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

Audit de la plateforme de numérisation

Secrétariat général du Département fédéral des finances

CDF-18532 | Prises de position incluses | 31.07.2019 | DélFin D5/2019

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	1.18532.600.00183
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

L'essentiel en bref 4

Das Wesentliche in Kürze 6

L'essenziale in breve 8

Key facts 10

1 Mission et déroulement 13

1.1 Contexte 13

1.2 Objectif et questions d'audit 13

1.3 Etendue de l'audit et principe 14

1.4 Documentation et entretiens 14

1.5 Discussion finale 14

2 Pilotage des activités et état des travaux 15

2.1 Les objectifs et les ressources sont adéquatement définis 15

2.2 Des premières applications livrées, un transfert de connaissances qui monte en puissance 16

2.3 Davantage de transparence requise dans le pilotage en place 17

2.4 Les frictions architecturales doivent être mieux gérées 19

3 Gestion de projet, développement et exploitation 21

3.1 Une gestion de projet adaptée, quelques aspects à compléter 21

3.2 Le cycle de développement est approprié, mais comporte quelques lacunes 23

3.3 Le modèle d'exploitation doit encore gagner en maturité 24

Annexe 1: Bases légales 26

Annexe 2: Abréviations 27

Annexe 3 : Glossaire 28

Audit de la plateforme de numérisation
Secrétariat général du Département fédéral des finances

L'essentiel en bref

La plateforme de numérisation (DIP) est une unité administrative du Département fédéral des finances (DFF). Depuis 2019, elle officie comme fournisseur de prestations informatiques pour le DFF et bénéficie durant quatre ans d'une exception à l'article 23 de l'Ordonnance sur l'informatique dans l'Administration fédérale (OIAF). La DIP développe et exploite des applications soutenant la numérisation de processus de bénéficiaires de prestation du département. Parallèlement, elle fonctionne comme un laboratoire d'essai de méthodes et technologies innovantes. Pour 2019, la DIP dispose d'un budget de 7,1 millions de francs. Le Contrôle fédéral des finances (CDF) a examiné si le pilotage des activités, le processus de développement, la gestion des projets de la DIP et l'exploitation sont judicieusement menés.

Des premiers résultats encourageants, mais des améliorations à apporter au pilotage

Après quelques 18 mois d'existence, la DIP a déployé trois applications et microservices. Elle a aussi engrangé de l'expérience dans l'emploi de techniques modernes de développement. D'autres travaux sont en cours et, selon les objectifs prévus, le transfert des connaissances a commencé. Les buts de la DIP et ses ressources sont adéquatement définis pour une phase de démarrage. Néanmoins, le partage des ressources de management avec l'Administration fédérale des contributions (AFC) ainsi que la position et le statut de la DIP doivent faire l'objet de réflexions.

Le pilotage stratégique de la DIP est du ressort direct du chef du DFF, certes avec l'aide du Secrétariat général et d'un comité de pilotage. Les bases de la gestion du portefeuille sont définies. Les modalités du choix des priorités des projets doivent toutefois être plus transparentes, dans l'optique d'une hausse des mandats de développement de la DIP. La partie du pilotage devrait encore être améliorée, notamment le suivi de l'atteinte des objectifs et la gestion des risques. Le CDF a fait une recommandation dans ce sens.

Des « frictions architecturales » se sont fait jour lors de développements de la DIP. Les nouvelles technologies mises en œuvre empiètent en partie sur les pratiques et standards établis de l'informatique fédérale. Par exemple, le microservice PAMS de la DIP concurrence partiellement le service standard IAM de la Confédération de l'Unité de pilotage informatique de la Confédération (UPIC). Un compromis pour une recherche commune de solutions ne s'est dessiné qu'après de longues discussions. Autre exemple, l'utilisation du langage de programmation Go par la DIP. Ce langage n'est supporté ni par l'Office fédéral de l'informatique et de la télécommunication (OFIT), ni par un autre prestataire de services interne. La maintenance des applications des développements en Go risque donc de ne plus être assurée à moyen terme. Le CDF recommande d'établir un mécanisme de résolution de ces conflits architecturaux.

Gestion de projet et développement : les bases sont adéquates, mais doivent être complétées

Une méthodologie de projet pour les développements agiles est suivie à la DIP et incorpore les points de contrôle du déroulement des projets. Elle contient aussi une liste des documents requis. Des outils permettent le suivi systématique de l'avancement des travaux. Divers aspects doivent toutefois être mieux décrits dans la méthodologie, notamment la gestion des risques et les détails des changements dans les développements agiles. Dans cette phase de démarrage, le CDF n'a pas pu vérifier que les documents requis étaient produits dans tous les cas. Dans un cas précis, le CDF recommande d'actualiser les documents de sécurité.

Les étapes du développement sont définies adéquatement. En particulier, le traitement des besoins et les tests sont effectués systématiquement et avec la participation des domaines métier. Le CDF estime toutefois que les aspects des contrôles applicatifs et de la sécurité ne sont pas suffisamment incorporés au processus de développement agile. Il a fait une recommandation dans ce sens.

L'exploitation technique est assurée, les détails de son organisation sont encore incertains

Trois applications productives sont actuellement en exploitation. Elles se trouvent sur l'infrastructure technique en nuage de l'OFIT. Sur les plans techniques et organisationnels, l'exploitation de la DIP est séparée des grandes plateformes de l'AFC. A ce jour, aucun impact n'a été constaté sur le reste des applications fiscales.

Les responsabilités des différents intervenants de l'exploitation sont définies. Le déploiement des modifications apportées aux applications de la DIP est en grande partie automatisé. En outre, le processus de passage en production est encadré par diverses étapes de validation, y compris des tests par les utilisateurs. Les processus et les responsabilités de la gestion des incidents sont définis et sont en place. Le monitorage du fonctionnement de la plateforme est instauré et sa plus grande automatisation est prévue. Les divers intervenants sont en phase d'apprentissage dans la mise en œuvre de ces technologies. Les échanges d'expérience se poursuivent. Néanmoins, un flou subsiste sur certains détails de la répartition des tâches entre développeurs et spécialiste de l'exploitation. Les responsabilités de l'exploitation après la période de quatre ans accordée à la DIP ne sont pas définies. Les détails du fonctionnement et de l'organisation de l'exploitation restent donc à élaborer.

Prüfung der Plattform Digitalisierung
Generalsekretariat des Eidgenössischen Finanzdepartements

Das Wesentliche in Kürze

Die Plattform Digitalisierung (DIP) ist eine Verwaltungseinheit des Eidgenössischen Finanzdepartements (EFD). Seit 2019 ist sie IT-Leistungserbringerin für das EFD und als solches während vier Jahren von Artikel 23 der Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) ausgenommen. Die DIP entwickelt und betreibt Anwendungen, mit denen die Digitalisierung der Prozesse von Leistungsbezügern des Departements unterstützt werden. Parallel dazu ist sie ein Versuchslabor für innovative Methoden und Technologien. Die DIP verfügt für 2019 über ein Budget von 7,1 Millionen Franken. Die Eidgenössische Finanzkontrolle (EFK) hat geprüft, ob die Steuerung der Tätigkeiten, der Entwicklungsprozess, das Projektmanagement der DIP und ihr Betrieb ordnungsgemäss erfolgen.

