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

Audit du programme de migration d'applications Rehosting

Centrale de compensation

CDF-19411 | Prises de position incluses | 20 avril 2020 | DélFin D4/2020

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	1.19411.602.00191
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)

Sauf indication contraire, les dénominations de fonction dans ce rapport s'entendent aussi bien à la forme masculine que féminine.

Table des matières

Audit du programme de migration d'applications Rehosting

Centrale de compensation

L'essentiel en bref

L'Office fédéral de l'informatique et de la télécommunication (OFIT) héberge une partie importante des applications de la Centrale de compensation (CdC). La plateforme technique actuelle sera mise hors service en 2021. La CdC a lancé le programme « Rehosting » pour une nouvelle infrastructure dans ses locaux et rapatrier une trentaine d'applications. Prévus entre 2017 et 2021, ces travaux de migration ont été structurés en sept projets, le tout devisé initialement à quelque 19,8 millions de francs. Les coûts externes représentent environ 30 % de ce montant.

Par cette révision, le Contrôle fédéral des finances (CDF) évalue l'état de l'avancement et les risques du programme. Celui-ci est en cours mais des retards et des hausses des coûts sur certains projets sont visibles.

La direction du programme est globalement adéquate

Le CDF n'a pas constaté de défaut majeur dans le processus de pilotage du programme et de ses projets. Les instances de pilotage du programme sont correctement définies. Les décisions de libération des phases sont dûment validées et documentées et les priorités des chantiers sont gérées de manière adéquate. La majorité des outils et des processus de conduite des projets est appropriée. Des plans de gestion de projets sont définis et l'état d'avancement est régulièrement suivi. Les dépendances entre les tâches de projets sont identifiées. Des éléments de méthodologie agile sont définis et mis en œuvre, le processus d'apprentissage est en cours.

Le CDF relève que les risques des projets et du programme, ainsi que les mesures compensatoires, sont régulièrement suivis. La gestion de la qualité est bien outillée. Les tests de l'infrastructure mise en place sont effectués régulièrement mais les détails des tests des migrations applicatives sont encore en cours d'élaboration. Le CDF recommande à la CdC d'approfondir et de finaliser la planification et les concepts de tests.

Des dépassements de coûts et des décalages de phases sont observés

Malgré ces efforts, les projets du programme Rehosting ont affronté des difficultés importantes. La complexité technique des travaux, les tensions entre les intervenants et la durée des procédures d'achats ont engendré des décalages de phases et des dépassements des estimations initiales de coûts. La CdC doit continuer de tirer les enseignements de ces écueils.

La mise en place de l'infrastructure cible était en phase de réalisation lors de l'audit. Il a été observé un dépassement par rapport au budget initial. Les projections des besoins financiers pour le programme entier se montent désormais à 22,9 millions de francs. Les projets

de migrations applicatives s'approchent de la fin de leur phase de conception mais des retards sont prévisibles. La date prévue pour la finalisation du programme pourrait être remise en question par un des projets.

Le pilotage du programme doit continuer de suivre attentivement ces évolutions. Le CDF a recommandé à la CdC d'améliorer ses outils de suivi temporel des projets et de déterminer le chemin critique au niveau du programme.

La première étape de l'évolution architecturale est fondée mais comporte quelques manques

Lors de l'initialisation du programme, la CdC a évalué deux grands types de solutions pour le nouvel hébergement de ses applications. Les mises en place d'une nouvelle plateforme hébergée à l'OFIT ou à la CdC ont été comparées. Une étude documente l'évaluation de ces options et retient la seconde. Les critères économiques ont été prépondérants dans ce choix. Les hypothèses de calcul n'ont pas été documentées. Le CDF a recommandé à la CdC d'actualiser le calcul de rentabilité de la solution choisie et d'expliciter les bases de travail. Ces éléments sont incontournables à la préparation des prochaines décisions stratégiques d'hébergement de la plateforme.

La CdC a dû demander une autorisation pour mettre en place et exploiter une infrastructure sur site. L'Unité de pilotage informatique de la Confédération la lui a accordée jusqu'à la fin 2024 mais l'a assortie de conditions. La CdC doit notamment prévoir, dès 2025, le rapatriement des services et composantes d'infrastructure vers le réseau de centres de calcul de la Confédération. Le CDF relève qu'une planification de ce rapatriement est attendue dès 2021.

Pour la partie infrastructurelle du programme, des études architecturales sont élaborées et approfondies de manière itérative. Le CDF considère que ces artefacts constituent une base adéquate pour la mise en œuvre de la nouvelle plateforme. Il relève toutefois que ces résultats n'ont pas été formellement validés par les comités ad hoc au sein de la CdC.

Les exigences de l'exploitation et de la sécurité de l'information doivent être mieux intégrées

La mise en œuvre de la nouvelle infrastructure a un fort impact sur les activités de l'exploitation informatique. Les difficultés initiales dans l'intégration de ce domaine sont largement résolues. Le service a été réorganisé et le développement de ses compétences est en cours. Sa mue n'est toutefois pas achevée et la collaboration avec le programme reste sensible. Le CDF recommande à la CdC de mieux intégrer l'exploitation informatique au programme et d'élaborer une planification réaliste des ressources du service pour le programme.

La sécurité de l'information est aussi un aspect sensible et essentiel de la mise en place de la nouvelle infrastructure. Le CDF relève les nombreuses initiatives en cours. Mais, le volume de travail reste ici très important sur le plan de l'infrastructure, des applications et des processus de sécurité (actualisation de la documentation, mise en œuvre, vérification…). Le CDF recommande à la CdC de faire le point des travaux en cours, d'actualiser la documentation et d'élaborer une planification réaliste des tâches restantes.

Prüfung des Programms Anwendungsmigration Rehosting

Zentrale Ausgleichsstelle

Das Wesentliche in Kürze

Das Bundesamt für Informatik und Telekommunikation (BIT) hostet einen wichtigen Teil der Anwendungen der Zentralen Ausgleichsstelle (ZAS). Die aktuelle technische Plattform wird 2021 ausser Betrieb genommen. Die ZAS hat das Programm «Rehosting» für eine neue Infrastruktur in ihren Räumlichkeiten sowie die Rückführung von rund 30 Anwendungen initiiert. Die zwischen 2017 und 2021 geplanten Migrationsarbeiten sind in sieben Projekte unterteilt für ursprünglich insgesamt ca. 19,8 Millionen Franken. Davon entfallen etwa 30 % auf externe Kosten.

Im Rahmen der vorliegenden Prüfung evaluiert die Eidgenössische Finanzkontrolle (EFK) den Arbeitsfortschritt und die Risiken des Programms. Dieses ist auf Kurs, doch in einigen Projekten zeichnen sich Verzögerungen und Kostensteigerungen ab.

Das Programmmanagement ist insgesamt angemessen

Die EFK hat im Steuerungsprozess des Programms und der dazugehörigen Projekte keine wesentlichen Mängel festgestellt. Die Steuerungsinstanzen des Programms sind korrekt bestimmt. Die Entscheide zu den einzelnen Phasenfreigaben sind vorschriftsgemäss validiert und dokumentiert, und die Baustellen-Prioritäten werden angemessen gemanagt. Die meisten Projektmanagementtools und -prozesse erfüllen ihren Zweck. Projektmanagementpläne sind festgelegt und der Arbeitsfortschritt wird regelmässig überprüft. Die Abhängigkeiten zwischen den Projektaufgaben wurden erkannt. Agile Methodikelemente sind definiert und umgesetzt, der Lernprozess ist im Gange.

