EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Audit de l'application d'aide au calcul et à l'octroi des rentes ACOR

Centrale de compensation

CDF-17495 | Prises de position incluses | 8 octobre 2018 | DélFin D1/2019

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Contrôle fédéral des finances (CDF) Monbijoustrasse 45 3003 Berne Suisse
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.17495.602.00191
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Table des matières

Audit de l'application d'aide au calcul et à l'octroi des rentes ACOR

Centrale de compensation

L'essentiel en bref

L'application d'aide au calcul et à l'octroi de rentes (ACOR) est un développement informatique de la Centrale de compensation (CdC). Elle aide les gestionnaires de la Caisse suisse de compensation (CSC) et des caisses cantonales et professionnelles à déterminer le droit d'un assuré à une rente et son montant. En 2017, plus de 136 000 nouvelles rentes de l'assurance-vieillesse et survivants (AVS) ont été octroyées.

La CdC joue ainsi un rôle de prestataire de services auprès des organes d'exécution du 1er pilier. Elle peut être amenée à fournir une assurance quant à la fiabilité de ses prestations. Dès lors, le Contrôle fédéral des finances (CDF) a évalué les contrôles informatiques généraux de l'application ACOR. Il a aussi examiné la capacité de l'environnement à former une base solide pour les développements futurs. Enfin, il a effectué le suivi d'une recommandation d'un précédent audit informatique (mise en place d'accords décrivant les niveaux de service des systèmes d'information (SI) de la CdC envers ses partenaires institutionnels).

Gestion des changements : une efficacité des contrôles à renforcer

Pour le CDF, la CdC a mis en place des outils et un processus de gestion des changements selon ses directives internes. Chaque modification dans ACOR est soumise à des tests pour assurer qu'elle n'impacte pas négativement le système (tests de non régression).

Néanmoins, le CDF ne peut garantir que tous les changements passés en production ont été demandés, testés et validés selon le principe des quatre yeux. Grâce aux tests de non régression systématiques, le risque lié à des fautes de calculs ou à des dysfonctionnements d'ACOR est certes limité. Il est toutefois essentiel de renforcer l'efficacité des contrôles de la gestion des changements pour assurer la traçabilité des événements et la séparation des tâches.

Une gestion des accès appropriée, une base adéquate pour des développements futurs

Les droits d'accès sont gérés pour les développeurs de l'application ACOR, mais pas pour les utilisateurs finaux. Le risque lié à l'absence de gestion des droits de ces utilisateurs reste faible en raison de l'installation locale et au mode d'utilisation (pas de modification de données possibles).

L'accès au code source est donné aux seuls développeurs du groupe ACOR et aux administrateurs de l'Office fédéral de l'informatique et de la télécommunication. Le CDF n'a pas observé d'exception à ce principe. Il n'a pas découvert de défaut majeur dans l'organisation et les processus de l'exploitation de l'application ACOR.

Le CDF estime que la plateforme ACOR constitue une base globalement adéquate pour les développements futurs de l'application. Dans l'optique de la nouvelle version, il encourage

la CdC à évaluer soigneusement les défis posés par la nouvelle architecture – sécurité, disponibilité, acquisition de nouvelles compétences. Il pousse aussi l'équipe ACOR à repenser les processus d'exploitation et les activités de contrôle en fonction de la future application.

Une recommandation pas encore entièrement mise en œuvre

Le CDF constate que les accords décrivant les niveaux de service des SI envers les partenaires institutionnels externes ne sont pas mis en place. Des principes de mise en œuvre sont toutefois définis et globalement appropriés. La CdC doit finaliser la définition de la forme des accords décrivant les niveaux de service et les mettre en œuvre rapidement.

Prüfung der Anwendung ACOR zur Rentenberechnung und -festsetzung

Zentrale Ausgleichsstelle

Das Wesentliche in Kürze

Die Anwendung zur Rentenberechnung und -festsetzung ACOR ist eine IT-Entwicklung der Zentralen Ausgleichsstelle (ZAS). Sie unterstützt die Sachbearbeiterinnen und Sachbearbeiter der Schweizerischen Ausgleichskasse (SAK) sowie der kantonalen und der Verbandsausgleichskassen bei der Ermittlung der Anspruchsberechtigung der Versicherten und bei der Rentenberechnung. 2017 wurden über 136 000 neue Renten der Alters- und Hinterlassenenversicherung (AHV) ausgerichtet.

