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

Audit de suivi de la mise en œuvre des recommandations essentielles

Office fédéral de l'informatique et de la télécommunication, Administration fédérale des contributions

CDF-22737 | Prises de position incluses | 29 novembre 2022 | DélFin D1/2023

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	609.22737
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 de suivi de la mise en œuvre des recommandations essentielles

Office fédéral de l'informatique et de la télécommunication, Administration fédérale des contributions

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a mené un audit de suivi de la mise en œuvre des recommandations essentielles auprès de l'Office fédéral de l'informatique et de la télécommunication (OFIT). Il s'agit de sept recommandations émises lors de différents audits[1], dont cinq peuvent être clôturées et deux restent ouvertes.

Cinq recommandations peuvent être clôturées

La première de ces recommandations concernait l'Administration fédérale des contributions (AFC). En collaboration avec l'OFIT, l'AFC devait soumettre les portails en ligne à des tests de sécurité TIC supplémentaires. Le CDF estime que cette recommandation a été mise en œuvre.

Par ailleurs, l'OFIT devait planifier et effectuer régulièrement des tests « de bout en bout » dans le cadre des procédures de restauration du Central Identity Store, formaliser une procédure de gestion des changements dans l'environnement FileNet Dala, mettre en place un processus de recherche proactive d'informations sur les vulnérabilités dans l'environnement de gestion des appareils mobiles et enfin, définir plus clairement les processus de développement des applications mobiles. Pour le CDF, ces quatre recommandations ont été mises en œuvre.

Deux recommandations demeurent ouvertes

La première concerne la sauvegarde des documents reçus dans FileNet Dala uniquement dans un format pérenne conforme à la pratique des Archives fédérales suisses. La seconde réside dans la mise en œuvre des capteurs et des activités de surveillance sur l'ensemble du territoire des appareils mobiles.

Pour le CDF, ces deux recommandations ne sont pas mises en œuvre par l'OFIT.

[1] Le rapport d'audit « Projet informatique clé FISCAL-IT » (nr. d'audit 18466) est disponible sur le site Internet du CDF (www.cdf.admin.ch). Les rapports d'audit 18502, 19478 et 20206 ont été présentés à la Délégation des finances.

Nachprüfung der Umsetzung wesentlicher Empfehlungen

Bundesamt für Informatik und Telekommunikation, Eidgenössische Steuerverwaltung

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hat eine Nachprüfung zur Umsetzung wesentlicher Empfehlungen beim Bundesamt für Informatik und Telekommunikation (BIT) durchgeführt. Es geht um sieben im Rahmen verschiedener Prüfungen[1] abgegebene Empfehlungen, von denen fünf abgeschlossen werden können und zwei weiterhin offen sind.

Fünf Empfehlungen können abgeschlossen werden

Die erste dieser Empfehlungen betraf die Eidgenössische Steuerverwaltung (ESTV). Die ESTV sollte zusammen mit dem BIT die Online-Portale noch weiteren IKT-Sicherheitstests unterziehen. Nach Ansicht der EFK wurde diese Empfehlung umgesetzt.

Des Weiteren sollte das BIT End-to-End-Tests im Rahmen der Wiederherstellungsverfahren zum Central Identity Store planen und regelmässig durchführen, ein formalisiertes Verfahren für das Changemanagement in der FileNet-Dala-Umgebung festlegen, einen Prozess zur proaktiven Informationsbeschaffung bezüglich Verwundbarkeiten in der Mobile-Device-Management-Umgebung etablieren und schliesslich die Prozesse für die Entwicklung von Apps klarer definieren. Aus Sicht der EFK wurden diese vier Empfehlungen umgesetzt.

Zwei Empfehlungen weiterhin offen

Die erste Empfehlung betrifft das Abspeichern der in FileNet Dala erhaltenen Dokumente ausschliesslich in einem archivtauglichen Format entsprechend der Praxis des Schweizerischen Bundesarchivs. Die zweite Empfehlung bezieht sich auf die flächendeckende Implementierung der Sensorik und der Monitoring-Aktivitäten bei den mobilen Geräten.