Die EFK hält fest, dass die Projekt- und Programmrisiken sowie die Ausgleichsmassnahmen regelmässig überwacht werden. Das Qualitätsmanagement ist gut ausgestattet. Regelmässig finden Infrastrukturtests statt, doch noch sind die Einzelheiten der Migrationstests für die Anwendungen erst in Entwicklung. Die EFK empfiehlt der ZAS, die Planung und die Testkonzepte zu vertiefen und fertigzustellen.

Kostenüberschreitungen und Phasenverschiebungen sind zu verzeichnen

Trotz aller Bemühungen sahen sich die Projekte des Rehosting-Programms mit erheblichen Schwierigkeiten konfrontiert. Die technische Komplexität der Arbeiten, die Spannungen zwischen den Akteuren und die Dauer der Beschaffungsverfahren führten zu Phasenverschiebungen und Überschreitungen der ursprünglichen Kostenschätzungen. Die ZAS muss aus diesen Problemen noch weitere Lehren ziehen.

Zum Prüfungszeitpunkt befand sich die Errichtung der Zielinfrastruktur in der Realisierungsphase. Gegenüber dem ursprünglichen Budget wurde eine Überschreitung festgestellt. Die Projektion des Finanzbedarfs für das ganze Programm beläuft sich neu auf 22,9 Millionen

Franken. Die Projekte der Anwendungsmigrationen nähern sich dem Ende ihrer Konzeptphase, doch Verzögerungen sind absehbar. Eines der Projekte könnte das geplante Datum für den Programmabschluss gefährden.

Diese Entwicklungen müssen im Rahmen der Programmsteuerung weiter aufmerksam verfolgt werden. Die EFK hat der ZAS empfohlen, ihre Werkzeuge zur Verfolgung des zeitlichen Projektablaufs zu verbessern und den kritischen Pfad auf Stufe Programm zu bestimmen.

Die erste Etappe der Architektur-Entwicklung ist fundiert, weist jedoch einige Mängel auf

Bei der Programminitialisierung hat die ZAS zwei Haupttypen von Lösungen für das neue Hosting ihrer Anwendungen evaluiert. Die Implementierung einer neuen Hosting-Plattform beim BIT oder bei der ZAS wurde verglichen. Eine Studie dokumentiert die Evaluation dieser Optionen und plädiert für die zweite. Ausschlaggebend für diese Wahl waren die wirtschaftlichen Kriterien. Die Berechnungsannahmen wurden nicht dokumentiert. Die EFK hat der ZAS empfohlen, die Wirtschaftlichkeitsberechnung der gewählten Option zu aktualisieren und die Arbeitsgrundlagen klarer zu erläutern. Das ist für die Vorbereitung der nächsten Strategieentscheide für das Hosting der Plattform unerlässlich.

Die ZAS musste eine Genehmigung für die Errichtung und den Betrieb einer Vor-Ort-Infrastruktur einholen. Sie wurde ihr vom Informatiksteuerungsorgan des Bundes bis Ende 2024 erteilt, jedoch mit Auflagen. So muss die ZAS ab 2025 unter anderem die Rückführung der Dienste und Infrastrukturkomponenten in das Netzwerk der Rechenzentren des Bundes vorsehen. Die EFK hält fest, dass eine Planung dieser Rückführung für den Zeithorizont 2021 erwartet wird.

Für die Programminfrastruktur werden Studien zur IT-Architektur entwickelt und immer wieder vertieft. Die EFK sieht darin eine geeignete Grundlage für die Umsetzung der neuen Plattform. Sie konstatiert jedoch, dass diese Ergebnisse nicht formell durch die zuständigen Ausschüsse der ZAS validiert worden sind.

Die betrieblichen und für die Informationssicherheit relevanten Anforderungen müssen besser integriert werden

Die Umsetzung der neuen Infrastruktur hat starke Auswirkungen auf den Informatikbetrieb. Die anfänglichen Schwierigkeiten bei der Integration dieses Bereichs sind weitgehend überwunden. Der Dienst wurde neu organisiert und seine Kompetenzen werden weiterentwickelt. Die Erneuerung des Dienstes ist jedoch noch nicht abgeschlossen und die Zusammenarbeit mit dem Programm bleibt heikel. Die EFK empfiehlt der ZAS, den Informatikbetrieb besser in das Programm zu integrieren und eine realistische Planung der dienstеigenen Ressourcen für das Programm zu erarbeiten.

Auch die Informationssicherheit ist ein heikler und wesentlicher Aspekt der Errichtung der neuen Infrastruktur. Die EFK verweist auf die zahlreichen laufenden Initiativen. Allerdings ist der Arbeitsaufwand hinsichtlich der Infrastruktur, der Anwendungen und der Sicherheitsprozesse (Aktualisierung der Unterlagen, Umsetzung, Überprüfung etc.) nach wie vor sehr hoch. Die EFK empfiehlt der ZAS, eine Überprüfung der laufenden Arbeiten vorzunehmen, die Unterlagen zu aktualisieren und eine realistische Planung der verbleibenden Aufgaben zu erstellen.

Originaltext auf Französisch

Verifica del programma di migrazione di applicazioni Rehosting

Ufficio centrale di compensazione

L'essenziale in breve

L'Ufficio federale dell'informatica e della telecomunicazione (UFIT) è host di gran parte delle applicazioni dell'Ufficio centrale di compensazione (UCC). L'attuale piattaforma tecnica sarà disattivata nel 2021. L'UCC ha lanciato il programma «Rehosting» per installare una nuova infrastruttura nei suoi locali e migrare una trentina di applicazioni. Previsti tra il 2017 e il 2021, i lavori di migrazione sono stati articolati in sette progetti, per un totale inizialmente stimato a circa 19,8 milioni di franchi. I costi esterni rappresentano circa il 30 per cento di tale importo.

Nel quadro della presente verifica, il Controllo federale delle finanze (CDF) valuta lo stato di avanzamento e i rischi del programma, che, sebbene sia ancora in corso, presenta ritardi e sforamenti dei costi in relazione ad alcuni progetti.

Gestione del programma complessivamente adeguata

Il CDF non ha riscontrato rilevanti carenze nel processo di gestione del programma e dei suoi progetti. Le relative istanze di gestione sono definite correttamente. Le decisioni concernenti le fasi di rilascio vengono convalidate e documentate adeguatamente e le priorità dei cantieri sono gestite in modo consono. La maggioranza degli strumenti e dei processi di gestione dei progetti è appropriata. I piani di gestione dei progetti sono stilati e lo stato di avanzamento è monitorato regolarmente. Sono individuate le interdipendenze tra i compiti dei progetti, gli elementi del metodo agile sono stabiliti e applicati, mentre il processo di apprendimento è in corso.

Il CDF constata che i rischi dei progetti e del programma, nonché le misure di compensazione, sono sottoposti a un monitoraggio regolare. La gestione della qualità è ben attrezzata e i test dell'infrastruttura realizzata vengono condotti regolarmente; in compenso, i dettagli dei test delle migrazioni delle applicazioni sono ancora in fase di elaborazione. Il CDF raccomanda all'UCC di sviluppare e ultimare la pianificazione e i piani di test.