Erste ermutigende Ergebnisse, aber Verbesserungsbedarf bei der Steuerung

Die DIP hat in den 18 Monaten ihres Bestehens drei Anwendungen und Mikrodienste entwickelt. Ausserdem hat sie Erfahrung im Einsatz moderner Entwicklungsmethoden gesammelt. Weitere Arbeiten sind in Gang und der Wissenstransfer hat, gemäss den vereinbarten Zielen, begonnen. Die definierten Ziele und Ressourcen der DIP sind für eine Anlaufphase angemessen. Die gemeinsame Nutzung von Managementressourcen mit der Eidgenössischen Steuerverwaltung (ESTV) sowie die Position und den Status der DIP müssen jedoch Gegenstand von Überlegungen sein.

Die strategische Steuerung der DIP fällt in die direkte Zuständigkeit des Vorstehers des EFD, wenn auch mit der Unterstützung des Generalsekretariats sowie eines Steuerungsausschusses. Die Grundlagen für das Portfolio-Management sind definiert. Die Modalitäten der Schwerpunktsetzung der Projekte müssen allerdings im Hinblick auf eine Zunahme der Entwicklungsaufträge der DIP transparenter definiert werden. Auch bei der Steuerung besteht Verbesserungsbedarf, namentlich was die Kontrolle der Zielerreichung und das Risikomanagement angeht. Die EFK hat eine entsprechende Empfehlung abgegeben.

Im Zuge der Weiterentwicklung der DIP sind «Reibungspunkte in der Systemarchitektur» zutage getreten. Einige der neu umgesetzten Technologien greifen partiell in die Praxisvorgaben der Bundesinformatik und in deren Standards ein. So konkurrenziert der Mikrodienst PAMS der DIP teilweise den Standarddienst IAM des Bundes vom Informatiksteuerungsorgan des Bundes (ISB). Erst nach langwierigen Diskussionen zeichnete sich ein Kompromiss für die gemeinsame Lösungssuche ab. Ein weiteres Beispiel ist die Verwendung der Programmiersprache Go durch die DIP. Für diese Programmiersprache bieten weder das Bundesamt für Informatik und Telekommunikation (BIT) noch andere interne Leistungserbringer einen Support an. Es besteht also das Risiko, dass die Wartung der Entwicklungsanwendungen in Go mittelfristig nicht mehr gewährleistet sein wird. Die EFK empfiehlt für solche Architekturfragen die Errichtung eines Konfliktlösungsmechanismus.

Projektmanagement und Entwicklung: Grundlagen sind angemessen, aber ergänzungsbedürftig

Die DIP befolgt eine Projektmethodik für agile Entwicklungen, die auch verschiedene Kontrollpunkte hinsichtlich des Projektablaufs beinhaltet. Diese Methodik enthält ferner eine Liste aller erforderlichen Dokumente. Tools ermöglichen die systematische Nachverfolgung des Arbeitsfortschritts. Einige Aspekte in der Methodologie, unter anderem das Risikomanagement und die Änderungen in den agilen Entwicklungen, müssen noch besser beschrieben werden. In der Anlaufphase konnte die EFK nicht überprüfen, ob die geforderten Unterlagen in jedem Fall erstellt wurden. In einem spezifischen Fall empfiehlt die EFK die Sicherheitsunterlagen zu aktualisieren.

Die Entwicklungsetappen sind angemessen definiert. Insbesondere die Bedarfsbearbeitung und die Tests werden systematisch und unter Einbezug der betroffenen Geschäftsbereiche durchgeführt. Die EFK vertritt jedoch die Auffassung, dass die Aspekte Anwendungskontrollen und Sicherheit nicht ausreichend in den Prozess der agilen Entwicklung eingebettet sind. Sie hat eine entsprechende Empfehlung abgegeben.

Der technische Betrieb ist gewährleistet, die organisatorischen Details sind noch nicht geklärt

Aktuell sind drei produktive Anwendungen in Betrieb. Sie befinden sich auf der technischen Cloud-Infrastruktur des BIT. In technischer und organisatorischer Hinsicht wird die DIP getrennt von den grossen Plattformen der ESTV betrieben. Bisher wurden keinerlei Auswirkungen auf die übrigen Steueranwendungen festgestellt.

Die betrieblichen Verantwortlichkeiten der einzelnen Akteure sind definiert. Die Änderungen an den Anwendungen der DIP erfolgen weitgehend automatisch. Ausserdem sind dem Prozess der Produktionsaufnahme verschiedene Validierungsetappen, einschliesslich Benutzertests, vorgelagert. Für die Handhabung von Zwischenfällen sind im System entsprechende Prozesse und Verantwortlichkeiten definiert und implementiert. Implementiert ist auch die Überwachung des Betriebs der Plattform, deren stärkere Automatisierung ist vorgesehen. Die verschiedenen Akteure sind dabei, die Umsetzung dieser Technologien zu erlernen. Der Erfahrungsaustausch geht weiter. Bei einzelnen Punkten in der Aufgabenverteilung zwischen Entwicklern und Betriebsfachleuten besteht allerdings noch Klärungsbedarf. Die Verantwortlichkeiten für den Betrieb nach Ablauf der vierjährigen Zeitspanne, die der DIP eingeräumt wurde, sind nicht definiert. Die Details der Funktionsweise und der betrieblichen Organisation müssen folglich noch ausgearbeitet werden.

Originaltext auf Französisch

Verifica della piattaforma per la digitalizzazione
Segreteria generale del Dipartimento federale delle finanze

L'essenziale in breve

La piattaforma per la digitalizzazione (DIP) è un'unità amministrativa del Dipartimento federale delle finanze (DFF). Dal 2019 la DIP funge da fornitore di prestazioni informatiche per il DFF e per quattro anni beneficia di un'eccezione all'articolo 23 dell'ordinanza sull'informatica nell'Amministrazione federale (OIAF). Essa sviluppa e gestisce applicazioni supportando la digitalizzazione dei processi riguardanti i beneficiari di prestazioni del Dipartimento. Parallelamente, la DIP funziona quale laboratorio di prova per tecnologie e metodi innovativi. Per il 2019 essa dispone di un budget di 7,1 milioni di franchi. Il Controllo federale delle finanze (CDF) ha verificato se la direzione strategica delle attività, il processo di sviluppo, la gestione dei progetti della DIP e l'esercizio sono stati effettuati correttamente.

Primi risultati incoraggianti, occorre tuttavia apportare miglioramenti nella direzione strategica

Dopo circa 18 mesi dal suo avvio, la DIP ha introdotto tre applicazioni e microservizi, accumulando esperienze nell'utilizzazione di tecniche moderne di sviluppo. Altri lavori sono in corso e, in base agli obiettivi previsti, il trasferimento delle conoscenze è iniziato. Gli obiettivi della DIP e le sue risorse sono stati definiti in modo adeguato per la fase di avvio. Tuttavia, la ripartizione con l'Amministrazione federale delle contribuzioni (AFC) delle risorse per la gestione, il ruolo e lo statuto della DIP devono essere oggetto di riflessioni.

La direzione strategica della DIP spetta direttamente al capo del DFF, ovviamente con l'aiuto della Segreteria generale e di un comitato direttivo. Le basi della gestione del portafoglio sono definite. Le modalità di scelta delle priorità dei progetti devono tuttavia essere più trasparenti, in vista di un maggiore numero di mandati di sviluppo della DIP. Occorrerebbe migliorare ulteriormente la parte relativa alla direzione strategica, in particolare la verifica del raggiungimento degli obiettivi e la gestione dei rischi. Il CDF ha formulato una raccomandazione in questo senso.