Die EFK ist der Ansicht, dass diese beiden Empfehlungen vom BIT nicht umgesetzt wurden.

Originaltext auf Französisch

[1] Der Prüfbericht «IKT-Schlüsselprojekt FISCAL-IT» (PA 18466) ist auf der Website der EFK verfügbar (www.efk.admin.ch). Die Prüfberichte 18502, 19478 und 20206 wurden der Finanzdelegation vorgelegt.

Verifica successiva concernente l'attuazione di raccomandazioni importanti

Ufficio federale dell'informatica e della telecomunicazione, Amministrazione federale delle contribuzioni

L'essenziale in breve

Il Controllo federale delle finanze (CDF) ha verificato nuovamente l'attuazione di raccomandazioni di particolare rilevanza da parte dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT). Si tratta di sette raccomandazioni formulate in occasione di diverse verifiche[1], di cui cinque possono considerarsi attuate, mentre due sono ancora in sospeso.

Cinque raccomandazioni possono considerarsi attuate

La prima di queste raccomandazioni riguardava l'Amministrazione federale delle contribuzioni (AFC). In collaborazione con l'UFIT, l'AFC doveva sottoporre i portali online a ulteriori test di sicurezza delle TIC. Secondo il CDF, questa raccomandazione è stata attuata.

Inoltre, l'UFIT doveva pianificare ed eseguire regolarmente test «end-to-end» nel quadro delle procedure di ripristino del Central Identity Store, formalizzare una procedura di gestione dei cambiamenti nell'ambiente FileNet Dala, implementare una procedura di ricerca proattiva di informazioni sulle vulnerabilità nell'ambiente di gestione dei dispositivi mobili nonché definire in modo più chiaro i processi di sviluppo delle applicazioni mobili. Il CDF ritiene che queste quattro raccomandazioni siano state attuate.

Due raccomandazioni sono ancora in sospeso

La prima riguarda il salvataggio dei documenti ricevuti in FileNet Dala esclusivamente in un formato permanente secondo la prassi dell'Archivio federale svizzero. La seconda concerne l'implementazione di sensori e attività di monitoraggio per l'insieme dei dispositivi mobili.

Secondo il CDF, queste due raccomandazioni non sono state attuate dall'UFIT.

Testo originale in francese

[1] Il rapporto di verifica «Progetto chiave TIC Fiscal-IT» (n. della verifica 18466) è disponibile sul sito Internet del CDF (www.cdf.admin.ch). I rapporti di verifica 18502, 19478 e 20206 sono stati sottoposti alla Delegazione delle finanze.

Follow-up audit on the implementation of key recommendations

Federal Office of Information Technology, Systems and Telecommunication, Federal Tax Administration

Key facts

The Swiss Federal Audit Office (SFAO) conducted a follow-up audit on the implementation of key recommendations at the Federal Office of Information Technology, Systems and Telecommunication (FOITT). It concerned seven recommendations from various audits[1], five of which can be closed and two remain open.

Five recommendations can be closed

The first of these recommendations concerned the Federal Tax Administration (FTA). In collaboration with the FOITT, the FTA was to carry out additional ICT security tests on the online portals. The SFAO considers that the recommendation has been implemented.

In addition, the FOITT was urged to plan and carry out regular end-to-end tests as part of the recovery procedures for the Central Identity Store, to formalise a change management procedure for the FileNet Dala environment, to introduce a process for proactively searching for information on vulnerabilities in the mobile device management environment and, finally, to define the development processes for mobile applications more clearly. In the SFAO's view, these four recommendations have been implemented.

Two recommendations remain open

The first concerns saving incoming documents in FileNet Dala only in a permanent format in accordance with the practice of the Swiss Federal Archives. The second relates to the introduction of sensors and surveillance activities across the entire territory covered by mobile devices.

In the SFAO's view, neither of these recommendations has been implemented by the FOITT.

Original text in French

[1] The report "Key ICT project Fiscal IT" (audit mandate 18466) is available on the SFAO's website (www.sfao.admin.ch). The reports for audit mandates 18502, 19478 and 20206 were submitted to the Finance Delegation.