Sforamenti dei costi e ritardi

Nonostante questi sforzi, i progetti del programma Rehosting hanno dovuto far fronte a grandi difficoltà. La complessità tecnica dei lavori, le tensioni tra gli operatori e la durata delle procedure di acquisto hanno causato ritardi e sforamenti dei costi inizialmente stimati. L'UCC deve continuare a trarre insegnamenti da questi inconvenienti.

La realizzazione dell'infrastruttura target era in corso durante la verifica. È stato osservato un superamento del budget preventivato: il fabbisogno finanziario previsto per l'intero programma ammonta ormai a 22,9 milioni di franchi. I progetti di migrazione delle applicazioni sono prossimi al termine della loro fase di elaborazione, ma sono attesi possibili ritardi. La data stabilita per la conclusione del programma potrebbe essere rimessa in discussione da uno dei progetti.

La gestione del programma deve continuare a seguire attentamente queste evoluzioni. Il CDF ha raccomandato all'UCC di migliorare i suoi strumenti di monitoraggio temporale dei progetti e di determinare il percorso critico a livello di programma.

Prima fase di evoluzione dell'architettura consolidata, malgrado alcune lacune

Durante la fase d'inizializzazione del programma, l'UCC ha valutato due grandi soluzioni per il nuovo servizio di host delle sue applicazioni. Sono state messe a confronto le possibilità dell'installazione di una nuova piattaforma presso l'UFIT o presso l'UCC. Uno studio documenta la valutazione di entrambe le opzioni, premiando la seconda. A pesare ai fini della decisione sono stati i criteri economici. Le ipotesi di calcolo non sono state documentate. Il CDF ha raccomandato all'UCC di aggiornare il calcolo della redditività della soluzione scelta e di esplicitare le basi di lavoro. Questi elementi sono indispensabili per la preparazione delle prossime decisioni strategiche di hosting della piattaforma.

L'UCC ha dovuto richiedere un'autorizzazione per realizzare e utilizzare un'infrastruttura in loco. L'Organo direzione informatica della Confederazione ha concesso tale autorizzazione fino alla fine del 2024, ponendo alcune condizioni. In particolar modo, dal 2025, l'UCC deve prevedere il trasferimento dei servizi e degli elementi dell'infrastruttura verso la rete del centro di calcolo della Confederazione. Il CDF osserva che una pianificazione di questo trasferimento sarà attesa dal 2021.

Per la parte infrastrutturale del programma, sono in corso e in continuo sviluppo studi relativi all'architettura. Il CDF ritiene che questi risultati costituiscano una base adeguata per l'attuazione della nuova piattaforma, pur osservando che non sono stati formalmente convalidati dai comitati specifici in seno all'UCC.

Necessità di migliore integrazione dell'esercizio e della sicurezza delle informazioni

La realizzazione della nuova infrastruttura ha un forte impatto sulle attività dell'esercizio informatico. Le difficoltà iniziali nell'integrazione di questo ambito sono ampiamente risolte. Il servizio è stato riorganizzato e lo sviluppo delle sue competenze è in corso. La sua mutazione non è tuttavia completata e la collaborazione con il programma rimane delicata. Il CDF raccomanda all'UCC di integrare meglio l'esercizio informatico all'interno del programma e di elaborare una pianificazione realistica delle risorse del servizio per il programma.

La sicurezza delle informazioni è un altro aspetto sensibile ed essenziale della realizzazione della nuova infrastruttura. Il CDF individua le numerose iniziative in corso, tuttavia il carico di lavoro rimane elevato sul piano dell'infrastruttura, delle applicazioni e dei processi di sicurezza (aggiornamento della documentazione, realizzazione, verifica…). Il CDF raccomanda all'UCC di fare il punto dei lavori in corso, di aggiornare la documentazione e di elaborare una pianificazione realistica dei compiti rimanenti.

Testo originale in francese

Audit of the Rehosting application migration programme

Central Compensation Office

Key facts

The Federal Office of Information Technology, Systems and Telecommunication (FOITT) hosts a large number of the applications of the Central Compensation Office (CCO). The current technical platform will be taken out of service in 2021. The CCO launched the "Rehosting" programme to set up a new infrastructure on its premises and repatriate around 30 applications. The migration work, which began in 2017 and is scheduled to continue until 2021, has been structured into seven projects, initially costing around CHF 19.8 million. External costs account for around 30% of this amount.

With this audit, the Swiss Federal Audit Office (SFAO) assessed the progress and risks of the programme, which is ongoing, but delays and cost increases on some projects are visible.

Programme management generally adequate

The SFAO did not find any major shortcomings in the management of the programme and its projects. The programme's steering bodies are correctly defined. Decisions to release phases are properly validated and documented, and work priorities are adequately managed. The majority of project management tools and processes are appropriate. Project management plans are defined and progress is regularly monitored. Dependencies between project tasks are identified. Elements of agile methodology are defined and implemented, and the learning process is ongoing.

The SFAO noted that project and programme risks, as well as mitigation measures, are regularly monitored. Quality management is well equipped. Implemented infrastructure tests are carried out regularly, but the details of the application migration tests are still under development. The SFAO recommends that the CCO further develop and finalise the planning and test concepts.

Cost overruns and delays to phases observed

Despite these efforts, the Rehosting programme projects have faced significant difficulties. The technical complexity of the work, tensions between the parties involved and the length of the procurement procedures have led to delays in the phases and cost overruns compared to the initial estimates. The CCO must continue to learn from these difficulties.

The target infrastructure was in the process of being implemented at the time of the audit. An overrun of the original budget was observed. Projected financial requirements for the entire programme now total CHF 22.9 million. The application migration projects are nearing the end of their design phase but delays are foreseeable. The planned completion date of the programme could be threatened by one of the projects.

Programme management must continue to monitor these developments closely. The SFAO recommended that the CCO should improve its tools for monitoring the timing of projects and determine the critical path at the programme level.

First stage of architecture development is well-grounded, but some shortcomings exist

During the initial phase of the programme, the CCO evaluated two main types of solutions for the new hosting of its applications. A comparison was made between the implementation of a new platform hosted at the FOITT or at the CCO. A study documented the evaluation of these options and opted for the latter. The economic criteria were decisive in this choice. The calculation assumptions were not documented. The SFAO recommended that the CCO update the cost-effectiveness calculation of the chosen solution and clarify the bases for work. These elements are essential in order to prepare the next strategic decisions concerning the hosting of the platform.

The CCO had to apply for authorisation to install and operate an on-site infrastructure. The Federal IT Steering Unit granted permission for this until the end of 2024, subject to conditions. In particular, the CCO must envisage the repatriation of services and infrastructure components to the Confederation's network of data centres from 2025 onwards. The SFAO noted that plans for this repatriation are expected as early as 2021.

For the infrastructure part of the programme, architectural studies are being drawn up and further developed on an iterative basis. The SFAO considers these artefacts to be an adequate basis for implementing the new platform. It notes, however, that these results have not been formally validated by the CCO's ad hoc committees.

Operational and information security requirements need better integration

The implementation of the new infrastructure had a strong impact on IT operations. The initial difficulties in integrating this area have largely been resolved. The unit has been reorganised and its competencies are being developed. However, its transformation is not yet complete and collaboration with the programme remains sensitive. The SFAO recommends that the CCO better integrate IT operations into the programme and develop a realistic resource plan for the unit with regard to the programme.