Die ZAS spielt somit für die Vollzugsorgane der 1. Säule die Rolle eines Dienstleisters. Sie kann dazu aufgefordert werden, die Zuverlässigkeit ihrer Leistungen zu garantieren. Die Eidgenössische Finanzkontrolle (EFK) hat deshalb die allgemeinen Informatikkontrollen der Anwendung ACOR evaluiert. Ausserdem untersuchte sie, ob die Kapazität der Informatikumgebung eine solide Basis für zukünftige Entwicklungen bietet. Schliesslich überprüfte sie, ob eine im Rahmen einer früheren Informatikprüfung abgegebene Empfehlung unterdessen umgesetzt wurde (Abschluss von Service Level Agreements zwischen der Abteilung Informatiksysteme (IS) der ZAS und ihren institutionellen Partnern).

Änderungsmanagement: Die Wirksamkeit der Kontrollen muss verstärkt werden

Nach Ansicht der EFK hat die ZAS nach Massgabe ihrer internen Weisungen Tools sowie einen Änderungsmanagement-Prozess errichtet. Alle Änderungen in ACOR werden Tests unterzogen, um sicherzustellen, dass sie sich nicht negativ auf das System auswirken (Regressionstests).

Dennoch kann die EFK nicht gewährleisten, dass alle in Betrieb genommenen Änderungen nach dem Vier-Augen-Prinzip beantragt, getestet und validiert wurden. Es ist der systematischen Durchführung von Regressionstets zu verdanken, dass nur ein begrenztes Risiko von Berechnungsfehlern oder Störungen von ACOR besteht. Allerdings ist es sehr wichtig, die Wirksamkeit der Kontrollen des Änderungsmanagements zu verstärken, um die Nachverfolgbarkeit der Vorfälle und die Aufgabenteilung sicherzustellen.

Eine sachgerechte Zugangsverwaltung und eine für zukünftige Entwicklungen zweckdienliche Basis

Die Zugangsrechte der Applikationsentwickler von ACOR werden verwaltet, nicht aber diejenigen der Endnutzer. Da es sich jedoch um eine lokale Installation handelt, bei deren Verwendung keine Möglichkeit zur Änderung der Daten besteht, stellt das Fehlen einer Verwaltung der Zugangsrechte der Endnutzer nur ein geringes Risiko dar.

Zugang zum Quellcode haben ausschliesslich die Entwickler der Gruppe ACOR und die Administratoren des Bundesamtes für Informatik und Telekommunikation. Die EFK hat keine Abweichungen von diesem Grundsatz beobachtet, und auch in der Organisation und den Betriebsabläufen der Anwendung ACOR keine wesentlichen Mängel festgestellt.

Nach Meinung der EFK bietet die Plattform ACOR eine insgesamt zweckdienliche Basis für die zukünftigen Entwicklungen der Anwendung. Sie ermuntert die ZAS, sich im Hinblick auf die neue Version eingehend mit den Herausforderungen der neuen Architektur – Sicherheit, Verfügbarkeit, Erwerb neuer Kompetenzen – auseinanderzusetzen. Ausserdem ermutigt sie das ACOR-Team, die Betriebsprozesse und die Kontrolltätigkeiten anhand der neuen Anwendung zu überdenken.

Eine noch nicht vollständig umgesetzte Empfehlung

Die EFK stellt fest, dass die Leistungsvereinbarungen zwischen der Abteilung IS und ihren externen institutionellen Partnern nicht umgesetzt sind. Insgesamt sind jedoch zweckmässige Umsetzungsprinzipien definiert worden. Die ZAS muss nun die Definition der Form der Leistungsvereinbarungen zum Abschluss bringen und sie rasch umsetzen.

Originaltext auf Französisch

Verifica del programma di aiuto al calcolo e all'assegnazione delle rendite ACOR

Ufficio centrale di compensazione

L'essenziale in breve

Il programma di aiuto al calcolo e all'assegnazione delle rendite (ACOR) è stato sviluppato dall'Ufficio centrale di compensazione (UCC). Il programma fornisce un valido aiuto ai gestori della Cassa svizzera di compensazione (CSC) e delle casse cantonali e professionali nel determinare il diritto di un assicurato a una rendita e l'ammontare della stessa. Nel 2017 sono state assegnate oltre 136 000 nuove rendite dell'Assicurazione per la vecchiaia e per i superstiti (AVS).