Durante lo sviluppo della DIP si sono verificati attriti a livello di architettura informatica. Le nuove tecnologie interferiscono in parte con la prassi e gli standard definiti dall'informatica federale. Ad esempio, il microservizio PAMS della DIP fa in parte concorrenza al servizio standard IAM della Confederazione all'Organo direzione informatica della Confederazione (ODIC). È stato possibile giungere a un compromesso per una ricerca comune di soluzioni solo dopo lunghe discussioni. Un altro esempio è dato dal linguaggio di programmazione Go utilizzato dalla DIP. Questo linguaggio non è supportato né dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT) né da un altro fornitore di servizi interno. La manutenzione delle applicazioni per i futuri sviluppi di GO rischia pertanto di non essere più garantita a medio termine. Il CDF raccomanda di istituire un meccanismo di risoluzione di questi conflitti dell'ambito dell'architettura.

Gestione del progetto e sviluppo: le basi sono adeguate, ma devono essere completate

La DIP applica una metodologia di progetto per il raggiungimento di uno sviluppo agile, che comprende i punti di controllo relativi allo svolgimento dei progetti e un elenco dei documenti richiesti. Strumenti permettono di verificare costantemente lo svolgimento dei lavori. Occorre tuttavia descrivere più dettagliatamente differenti aspetti metodologici, in particolare la gestione dei rischi e i dettagli relativi ai cambiamenti concernenti lo sviluppo agile. In questa fase di avvio il CDF non è stato in grado di verificare se i documenti richiesti fossero allestiti per ogni caso. In un caso specifico, il CDF raccomanda di aggiornare i documenti di sicurezza.

Le fasi di sviluppo sono definite in modo adeguato. Viene monitorato in particolare il fabbisogno e i test sono effettuati sistematicamente con la partecipazione dei settori specialistici. Il CDF ritiene tuttavia che gli aspetti relativi ai controlli dell'applicazione e alla sicurezza non siano sufficientemente inclusi nel processo di sviluppo agile. Il CDF ha formulato una raccomandazione in questo senso.

Il funzionamento tecnico è garantito, ma i dettagli della sua organizzazione sono ancora incerti

Tre applicazioni produttive sono attualmente in esercizio, reperibili sull'infrastruttura tecnica cloud dell'UFIT. Sul piano tecnico e organizzativo, il funzionamento della DIP è autonomo rispetto alle grandi piattaforme dell'AFC. Nessun impatto è stato finora rilevato sulle altre applicazioni fiscali.

Sono state anche definite le responsabilità dei diversi partecipanti all'esercizio. L'introduzione delle modifiche apportate alle applicazioni della DIP è in gran parte automatizzata. Inoltre, il processo di messa in produzione è contrassegnato da differenti fasi di convalida, compresi i testi effettuati dagli utenti. I processi e le responsabilità della gestione degli incidenti sono definiti e applicati. Il monitoraggio concernente il funzionamento della piattaforma è avviato ed è previsto di automatizzarlo il più possibile. I diversi partecipanti sono in fase d'apprendimento nell'attuazione di queste tecnologie. Gli scambi di esperienze proseguono. Tuttavia permane una zona d'ombra su alcuni dettagli in merito alla ripartizione dei compiti tra sviluppatori e specialisti. Le responsabilità concernenti il funzionamento dopo il periodo di quattro anni concesso alla DIP non sono state ancora definite. I dettagli concernenti il funzionamento e l'organizzazione dell'esercizio sono quindi ancora da definire.

Testo originale in francese

Audit of the digitisation platform
General Secretariat of the Federal Department of Finance

Key facts

The digitisation platform (DIP) is an administrative unit of the Federal Department of Finance (FDF). Since 2019, it has been acting as an IT service provider for the FDF and has been exempt from Article 23 of the Ordinance on Informatics and Telecommunications in the Federal Administration (FAITO) for four years. The DIP develops and operates applications that support the digitisation of processes of service recipients in the department. At the same time, it serves as a laboratory for testing innovative methods and technologies. The DIP has a budget of CHF 7.1 million for 2019. The Swiss Federal Audit Office (SFAO) has examined whether the management of activities, the development process, the management of DIP projects and operations are being carried out properly.

Encouraging initial results, but management requires improvements

After some 18 months in existence, the DIP has deployed three applications and microservices. It has also gained experience in the use of modern development techniques. Further work is underway and, according to the planned objectives, knowledge transfer has begun. The aims of the DIP and its resources are adequately defined for a start-up phase. Nevertheless, the sharing of management resources with the Federal Tax Administration (FTA) and the position and status of the DIP should be considered.

The strategic management of the DIP is the direct responsibility of the Head of the FDF, albeit with the assistance of the General Secretariat and a steering committee. The basis for portfolio management is defined. However, the procedures for selecting project priorities must be more transparent, with a view to increasing the DIP's development mandates. The management aspect should be further improved, in particular monitoring the achievement of objectives and risk management. The SFAO has made a recommendation to this effect.

"Architectural frictions" have emerged during DIP developments. The new technologies that have been implemented partly encroach on the established practices and standards of federal IT. For example, the DIP's PAMS microservice partially competes with the Confederation's standard IAM service of the Federal IT Steering Unit (FITSU). A compromise to find common solutions was only reached after long discussions. Another example is the use of the Go programming language by the DIP. This language is not supported by the Federal Office of Information Technology, Systems and Telecommunication (FOITT) or by any other internal service provider. The maintenance of applications for Go developments may therefore no longer be ensured in the medium term. The SFAO recommends that a mechanism be established to resolve these architectural conflicts.

Project management and development: groundwork is adequate but needs completing

At the DIP, a project methodology for agile developments is followed that incorporates project flow control points. It also contains a list of required documents. Tools are available to systematically monitor work progress. However, various aspects need to be better described in the methodology, including risk management and details of changes in agile developments. In this start-up phase, the SFAO could not verify that the required documents were produced in all cases. In one specific case, the SFAO recommends updating the security documents.

The development stages are adequately defined. In particular, needs processing and tests are carried out systematically and with the participation of the business sectors. However, the SFAO considers that application controls and security aspects are not sufficiently incorporated into the agile development process. It has made a recommendation to this effect.

Technical operation is assured, organisational details still uncertain

Three productive applications are currently in operation. They are located on the FOITT's cloud-based technical infrastructure. From a technical and organisational point of view, the operation of the DIP is separate from the major platforms of the FTA. To date, no impact has been observed on the rest of the fiscal applications.

The responsibilities of the various operational stakeholders are defined. The deployment of changes to DIP applications is largely automated. In addition, the process of transition to production is supported by various validation steps, including user testing. Incident management processes and responsibilities are defined and in place. The monitoring of the platform's operations has been implemented and greater automation is planned. The various stakeholders are in the learning phase of implementing these technologies. Experiences continue to be shared. However, there is still some uncertainty concerning certain details of the division of tasks between developers and operations specialists. Operating responsibilities after the four-year period granted to the DIP are not defined. Details of the working and organisation of the operations are therefore still to be defined.

