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

Audit de l'intégration sécurisée des applications métier dans l'ePortal

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

CDF-23532 | Version inclus les prises de position | 16 mai 2024

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	606.23532
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch + 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**

1 Mission et déroulement **6**

1.1 Contexte 6

1.2 Objectif et questions d'audit 7

1.3 Etendue de l'audit et principe 8

1.4 Documentation et entretiens 8

1.5 Discussion finale 8

2 Office fédéral de l'informatique et de la télécommunication **9**

2.1 L'architecture du portail et les services mis à disposition des clients sont bien conçus 9

2.2 Le cycle de vie du portail est bien structuré et des améliorations sont en cours 13

3 Office fédéral de la douane et de la sécurité des frontières **15**

3.1 Les interactions avec le portail sont conformes aux directives et la mesure supplémentaire pour l'accès aux données sensibles est un point fort 15

3.2 Le cycle de vie des applications est bien structuré mais le concept de suppression des données doit être étendu 16

4 Administration fédérale des contributions **18**

4.1 Les interactions avec le portail sont conformes aux directives 18

4.2 La coordination dans le cycle de vie peut être amélioré 19

Annexe 1 : Bases légales **21**

Annexe 2 : Abréviations **22**

Annexe 3 : Glossaire **23**

Audit de l'intégration sécurisée des applications métier dans l'ePortal

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

L'essentiel en bref

L'administration fédérale dispose de plusieurs portails de transaction pour la mise à disposition de services numériques de l'administration à la population, aux entreprises et aux autres administrations. Les portails poursuivent l'objectif de rendre la communication avec l'administration plus simple, plus efficace et plus conviviale. Ils constituent un élément important de la transformation numérique de l'administration. L'avantage de la présentation de services sur des plates-formes est qu'elle facilite l'accès en regroupant les offres. La standardisation de l'accès réduit les coûts et permet d'exploiter les synergies. De plus, une seule authentification suffit pour accéder à différents services.

Le Département fédéral des finances (DFF) a entrepris son projet du portail électronique à l'été 2018 avec pour objectif de regrouper et d'offrir ses prestations administratives en ligne. À cet effet, il a mis l'accent sur la convivialité : les applications métier doivent être accessibles de manière directe et centralisée. Le portail est utilisé depuis novembre 2020 et peut accueillir des applications de toutes les unités de l'administration fédérale. Au moment de l'audit, les applications de l'Administration fédérale des contributions (AFC) et de l'Office fédéral des douanes et de la sécurité à la frontière (OFDF) sont mises à disposition.

Depuis 2021, le portail électronique est proposé par l'Office fédéral de l'informatique et de la télécommunication (OFIT) en tant que prestation de marché au sens d'un produit de catalogue et est donc ouvert à toutes les unités administratives de l'administration fédérale.

Dans cet audit, le Contrôle fédéral des finances (CDF) examine la sécurité de l'intégration de nouvelles applications métier de l'AFC et de l'OFDF dans le portail électronique. Dans ce contexte, l'authentification au moyen du systèmes [redacted] et la gestion des autorisations au moyen du système [redacted] est importante. Le CDF constate que la sécurité de l'environnement du portail et des applications métier ainsi que l'intégration des applications métier dans le portail sont conformes aux directives de la Confédération. Cependant, il y existe des points à améliorer dans la gestion de la continuité du portail ainsi que du cycle de vie de celui-ci.

La gestion de la continuité du portail est un point faible

Les mesures prises pour la confidentialité, l'intégrité et la disponibilité correspondent aux directives. L'OFIT travaille à la mise en place d'une procédure visant à réduire [redacted] par le portail, ce qui le rendrait encore moins vulnérable. Un point d'amélioration serait de surveiller [redacted] et de déclencher [redacted].

[redacted], ainsi qu'une mauvaise réputation. L'OFIT devrait élaborer les outils correspondants. L'OFIT devrait en outre organiser [redacted] afin de vérifier que les procédures documentées dans les plans d'urgence fonctionnent et sont connues de toutes les personnes concernées.