1 Mission et déroulement

1.1 Contexte

Après une série d'audits auprès de l'Office fédéral de l'informatique et de la télécommunication (OFIT), le Contrôle fédéral des finances (CDF) a vérifié la mise en œuvre de sept recommandations annoncées come réalisées.

1.2 Objectif et questions d'audit

L'objectif de l'audit de suivi était d'évaluer si les recommandations, restées en suspens, ont été mises en œuvre.

1.3 Étendue de l'audit et principe

L'audit a été mené du 15 août au 31 août 2022 par Warren Paulus (responsable de révision). Il a été conduit sous la responsabilité de Bernhard Hamberger. Le présent rapport ne prend pas en compte les développements ultérieurs à l'audit.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par l'OFIT. 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 19 octobre 2022. L'OFIT était représenté par le chef du département des services domestiques, le responsable business des solutions d'entreprise, une responsable de la conformité, le suppléant du responsable de la sécurité de SAP, le suppléant du responsable du domaine de Filenet Dala, et le responsable business des services de gestion des identités et des accès. L'AFC était représenté par un membre de l'inspection des finances ainsi que le suppléant d'un membre de la direction. Le CDF était représenté par le responsable de centre de compétence et 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

Dans cet audit de suivi, le CDF évalue individuellement les recommandations ouvertes.

2.1 Les tests de sécurité des portails ont eu lieu

Dans le cadre de l'audit « Prüfung des IKT Schlüsselprojektes FISCAL-IT », la recommandation suivante a été émise :

«Die EFK empfiehlt der ESTV, zusammen mit dem BIT die Online-Portale noch weiteren IKT-Sicherheitstests zu unterziehen.»

En réponse à cette recommandation (nr. d'audit 18466.003[2]), l'Administration fédérale des contributions (AFC) a élaboré une documentation pour la réalisation des tests d'intrusion et a chargé une entreprise externe d'effectuer ceux-ci. L'OFIT est chargé de corriger les problèmes de sécurité résultant de ces tests. Des tests d'intrusion sont effectués lorsqu'une nouvelle version ou des modifications importantes sont apportées aux applications. Toutefois, aucun test d'intrusion régulier n'est effectué sans modifications ou nouvelles versions.

L'OFIT réalise des scans applicatifs régulièrement. En plus de cela, l'AFC a un contrat avec l'OFIT pour trois scans applicatifs sur trois applications différentes par an. Le choix des applications à tester se fait après une discussion avec les responsables des applications. L'AFC a comme projet d'utiliser une plateforme de Bug Bounty.

Appréciation

Une meilleure collaboration a été mise en place entre l'AFC et l'OFIT en ce qui concerne les tests de sécurité des portails en ligne. Des contrôles de la plate-forme ont eu lieu. La documentation concernant les tests d'intrusion peut encore être améliorée en incluant des tests réguliers lorsqu'il n'y a pas de changements ou de nouvelles versions.

La recommandation 18466.003 est clôturée.

2.2 Les tests de bout en bout sont effectués lors du déploiement de nouvelle version

Dans le cadre de l'audit « Prüfung von Führung und Betrieb des Standarddienstes Identitäts- und Zugangsverwaltung », la recommandation suivante a été émise :

«Die EFK empfiehlt dem BIT, end-to-end-Tests im Rahmen der Wiederherstellungsverfahren zum Central Identity Store zu planen und regelmässig durchzuführen.»