Original text in French

Prise de position générale des audités

> Aufgrund der aktuellen Veränderungen, Empfehlungen aus der «Arbeitsgruppe Hug» und der neu zu besetzenden Leitung des BIT, wurde der Übertrag der Mitarbeitenden von der ESTV an das ISB sistiert. Der Direktor a. i. des BIT hat den Auftrag zu prüfen, ob allenfalls die DIP in das BIT integriert werden soll.

1 Mission et déroulement

1.1 Contexte

La plateforme de numérisation (Digitalisierungsplattform, ci-après DIP) est une unité administrative du Département fédéral des finances (DFF). Elle a pour objectif de développer des petites et moyennes applications soutenant la numérisation des processus des bénéficiaires de prestations. La DIP a démarré ses travaux le 1er janvier 2018 comme projet pilote au sein de l'Administration fédérale des contributions (AFC). Elle bénéficie depuis le 1er janvier 2019 d'une exception à l'article 23 alinéa 1 de l'Ordonnance sur l'informatique et la télécommunication dans l'administration fédérale (OIAF). Cet article stipule qu'un département dispose en principe d'un fournisseur de prestations interne au plus.

Pour le DFF, la nature des travaux de la DIP est trop spécifique pour bénéficier des gains en synergie d'une centralisation. L'intégration au sein d'un fournisseur de prestations interne existant prétériterait le caractère innovateur de la DIP et son efficience. L'exception demandée a été accordée pour quatre ans, elle permet à l'unité administrative de fournir des prestations de développement et d'exploitation d'applications. Au moment de la révision, quatre offices du DFF bénéficient d'une exception à l'article 23 alinéa 1 de l'OIAF : la Centrale de compensation, la DIP, l'Office fédéral des constructions et de la logistique et l'Unité de pilotage informatique de la Confédération (UPIC).

Rattachée administrativement à l'UPIC, la DIP dispose pour 2019 d'un budget global de quelque 7,1 millions de francs et de 37 équivalents plein temps. Le montant budgété comprend des frais de personnel à hauteur de 6,1 millions de francs (86 % du total).

1.2 Objectif et questions d'audit

Dans son examen des activités de la DIP, le Contrôle fédéral des finances (CDF) s'intéresse aux aspects suivants :

- Pilotage (fixation des objectifs, sélection et développement des projets)
- Processus de développement (gestion des besoins, tests, intégration)
- Produits développés
- Gestion de projet (surveillance, gestion des risques)
- Exploitation (impacts et gestion du changement).

Il vise à répondre aux questions suivantes :

- Les activités de la DIP sont-elles pilotées de manière appropriée ?
- Le processus de développement est-il judicieux ?
- Les projets de la DIP sont-ils menés de manière efficace ?
- Une exploitation sûre et durable des applications est-elle assurée ?

1.3 Etendue de l'audit et principe

L'audit a été mené en deux phases, la première du 25 octobre au 30 novembre 2018, la seconde du 29 avril au 17 mai 2019. Il a été conduit par André Stauffer (responsable de révision) et Hans Ulrich Wiedmer, sous la responsabilité de Bernhard Hamberger. La discussion des résultats a eu lieu le 27 mai 2019. Le présent rapport ne prend pas en compte les développements ultérieurs à cette discussion.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par la DIP. 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 27 juin 2019 en présence des personnes suivantes :

- Le responsable de la division principale des ressources de l'AFC
- Le responsable de la division informatique de l'AFC
- Le responsable des ressources du DFF
- Un responsable de centre de compétence du CDF
- Le responsable de révision du 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 Pilotage des activités et état des travaux

2.1 Les objectifs et les ressources sont adéquatement définis

Élaborée fin 2017, la mission de la DIP consiste à développer des compétences dans le domaine de la numérisation à travers la mise en œuvre d'applications. Ces activités ont un caractère d'innovation et de laboratoire d'essai, l'expérience engrangée est destinée à être partagée avec toutes les unités intéressées. Parallèlement, des applications informatiques productives doivent résulter des travaux de la DIP afin de soutenir la numérisation des processus des bénéficiaires de prestations et la mise en œuvre de processus de cyberadministration. Dans un premier temps, ce sont des processus des unités administratives du DFF qui feront l'objet des travaux de la DIP.

En 2018, la DIP a fonctionné comme projet-pilote de l'AFC, avec l'objectif d'être institutionnalisée à début 2019. Ce but a été atteint avec la demande d'exception à l'article 23 de l'OIAF, accordée pour quatre ans dès le 1er janvier 2019. Le dispositif accompagnant la demande d'exception complète ces objectifs de manière plus spécifique et décrit les détails des conditions-cadres applicables à la DIP.

Pour 2019, sa première année d'activité en tant que fournisseur de prestations informatiques, la DIP se voit attribuer un budget global de quelque 7,1 millions de francs. Ce montant comprend des charges de personnel à hauteur d'environ 6,1 millions de francs (86 %), pour un effectif de 37 équivalents plein temps.

Le budget 2019 fixe en outre les buts détaillés de la DIP dans les termes suivants :

- Mise à disposition de services (au moins quatre applications ou microservices)
- Transparence (mise à disposition de chiffres clés sur le progrès des projets)
- Efficience dans la fourniture de prestations (au moins 60 % de temps des développeurs passés sur des projets)
- Information (minimum deux publications internes et deux séances d'informations).

Le financement est assuré par des cessions de crédit des offices bénéficiant des prestations de la DIP, selon une clé de répartition fixée pour l'année. Ces cessions se matérialisent par un mécanisme de transfert de collaborateurs des offices clients sur les projets de réalisation de la DIP. Une partie de ces collaborateurs est assignée de façon permanente à la DIP. Selon la mission définie, aucun nouveau poste ne peut être créé pour la DIP. Les activités des développeurs de la DIP sont saisies sur un centre de coûts de l'UPIC. Celui-ci refacture les prestations aux bénéficiaires au prix coûtant sur la base des heures saisies par les développeurs sur les différents projets. Un outil soutient la saisie et la validation de ces heures.

La direction de la DIP et certains de ses services partagés (par ex. architecture informatique, sécurité) sont assurés par des collaborateurs et cadres de la division principale des ressources et de la division informatique de l'AFC. Pour ces personnes, la charge de travail découlant de ces tâches en parallèle peut s'avérer substantielle.

Appréciation

Pour le CDF, les objectifs de la DIP sont fixés de manière appropriée. La mission s'inscrit dans le sillage de la mesure prioritaire « Début du passage à l'administration numérique » de l'axe stratégique S01 (« Orientation vers les affaires ») du plan directeur informatique de la Confédération. Les priorités du développement sont définies, assorties de buts mesurables, de même que les principes du transfert de connaissance.

Le CDF prend note des modalités de la mise à disposition du personnel de la DIP. Le modèle de la cession temporaire favorise le transfert de connaissances vers les bénéficiaires de prestations. Le CDF ne dispose pas d'indices lui permettant de conclure que ce modèle prétérite certains domaines des bénéficiaires de prestations, notamment l'exploitation informatique de l'AFC. Pour l'encadrement et certains spécialistes transverses, la double casquette n'est par contre pas un modèle durable à terme. Une réflexion sur l'organisation et la position de la DIP doit aboutir avant la fin du mandat de fournisseur de prestations.