Le cycle de vie du portail est bien structuré et des améliorations sont en cours

L'architecture du portail ainsi que les différents services mis à disposition des applications métier et du système d'authentification [redacted] suivent les directives en termes de sécurité et d'architecture. Un processus d'intégration et de décommissionnement des clients ainsi qu'un processus de gestion des changements ont été formalisés et mis en place. Des tests d'intrusion sont normalement effectués chaque année, mais un rythme minimal n'a toutefois pas encore été fixé.

La gestion des droits d'accès et des rôles des utilisateurs du portail [redacted]. Afin de rendre ce processus moins sujet aux erreurs, il serait judicieux d'envisager [redacted].

Les interactions entre les applications métier de l'OFDF et de l'AFC et le portail sont conformes aux directives

L'implémentation de la communication entre les applications métier de l'OFDF et l'AFC et les différents composants de l'environnement est mise en œuvre conformément à l'architecture du portail, y compris avec le système d'autorisation [redacted]. Les mesures de sécurité sont conformées aux directives. Les exigences accrues pour l'accès aux données sensibles de l'OFDF ont été satisfaites par l'ajout d'une étape d'authentification supplémentaire.

Le cycle de vie des applications métier de l'OFDF et l'AFC est bien structuré, mais il y a des possibilités d'amélioration

Le processus du cycle de vie des applications de l'OFDF et de l'AFC est bien défini et formalisé, ce qui est essentiel pour garantir la cohérence et la qualité pendant le développement et la maintenance des applications. L'AFC elle-même estime que la coordination entre les équipes peut encore être améliorée afin d'éviter les retards ou les erreurs dans la mise en œuvre des changements.

D'autre part, il serait judicieux pour l'AFC et l'OFDF d'établir [redacted].

La mise en œuvre d'un concept de suppression par l'OFDF est une obligation légale. Elle doit garantir que toutes les données dans les applications sont supprimées de manière permanente et sûre lorsqu'elles ne sont plus nécessaires. Aujourd'hui, le concept ne couvre pas encore toutes les applications métier pertinentes.

Prise de position générale des audités

Prise de position générale de l'OFIT

Das BIT bedankt sich bei der EFK für die konstruktive Zusammenarbeit mit den Prüfexperten und für die geschätzten Hinweise in den Beurteilungen. Für zukünftige Audits ist es essenziell, dass das ePortal unabhängig von den Applikationen unserer Kunden geprüft wird, da Workflows und Prozesse innerhalb dieser Applikationen nicht im Scope des ePortals liegen und technische sowie architektonische Lösungen in jeder Applikation individuell betrachtet werden müssen.

Prise de position générale de l'OFDF

Verzicht auf eine allgemeine Stellungnahme.

Prise de position générale de AFC

Die ESTV verzichtet auf eine generelle Stellungnahme.

1 Mission et déroulement

1.1 Contexte

L'administration fédérale dispose de plusieurs portails de transaction pour la mise à disposition de services numériques de l'administration à la population, aux entreprises et aux autres administrations[1]. Les portails poursuivent tous l'objectif de rendre la communication avec l'administration plus simple, plus efficace et plus conviviale. Ils constituent un élément important de la transformation numérique de l'administration. L'avantage de la présentation de services sur des plates-formes est qu'elle facilite l'accès en regroupant les offres. La standardisation de l'accès réduit les coûts et permet d'exploiter les synergies. De plus, une seule authentification suffit pour accéder à différents services. Toutefois, bien qu'ils aient le même objectif, les différents portails utilisent des technologies différentes pour fournir les services ou les applications proposés.

Le Département fédéral des finances (DFF) a entrepris son projet du portail électronique à l'été 2018 avec pour objectif de regrouper et d'offrir ses prestations administratives en ligne. À cet effet, il a mis l'accent sur la convivialité : les applications métier doivent être accessibles de manière directe et centralisée.