L'UCC funge pertanto da fornitore di servizi per gli organi d'esecuzione del 1° pilastro e può essere chiamato a garantire l'affidabilità delle sue prestazioni. Per questo motivo, il Controllo federale delle finanze (CDF) ha esaminato i sistemi di controllo informatici generali del programma ACOR e la propensione dell'ambiente a formare una base solida per gli sviluppi futuri. Infine, ha verificato e seguito una raccomandazione di una verifica informatica precedente per la creazione di accordi che specifichino i livelli di servizio dei sistemi d'informazione (SI) dell'UCC nei confronti dei suoi partner istituzionali.

Gestione dei cambiamenti: rafforzare l'efficacia dei controlli

Secondo il CDF, gli strumenti e il processo di gestione dei cambiamenti adottati dall'UCC sono conformi alle direttive interne. Tutte le modifiche all'interno del programma ACOR sono sottoposte a verifica per accertare che non danneggino il sistema (test di non regressione).

Tuttavia, il CDF non può garantire che tutti i cambiamenti apportati durante la produzione siano stati richiesti, testati e convalidati secondo il principio dei quattro occhi. I test di non regressione sistematici permettono di limitare i rischi legati agli errori di calcolo o ai malfunzionamenti del programma ACOR. È comunque necessario rafforzare l'efficacia dei controlli di gestione dei cambiamenti per garantire la tracciabilità degli eventi e la separazione dei compiti.

Una gestione appropriata degli accessi e una base adeguata per gli sviluppi futuri

La gestione dei diritti di accesso concerne gli sviluppatori del programma ACOR, ma non gli utenti finali. Grazie all'installazione in locale e all'impiego che non consente di modificare i dati è comunque possibile limitare i rischi legati a questa mancanza.

Solo gli sviluppatori del gruppo ACOR e gli amministratori dell'Ufficio federale dell'informatica e della telecomunicazione hanno accesso al codice sorgente. Il CDF non ha constatato eccezioni a questo principio e non ha riscontrato gravi mancanze nell'organizzazione e nei processi di gestione del programma ACOR.

Il CDF considera la piattaforma ACOR una base complessivamente adeguata per gli sviluppi futuri del programma. In prospettiva di una nuova versione, il CDF incoraggia l'UCC ad analizzare accuratamente le sfide poste dalla nuova architettura dal punto di vista della sicurezza, della disponibilità e dell'acquisizione di nuove competenze, e sprona il gruppo ACOR a riconsiderare i processi di gestione e le attività di controllo in funzione del programma futuro.

Una raccomandazione attuata solo parzialmente

Il CDF ha constatato che gli accordi che specificano i livelli di servizio dei SI nei confronti dei partner istituzionali esterni non sono ancora stati attuati. Tuttavia, i principi per l'attuazione sono stati definiti e giudicati complessivamente appropriati. L'UCC deve portare a termine la definizione di tali accordi e concretizzarli rapidamente.

Testo originale in francese

Audit of the application for assisting with the calculation and granting of pensions ACOR

Central Compensation Office

Key facts

The application for assisting with the calculation and granting of pensions (ACOR) is an IT product developed by the Central Compensation Office (CCO). It helps the managers of the Swiss Compensation Office (SCO) and the cantonal and occupational funds to determine an insured person's entitlement to a pension and its amount. In 2017, more than 136,000 new old-age and survivors' insurance (AHV) pensions were granted.

The CCO thus plays a role as service provider for the first pillar implementing bodies. It can be required to provide assurances as to the reliability of its services. Consequently, the Swiss Federal Audit Office (SFAO) assessed the general IT controls of the application ACOR. It also examined the environment's capacity to form a sound basis for future developments. Finally, it followed up on a recommendation from an earlier IT audit (establishment of agreements describing the service levels of the CCO's information systems (IS) vis-à-vis its institutional partners).