Parallèlement, des travaux d'analyse sont en cours sur les moyens de favoriser la transformation digitale et sur l'organisation de l'informatique fédérale. Ces travaux et les développements dans le domaine de la stratégie informatique de l'Administration fédérale pourraient avoir un impact profond sur le futur de la DIP.

2.2 Des premières applications livrées, un transfert de connaissances qui monte en puissance

En regard de ces objectifs, les réalisations de la DIP étaient les suivantes lors de la révision :

- Mise en œuvre productive d'applications et microservices (composantes logicielles) :
    - myTaxWorld, portail d'accès à l'AFC, inclus le microservice pour l'identification, l'authentification et l'accès (Polymorphic Access Management System, PAMS)
    - SIA, application de l'AFC d'échange spontané d'informations
    - AIA-DIP, application de l'AFC d'échange automatique d'informations
- Développement d'applications et de microservices en cours:
    - F85, formulaire électronique de l'AFC pour la récupération de l'impôt anticipé pour les résidents allemands
    - Portails d'accès du DFF et de l'Administration fédérale des douanes
- Prototypes d'applications et de microservices :
    - Prototype eTVA, application de l'AFC pour le remboursement de la taxe à la valeur ajoutée
    - Prototype dOperations, application pour l'automatisation des opérations de maintenance et monitorage des applications et microservices de la DIP
    - Essai OutSystems, plateforme de développement d'applications.

La DIP a également poursuivi diverses activités de transfert de connaissance (ateliers, formation, échange d'expériences) et de formalisation du savoir (concepts, méthodologies).

Pour 2019 et les années suivantes, le développement des applications suivantes de l'AFC est planifié:

- CbCR, reporting pays par pays
- eTVA, remboursement de la taxe à la valeur ajoutée
- eDVS, gestion électronique des remboursements
- eMWST, traitement des décomptes de la TVA.

Une étude sur la collaboration entre la plateforme easyGov du Secrétariat à l'économie (SECO) et la DIP est également planifiée.

Appréciation

En mettant trois applications et microservices en production, la DIP a fourni des premiers résultats concrets qui s'inscrivent dans la lignée des objectifs définis. D'autres développements sont en cours. Le CDF relève aussi que des expériences sont récoltées dans l'emploi de technologies et de méthodes de développement récentes. Le transfert de connaissances prend de l'ampleur. Ces éléments du bilan sont positifs. Le CDF n'a toutefois pas vérifié le nombre et le niveau de satisfaction des utilisateurs des nouvelles applications.

2.3 Davantage de transparence requise dans le pilotage en place

Avec l'aide du Secrétariat général, le chef du DFF assure le pilotage stratégique des activités de la DIP. Le comité de pilotage, instance consultative du pilotage stratégique, a commencé à se réunir périodiquement. Il regroupe la direction du Secrétariat général, les directeurs des offices du DFF clients potentiels de la DIP et les directeurs des offices transversaux. Le CDF note qu'une autre instance définie dans la mission de la DIP, le « Sounding board », groupe d'échange avec les offices intéressés, n'a pas démarré ses travaux.

La mission de la DIP décrit les principes du choix des projets à mettre en œuvre. Ce sont les critères de l'utilité présentée par l'application et l'urgence pour le DFF qui doivent primer. Dans les faits, la sélection des projets s'effectue sur la base d'une première liste établie par la direction de la DIP. Des projets de l'AFC ont ainsi constitué la grande majorité de la dizaine de propositions contenues dans cette liste. Ceux-ci sont issus du processus de sélection des projets de l'AFC (le Multiprojektmanagement, MPM). Le chef du DFF a par la suite priorisé ces propositions pour aboutir au plan des applications à développer.

Le progrès des activités est discuté lors des réunions périodiques du comité de pilotage. En outre, l'état des travaux fait l'objet d'échanges réguliers entre le chef du DFF, le Secrétariat général et la direction de la DIP. Au niveau du pilotage, plusieurs outils sont utilisés pour le suivi des projets en cours : ceux-ci sont contenus dans le Cockpit TIC de l'UPIC, comme tous les autres projets informatiques. Ils font aussi l'objet de rapports de projet mensuels, qui informent sur l'évolution des développements, des coûts et des risques, ainsi que sur la tenue des délais. Un tableau de bord contenant un ensemble de valeurs clés (le « dashboard DIP ») suit par ailleurs l'évolution des activités de la DIP. Ce dashboard DIP permet de visualiser des informations telles que l'évolution du pipeline de développement, la capacité disponible ou encore l'utilisation des ressources. En revanche, il ne permet pas un suivi des buts détaillés mentionnés plus haut.

Le CDF note que l'évolution de la situation des risques ne figure pas explicitement à l'agenda des réunions du comité de pilotage.

Appréciation

Les travaux de la DIP sortent à peine de la phase de démarrage et le portefeuille de projets est encore réduit. L'importance stratégique accordée à la numérisation et le caractère innovant demandent une attention soutenue de la part du management. Dans ces conditions, le CDF ne voit pas d'inconvénient majeur à un pilotage direct par le chef du DFF, avec le soutien des autres instances de pilotage. Le statut du « Sounding board » devra être clarifié.

Le CDF estime par contre que le processus actuel de gestion du portefeuille des projets de la DIP est peu transparent. Or, les demandes de développement de la part de l'ensemble des offices du DFF, et d'autres départements, sont appelées à augmenter. Dans cette perspective, les tenants et les aboutissants des décisions de priorisation des projets devraient être mieux explicités et communiqués. Pour boucler le cycle de la gestion du portefeuille des projets, les statistiques de l'utilisation effective des applications et microservices réalisés (par ex. nombre d'utilisateurs annoncés, nombre de formulaires saisis, etc.) ne sont pas systématiquement calculées. Ces données livrent pourtant des indications précieuses sur la pertinence de la sélection des projets et devraient être mises à disposition des décideurs.

Des processus et outils de suivi au niveau pilotage sont utilisés. Le CDF note toutefois que divers éléments ne sont pas suivis systématiquement dans le cadre des outils et processus de pilotage en place. La situation des risques et les progrès dans l'atteinte des buts détaillés de la DIP devraient notamment être mieux suivis.

Recommandation 1 (Priorité 2)

Le CDF recommande au Secrétariat général du DFF de prendre les mesures pour améliorer la transparence du processus de pilotage. Sont concernés notamment : la gestion du portefeuille de la DIP, les statistiques d'utilisation des applications développées, le suivi de l'atteinte des objectifs fixés à la DIP et la gestion des risques au niveau pilotage.

Prise de position des audités

Avec l'introduction de l'outil SciForma 7 au 1er juin 2019 (Instrument de Control), la DIP a intégré la gestion détaillée des objectifs à atteindre. Chaque objectif fait l'objet d'une quantification et d'un monitoring de l'effort consenti. Les statistiques d'utilisation des applicatifs ne sont en revanche pas concernées par l'introduction de SciForma. Ce chapitre sera pris en charge dans le cadre du développement du moteur dOperations en cours de développement. La réalisation de dOperations ne figurant pas dans le Main Stream des projets constituant la feuille de route actuelle de la DIP, cet applicatif joue le rôle de « Lückenfüller ». En ce sens, les délais fixés par la DIP jusqu'à sa mise en œuvre définitive sont de 18 mois, soit Q1 2021.