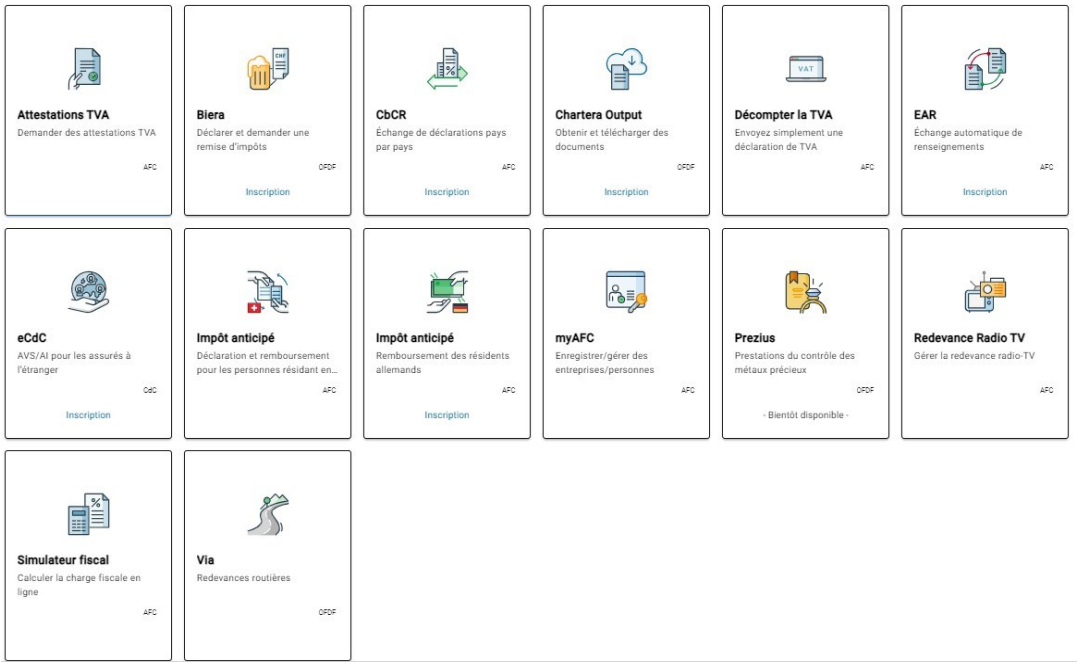
L'ePortal ou portail électronique est léger et les applications qu'il propose ont leur propre frontal et dorsal ainsi que leur propre gestion des données. L'utilisateur se connecte au portail et voit les applications métier disponibles pour lui. Lorsqu'il choisit une application, il est redirigé directement vers celle-ci sans avoir à se connecter à nouveau. Cette redirection est facilitée par l'interaction entre l'application et les différents composants qui identifient, authentifient [redacted] l'utilisateur et lui permettent d'accéder correctement à l'application. L'utilisateur peut revenir au portail via une bannière dans l'application.

Dans un contexte B2B (Business to Business), les services externes peuvent utiliser une passerelle API (Interface de programmation d'application) pour accéder à différents services mis à disposition par les applications métier. L'authentification des services externes se fait via le système [redacted].

Le portail est utilisé depuis novembre 2020. Depuis 2021, il est proposé par l'Office fédéral de l'informatique et de la télécommunication (OFIT) en tant que prestation de marché au sens d'un produit de catalogue et est donc ouvert à toutes les unités administratives de l'administration fédérale. Au moment de l'audit, les applications de l'Administration fédérale des contributions (AFC) et de l'Office fédéral des douanes et de la sécurité à la frontière (OFDF) sont mises à disposition. Des applications d'autres unités administratives sont en préparation.

Voici la liste des applications du portail électronique en date de novembre 2023 (14 applications) :

[1] Cf. aussi PA 20368 Examen des synergies potentielles des portails informatiques de la Confédération, disponible sur le site du CDF



Le Contrôle fédéral des finances (CDF) a décidé d'auditer ce portail car il a constaté plusieurs défis techniques dans cette constellation tels que :

- La sécurité générale de l'environnement du portail électronique ;
- La coexistence entre le système d'authentification [redacted], le système d'autorisation [redacted] et les applications métier ;
- L'intégration et mise en œuvre de l'authentification et des droits d'accès dans l'environnement du portail électronique, y compris avec les différentes applications ;
- Et le fonctionnement de la passerelle API pour l'accès depuis l'extérieur à certaines applications métier.

1.2 Objectif et questions d'audit

L'objectif de l'audit est d'évaluer si la sécurité d'accès et d'exploitation est garantie lors de l'intégration d'applications métiers dans le portail électronique. Le CDF complète cet examen par les questions suivantes :

1. Est-ce qu'il existe des mécanismes de sécurité suffisants pour l'accès aux applications métiers via le portail électronique ?
2. Lors de l'exploitation opérationnelle, est-il garanti que le portail électronique répond aux exigences de disponibilité, d'intégrité et de confidentialité ?
3. Est-ce qu'une gestion prévoyante du cycle de vie garantit une sécurité d'accès et d'exploitation efficace et durable ?