Information security is also a sensitive and essential aspect of implementing the new infrastructure. The SFAO noted the many initiatives that are currently under way. However, the volume of work here remains very high in terms of security infrastructure, applications and processes (updating documentation, implementation, verification, etc.). The SFAO recommends that the CCO take stock of the work in progress, update the documentation and draw up a realistic plan for the remaining tasks.

Original text in French

Prise de position générale de la Centrale de compensation

Le programme de Rehosting est fondamental pour la CdC dans sa démarche de modernisation de son Système d'Information. Il permettra au premier pilier des assurances sociales de réaliser des économies substantielles, tout en améliorant la qualité et l'efficience de ses prestations.

La CdC remercie le CDF pour le présent audit du programme de Rehosting. Nous avons notamment apprécié l'esprit constructif de cet audit, axé sur la recherche d'améliorations tangibles, qui apportent une plus-value au programme. Nous avons aussi apprécié que nos retours soient compris et intégrés.

La CdC partage fondamentalement et accepte toutes les recommandations du CDF. La mise en œuvre de ces recommandations a déjà commencé, en particulier en ce qui concerne celles qui portent sur la sécurité de l'information. Pour ces dernières, les effets ne se limiteront d'ailleurs pas seulement au programme de Rehosting mais bénéficieront à l'ensemble des applications de la CdC. La CdC a démarré son programme dès 2017 avec comme objectif d'assurer une mise en œuvre impeccable, « juste du premier coup », car les responsabilités de la CdC dans l'exécution du 1er pilier les assurances sociales sont énormes : Elle doit en effet assurer le paiement de 10 milliards de rentes AVS/AI aux ayants droit résidants à l'étranger, assurer des flux financiers de plus de 40 milliards, et garantir la tenue des registres centraux utilisés par un très grand nombre d'utilisateurs et indispensable pour la bonne marche du 1er pilier des assurances sociales en Suisse et à l'étranger.

La CdC n'a donc jamais sous-estimé la charge et l'importance de ce programme qui représente son plus grand projet informatique de ces 25 dernières années, et elle continuera de tout mettre en œuvre pour qu'il soit une réussite.

Les effets de la pandémie de COVID-19 actuelle n'ont pas encore pu être mesurés au moment où nous donnons notre prise de position. Il est néanmoins possible que l'effet principal soit un allongement des délais. Mais quoiqu'il en soit, la CdC restera déterminée à garantir une exécution impeccable du programme.

1 Mission et déroulement

1.1 Contexte

Une partie importante du patrimoine informatique de la Centrale de compensation (CdC) est hébergée à l'Office fédéral de l'informatique et de la télécommunication (OFIT). La plateforme de type « mainframe »[1] qui abrite ce patrimoine arrive en fin de vie et l'OFIT a décidé sa mise hors service à la fin 2021. Pour mettre en place une nouvelle solution d'hébergement, la CdC a lancé le programme de Rehosting (« changement d'hébergement »). Dans une phase d'initialisation, elle a identifié deux variantes de solution principales (nouvelle infrastructure à l'OFIT ou sur site à la CdC) et a tranché en faveur de la seconde. Sept projets sont définis et planifiés entre 2017 et 2021 et estimés à quelque 19,8 millions de francs. Les travaux visent principalement à mettre en service la nouvelle infrastructure et à y migrer les applications de la plateforme « mainframe ». Celles-ci restent inchangées sur le plan fonctionnel, mais sur le plan technique, les évolutions sont importantes.

1.2 Objectif et questions d'audit

Dans cette révision, le Contrôle fédéral des finances (CDF) évalue l'état de l'avancement et les risques du programme. Pour ceci, il utilise la démarche d'audit des projets informatiques clés de la Confédération et vise à répondre aux questions suivantes :

- Les projets du programme se déroulent-t-ils comme prévu en termes de résultats, de calendrier et de coûts, et sont-ils pilotés et conduits de manière adéquate ?
- Est-ce qu'une gestion appropriée des risques et de la qualité est en place ?
- Différentes variantes de solution ont-elles été considérées pour la mise en œuvre du programme, et la plus économique a-t-elle été choisie ?
- La planification architecturale est-elle adéquate dans le programme et une éventuelle migration vers un centre de calcul de la Confédération a-t-elle été considérée ?
- Des risques accrus existent-ils en relation avec le choix de la solution organisationnelle et technique choisie ?
- Les exigences de la sécurité de l'information sont-elles prises en compte dans le programme ?

1.3 Etendue de l'audit et principe

L'audit a été mené du 4 novembre au 13 décembre par André Stauffer (responsable de révision), Hans Ulrich Wiedmer et Grégory Le Mintier (Deloitte SA). Il a été conduit sous la responsabilité de Bernhard Hamberger. La discussion des résultats a eu lieu le 3 décembre 2019. Le présent rapport ne prend pas en compte les développements après cette discussion.

[1] Architecture informatique basée sur un ordinateur central de grande puissance et un réseau de terminaux. Un glossaire figure en fin de rapport pour les termes techniques (Annexe 3).

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par la CdC. 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 9 mars 2020 en présence des représentants suivants de la CdC :

- Le directeur
- Le chef de la division des systèmes d'information
- Le chef de l'inspectorat interne
- Un chef de programme
- Deux chefs de domaines de portefeuilles applicatifs
- Le chef du domaine projets et architecture
- Le chef du domaine infrastructure

Le CDF était représenté par :

- La responsable de mandat
- Un responsable de centre de compétence
- Le responsable de révision

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 Constats et appréciations

2.1 Les travaux sont en cours, des retards et des surcoûts sont constatés

Des sept projets du périmètre initial, un projet s'est terminé à la fin 2018 et un autre a été abandonné. Le coût des travaux est estimé initialement à quelque 19,8 millions de francs, dont environ 30 % de coûts externes. Les tableaux ci-dessous donnent un condensé de la phase d'initialisation et des projets sous l'angle des coûts et des délais (état au 31 octobre 2019).

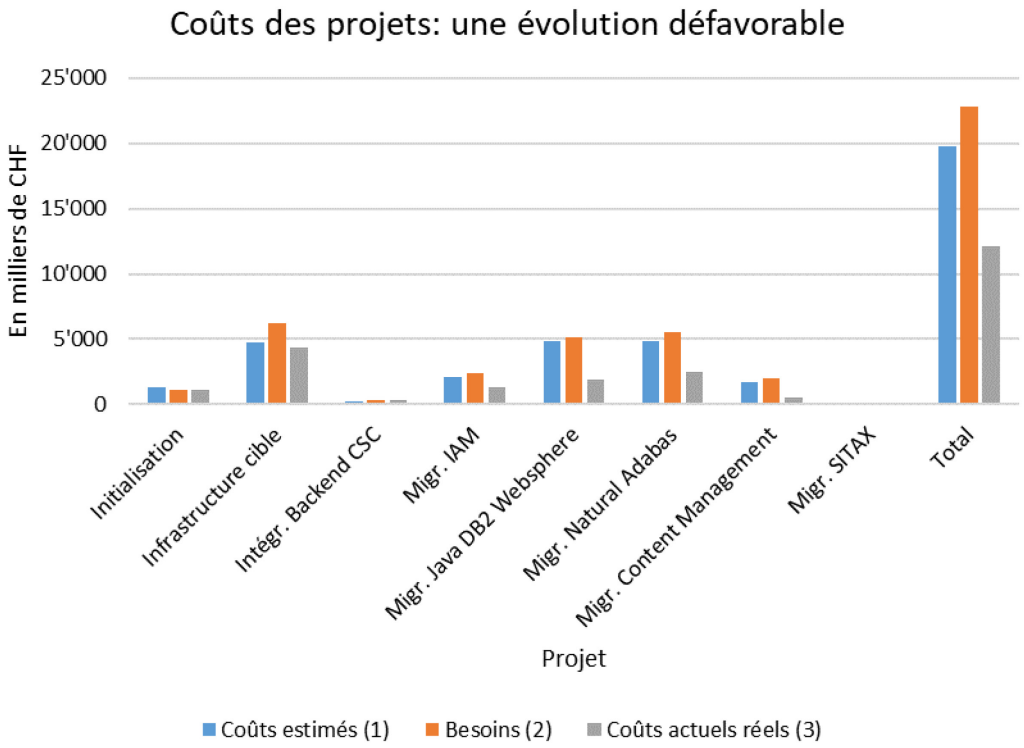

Tableau 1 : Evolution des coûts des projets, montants en milliers de francs. Sources : Mandats de projets (1), Cockpit IKT[2] du 31.10.2019 (2, 3).