Gestion des risques

Cette mesure sera intégrée dans la refonte des processus IT en cours. Elle sera clairement identifiable et mise en œuvre entre le 1er janvier et le 30 juin 2020 (période d'implémentation des nouveaux processus et des workflows)

2.4 Les frictions architecturales doivent être mieux gérées

Parmi les divers éléments des conditions-cadres des activités de la DIP, le CDF relève notamment :

- L'exception accordée de travailler comme fournisseur de prestations informatiques du DFF, limitée à quatre ans
- La DIP doit développer des solutions permettant aux utilisateurs internes et externes à l'Administration fédérale d'accéder facilement aux systèmes back-end importants
- La possibilité de déroger à certaines instructions du domaine de l'informatique fédérale, sur la base d'une exception accordée par le Conseil fédéral ou l'UPIC, et à condition que la sécurité de l'information soit assurée.

Le CDF rappelle le caractère hybride de la mission de la DIP, laboratoire d'expérimentation et fournisseur de prestations réalisant des applications et services productifs. Ces deux facettes coexistent dans le contexte de l'informatique fédérale actuelle, avec ses règles, ses acteurs et le poids de son paysage existant. Cette constellation a donné naissance à des tensions avec l'Office fédéral de l'informatique et de la télécommunication (OFIT) et l'UPIC. Certains produits de la DIP et l'emploi de certaines technologies sortent du cadre de référence actuellement défini. A ce jour, aucune demande d'exception n'a été cependant demandée par la DIP.

Dans le domaine des services d'identification et d'authentification, la DIP a produit par exemple le microservice PAMS. Celui-ci concurrence en partie le service standard IAM de la Confédération de l'UPIC. Après des mois de discussions infructueuses, un compromis s'est dessiné pour une recherche commune de solutions d'ici à l'automne. Dans ce cas, il est prévu que la gouvernance normale des services standards de l'UPIC s'applique à nouveau. Autre exemple, l'utilisation productive par la DIP du langage de programmation Go. Ce langage n'est supporté ni par l'OFIT, ni par un autre prestataire de services. Dans l'hypothèse du non-renouvellement de l'exception à l'Art. 23 OIAF pour la DIP, ces applications ne seraient plus maintenues à l'interne. Le problème n'est à ce jour pas résolu.

Appréciation

Au vu des standards et des règlements existants et de la double mission de la DIP, les tensions architecturales devraient persister avec les tenants établis de l'informatique fédérale. Elles seront d'autant plus importantes que les innovations proposées par la DIP se rapprocheront de la couche technique de l'architecture fédérale[1]. Des problèmes peuvent aussi survenir en relation avec la couche des données de base, dont les principes de règlement sont en cours d'élaboration. Le CDF constate que les conflits architecturaux issus de l'activité de la DIP sont pour l'instant résolus au coup à coup, dans un processus souvent long.

[1] Selon le référentiel TOGAF, il s'agit de la couche qui comporte le matériel, les composantes logicielles de bas niveau et les plateformes.

Le CDF estime que la DIP doit respecter les conditions-cadres qui lui sont posées. Les solutions de la DIP doivent s'intégrer dans l'architecture des systèmes back-end existants. Pour cette raison, les exceptions aux standards et aux règlements informatiques pour la mise en œuvre productive d'applications de la DIP ne devraient être accordées qu'avec parcimonie. La sécurité de l'information doit en outre être assurée dans tous les cas. Le mécanisme proposé dans la décision du Conseil fédéral sur la DIP prévoit le recours à des demandes d'exception, avec la validation du Conseil fédéral ou de l'UPIC. Il doit être appliqué. Pour les éléments ne relevant pas de standards établis de l'informatique fédérale (par exemple architectures techniques de référence des fournisseurs de prestations), un mécanisme de résolution des conflits architecturaux manque. Dans tous les cas, les activités de coordination de la DIP avec les gros projets et les fournisseurs de prestations informatiques de l'administration fédérale doivent se poursuivre.

Recommandation 2 (Priorité 1)

Le CDF recommande au Secrétariat général du DFF d'établir un mécanisme de résolution des conflits architecturaux informatiques opposant les innovations de la numérisation et les architectures techniques de référence des fournisseurs de prestations.

Prise de position des audités

En cours de réalisation. Le sujet sera abordé à l'occasion du groupe de travail Hug.

3 Gestion de projet, développement et exploitation

3.1 Une gestion de projet adaptée, quelques aspects à compléter

Une méthode spécifique (« HERMES@ESTV agile »), documentée dans un guide d'utilisation, est mise en œuvre pour la gestion des projets de la DIP. Elle reprend les bases de la méthode HERMES de la Confédération, mais contient des extensions décrivant les modalités du développement agile selon le cadre de travail Scrum. Pour les projets de la DIP, la méthode définit notamment :

- l'organisation à adopter : rôles traditionnels et rôles agiles
- les phases et les points de contrôle à respecter
- les méthodes et outils à utiliser pour le suivi de projets
- les résultats à produire : documents, artefacts techniques.

Selon un processus inspiré de la gestion multiprojets de l'AFC, une première planification est effectuée lors de la phase d'avant-projet. Dans cette phase, sur la base des besoins exprimés, une charge de travail (jours-hommes de développement) et les coûts de projet sont estimés. La charge de travail est mise en regard de la capacité de développement disponible. Si le projet reçoit le feu vert, les capacités nécessaires sont réservées. Les développeurs rapportent par la suite les heures de travail sur les projets. Des outils spécialisés dans la gestion des projets agiles soutiennent et documentent ces étapes du processus.

La gestion des risques du projet s'effectue principalement dans le logiciel de suivi de projets Jira. Pour chaque projet suivi, des risques peuvent être identifiés et saisis et des responsables assignés. La méthode utilisée mentionne le plan de gestion de projet comme résultat obligatoire de la phase de concept. Ce plan contient un chapitre dédié à la gestion des risques. Par contre, la méthode ne contient pas de chapitre particulier ou de détails sur la manière de gérer les risques dans un environnement agile.

La méthode décrit les différents rapports d'état de projet requis ainsi que les outils à utiliser. Au niveau du projet, Jira est utilisé pour suivre l'avancement des itérations de développement, en termes de points ouverts ou réglés et d'heures de développement consommées. Des rapports d'état détaillés peuvent être édités à la demande et sont discutés lors des réunions de suivi des itérations de projet (« sprints »). Ces données relatives à l'avancement sont consolidées périodiquement dans le cockpit TIC et les rapports d'états mensuels. Ceux-ci contiennent des indications relatives à l'évolution des risques des projets. Le dashboard DIP est également mis à jour. Les rapports d'état d'avancement sont discutés à différents niveaux de l'organisation et à différents niveaux de détail.

Le traitement des demandes de changements dans les projets suit deux processus, selon l'importance du changement. Une majorité des demandes dans les projets sont absorbées dans le processus de développement agile (par exemple, extensions fonctionnelles). Ces demandes sont incorporées dans le carnet de produit (« product backlog » la liste des spécifications fonctionnelles), visible en tout temps par les représentants métier. Pour les demandes de plus grande importance (par exemple augmentation substantielle des coûts budgétés ou dépassement des délais prévus), une demande de modification formelle doit être établie et validée par le donneur d'ordre. Pour cette première période d'activité, le DIP

n'a pas enregistré pour les projets en cours ou achevés de modification nécessitant une demande formelle de changement. Cette typologie et le mécanisme de traitement ne sont pas décrits dans la méthodologie.