Change management: control effectiveness to be strengthened

For the SFAO, the CCO has established tools and a change management process in accordance with its internal guidelines. Each ACOR modification is tested to ensure that it does not adversely affect the system (regression testing).

Nevertheless, the SFAO cannot guarantee that all past changes in production were requested, tested and validated according to the four eyes principle. Although the risk of ACOR malfunctions or miscalculations is limited thanks to systematic regression testing, it is essential to strengthen the effectiveness of change management controls to ensure the traceability of events and task segregation.

Appropriate access management; an adequate basis for future developments

Access rights are managed for ACOR application developers, but not for end users. The risk associated with having no management of these users' rights remains low due to the local installation and the method of use (no data modification possible).

Access to the source code is granted only to ACOR group developers and to administrators of the Federal Office of Information Technology, Systems and Telecommunication. The SFAO found no exceptions to this principle. It did not discover any major defects in the organisation and operating processes of the application ACOR.

The SFAO believes that the ACOR platform provides a generally adequate basis for future developments of the application. In terms of the new version, it encourages the CCO to carefully assess the challenges posed by the new architecture – security, availability, acquisition of new skills. It also urges the ACOR team to rethink the operating processes and control activities according to the future application.

A recommendation not yet fully implemented

The SFAO found that the agreements describing IS service levels for external institutional partners have not been established. Nonetheless, implementation principles are defined and generally appropriate. The CCO has to finalise the definition of the form of the agreements describing the service levels and implement them quickly.

Original text in German

Prise de position générale de la CdC

La CDC tient à souligner l'esprit positif dans lequel l'audit c'est déroulé et accepte la recommandation 1 ainsi que les appréciations qui permettront d'améliorer les contrôles informatiques généraux de l'application ACOR.

Concernant une ancienne recommandation de l'audit 15381 de février 2016 qui a été reprise sous forme de recommandation dans le chapitre 2.5 la CDC tient à donner les informations suivantes :

- Les conditions générales d'utilisation des logiciels et applications mis à disposition des organes d'exécution du premier pilier ont été approuvées et validées par le directeur de la CDC le premier septembre 2018.
- Ces CG ont été traduites en allemands et sont (version FR et DE) mise à disposition sur le site internet de la CDC dès mi-septembre 2018, une version italienne est en cours de traduction.
- Une information active de la part de la CDC sera entreprise (dès la version italienne disponible) en informant les directeurs de la conférence des caisses cantonales de compensation resp. l'association suisse des caisses de compensation professionnelles, l'association des offices AI ainsi que l'association eAVS/AI par un courrier. L'OFAS sera mis en copie des 4 courriers pour information.
- Ces actions permettront au CdF de clore la recommandation numéro 1 de l'audit 15381 de février 2016.

1 Mission et déroulement

1.1 Contexte

L'application d'aide au calcul et à l'octroi de rentes (ACOR) est un développement spécifique de la Centrale de compensation (CdC). Elle fonctionne comme une feuille de calcul aidant à déterminer le droit d'un assuré à une rente et son montant. Les gestionnaires de la Caisse suisse de compensation (CSC) s'en servent depuis 1996 pour calculer les rentes des assurés résidant hors de Suisse. ACOR est aussi utilisée sur base volontaire par les gestionnaires de l'assurance vieillesse et survivants (AVS) des 96 caisses cantonales et professionnelles. En 2017, près de 136 300 nouvelles rentes ont été octroyées, autant de rentes que l'application contribue à calculer.

La législation en matière de prévoyance vieillesse est complexe. Les règles de calcul et d'octroi doivent répondre à des situations qui ne le sont pas moins. Divers paramètres – situation personnelle et familiale, moment de la prise de la retraite, versement d'autres rentes, cotisations, etc. – sont pris en compte dans les calculs. L'application est intégrée à d'autres applications de la CdC, de la CSC et des caisses cantonales et professionnelles. Des mécanismes d'échange de données permettent l'import de ces informations en vue du calcul.

L'avenir de la prévoyance vieillesse continue de susciter le débat. Le peuple a refusé le 24 septembre 2017 la réforme de la Prévoyance vieillesse 2020. Le projet de mise à jour d'ACOR, qui avait été lancé en prévision des modifications induites par la réforme, a en toute logique été arrêté.