En réponse à cette recommandation (nr. d'audit 18502[3]), l'OFIT a établi un calendrier pour tester la sauvegarde et la restauration des sauvegardes du CIS (Central Identity Store). Ce test est documenté dans leur outil de collaboration interne. Il est effectué manuellement tous les trois mois dans un environnement similaire à l'environnement de production,

[2] Le rapport d'audit 18466 est disponible sur le site Internet du CDF (www.cdf.admin.ch).
[3] Le rapport d'audit 18502 a été présenté à la Délégation des finances.

lorsqu'une nouvelle version est mise en production. Les sauvegardes du CIS sont conservées pendant deux ans. Les tâches et les tests à effectuer lors du lancement d'une nouvelle version sont documentés et suivis dans leur système interne de suivi des erreurs, de gestion des incidents et de gestion de projet. Ils effectuent des tests de bout en bout, jusqu'au niveau des systèmes finaux, lorsqu'il s'agit d'introduire de nouvelles fonctionnalités. Dans ce cas, ils travaillent avec les systèmes concernés et créent les tests nécessaires à l'introduction des fonctionnalités. Lors de l'introduction de nouvelles versions, ils effectuent également des tests de fin de cycle jusqu'au niveau des systèmes finaux. Ils mesurent ensuite les changements sur les systèmes finaux et décident de la validation de la version sur la base de ces mesures. Le CDF constat l'absence de tests de bout en bout comprenant la sauvegarde de la base de données du CIS, la création d'une nouvelle instance CIS, la restauration de la base de données du CIS et le test de la connectivité avec d'autres services. Toutefois, si une nouvelle instance du CIS doit être créée, les tests sont identiques à ceux d'une nouvelle version. Toutes les bases de données, la mémoire interne et les systèmes finaux sont vérifiés. La connectivité et les changements de données dus aux synchronisations sont testés.

Appréciation

Les tests de bout en bout sont en grande partie réalisés. La mise en place de tests automatiques permettra de gagner du temps et de mieux contrôler l'exécution des tests afin d'éviter d'éventuelles erreurs.

La recommandation 18502.004 est clôturée.

2.3 La conversion au format PDF/A n'est pas totalement mise en place

Dans le cadre de l'audit « Audit de la conformité de FileNet pour SAP P07 », la recommandation suivante a été émise :

« Le CDF recommande à l'OFIT de sauvegarder les documents reçus dans FileNet Dala uniquement dans un format pérenne au sens des Archives fédérales suisses (AFS) et si possible au format PDF/A afin de respecter les directives de l'AFF (Directives et instructions relatives à la gestion budgétaire et comptable de la Confédération). »

En réponse à cette recommandation (nr. d'audit 19478[4]), le CDF a réalisé un échantillonnage sur base de 50 fichiers extraits de FileNet DALA, le CDF constate que neuf fichiers PDF n'ont pas été sauvegardés au format PDF/A soit environ 18 % des cas.

Ce résultat ne peut être extrapolé à l'ensemble de la population de FileNet DALA car le CDF constate également que certains processus tels que l'enregistrement des factures fournisseurs via le workflow fournisseurs ou la génération de certaines factures débitrices, sauvegardent systématiquement au format PDF/A.

Pour la majorité des factures sortantes de SAP, l'OFIT peut aujourd'hui garantir que les documents sont créés au format PDF/A. Les exceptions restantes peuvent également être couvertes par le programme SUPERB. Selon l'OFIT, la responsabilité et le financement incombent toutefois aux unités administratives concernées.

[4] Le rapport d'audit 19478 a été présenté à la Délégation des finances.

Les factures entrantes qui sont scannées peuvent être archivées au format PDF/A. Après la mise en œuvre du programme SUPERB, les unités administratives utiliseront le flux de travail standard de réception des factures et le classement des documents scannés dans le format requis pourra être assuré. Des solutions spécifiques doivent encore être trouvées pour les fichiers transmis sous forme binaire (e-mail, XML, fax, etc.).

Appréciation

La justification de chaque enregistrement par une pièce comptable est une composante du principe de régularité de la comptabilité (Art. 957a, al. 2 CO), il est donc essentiel de garantir sa lisibilité sur le long terme. Par ailleurs, la directive 4.6.2.3 de l'Administration fédérale des finances (AFF)[5] sur la tenue régulière des comptes oblige de sauvegarder les pièces justificatives au format PDF/A :

« La gestion comptable s'effectue dans SAP. Pour la documentation et la conservation, toutes les pièces comptables et les pièces justificatives relatives à l'écriture comptable doivent être jointes au justificatif SAP au format PDF/A (business document). »

Le CDF prend note du fait qu'avec la mise en œuvre du programme SUPERB, les possibilités techniques contraignantes seront épuisées et que des mesures organisationnelles complémentaires, telles que des directives et des formations, seront nécessaires pour classer correctement les documents reçus sous forme binaire. L'OFIT devrait aborder la question des exceptions restantes dans les factures sortantes avec le programme SUPERB et tenter d'adapter les processus avec toutes les unités administratives concernées.