Des surcoûts apparaissent dans tous les projets pour un total de près de 3,1 millions de francs (+ 16 %). Ce constat est obtenu en comparant les besoins (comme estimation à l'achèvement des travaux) et les coûts estimés dans les mandats de projets. En termes absolus, les projets d'infrastructure cible et de migration Natural Adabas contribuent le plus fortement à cette hausse (env. + 2,2 millions de francs). Parmi les causes évoquées des dépassements pour le projet infrastructure, le CDF retient notamment les problèmes de matériel (installation / configuration), le fort taux de rotation des spécialistes dans le projet et les retards dans le processus d'achat. Dans le cas du projet de migration Natural Adabas, la CdC juge son estimation initiale trop basse. Elle invoque la difficulté à parvenir à une

[2] Outil de contrôle de gestion pour les projets informatiques et les applications de l'administration fédérale.

estimation du coût des travaux en raison du caractère très spécifique de l'opération. L'impossibilité de procéder à des demandes d'informations dans le cadre de marchés publics est également avancée.

Dans ces deux cas, le CDF a pu vérifier que la Commission informatique (organe de direction stratégique de l'informatique de la CdC) a approuvé ces dépassements.

Projet	Phase actuelle (6)	Date de fin estimée (7)	Date de fin révisée (8)
Initialisation	Terminé		
Infrastructure cible	Réalisation	30.04.2020	30.04.2020
Intégr. Backend CSC	Terminé		
Migr. IAM	Réalisation	31.12.2021	31.12.2021
Migr. Java DB2 Websphere	Conception	30.09.2021	30.09.2021
Migr. Natural Adabas	Conception	30.04.2020	31.12.2020
Migr. Content Management	Conception	30.06.2021	30.06.2021
Migr. SITAX	Abandonné		

Tableau 2 : Statut des projets et évolution des dates de fin de projet. Sources : Mandats de projets (7), Cockpit ICT du 31.10.2019 (6, 8).

Sur le plan des délais, seul le projet de migration Natural Adabas prévoit un dépassement par rapport à la date de fin initialement estimée. Le CDF a toutefois vérifié avec les chefs de projet que ces estimations n'étaient pas toutes systématiquement actualisées dans le Cockpit IKT. La fin de la conception du projet de migration Java est déjà repoussée d'au moins six mois par rapport à l'estimation d'origine. Pour les projets de migration Java et Content Management, des mises à jour sont prévues en fin de phase de conception.

Appréciation

Le CDF constate les dépassements encourus par les projets. Il voit le risque d'une poursuite des glissements pour les coûts et les délais. Le cas du projet de migration Java DB2 Websphere est particulièrement délicat. L'impact d'un éventuel retard de ce projet sur la fin prévue du programme ne peut pas être déterminé au moment de la révision (voir chapitre 2.4 ci-dessous pour une recommandation). Les mandants des projets et le management de la CdC doivent poursuivre leur surveillance serrée de ces éléments.

2.2 Le pilotage et la conduite sont globalement appropriés

Le CDF a constaté que l'organisation du programme et des projets au niveau pilotage est adéquatement définie. Il a également pu vérifier que les objectifs du programme et des projets sont définis et validés par la Commission Informatique et par le mandant. Les décisions de pilotage (démarrage des projets, libérations de phases) sont documentées et validées. L'UPIC est intervenue dans le processus de pilotage en évaluant si les conditions étaient réunies pour un lancement du programme. Elle a validé l'octroi d'une extension de sa dérogation à l'Art. 23 al. 1 de l'Ordonnance sur l'informatique dans l'Administration fédérale (OIAF). Selon cette extension accordée jusqu'à fin 2024, la CdC est habilitée à exploiter une infrastructure informatique pour ses applications.

Le responsable du portefeuille d'activités suit le programme et ses projets dans le cadre de sa fonction. Les priorités des différents projets et programmes de la CdC sont définies et suivies dans le cadre d'un processus annuel. Elles sont fixées en fonction de critères établis et validées par la Commission informatique. Le programme Rehosting est défini comme une des priorités de la CdC.

La surveillance périodique de l'état d'avancement est assurée à plusieurs niveaux (programme, projets) et par différents biais (réunions de suivi, états d'avancement réguliers ad hoc et dans le Cockpit IKT ; informations à l'Administration fédérale des finances). L'évolution des résultats, des coûts, des délais et des risques est ainsi rapportée régulièrement aux instances de pilotage du programme et des projets. En plus de l'avancement, la charge des ressources est examinée sur une base mensuelle par le responsable du portefeuille d'activités. Les éventuels problèmes de disponibilité des ressources personnelles du projet peuvent ainsi être décelés.

Des versions validées des plans de gestion du projet sont disponibles pour chacun des six projets actifs du programme à l'exception de la migration Java. Ces documents décrivent notamment les objectifs, les phases, l'organisation et les bases de la planification et du suivi des projets. Dans le cas des projets de migration applicative, une mise à jour de ces plans est prévue à la fin de la phase de conception. Les projets sont conduits selon la méthodologie HERMES et des éléments d'une démarche agile sont mis en œuvre (voir ci-dessous).

Appréciation

Le CDF n'a pas constaté de défaut majeur dans le processus de pilotage du programme Rehosting et de ses projets. La majorité des outils et processus de conduite mis en œuvre dans les projets sont adéquats. Le CDF relève que les plans de gestion de projets ne sont pas tous actuels. Ils doivent être mis à jour en fin de phase de conception comme le prévoit la méthode HERMES.

2.3 Les apprentissages ont nécessité de gros efforts

Plusieurs projets du programme Rehosting ont connu des difficultés de nature similaire. Parmi celles-ci, le CDF relève les éléments suivants:

- Les procédures d'achat comportent des contraintes importantes qui ont conduit à des retards de plusieurs mois;
- Les questions techniques sont complexes, la recherche de solutions et leur vérification ont nécessité d'importants investissements (études supplémentaires, preuves de concept);
- Les nominations des personnes adéquates (internes et externes) aux postes clés du programme ont parfois été délicates, les erreurs en la matière ont provoqué des retards et des tensions;
- Ces tensions entre intervenants ont parfois été difficiles à gérer, elles ont ralenti la bonne marche des travaux.