En mettant le logiciel ACOR à disposition des organes d'exécution du 1er pilier, la CDC joue un rôle de prestataire de services. En tant que tel, elle peut être amenée à fournir une assurance quant à la fiabilité de ses prestations. Elle a mandaté une entreprise de conseil afin de l'accompagner dans une démarche visant à l'obtention d'une attestation ISAE 3402[1]. Les travaux étaient en cours au moment de l'audit du CDF.

1.2 Objectif et questions d'audit

Dans son périmètre initial, l'audit visait principalement la mise en œuvre des modifications en relation avec la réforme. Avec l'échec de la réforme, l'objectif d'audit a été adapté et l'examen du projet de mise à jour d'ACOR a été abandonné. La révision se concentre sur l'état de l'environnement de contrôle de l'application ACOR, notamment les contrôles informatiques généraux (gestion des changement, exploitation, droits d'accès). Il s'agit aussi de s'assurer que l'environnement de l'application ACOR constitue une base solide pour les développements futurs. Enfin, la mise en œuvre d'une recommandation d'un audit antérieur est contrôlée.

[1] L'ISAE 3402 est une norme d'audit permettant aux utilisateurs de prestations externalisées d'obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de services. Il se concentre sur les contrôles informatiques généraux. ISAE 3402 implique un audit du système de contrôle interne, mais ne constitue pas une certification, ni du processus, ni de l'application.

Les questions d'audit suivantes sont traitées :

1. Les conditions sont-elles réunies pour une exploitation stable de l'application ACOR ?
2. L'application ACOR constitue-t-elle une base solide pour les développements futurs ?
3. La recommandation 15381.001 est-elle mise en œuvre (Audit informatique de la CdC : mise en place d'accords décrivant le niveau de service envers les bénéficiaires de prestations institutionnels externes) ?

1.3 Etendue de l'audit et principe

L'audit a été mené du 12 au 27 juillet 2018 par André Stauffer (responsable de révision) et Emmanuel Hofmann. Il a été conduit sous la responsabilité de Bernhard Hamberger. La discussion des résultats a eu lieu le 2 août 2018. Le présent rapport ne prend pas en compte les développements après cette discussion.

1.4 Documentation et entretiens

Les spécialistes de la CdC et de la CSC ont fourni les informations nécessaires au CDF de manière exhaustive et compétente. Les documents (ainsi que l'infrastructure) requis ont été mis à disposition de l'équipe d'audit sans restriction.

1.5 Discussion finale

La discussion finale a eu lieu le 18 septembre 2018. Les participants étaient:

- Le directeur de la CdC
- Le chef de division des systèmes d'information, CdC
- Un responsable de centre de compétences, CDF
- Le responsable de révision, CDF

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux directions d'office, respectivement aux secrétariats généraux, de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 Un environnement de contrôle et une application en évolution

Un environnement de contrôle efficace forme la base du bon fonctionnement d'une application. Les contrôles généraux comprennent les contrôles de l'infrastructure informatique, comme la gestion des opérations, la sécurité des accès et la gestion des changements.

2.1 Gestion des changements : une efficacité des contrôles à renforcer

Le CDF confirme que la CdC a mis en place un processus de gestion des changements conformément aux directives internes. Une matrice des contrôles IT existe (Système de contrôle interne, SCI). Selon les directives, chaque demande de changement doit être traitée via l'outil de suivi des tickets et des projets (JIRA), quelle que soit l'origine de la requête (commission ACOR, modification légale, incidents ou maintenance). Une demande comporte différentes étapes (requête, validation, test, etc.).

Les modifications sont réalisées dans un environnement de développement. Le CDF constate que chaque modification est sujette à une validation technique obligatoire. Quelque 2086 cas métiers éprouvés sont ainsi testés pour assurer que les modifications n'impactent pas négativement le système (non régression). En cas d'échec de la validation, les changements ne peuvent être importés dans l'environnement de production. Les nouvelles règles en cours de développement ne sont par contre pas contenues dans cette palette de cas de tests de non régression.