1.3 Etendue de l'audit et principe

L'audit a été mené du 18 octobre au 27 novembre 2023 par Warren Paulus (responsable de révision) avec le soutien d'une entreprise externe. Il a été conduit sous la responsabilité de Bernhard Hamberger. Le présent rapport ne prend pas en compte les développements ultérieurs à l'audit.

Pour ses travaux, le CDF s'est appuyé sur la norme ISO 27001[2] et la directive sur la protection informatique de base dans l'administration fédérale[3] qui définit de manière contraignante les directives de sécurité minimales (protection de base) sur les plans de l'organisation, du personnel et de la technique en matière de sécurité informatique.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par l'OFIT, l'OFDF, et l'AFC. 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 12 01 2024. L'OFIT était représenté par la responsable du portail électronique, le responsable de la sécurité, le responsable de la gestion des identités et des accès et l'architecte logiciel. L'OFDF était représenté par la responsable du domaine de direction planification et pilotage et par le responsable de l'architecture d'entreprise et de la gouvernance. L'AFC était représenté par le responsable de l'audit interne et le responsable de l'informatique. 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

[redacted] i.V. [redacted]

[redacted] [redacted]

Responsable de centre de compétences Expert en audit

[2]https://fr.wikipedia.org/wiki/ISO/CEI_27001

[3]https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/grundschutz.html

2 Office fédéral de l'informatique et de la télécommunication

En ce qui concerne l'OFIT, le CDF a évalué les questions d'audit du point de vue du responsable de l'exploitation du portail électronique.

2.1 L'architecture du portail et les services mis à disposition des clients sont bien conçus

Le portail électronique peut être visité en tant qu'utilisateur anonyme. Cependant, selon l'application métier, un enregistrement peut être nécessaire. Toutes les applications intégrées peuvent être utilisés avec le même système d'authentification [redacted].

L'accès utilisateurs fait partie du type d'accès le plus important comparé à, par exemple, l'accès machine à machine qui est réalisé par l'intermédiaire d'une passerelle API (Interface de programmation d'application). Pour les utilisateurs, il existe six niveaux d'accès. Ces niveaux vont de l'accès anonyme à l'accès via une connexion fédérale interne utilisant l'authentification par carte à puce.

Un widget est implémenté dans chaque application métier afin d'interagir avec le système d'autorisation par l'intermédiaire d'une passerelle API sécurisée. Celui-ci vérifie si l'utilisateur dispose d'une session et met cette information à disposition de l'application. Si l'utilisateur n'est pas connecté alors l'application doit décider si la page demandée peut être affichée sans être connectée. Si c'est le cas, elle est affichée sinon l'application envoie une requête au système d'autorisation [redacted] pour permettre à l'utilisateur de s'authentifier avec [redacted]. La communication entre [redacted] et [redacted] se fait via le navigateur du client. [redacted] qui se déclenche lorsque l'utilisateur est déconnecté ou, en d'autres termes, lorsque la session n'est plus valide.

Dans le cadre des utilisateurs, [redacted] peut fournir à certaines applications métier [redacted], mais ces informations ne permettent pas de définir [redacted]. Pour résoudre ce problème, un module supplémentaire est utilisé entre les applications métier et [redacted].

Il existe des interactions entre les applications métier et [redacted]. Une application métier peut se connecter par l'intermédiaire [redacted]. Le serveur appelé peut alors [redacted].

Dans un contexte B2B (Business to Business), les services externes se connectent à une passerelle API (Interface de programmation d'application) et reçoivent [redacted] et [redacted] dans le cadre de son abonnement. [redacted] via la passerelle pour accéder aux applications métier. Le serveur appelé peut également [redacted] de cette manière [redacted] à l'aide [redacted].

Plusieurs documents de sécurité sont disponibles et signés pour le portail électronique et [redacted], tels que l'analyse des besoins de protection (Schuban), la protection informatique de base dans l'administration fédérale et le concept de sécurité de l'information et de protection des données (Concept SIPD). Le concept de sécurité de l'information et de protection des données inclut le portail et [redacted], car celui-ci est inclus dans le portail.