La recherche de solutions à ces divers problèmes a parfois nécessité plusieurs étapes. Elle a passé par le recours à des ressources externes. Dans leur majorité, les intervenants interrogés estiment toutefois que la plus grande partie de ces problèmes est résolue ou est en passe de l'être.

Appréciation

La mise en place et l'exploitation d'une infrastructure de cette taille constituent un nouveau métier et un défi conséquent. Mener un chantier de l'ampleur du programme de Rehosting n'est pas un exercice facile pour la CdC. En naviguant entre les écueils de la gestion d'une telle entreprise, les responsables du pilotage et de la conduite ont engrangé d'importants apprentissages. Il s'agit pour la CdC de continuer de tirer les leçons des difficultés rencontrées et d'en diffuser les enseignements auprès des personnes concernées.

2.4 Le suivi du chemin critique doit être amélioré

Les dépendances entre les tâches des projets et au niveau du programme sont gérées de manière dédiée et suivies régulièrement. Pour chaque projet, les tâches, les jalons et les dépendances sont représentés sur un axe temporel, permettant de visualiser le déroulement prévu des chantiers du projet. Une variante de haut niveau de cette représentation est utilisée lors des réunions de point de situation du programme. Par contre, cet outil n'incorpore pas la notion de durée prévue des tâches. Ainsi, il n'est pas possible d'identifier un chemin critique au niveau du programme.

Appréciation

Le suivi dédié et régulier des dépendances entre les tâches au sein du programme de Rehosting est une bonne pratique. Les fortes dépendances entre certaines tâches des projets sont ainsi prises en compte dans le déroulé temporel de l'avancement du programme. Le CDF relève toutefois que la durée prévue des tâches n'est pas rendue dans la représentation. Ainsi, il est plus difficile de visualiser l'impact du retard d'une des tâches sur les autres tâches et sur la date de fin du programme. Or, un projet de migration applicative au moins risque de durer au-delà de la date de fin prévue du programme. Ce risque doit pouvoir être mieux cerné, notamment pour pouvoir décider de l'activation d'un plan alternatif en cas de retard du programme.

Recommandation 1 (Priorité 1)

Le CDF recommande à la CdC d'améliorer les éléments du suivi temporel des tâches du programme. Il s'agit notamment de visualiser l'impact du retard des tâches situées sur le chemin critique sur la date de fin prévue du programme.

Prise de position de la CdC

La recommandation est acceptée.

Le programme a veillé à découpler les tâches du programme de façon à ce qu'un retard local n'impacte pas durablement l'ensemble du planning du programme de Rehosting. Il subsiste pourtant des dépendances qui feront l'objet d'une documentation précise afin de mettre en évidence le chemin critique à considérer pour la planification du programme.

2.5 Gestion des risques et de la qualité : des développements en cours

La gestion des risques et de la qualité au sein du programme est confiée depuis octobre 2018 à un spécialiste externe. Il est rattaché directement au mandant du programme, son rôle est défini par référence à la méthodologie HERMES. Ses prestations sont décrites en

détail dans son contrat. Les processus de suivi des risques et de la qualité ainsi que les résultats attendus sont également décrits.

Les risques sont identifiés au niveau des projets et suivis sur une base hebdomadaire, les mesures compensatoires sont définies. Les probabilité d'occurrence, les impacts et l'effet des mesures sont consignés sur une base mensuelle dans le Cockpit IKT. Un historique de l'évolution de ces éléments est également disponible. Les risques sont ensuite consolidés au niveau du programme et remontés sur demande aux instances de pilotage. Au moment de la révision, la CdC annonce les cinq risques suivants comme étant les plus importants du programme:

- Résistance au changement
- Achats pour la migration du système de Content Management
- Exploitation défectueuse
- Ressources insuffisantes
- Complexité et maturité des tests.

Dans le cadre de la gestion de la qualité, les points suivants sont considérés :

- Conformité des résultats HERMES
- Conformité des processus de livraison et de mise en production (y compris qualité des résultats techniques et tests).

La conformité des résultats HERMES est suivie au niveau des projets par des listes de contrôle et des plans de vérification. Un état d'avancement de la documentation par projet est édité dans le cadre du suivi du programme. Le CDF a par contre constaté que les plans de vérification contenus dans les plans de gestion de projets ne sont pas systématiquement tenus à jour.

Pour chaque projet, des concepts de tests détaillant les modalités de l'inspection de la qualité des résultats techniques sont prévus. Les types de tests sont définis en fonction de la nature de l'objet à contrôler. Concernant les composantes de l'infrastructure, là aussi divers tests sont exécutés, entre autres de performance et de charge. Pour les migrations applicatives, les concepts de test ne sont pas encore tous disponibles, leur élaboration est en cours. Selon les cas, le choix des types de test à exécuter (par exemple tests de non-régression) est laissé aux responsables applicatifs (RA). Il est également prévu que ces derniers coordonnent l'implication des utilisateurs finaux selon la nécessité.

Un spécialiste dédié suit la définition, l'organisation et l'exécution des tests, ainsi que les tâches correctives. Des outils le soutiennent dans ses tâches et lui permettent d'éditer divers rapports de contrôle de l'état des tests que le CDF a pu consulter.

Appréciation

L'organisation et les processus de la gestion des risques et de la qualité sont globalement adéquats. Le CDF juge plausible l'inventaire des cinq risques les plus importants du programme. Il s'interroge pourtant sur l'absence d'un risque sur la tenue des délais du programme. Les derniers développements dans le projet de migration Java DB2 Websphere pourraient en effet mettre en danger la date de fin de programme. La situation va pouvoir être analysée à la faveur du prochain rapport sur les risques du programme.

Sur le plan de la gestion de la qualité, le CDF constate que l'inspection de la conformité des résultats HERMES est bien outillée. Toutefois, les listes de contrôles dans les plans de gestion de projet sont partiellement périmées. Du côté des migrations applicatives, les concepts de tests ne sont pas tous disponibles. La planification de la charge liée aux tests est ainsi encore incertaine. Le CDF voit aussi dans la délégation aux RA du choix des types de test le risque qu'ils soient incomplets. Pour des raisons de cohérence et de contrôle, le choix des types de tests par les RA doit être validé par le spécialiste des tests.

Recommandation 2 (Priorité 2)

Le CDF recommande à la CdC de veiller à la mise à jour des documents de la gestion de la qualité et des tests. Pour les migrations applicatives, les plans de vérification et les concepts de tests doivent notamment être actualisés et finalisés. Pour ceux-ci, les types et la couverture de test définis doivent être validés par le spécialiste des tests.

Prise de position de la CdC

La recommandation est acceptée.

Pour permettre l'exécution de tests en qualité et en quantité suffisantes pour garantir une mise en œuvre impeccable, 2 testeurs externes ont été engagés le 2 mars 2020 en renfort des responsables d'application, l'un pour le projet Migration Natural/Adabas et le second pour le projet Migration Java/DB2. Par ailleurs les métiers ont été dotés de ressources supplémentaires pour faire face au volume de tests considérable qui est anticipé.

2.6 Choix des variantes de solution : une démarche fondée mais insuffisamment documentée

Lors de la phase d'initialisation du programme en 2016, la CdC a analysé deux grands types de variantes d'hébergement de ses applications : l'hébergement sur une nouvelle plateforme à l'OFIT et la mise en place d'une infrastructure sur site à la CdC. Les réflexions sur les possibilités d'un hébergement sur l'infrastructure d'un fournisseur extérieur (par exemple selon un modèle « Platform as a Service »[3]) ont été vite abandonnées. Pour la CdC, les impératifs de la sécurité de l'information et le manque d'expérience parlaient contre ce type de solution. Ces réflexions n'ont toutefois pas été documentées.