La recommandation 19478.003 reste ouverte.

2.4 La gestion du changement a été améliorée, mais il y a encore du potentiel

Dans le cadre de l'audit « Audit de la conformité de FileNet pour SAP P07 », la recommandation suivante a été émise :

« Le CDF recommande à l'OFIT de formaliser une procédure de gestion des changements et de tester (et documenter) systématiquement les modifications avant leur transfert dans l'environnement de production FileNet Dala. »

En réponse à cette recommandation (nr. d'audit 19478[6]), l'OFIT a élaboré, sur un outil de collaboration, une documentation pour les changements dans l'environnement FileNet Dala ainsi qu'un processus de gestion du changement. Il existe deux types de changements. Le premier type n'a pas d'impact sur les clients (les micro-changements). Le deuxième a un impact sur les clients. La gestion des changements se fait à l'aide de deux outils différents qui fonctionnent en parallèle à cause du processus de réorganisation de l'OFIT. En théorie, les administrateurs peuvent réaliser des changements directement sur la production sans passer par leur outil de déploiement automatique d'applications mais ceux-ci sont traçables. Si les changements passent par l'outil de déploiement automatique d'applications alors ceux-ci sont aussi traçables. Pour les micro-changements, les tests sont effectués à

[5] https://intranet.accounting.admin.ch/accounting/fr/home/manuel-de-gestion-budgetaire-et-de-tenue-des-comptes/principes-regissant-la-tenue-des-comptes/tenue-reguliere-des-comptes.html#-955506152

[6] Le rapport d'audit 19478 a été présenté à la Délégation des finances.

l'aide de smoke tests avec cet outil et validés par l'OFIT. Ils sont documentés dans l'outil de déploiement des applications. Il est possible de voir les tests réussis ou échoués, la date du test, ce qui a été exécuté et qui l'a exécuté. Pour l'autre type de changement, les tests sont effectués et validés par les clients (par exemple, pour de nouvelles fonctionnalités). Il y a un suivi dans les outils de gestion des changements et par courriel. Pour finir, il existe aussi quelques tests sur l'outil de collaboration interne. Ce sont des tests qui n'ont pas encore été automatisés. En plus des tests, l'OFIT a mis en place une liste de contrôle système après la mise en place de changements.

Appréciation

La documentation et le processus de changement sont bien définis sur l'outil de collaboration interne de l'OFIT.

Les outils utilisés permettent un bon suivi des changements ainsi qu'une bonne gestion des tests. Le fait que l'OFIT utilise deux outils augmente potentiellement la complexité.

La liste de contrôle système est une bonne initiative qui permet de bien vérifier l'état du système après un changement.

La possibilité d'apporter des modifications à la production sans passer par des contrôles préventifs en amont va à l'encontre des exigences en matière de contrôle général des technologies de l'information (les contrôles généraux informatiques), qui s'appliquent à l'OFIT pour les systèmes ayant trait à la comptabilité. Il est important que les modifications apportées aux systèmes de production puissent être associées aux tickets créés dans les outils de gestion des modifications et que ces modifications soient régulièrement vérifiées par les responsables des opérations informatiques, dans un esprit de contrôle compensatoire.

La recommandation 19478.004 est clôturée.

2.5 Les vulnérabilités dans la gestion des appareils mobiles sont systématiquement traitées

Dans le cadre de l'audit « Prüfung der Sicherheit und des Betriebs von Mobile Device Management », la recommandation suivante a été émise :

«Die EFK empfiehlt dem BIT, für die eingesetzten Komponenten und Werkzeuge einen Prozess zur proaktiven Informationsbeschaffung bezüglich Verwundbarkeiten zu etablieren.»

