introduire un système dédié pour la comptabilité auxiliaire des tiers. Les résultats de l'analyse doivent mettre en lumière les besoins spécifiques non couverts ou partiellement couverts par les systèmes informatiques actuels et servir de base à l'élaboration d'un cahier des charges ayant pour cible d'homogénéiser et de simplifier le SI comptable et financier.<br><br>Disposer d'une solution de comptabilité auxiliaire permettra au service 321 d'avoir une approche centralisée et multi-banque procurant une vision d'ensemble de tous les états de comptes et des flux de paiements. Une telle solution permettra d'éviter bon nombre de traitements aujourd'hui manuels et simplifierait les procédures tout en offrant un niveau de sécurité élevé dans le traitement et les échanges avec les partenaires financiers. | | Les étapes prévues par le TPI afin de procéder aux analyses métier sont les suivantes :<br><br>1. Validation du nouveau descriptif de poste par les RH et l'OFPER en vue de recruter un candidat ayant les compétences nécessaires.<br>2. Recrutement du collaborateur.<br>3. Formation du collaborateur.<br>4. Définition des interfaces et des responsabilités entre la GETI et le TPI.<br>5. Lancement des analyses métier : identifications des données, identification de la source des données, identification des possibilités d'extractions etc. | Février 2014 (dépendance RH)<br>Mars 2014<br><br>Octobre 2014<br><br>A convenir avec la GETI (décembre 2014)<br>Janvier 2015 | [redacted] |
| | | AVS<br>AFac<br>OAIE | Les Unités AVS, AFac et OAIE ont discuté ensemble et se sont mis d'accord sur une prise de position commune.<br>Les trois Unités métier sont à disposition de la GETI. | - | [redacted] |
| 28. | A court terme, faire un recensement des listes utiles pour le secteur TPI et ne fournir que celles répondants aux besoins métiers ; La mise en œuvre des recommandations mentionnées ci-dessus doit s'inscrire dans une approche méthodique et pragmatique en | GETI | Un mandat relatif aux corrections et modifications des listes nécessaires a été évalué dans le passé. Ce mandat à été abandonné par la CENT. | - | [redacted] |
| | | CENT | La prise en charge de cette recommandation à court terme semble difficile vu le manque de ressources.<br><br>Les étapes prévues par le TPI afin de procéder à un recensement des listes | | |

| N° | Recommandation | Unité concernée | Position de l'audité | Délai de mise en œuvre proposé par l'audité | Responsable de la mise en œuvre |
|---|---|---|---|---|---|
| | répondant aux besoins métiers et en se conformant à la stratégie des SI. | | utiles sont les suivantes:<br>1. Validation du nouveau descriptif de poste par les RH et l'OFPER en vue de recruter un candidat ayant les compétences nécessaires.<br>2. Recrutement du collaborateur.<br>3. Formation du collaborateur.<br>4. Lancement du recensement des listes utiles pour le secteur TPI. | Février 2014 (dépendance RH)<br>Mars 2014<br>Octobre 2014<br>Décembre 2014 | [redacted] |