Le CDF confirme que le processus de gestion des changements est effectué dans JIRA. Partant de la forme actuelle du processus, le CDF n'est cependant pas en mesure de retracer les événements ayant conduit aux changements. Les liens manquent pour naviguer de la demande de base jusqu'à la mise en production via la version de l'application dans l'outil de gestion des versions SVN. Par ailleurs, un même développeur peut dérouler l'entier du processus de développement sans contrôle par une tierce personne (séparation des tâches). Ceci lui permet en théorie de développer et de mettre en production des changements non désirés, non approuvés ou non testés, pour une nouvelle règle par exemple (les règles existantes continuent de faire l'objet de tests de non régression).

Appréciation

Une politique de gestion des changements a pour but de s'assurer que seules les modifications nécessaires, testées et validées sont transportées dans l'environnement de production. Elle contribue ainsi à limiter les risques d'erreur de calcul ou de dysfonctionnement lors d'une modification. La thématique du calcul des rentes est très sensible. Le CDF estime qu'il est primordial de pouvoir démontrer que le processus de gestion des changements de l'application ACOR est suivi et contrôlé.

Le CDF ne peut donner l'assurance que tous les changements effectués en production ont été demandés, validés et testés. Il estime cependant que le risque lié à des fautes de calculs ou à des dysfonctionnements de ACOR est limité. Les tests de non régression systématiques avant toute mise en production assurent que les règles existantes (mais non pas futures) continuent de fonctionner correctement.

Le CDF estime toutefois nécessaire de renforcer l'efficacité des contrôles de la gestion des changements pour assurer la traçabilité des événements et la séparation des tâches.

Recommandation 1 (Priorité 2)

Le CDF recommande à la Centrale de compensation d'améliorer les contrôles assurant la traçabilité des étapes et la séparation des tâches dans le processus de gestion des changements apportés à la solution ACOR. Pour les règles nouvellement mises en place, celui-ci contiendra une référence aux résultats des tests.

Prise de position de la Centrale de compensation

La CdC accepte cette recommandation.

2.2 Une gestion des droits d'accès globalement adéquate

Pour les utilisateurs finaux, la notion de droits d'accès n'est pas directement applicable dans ACOR. L'application est déployée sur les postes de travail des utilisateurs, il n'existe pas de gestion d'utilisateurs finaux et de droits. L'utilisation ne prévoit en outre pas de modifications de données (ajout, suppression, modifications, extractions en masse, etc.).

Pour les accès des développeurs, le CDF constate que seuls les collaborateurs autorisés ont accès en écriture au répertoire contenant le code source. Il note qu'aucune revue périodique n'est effectuée pour assurer que seuls les collaborateurs actifs du groupe ACOR ont accès au code source.

Appréciation

Eu égard à l'installation locale et au mode d'utilisation de l'application, le CDF ne considère pas qu'un risque découle de l'absence de gestion des droits des utilisateurs finaux.

L'accès au code source est donné uniquement aux développeurs du groupe ACOR conformément aux attentes. Hormis les comptes des administrateurs de l'OFIT, le CDF n'a pas constaté d'exception. Il estime toutefois qu'une revue périodique de la liste des développeurs autorisés doit être envisagée conformément aux bonnes pratiques en matière de gestion des accès privilégiés.

2.3 Des opérations informatiques sous contrôle

Une partie de l'infrastructure informatique de la CdC est hébergée à l'OFIT, l'autre partie sous sa propre responsabilité à Genève. La CdC est au bénéfice d'un règlement d'exception pour être active en tant que fournisseur de prestations internes[2].

Un concept décrit les activités, les responsabilités et les détails des sauvegardes, à Berne et à Genève. Pour les composantes d'ACOR hébergées à Berne, des accords de niveau de service existent avec l'OFIT. Selon ces accords, des sauvegardes journalières incrémentales et hebdomadaires et mensuelles complètes sont assurées. Pour l'infrastructure à Genève, les serveurs sont sauvegardés quotidiennement. Une feuille de contrôle rend compte au quotidien du résultat des sauvegardes et mentionne les éventuelles situations d'exception.

[2] Article 23 Al.1 de l'Ordonnance sur l'informatique et la télécommunication dans l'administration fédérale (OIAF)

Les reconstructions sont testées trimestriellement, les serveurs sont « remontés » individuellement. La définition d'un plan de reprise d'activités (Disaster Recovery Plan, DRP) est en cours. Un plan actuel et validé de la séquence des activités de reconstruction de l'infrastructure et de remise en route des applications à Genève n'est donc pas encore disponible.