En réponse à cette recommandation (PA 20206[7]), l'OFIT a internalisé l'environnement qui était géré avant par Abraxas. Un manuel d'utilisation a été réalisé pour l'environnement MDM (Mobile Device Management) où on peut y trouver l'architecture et d'autres informations essentielles. La collecte des journaux se fait comme pour le reste de l'infrastructure de l'OFIT. Les journaux sont centralisés et envoyés au CSIRT (Computer Security Incident Response Team) pour analyse. Le CSIRT est assez actif dans la résolution des incidents de sécurité. Il génère un rapport tous les trois mois. Celui-ci contient les incidents qui ont été adressés et les actions qui en découlent. Des scans avec un outil de sécurité informatique sont réalisés afin de potentiellement relever les vulnérabilités. Des tests d'intrusions sont

[7] Le rapport d'audit 20206 a été présenté à la Délégation des finances.

aussi mis en place. Si des problèmes sont détectés, alors des mesures sont définies et l'implémentation se fait avec les départements concernés.

Appréciation

L'intégration de l'environnement précédemment géré par Abraxas a permis à l'OFIT de surveiller cet environnement avec les processus normaux, par exemple en ce qui concerne la sécurité et la gestion des journaux.

La documentation de l'environnement MDM (Mobile Device Management) doit encore être adaptée à cause de la restructuration de l'OFIT.

La recommandation 20206.001 est clôturée.

2.6 Mise en place partiel de capteurs et de la surveillance sur l'ensemble du territoire

Dans le cadre de l'audit « Prüfung der Sicherheit und des Betriebs von Mobile Device Management », la recommandation suivante a été émise :

«Die EFK empfiehlt dem BIT, die Sensorik und die Monitoring-Aktivitäten flächendeckend zu implementieren und die gewonnenen Daten unter Berücksichtigung des Datenschutzes auszuwerten.»

En réponse à cette recommandation (nr. d'audit 20206[8]), l'OFIT collecte les journaux des passerelles et de l'environnement isolé (Sandbox) où se trouvent les applications utilisées par les appareils mobiles. Les journaux sont centralisés. Une surveillance de ces applications du point de vue de la sécurité est effectuée par l'OFIT. Seul le CSIRT et les administrateurs peuvent voir les journaux. L'enregistrement et l'analyse des journaux sont effectués conformément aux dispositions des art. 57i-f. de la loi sur l'organisation du gouvernement et de l'administration[9] et l'ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération[10]. Un rapport journalier est généré et celui-ci contient les différentes versions IOS qui sont utilisés par les appareils mobiles. Pour la synchronisation de ceux-ci, l'OFIT utilise un outil de gestion des appareils mobiles. Une directive a été mise en place pour la mise à jour du système d'exploitation des appareils mobiles. Les employés ont 30 jours pour faire la mise à jour, après ce délai un rappel est envoyé. Si ce n'est toujours pas fait alors l'appareil mobile est déconnecté de la synchronisation.

Il n'existe pas, à l'heure actuelle, de collecte de logs ni de surveillance des appareils mobiles.

Un projet est en cours pour utiliser un nouvel outil qui permettra la gestion (par exemple, la surveillance et la collecte de journaux) des appareils mobiles.

Appréciation

Les directives utilisées sont adéquates.

8 Le rapport d'audit 20206 a été présenté à la Délégation des finances.

9 La Loi sur l'organisation du gouvernement et de l'administration (LOGA, RS 172.010) est disponible sur le site Internet du Fedlex (www.fedlex.admin.ch).

10 L'Ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS 172.010.442) est disponible sur le site internet du Fedlex (www.fedlex.admin.ch).

La surveillance de l'ensemble du territoire n'a été que partiellement réalisée, mais la portée sera augmentée par un projet. L'accès aux informations de configuration, à la liste des applications installées, et aux journaux donnera à l'OFIT une meilleure vue d'ensemble de la surveillance des appareils mobiles. Cela permettra de prendre les mesures appropriées pour réduire les risques de sécurité.

La recommandation 20206.002 reste donc ouverte.