Le CDF a examiné trois projets (deux terminés et un en cours) et a contrôlé pour une sélection de résultats requis s'ils avaient été documentés conformément à la méthodologie. Les documents requis de cette sélection ont été élaborés à quelques exceptions près : la pré-réception du système informatique (Vorabnahme) de la phase réalisation manque pour les deux applications en production. Le protocole de validation du système pour une des applications en production était en cours de finalisation.

En outre, le CDF note que le microservice PAMS a été développé dans un premier temps conjointement à l'application SIA. Pour ce microservice, qui occupe une place centrale dans l'architecture du DIP, les documents n'ont pas été produits séparément. Une analyse des besoins de protection et un concept de sécurité de l'information et de protection des données spécifiques font donc défaut.

Appréciation

Pour le CDF, la gestion de projet est fondamentalement adaptée à la nature des travaux. Une méthodologie de projet adéquate est définie et mise en œuvre. Des étapes de planification, d'exécution, de contrôle et de correction sont définies et suivies au sein des projets. Dans les grandes lignes, les processus et outils mis en œuvre permettent une surveillance appropriée de l'état d'avancement des projets.

Le CDF estime toutefois que divers aspects de la méthodologie sont incomplets. La gestion des risques en environnement agile est notamment insuffisamment traitée. De même, la description des cas et de la marche à suivre lors de changements dans un projet agile (périmètre, coûts ou délais prévus) manque. Le CDF a également remarqué que les rôles prescrits dans les équipes de projets ne comprenaient ni les représentants de l'exploitation ni ceux des contrôles applicatifs et de la sécurité informatique.

Sur la base de l'échantillon des résultats sélectionné, le CDF n'a pas pu vérifier que tous les documents requis étaient disponibles. Il souligne que la méthodologie n'était pas encore finalisée au moment de la mise en production des deux projets terminés. Pour le CDF, il n'est pas nécessaire de documenter *a posteriori* les résultats manquants (pré-réception) pour les projets déjà terminés. La DIP veillera toutefois à documenter les projets en cours et futurs conformément à la méthodologie. Par ailleurs, le CDF estime que les documents de sécurité pour le microservice PAMS doivent être édités et validés.

Recommandation 3 (Priorité 2)

Le CDF recommande à la DIP de compléter les documents méthodologiques sur les aspects de la gestion des risques en environnement agile, la gestion des demandes de modification dans les projets et les rôles (représentants de l'exploitation, des contrôles applicatifs et de la sécurité informatique).

Prise de position des audités

Cette mesure sera intégrée dans la refonte des processus IT en cours. Elle sera clairement identifiable et mise en œuvre entre le 1er janvier et le 30 juin 2020 (période d'implémentation des nouveaux processus et des workflows).

Recommandation 4 (Priorité 1)

Le CDF recommande à la DIP d'éditer et de valider des documents de sécurité séparés pour le microservice PAMS.

Prise de position des audités

En cours de réalisation. Les documents seront disponibles au plus tard le 30 octobre 2019.

3.2 Le cycle de développement est approprié, mais comporte quelques lacunes

Pour les travaux de la DIP, les techniques du développement agile de type Scrum sont mises en œuvre. Dans un premier temps, les exigences fonctionnelles des utilisateurs sont répertoriées. Elles sont reprises pour la production automatisée d'un prototype destiné à faciliter la discussion avec le domaine métier. Dans un deuxième temps, les exigences des processus à réaliser sont systématiquement saisies dans l'outil de gestion des projets agiles Jira. Les détails des fonctions désirées et les contraintes à respecter sont décrits dans des critères d'acceptation. Une première version des exigences est consignée dans un document validé par le représentant du domaine métier (« propriétaire du produit » ou « Product owner »). La liste des besoins identifiés et pas encore mis en œuvre forment le carnet de produit. Dans l'esprit agile, ces exigences sont appelées à évoluer, selon les besoins du domaine métier. Ce sont les développeurs qui modifient les exigences dans l'outil Jira, mais le propriétaire du produit peut en tout temps accéder au carnet de produit.

Le CDF constate que les aspects des contrôles applicatifs et de la sécurité de l'information ne sont pas systématiquement pris en compte dans le traitement des besoins. Pour le second, la méthodologie employée prescrit certes une analyse des besoins de sécurité et un concept de sécurité de l'information et de protection des données. Ces points ne sont toutefois pas systématiquement repris dans les critères d'acceptation et intégrés au développement. Le CDF note que des tests de pénétration sont organisés pour les applications.

La production et la documentation des logiciels de la DIP se basent sur une chaine d'outils qui soutient les cycles de développement itératif (« Sprints »). Le développement vise à mettre à disposition des composantes réutilisables sous la forme de microservices (par exemple le PAMS). A ce jour, il n'existe pas de répertoire publié et de description normée (fonction, interfaces de programmation, propriétaires) des microservices. Le concept réglant la définition et la gouvernance des services de l'AFC est en cours d'élaboration.

Un concept de test général existe pour les travaux de la DIP. Un concept de test spécifique est aussi édité pour chaque projet. Les cas de test doivent refléter les critères d'acceptation définis dans le carnet de produit. Les tests se déroulent en premier lieu lors des itérations, par les développeurs. A la fin d'une itération, une version du produit est transportée en environnement de test et remise aux utilisateurs métier. Ceux-ci procèdent aux tests fonctionnels et se prononcent sur l'acceptation du produit. Un journal des tests est tenu et validé. Les erreurs constatées sont consignées dans l'outil Jira et intégrées dans le carnet de produit. Le processus de test est facilité par divers outils supplémentaires.

L'architecture de la solution forme un des résultats du processus de développement. Elle doit être documentée et doit respecter les principes architecturaux en vigueur au sein du domaine informatique de l'AFC. Ceux-ci règlent notamment les modalités de l'intégration des solutions de la DIP avec la plateforme informatique centrale de l'AFC, Core-IT (issue du

projet Fiscal-IT). L'architecte informatique de l'AFC est d'ailleurs impliqué dans le processus de développement de la DIP. Il participe à la validation des architectures des applications développées.

Dans le modèle de développement de la DIP, ce sont les domaines métier qui portent la responsabilité de l'introduction des nouveaux produits. La DIP les soutient en cas de besoin, notamment pour la formation et la préparation des scénarios de tests.

Appréciation

Pour le CDF, la gestion des besoins des utilisateurs est systématique et valablement documentée. Les exigences en terme de contrôles applicatifs et de sécurité de l'information ne sont toutefois pas suffisamment prises en compte et manifestées dans le processus de développement (« security by design »). Les porteurs de ces aspects devraient être représentés dans l'équipe de développement. Les domaines métier, eux, sont représentés de manière appropriée tout au long du processus de développement.

Le CDF estime que le processus de test et sa documentation sont définis de manière adéquate. Le déroulement décrit assure que les erreurs constatées soient traitées. Le CDF n'a toutefois pas vérifié que les documents de test soient édités systématiquement.

Le CDF relève que la description de la gouvernance des services doit encore être finalisée. Il rappelle que les microservices sont appelés à être utilisés dans toute l'Administration fédérale et les cantons. Sur le plan des architectures de solutions, il note que le processus défini assure leur intégration dans le paysage informatique de l'AFC. Par contre, comme il l'a relevé plus haut, des frictions avec les architectures du niveau de la Confédération sont encore en cours de résolution.