Un outil de monitorage surveille le bon fonctionnement de l'infrastructure et signale les éventuelles anomalies. Dans la cas d'ACOR, un serveur est surveillé. Le principal de l'application fonctionnant sur des postes clients, aucun autre monitorage central n'est indiqué.

Un processus de gestion des incidents existe et est documenté. Selon les intervenants (internes ou externes à la CdC), le canal utilisé pour le transfert du problème diffère. Un ticket est ensuite saisi pour traitement dans l'outil Remedy. La résolution est documentée.

Des statistiques d'incidents du service utilisateurs de la CdC sont éditées. La moitié des 177 incidents enregistrés entre janvier 2017 et juin 2018 pour ACOR ont été résolus en moins de 3 heures. Dans le 85 % des incidents, les objectifs en termes de temps de résolution sont tenus. Selon une enquête de satisfaction réalisée en 2017, les utilisateurs externes en contact direct avec le groupe ACOR (env. 30 % des sondés) sont satisfaits du service de support.

Appréciation

Le CDF n'a pas constaté de défaut majeur dans l'organisation et les processus de l'exploitation de l'application ACOR. Les efforts en vue de la définition d'un plan de reprise d'activité doivent être poursuivis.

2.4 Une base adéquate pour les développements futurs

Des activités de « refactoring » (« réusinage » / optimisation du code) sont régulièrement effectuées. Une partie des modifications préparées dans le cadre du projet Prévoyance 2020 ont été reprises dans la version actuelle du logiciel.

Sur le plan du personnel, l'équipe de développement compte sept spécialistes polyvalents, dont l'âge moyen est dans la quarantaine.

Un projet de mise en œuvre d'une nouvelle version de l'application est prévu, son initialisation doit être décidée à l'automne 2018. Ce projet vise principalement à adapter l'architecture de la solution. Celle-ci devrait passer d'un fonctionnement basé sur un « client lourd » (installation locale de l'application) à une application de style Web (« client léger », basé sur un explorateur Internet, donc sans installation locale, et serveur applicatif centralisé). Selon l'architecture pressentie, l'interface utilisateurs (Graphical User Interface, GUI) serait basée sur des technologies du monde Java. Une veille technologique a aussi été effectuée sur les outils de construction de systèmes experts. L'étude a conclu que les règles resteraient dans l'outil déjà utilisé, nommé CLIPS[3].

Appréciation

Pour le CDF, les activités régulières de développement et de refactoring contribuent à garder un code évolutif et dépourvu de « bois mort » et autres scories. Les travaux de maintenance évolutive s'en trouvent facilités.

[3] CLIPS est un logiciel de domaine public hébergé par la forge logicielle sourceforge.net.

Le CDF estime plausible l'architecture pressentie pour la nouvelle version. Une des limitations de l'application actuelle, la nécessité du déploiement de la solution vers des postes clients, pourrait ainsi être éliminée. Des technologies « modernes » peuvent être mises en œuvre pour l'interface utilisateur. CLIPS reste un outil d'actualité pour la construction de systèmes experts.

Le CDF considère que la plateforme ACOR constitue une base globalement adéquate pour les développements futurs de l'application. Pour la nouvelle version, il encourage la CdC à évaluer soigneusement les défis posés par la nouvelle architecture – sécurité, disponibilité, acquisition de nouvelles compétences. Il pousse également l'équipe ACOR à repenser les processus d'exploitation et les activités de contrôle en fonction de la future application.

2.5 Une recommandation pas encore entièrement mise en œuvre

En 2015, le CDF a procédé à un audit informatique de la CdC. Une recommandation portait sur la mise en place d'accords décrivant le niveau de service envers les bénéficiaires institutionnels externes de prestations informatiques (organes d'exécution du 1er pilier). Les engagements des systèmes d'informations (SI) de la CdC en matière de disponibilité et de sécurité des informations devaient notamment être décrits. La CdC a accepté la recommandation.