2.7 Les outils et la documentation pour le développement des applications mobiles sont appropriés

Dans le cadre de l'audit « Prüfung der Sicherheit und des Betriebs von Mobile Device Management », la recommandation suivante a été émise :

«Die EFK empfiehlt dem BIT, die Prozesse für die Entwicklung von Apps klarer zu definieren, Vorgaben und Hilfsmittel zu erstellen und diese in geeigneter Weise den Entwicklern zur Verfügung zu stellen.»

En réponse à cette recommandation (PA 20206[11]), l'OFIT a mis en place de la documentation dans leur outil de collaboration. Cette documentation contient les objectifs et les différentes solutions techniques (par exemple, les outils) qui ont été mises en place pour adresser ces objectifs. Par exemple, un processus pour le déploiement des applications mobiles, lors d'un sprint, a été documenté ainsi que la chaine d'interactions des différents composants pour le développement et le déploiement des applications mobiles. La phase de tests est définie dans le processus de déploiement des applications mobiles. Celle-ci contient différents tests (par exemple, des tests de logiques et des tests de sécurité). Pour la sécurité, un outil a été mis en place pour scanner les dépendances à la recherche de risques de sécurité. Aucun code ne peut être intégré et mis en production sans l'accord d'au moins un réviseur. Celui-ci analyse le code d'un point de vue de la sécurité. En plus de cela, une analyse du code et de la sécurité est effectuée tous les soirs avec un outil. Chaque application mobile est soumise à la protection de base des TIC, aux directives de l'App Store de la Confédération (si l'application mobile est gérée par la Confédération) ainsi qu'à une analyse des besoins de protection (Schuban). L'OFIT a mis en place un certain nombre d'outils pour les développeurs, comme par exemple : un outil d'automatisation du déploiement des applications mobiles ; un outil qui permet de tester les applications mobiles sur des smartphones physiques ; un outil qui permet la gestion du code ; un outil qui permet la vérification de la qualité du code. Ceux-ci sont utilisés par les développeurs.

Appréciation

La documentation pour le développement d'applications mobiles est une bonne base de travail et les outils utilisés par les développeurs sont adaptés aux besoins.

La sécurité des applications mobiles est bien réglementée et les outils utilisés adressent de manière appropriée les risques de sécurité des applications mobiles.

La recommandation 20206.004 est clôturée.

[11] Le rapport d'audit 20206 a été présenté à la Délégation des finances.

Annexe 1 : Bases légales

Textes législatifs
Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques, OPCy), RS 120.73
Ordonnance du 22 février 2022 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération, RS 172.010.442

Annexe 2 : Abréviations

AFC	Administration fédérale des contributions
AFF	Administration fédérale des finances
AFS	Archives fédérales suisses
CDF	Contrôle fédéral des finances
CIS	Central Identity Store
CSIRT	Computer Security Incident Response Team
MDM	Mobile Device Management
OFIT	Office fédéral de l'informatique et de la télécommunication

Annexe 3 : Glossaire

Abraxas	Abraxas Informatik AG est une entreprise Suisse localisée à Saint-Gallen qui fournit des prestations dans le domaine de l'informatique.
Bug Bounty	C'est un programme de récompenses proposé par de nombreuses sociétés qui offre des récompenses aux personnes qui rapportent des bugs.
FileNet Dala	BM® FileNet Content Manager (version 3.0.4) est une solution de gestion électronique et d'archivage de documents qui se trouve au cœur de la plateforme FileNet P8 (version 5.5.0) propriétaire d'IBM®.
Contrôles généraux informatiques	Les contrôles généraux informatiques sont des contrôles qui s'appliquent à tous les systèmes, composants, processus et données d'une organisation ou d'un environnement informatique.
Sandbox	Zone isolée à l'intérieur de laquelle toute mesure n'a pas d'effet sur l'environnement extérieur.
Schuban	Analyse des besoins de protection (Schuban, Schutzbedarfsanalyse).[12]

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).

[12] https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/prozesse-methoden/p041-schutzbedarfsanalyse_schuban.html