Un rapport d'analyse documente le processus de choix des variantes. A l'intérieur des deux grands types de variantes considérées, des sous-variantes et des ébauches d'architectures-cibles ont été élaborées. La CdC a ensuite choisi une sous-variante de l'option « hébergement sur site ». Pour l'option de l'hébergement à l'OFIT, elle a demandé au fournisseur de prestations le chiffrage de cinq sous-variantes. Au final, une seule offre pour une des cinq sous-variantes demandées a été remise à la CdC. Elle a utilisé une grille d'analyse à huit critères (inclus le retour sur investissement) et comparé les deux sous-variantes de solution. Elle conclut que l'hébergement sur site est la meilleure solution. Dans le rapport d'analyse, des commentaires expliquent les notes attribuées aux sous-variantes par critère. La sous-variante sur site présente un profil de coûts (in-

[3] Plateforme en tant que Service (PaaS), modèle d'informatique en nuage (cloud computing), dans lequel un fournisseur propose des outils matériels et logiciels en tant que service via Internet, permettant au client de développer et de maintenir des applications.

vestissements + maintenance sur cinq ans) nettement plus favorable que l'hébergement à l'OFIT. Les documents remis donnent par contre peu d'explications sur les hypothèses de calcul de ce profil de coûts.

Une fois la sous-variante choisie au niveau du programme, la CdC a approfondi l'étude des variantes de solutions pour les différents projets. Le CDF a pu prendre connaissance des études produites dans ce cadre.

Appréciation

La démarche de choix des variantes de solution est globalement fondée et les critères de choix utilisés sont pertinents. Le CDF estime toutefois que la mise à l'écart de la variante d'hébergement sur une infrastructure en nuage aurait dû être mieux documentée. De même, le CDF ne peut pas juger de la qualité des chiffres de coûts (investissements + maintenance) utilisés pour la comparaison des variantes. Les hypothèses de calcul ne sont pas explicitées. De plus, celles-ci auront sûrement changé avec l'avancement des projets. La valeur du retour sur investissement estimé est ainsi obsolète. Cet élément est important pour préparer les prochaines décisions stratégiques d'hébergement de la plateforme.

Recommandation 3 (Priorité 2)

Le CDF recommande à la CdC d'actualiser son calcul de retour sur investissement pour la variante de solution choisie. Les hypothèses de calcul doivent être explicitées et l'analyse doit être validée par le service « Finance et Controlling » de la CdC.

Prise de position de la CdC

Concernant la documentation d'une infrastructure en nuage, en 2017 une solution en infrastructure en nuage externe à la confédération n'était pas autorisée par l'UPIC et le nuage interne de l'OFIT n'était pas disponible. C'est la raison pour laquelle cette solution n'a pas prise en compte pour des raisons de sécurité des données.

Nous produirons un ROI intermédiaire en fin de conception du dernier projet (ECM), donc courant 2020, puis un ROI final à la fin du programme.

2.7 La première étape de l'évolution architecturale est en cours

Divers résultats architecturaux sont produits au sein du programme, ils se concentrent sur la couche infrastructurelle de la solution. Déjà en phase d'initialisation, des ébauches des architectures-cibles sont éditées (voir ci-dessus). En phase de concept, une architecture technique cible de la solution choisie est élaborée, elle forme la base de la mise en œuvre de l'infrastructure. Cet artefact n'a toutefois pas été validé de manière documentée par le comité des architectes comme le prévoit le règlement de la CdC. Les critères de validation d'une architecture (« definition of done ») en phase de concept ne sont par ailleurs pas explicités.

En phase de réalisation, l'architecture-cible est retravaillée itérativement. Les travaux s'inscrivent dans le sillage de la feuille de route technologique de la CdC qui est largement alignée sur la stratégie technique de l'OFIT. Les différents aspects de détails sont approfondis dans des études spécialisées et des preuves de concept sont élaborées par des sociétés externes. L'installation et la configuration de l'infrastructure se poursuivent pendant l'audit. Une étape de la planification architecturale est donc en passe d'être atteinte avec la finalisation de la mise en œuvre de l'infrastructure, prévue au printemps 2020.

En 2017, l'UPIC a accordé une extension de la dérogation à la CdC pour l'exploitation de l'infrastructure du programme de Rehosting. Elle pose ainsi la base légale pour la mise en œuvre de cette infrastructure sur site (première étape) mais assortit sa décision d'une condition : dès 2025, les services et composantes d'infrastructure doivent être rapatriés vers le réseau de centres de calcul de la Confédération (deuxième étape). Toutes les mesures doivent ainsi être prises pour permettre un rapatriement facile et économique. L'usage de service standards est notamment préconisé. La CdC doit en outre fournir une planification de cette deuxième étape dès 2021.

Appréciation

Les résultats architecturaux de la première étape de la migration forment une base de travail globalement adéquate pour la mise en œuvre du programme Rehosting. Le CDF n'a pas constaté d'infraction majeure aux instructions et modèles de référence en matière d'architecture informatique de la Confédération. A l'avenir, la CdC doit cependant veiller à faire valider formellement et de manière fondée les artefacts produits par le comité ad hoc. Le CDF attend en outre que la planification de la deuxième étape de la migration soit élaborée comme prévu.

2.8 L'implication de l'exploitation doit continuer de se renforcer

Avec le programme de Rehosting, le service de l'exploitation informatique de la CdC va hériter d'une infrastructure plus conséquente que celle qu'il gérait auparavant. Le degré de complexité va aussi augmenter. La CdC répond à ce défi par l'augmentation de l'effectif de ce service (passé de trois à sept équivalents temps en une année) et par un plan de formation de son personnel. En parallèle, le domaine de l'exploitation et de l'infrastructure a été réorganisé, un nouveau responsable de domaine prend ses fonctions en novembre 2019.

L'intégration des spécialistes de l'exploitation dans le programme s'est accompagnée de frictions avec certains groupes d'intervenants, notamment avec les architectes. Les vues sur les choix techniques ont divergé, des conflits de personnes s'en sont ensuivis. Un spécialiste externe de la gestion du changement a été appelé en renfort pour traiter la situation. Les protagonistes s'accordent à dire aujourd'hui que les divergences sont largement aplanies. Des incertitudes subsistent cependant sur la planification détaillée des tâches des spécialistes de l'exploitation pour le programme et sa faisabilité.

Le programme est l'occasion pour la CdC d'expérimenter les méthodes agiles. Une initiative existe et les principes d'agilité à la CdC sont énoncés. Des éléments de gestion agile sont mis en œuvre, notamment des cycles courts de travail (cadences et sprints), des « cérémonies » agiles et des listes d'arriérés (« backlog »). Les leçons de l'utilisation de ces méthodes sont régulièrement tirées pour ajuster la situation. Les pratiques de type DevOps (intégration du développement et de l'exploitation informatique) sont encore naissantes.