Appréciation

L'architecture du portail ainsi que les différents services mis à disposition des applications métier et du système d'authentification [redacted] suivent les directives de la Confédération en matière d'architecture et de sécurité. Les documents de sécurité sont présents et de bonne qualité.

La confidentialité des données

Le portail lui-même ne contient pas d'autres données que celles des [redacted] des applications métier. Cette [redacted] permet au portail d'interagir avec les différentes applications [redacted].

Toutes les données sont stockées dans une base de données [redacted] et tous les accès sont enregistrés dans [redacted]. La confidentialité des données des clients est gérée par l'utilisation [redacted]. [redacted]. Cette technique permet aux clients d'avoir un accès en lecture à leurs propres données.

En ce qui concerne le code source du portail, l'OFIT a mis en place un système de protection [redacted]. Ce mécanisme contrôle [redacted].

La disponibilité du portail

Le portail doit être disponible 24x7 avec un temps d'arrêt maximum de 2 heures, puisqu'il s'agit d'un [redacted]. Cette disponibilité est garantie au niveau physique par l'architecture, et un accord de niveau de service a été conclu avec les unités administratives. À l'heure actuelle, une procédure de redémarrage du portail a été formalisée mais il n'existe pas de gestion de la continuité du service. Le temps d'arrêt maximal admissible et la durée maximale de stockage des données que l'OFIT peut accepter de perdre en cas d'incident sur le portail ne sont pas non plus documentés. Un concept/plan d'urgence doit également être élaboré dans le cadre du changement de classe de disponibilité de CD1 à CD3 du 1er janvier 2023 dernier.

Elément de niveau de service 4 – Disponibilité (par trimestre)						
Service Level Parameter	Nom SLP	CD0	VKE	CD1	CD2	CD3
1	Durée max. d'une panne	Best Effort	22h	12h	8h	2h
2	Nombre max. de pannes	Best Effort	n/a	3x	2x	1x
3	Délai max. de reprise	Best Effort	n/a	12h	8h	2h

4	**Durée max. de perte de données**	Best Effort	n/a	4h	2h	**< 10 min**

Tableau 1: Élément de niveau de service 4 : disponibilité[4]

Pour y remédier, l'OFIT a mis en place un processus de sauvegarde [redacted]. A cela s'ajoute un journal de toutes les transactions effectuées sur la base de données : cela permet de s'approcher le plus possible du temps maximum [redacted]. Des sauvegardes sont effectuées tous les jours et sont archivées après une semaine. Des tests de sauvegarde et de restauration de la base de données sont effectués [redacted]. Le temps de restauration d'une sauvegarde a été testé et a pris moins de [redacted]. Le processus de restauration du portail est également documenté, [redacted].

L'OFIT a créé une page contenant des informations telles que les incidents, les défaillances et les mises à jour du portail. Les clients peuvent s'abonner à cette page. En cas d'incident, une liste de contacts est documentée sur un outil interne, ainsi que dans une application mobile interne de l'OFIT.

Afin de contrôler l'architecture, l'OFIT surveille différentes métriques des serveurs (p. ex., l'unité centrale de traitement), ainsi que la base de données (p. ex., taille et mémoire). Un système d'alerte a été mis en place et envoie un message en cas de problème. De plus, un système de veille 24x7 est mis en place pour l'ensemble de l'équipe de développement, ce qui leur permet de réagir rapidement.

Pour vérifier la disponibilité, des tests de charge et de performance sont effectués et les résultats sont documentés. Cependant, il n'y a pas de planning, ils sont réalisés en fonction des demandes des clients ou après la création d'un nouveau service, par exemple. Deux tests ont été réalisés en 2023 et un troisième est encore prévu.

L'intégrité du portail

Le portail n'a pas d'exigences particulières en matière d'intégrité des données, car il ne contient qu'un minimum de données non sensibles. Cependant, les systèmes d'authentification [redacted] et d'autorisation [redacted] garantissent l'intégrité des données qu'ils partagent avec les différentes applications professionnelles via le navigateur du client. En ce qui concerne le code du portail, toutes les modifications sont documentées par une procédure formalisée. Les personnes qui ont accès aux serveurs de production et leurs droits d'accès sont documentés.