La division des SI de la CdC a dans un premier temps clarifié la situation de base donnée par les accords de niveaux de service (service level agreements ou SLA) de l'OFIT. L'engagement du service utilisateur des SI de la CdC a également été examiné. La description des canaux de communication disponibles pour les applications mises à disposition des organes d'exécution (ACOR, Registres centraux, module d'augmentation, SUMEX) existe. Les liens vers les directives réglant les responsabilités (comités et prérogatives) sont également établis. Enfin, les responsabilités et la marche à suivre pour la remise de jetons d'identification (« tokens ») sont décrits. Au moment de l'audit du CDF, ces éléments n'ont toutefois pas encore été traduits en engagements vis-à-vis des partenaires extérieurs.

Des pistes pour une mise en œuvre pragmatique de l'esprit de la recommandation existent. Une publication des niveaux de service généraux sur les pages du site de la CdC dédiées aux partenaires institutionnels est envisageable. Des compléments par application sont également possibles. Les accords pourraient aussi être conclus par l'intermédiaire des associations de caisses (Conférence des caisses cantonales de compensation, Association suisse des caisses de compensations professionnelles).

Appréciation

Le CDF considère que la recommandation n'est pas encore entièrement mise en œuvre mais estime globalement appropriés les principes de la solution proposée par la CdC. Il l'encourage à finaliser la définition de la forme des accords décrivant les niveaux de service et à les mettre en œuvre rapidement.

Annexe 1: Bases légales

Textes législatifs
Loi fédérale sur la partie générale du droit des assurances sociales (LPGA) du 6 octobre 2000, RS 830.1
Ordonnance du DFF sur la Centrale de compensation (Ordonnance sur la CdC) du 3 décembre 2008, RS 831.143.32
Loi fédérale sur l'assurance-vieillesse et survivants (LAVS) du 20 décembre 1946, RS 831.10
Règlement sur l'assurance-vieillesse et survivants (RAVS) du 31 octobre 1947, RS 831.101
Ordonnance concernant l'assurance-vieillesse, survivants et invalidité facultative (OAF) du 26 mai 1961, RS831.111
Ordonnance concernant la remise de moyens auxiliaires par l'assurance-vieillesse (OMAV) du 28 août 1978, RS 831.135.1
Ordonnance sur l'informatique dans l'administration fédérale (OIAF) du 9 décembre 2011, RS 172.010.58
Intervention parlementaire
17.4067 – Le Conseil fédéral est-il certain que toutes les rentes AVS et AI sont calculées avec exactitude dans tous les cas de figure ? Interpellation d'Olivier Feller, Conseiller national, 12.12.2017

Annexe 2: Abréviations

AVS	Assurance-vieillesse et survivants
CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
CSC	Caisse suisse de compensation
DRP	Disaster recovery plan, plan de reprise des activités
OFIT	Office fédéral de l'informatique et de la télécommunication
SCI	Système de contrôle interne
SI	Division des systèmes d'information de la CdC
SLA	Service level agreements, accords de niveau de service

Annexe 3: Glossaire

ACOR	Système d'aide au calcul et à l'octroi des rentes, application de type système-expert de la CdC, fonctionne comme une feuille de calcul pour déterminer le droit à une rente et son montant
CLIPS	Outil de construction de systèmes-experts, langage de programmation basé sur des règles, projet de la forge logicielle SourceForge
GUI	Graphical User Interface, interface graphique permettant l'interaction de l'utilisateur avec une application
ISAE 3402	Norme d'audit permettant aux utilisateurs de prestations externalisées d'obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de services
JIRA	Logiciel de suivi des tickets et des projets de l'éditeur Atlassian
Refactoring	Réusinage de code, opération consistant à retravailler le code source d'un programme informatique, sans toutefois y ajouter des fonctionnalités ni en corriger les bogues
Remedy	Application de gestion du support informatique de l'éditeur BMC
SUMEX	Solution de contrôle de factures, développé par ELCA S.A. pour la Caisse nationale suisse d'assurance en cas d'accidents (SUVA)
SVN	Système de gestion centralisée des versions de logiciel, projet de l'Apache software foundation
Test de non régression	Test permettant de vérifier que les modifications apportées à un logiciel n'ont pas entrainé d'impact non désiré dans une version antérieurement validée
Token	Jeton d'authentification, solution permettant de prouver une identité par voie électronique

Priorités des recommandations

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).