Recommandation 5 (Priorité 1)

Le CDF recommande à la DIP d'intégrer de manière accrue les aspects et représentants des contrôles applicatifs et de la sécurité de l'information dans le processus de développement.

Prise de position des audités

Cette mesure sera intégrée dans la refonte des processus IT en cours. Elle sera clairement identifiable et mise en œuvre entre le 1er janvier et le 30 juin 2020 (période d'implémentation des nouveaux processus et des workflows).

3.3 Le modèle d'exploitation doit encore gagner en maturité

Trois applications de la DIP sont actuellement en cours d'exploitation. Celle-ci est basée sur un modèle à trois niveaux, avec des intervenants différents. La couche applicative et processus est sous la responsabilité des domaines métier, une première couche logicielle (microservices) sous celle de la DIP, et la couche infrastructurelle sous celle de l'OFIT.

Les applications productives de la DIP sont hébergées sur la plateforme Atlantica Cloud de l'OFIT (informatique en nuage privée). C'est une offre de service de conteneurs (Containers as a Service, CaaS) qui est mise en œuvre. Cette offre et la technologie qui la sous-tend sont récentes. Elles présentent diverses difficultés, notamment un certain flou dans la délimitation des responsabilités entre développeurs et spécialistes de l'exploitation. L'offre fait l'objet d'une collaboration continue entre les spécialistes de la DIP et ceux de l'OFIT, mais un modèle organisationnel durable n'est pas encore établi.

Sur le plan des opérations, un processus de gestion des incidents est décrit et les responsabilités définies. Des tickets sont saisis en cas d'incident. Après analyse des statistiques des incidents, le CDF n'a pas constaté de problème particulier de fonctionnement et de disponibilité des applications. Du fait de l'hébergement sur une plateforme séparée, aucun impact n'a pu être constaté à ce jour en termes d'exploitation sur la plateforme centrale Core-IT de l'AFC. Le CDF note que la DIP prévoit d'introduire divers outils de surveillance de l'exploitation et de remédiation automatisées.

Un processus de passage en production (gestion des changements) existe, il repose sur un paysage système à quatre niveaux et diverses étapes de validation. Parmi celles-ci, le CDF note un rapport de phase de réalisation et la validation de la mise en production. Le CDF relève l'usage de pratiques de type « DevOps » : le déploiement des composantes est en partie automatisé et facilité par des outils de gestion de versions. Des cycles de développement et de mise en production courts (environ trois semaines) sont aussi mis en œuvre.

Appréciation

Le CDF note que l'exploitation technique fonctionne de manière satisfaisante pour les trois premiers applications et microservices productifs de la DIP. Tout en relevant le caractère novateur des plateformes techniques mises en œuvre, il constate les difficultés liées à l'organisation de l'exploitation. Pour le CDF, les premières bases de l'exploitation sont posées, mais son organisation est encore embryonnaire. La question de la responsabilité de l'exploitation après la fin du mandat de fournisseur de prestation de la DIP se pose notamment. Les travaux de définition de ces modalités et la collaboration avec l'OFIT doivent se poursuivre. L'architecture technique et l'organisation étant appelées à évoluer, le CDF renonce en l'état à vérifier l'efficacité des contrôles en place dans le domaine de l'exploitation et de la mise en production.

Annexe 1: Bases légales

Texte législatif
172.010.58 Ordonnance sur l'informatique et la télécommunication dans l'administration fédérale (OIAF) du 9 décembre 2011, état au 1er avril 2018
Messages et directives
Plan directeur concernant la stratégie informatique de la Confédération, édition 2018
Stratégie informatique de la Confédération 2016–2019

Annexe 2: Abréviations

AFC	Administration fédérale des contributions
CDF	Contrôle fédéral des finances
DFF	Département fédéral des finances
OFIT	Office fédéral de l'informatique et de la télécommunication
SECO	Secrétariat à l'économie
UPIC	Unité de pilotage informatique de la Confédération

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).

Annexe 3 : Glossaire

Agile (méthode)	Groupe de pratiques de pilotage et de réalisation de projets, reposant sur un cycle de développement itératif, incrémental et adaptatif
AIA-DIP	Application de l'AFC pour l'échange automatique d'informations
Atlantica Cloud	Offre de l'OFIT dans le domaine de l'informatique en nuage
CaaS	Container as a Service: Offre de technologies de conteneurs pour le développement et le déploiement dans le Cloud
CbCR	Application de l'AFC pour le reporting pays par pays
Cockpit TIC	Liste des projets et applications informatiques de la Confédération, gérée sous la houlette de l'UPIC
Core-IT	Plateforme informatique centrale de l'AFC soutenant les processus métier, fruit du projet Fiscal-IT
Dashboard	Table de bord regroupant des valeurs clés facilitant la gestion de projet ou d'unités administratives
DevOps	Mouvement et pratique de l'ingénierie informatique visant à l'unification du développement logiciel et de l'administration des infrastructures informatiques et des systèmes
DIP	Plateforme de digitalisation (Digitaliserungsplattform), unité administrative du DFF, dont l'objectif consiste à développer des applications soutenant la numérisation des processus de bénéficiaires de prestations
dOperations	Application de l'AFC pour l'automatisation des opérations de maintenance et surveillance des applications et microservices de la DIP
easyGov	Portail en ligne du SECO pour les entreprises suisses
eDVS	Application de l'AFC pour la gestion électronique des remboursements
eMWST	Application de l'AFC pour le traitement des décomptes de la TVA
eTVA	Application de l'AFC pour le remboursement de la taxe à la valeur ajoutée
Fiscal-IT	Projet informatique de l'AFC ayant donné naissance à la plateforme informatique Core-IT soutenant les processus métier

F85	Formulaire électronique de l'AFC pour la récupération de l'impôt anticipé pour les résidents allemands
Go	Langage de programmation développé par Google
HERMES	Méthode de management de projets de la Confédération, mise à disposition par l'UPIC
HERMES@ESTV agile	Méthode de management de projet et de développement agile de l'AFC, basée sur HERMES et complétée par des éléments spécifiques au développement agile
IAM de la Confédération	Service standard de l'UPIC pour l'identification et l'authentification d'utilisateurs
Jira	Logiciel de gestion de projets et de suivi de incidents
Microservice	Style d'architecture logicielle dans lequel les applications sont décomposées en plusieurs processus indépendants, faiblement couplés et souvent spécialisés dans une seule tâche
MPM	Multiprojektmanagement, processus de gestion multiprojets de l'AFC
myTaxWorld	Portail d'accès de l'AFC
Outsystems	Plateforme de développement d'applications Web et mobiles
PAMS	Polymorphic Access Management System, microservice réalisé par la DIP permettant l'identification des utilisateurs, leur authentification et les accès
Product backlog	Carnet du produit, liste ordonnée des éléments requis (besoin, amélioration, correctif) et unique source des besoins pour tous les changements à effectuer sur le produit
Product owner	Propriétaire du produit, rôle agile, représentant du client et de l'utilisateur dans le processus de développement
Scrum	Cadre de développement agile, basé sur une méthode de travail itérative
SIA	Application de l'AFC pour l'échange spontané d'informations
Sprint	Itération de développement dans la méthodologie Scrum
TOGAF	The Open Group Architecture Framework: Cadre et méthodologie d'architecture d'entreprise