Appréciation

La mise en œuvre d'une infrastructure de la taille de celle du programme a un fort impact sur les activités de l'exploitation informatique. Cet aspect est reconnu au sein du programme. Une grande partie des difficultés initiales de l'intégration de l'exploitation est résolue. Le CDF note que les activités en vue de la montée de compétences du domaine sont en cours. Il relève toutefois que la mue du domaine n'est pas encore achevée et que la collaboration avec le programme reste un point sensible. Le CDF salue les initiatives actuelles pour mettre en œuvre des pratiques agiles. Il est d'avis néanmoins que les pratiques

de type DevOps sont encore à un stade très rudimentaire. Une intégration plus poussée de l'exploitation dans le processus de développement peut conduire à une baisse des coûts des projets. Le changement organisationnel et culturel, corollaire de ce type de démarche, doit se poursuivre et être dument accompagné.

Recommandation 4 (Priorité 1)

Le CDF recommande à la CdC de définir les bases d'une intégration plus poussée de l'exploitation au sein du programme, tels que des principes de type DevOps et un calendrier de mise en œuvre. La planification des tâches des ressources de l'exploitation pour le programme doit également être révisée.

Prise de position de la CdC

La recommandation est acceptée.

Une intégration plus poussée dans l'agilité est une première étape réussie pour le domaine Infrastructure et la mise en place d'un fonctionnement DevSecOps reste l'objectif de la SI au-delà du programme de Rehosting.

2.9 Le défi de la sécurité de l'information

L'hébergement à la CdC de l'infrastructure supportant ses applications et sa modernisation ont des conséquences importantes en termes de sécurité de l'information. La transmission des données est toujours assurée au travers du service standard géré par l'UPIC. Avec le programme, le matériel (serveurs) et les couches logicielles de base (système d'exploitation, services infrastructurels) sont par contre sous la responsabilité de la CdC. Celle-ci conserve aussi ses prérogatives sur les couches applicatives.

Un responsable de la sécurité de l'information et de la protection des données (SIPD) est en charge de cet aspect pour le programme. Les objets de protection sont définis : en plus des applications à migrer, l'infrastructure constitue elle-même un objet de protection. Pour la trentaine d'applications, la documentation de sécurité n'a pas été systématiquement actualisée ou revalidée. Pour la partie infrastructure, une analyse actuelle des besoins de protection existe, tout comme une version intermédiaire du concept SIPD. Ce dernier adresse les exigences relatives à la protection de base mais les besoins accrus de sécurité n'y sont pas encore traités. Une analyse complémentaire de sécurité a été menée par un prestataire externe durant l'été 2019. Des rapports sont édités, un plan d'action existe. Au moment de la révision, les mesures correctives définies étaient en cours de mise en place. La description et la planification de la mise en œuvre des processus de sécurité liés à l'exploitation de la nouvelle plateforme sont aussi en cours d'élaboration.

Un des projets du programme vise à mettre en œuvre le service standard de gestion de l'identité et de l'accès de l'UPIC (Identity and Access Management) pour les applications de la plateforme migrée. Une documentation de sécurité actuelle existe pour ce projet qui est en phase de réalisation. Un élément important pour une meilleure sécurité des accès aux applications est donc en cours de mise en place.

Appréciation

Le CDF estime essentiel que la sécurité de l'information soit assurée sur la nouvelle plateforme et relève les nombreuses initiatives en cours dans ce domaine. Il considère toutefois que le volume de travail restant est très important (documentation, mise en œuvre, vérification de l'efficacité des mesures), sur le plan de l'infrastructure, des applications et des processus de sécurité. Pour le CDF, la planification de la suite des travaux dans le domaine de la sécurité de l'information n'est pas encore aboutie.

Recommandation 5 (Priorité 1)

Le CDF recommande à la CdC de produire un état de situation consolidé et réactualisé de la mise en œuvre de mesures de protection pour les objets du programme. Une planification réaliste de la suite des travaux en matière de sécurité de l'information doit aussi être mise sur pied. La CdC veillera à ce que les concepts de sécurité de l'information et de protection des données soient revalidés et incluent une analyse réactualisée des risques résiduels. Celle-ci doit être validée par la Direction.

Prise de position de la CdC

La recommandation est acceptée.

À titre indicatif les mesures suivantes ont déjà été décidées par la CdC :

- Responsable SIPD: Un responsable SIPD du programme a été désigné pour consolider, produire la documentation et aider à planifier la mise en place de tous les éléments de sécurité du programme. Les documents de sécurité seront revus et les risques résiduels présenté au directeur.
- Formations ciblées: Pour sensibiliser et ancrer une culture de la sécurité à la SI, des formations ciblées pour chaque métier de la SI seront organisées en 2020 : une formation de « base » pour toutes les collaboratrices et les collaborateurs de la SI (y compris les managers) et des formations ciblées pour le Design (architectes / business analysts), le Build (développeurs) et le Run (Administrateurs systèmes, exploitation et bases de données).
- Mise en place d'une cellule de sécurité opérationnelle dédiée: Il s'agit de faire travailler ensemble des architectes spécialisés dans la sécurité et des analystes sécurité pour que les travaux de sécurité opérationnelle (patchage des serveurs, vérifications les liens transmettant des mots de passe en HTTPS, changement des mots passes administrateurs, etc.…) soient effectués régulièrement et documentés.
- Mise en place d'un contrôle de conformité: Il s'agit de mettre en place un contrôle indépendant pour vérifier que les travaux de sécurisation opérationnelle sont bien effectués et pour informer le chef de division de tout écart. Les travaux en matière de sécurité de l'information seront planifiés et intégrés dans la planification des projets.
- Architectes de solutions Le rôle d'architecte de solution sera renforcé en tant que relais garant des bonnes pratiques de sécurité opérationnelle.

Annexe 1 : Bases légales

Texte législatif
Ordonnance sur l'informatique dans l'administration fédérale (OIAF) du 9 décembre 2011, RS 172.010.58

Annexe 2 : Abréviations

CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
OFIT	Office fédéral de l'informatique et de la communication
RA	Responsable applicatif
SIPD	Sécurité de l'information et protection des données
UPIC	Unité de pilotage informatique de la Confédération

Annexe 3 : Glossaire

Agile (méthode)	Groupe de pratiques de pilotage et de réalisation de projets. Ces méthodes se veulent pragmatiques, impliquent fortement le demandeur et permettent une grande réactivité à ses demandes. Elles consacrent également des cycles courts de livraison des produits.
Backlog	Liste d'arriérés, liste des choses à faire pendant une itération de travail agile
Commission informatique	Organe de direction stratégique de l'informatique de la CdC
Cockpit IKT	Outil de contrôle de gestion pour les projets informatiques et les applications de l'administration fédérale
DevOps	Mouvement en ingénierie informatique visant à l'unification du développement logiciel et de l'administration des infrastructures, notamment l'administration système.
HERMES	eCH-0054: HERMES Méthode de management de projets HERMES est une méthode de management de projets pour l'informatique, les services et prestations de services ainsi que l'organisation des affaires. Elle a été développée au sein de l'administration fédérale. Cette méthode est à disposition du public, selon les standards de l'Association eCH.
IAM	Identity and Access Management, service standard de gestion de l'identité et de l'accès, géré par l'UPIC
Mainframe	Architecture informatique basée sur un ordinateur central de grande puissance et un réseau de terminaux
PaaS	Plateforme en tant que Service (Platform as a Service), modèle d'informatique en nuage, dans lequel un fournisseur propose des outils matériels et logiciels en tant que service Web, permettant au client de développer et de maintenir des applications
Rehosting	Ré-hébergement, changement de l'infrastructure informatique abritant des applications ou des services d'un prestataire vers un autre ou d'une plateforme vers une autre

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).