Pour garantir l'intégrité des journaux, ils sont envoyés à un système [redacted] et sont également [redacted].

Appréciation

Confidentialité :

Les mesures mise en place tels que la restriction des accès, l'enregistrement dans un fichier journal, les tenants pour les clients ainsi que la documentation sont ciblés. Le potentiel d'amélioration réside notamment dans l'implémentation d'une procédure visant [redacted]

[4] https://intranet.bit.admin.ch/bit_kp/fr/home/angebot/service-level/die-service-level-elemente-ihre-parameter.html

[redacted] car cela peut potentiellement exposer le système à des acteurs malveillants qui pourraient exploiter [redacted]. L'OFIT y travaille. Le CDF renonce donc à une recommandation

Disponibilité :

[redacted] de garantir la continuité de l'activité.

[redacted] empêche de garantir que l'OFIT puisse réagir rapidement et efficacement en cas d'incident, augmentant ainsi la gravité de l'incident.

En revanche, [redacted] n'est effectué. Il [redacted], afin de réagir rapidement en cas d'incidents et de vérifier que [redacted].

Même s'il n'y a pas de données sensibles et que les données ne changent que très peu au fil du temps, il est important d'aborder les différents points mentionnés ci-dessus, car cela peut avoir un impact sur la crédibilité du portail.

Les mesures techniques mises en place tels que la surveillance et alertes, les tests de charge et de performance, et les sauvegardes sont approprié. Il convient de souligner la mise en place du service de piquet. Un point d'amélioration serait de [redacted].

Intégrité :

Les mesures en place tels que la restriction d'accès et la documentation des changements sont adéquat.

Recommandation 1 (Priorité 1)

Le CDF recommande à l'OFIT de développer et de mettre en œuvre une stratégie de gestion de la continuité du service, comprenant [redacted].

La recommandation est acceptée.

Prise de position de l'OFIT

Das BIT akzeptiert die Empfehlung der EFK bezüglich des Service Continuity Managements und dankt für die konstruktive Anregung. Es ist geplant, dass das ePortal im Q4 2024 aufgrund eines noch ausstehenden dedizierten Clusters auf die neue Zielplattform (RHOS) migriert wird. Dies bedeutet, dass ein umfassender Disaster Recovery Plan und Notfallplan erst nach der Migration erstellt werden kann. Dies wird es erlauben, regelmässige Tests durchzuführen, um die Sicherheit und Verfügbarkeit der Dienste zu gewährleisten. In der Zwischenzeit wird jedoch das generelle Notfallkonzept für die bestehende Plattform bis zum 1. Juni 2024 aktualisiert, um im Falle eines Major-Incident den Betrieb so schnell wie möglich wieder aufnehmen zu können. Das BIT wird beantragen, dass dies im Fachausschuss entsprechend priorisiert wird.

Recommandation 2 (Priorité 2)

Le CDF recommande à l'OFIT de surveiller [redacted] lorsqu'ils s'approchent des seuils déjà testés.

La recommandation est acceptée.

Prise de position de l'OFIT

Das BIT begrüsst die Empfehlung der EFK zur Überwachung der Last und Performance des Portals sowie zur Auslösung weiterführender Performancetests. Wie in der Prüfung und in der Schlussbesprechung ausgeführt, werden solche Tests regelmässig durchgeführt. Bereits vor Juli 2024 werden die nächsten Last- und Performance-Tests durchgeführt. Dies wird sicherstellen, dass proaktiv auf potenzielle Leistungsengpässe reagiert werden kann, bevor sie kritisch werden, und die optimale Leistungsfähigkeit des Portals sicherstellen.

2.2 Le cycle de vie du portail est bien structuré et des améliorations sont en cours

Le cycle de vie des applications métier est géré par un processus d'intégration et de décommissionnement qui comprend un certain nombre d'exigences, comme l'implémentation d'un widget dans les applications métier.

Concernant la mise en production des modifications apportées au portail électronique, l'OFIT travaille avec les méthodologies Scrum, DevOps et SAFe (Scaled Agile Framework). Le calendrier est établi par incréments constitué d'une période de dix semaines contenant cinq sprints. Tous les changements prévus sont documentés et passent par un groupe de validation pour s'assurer que les changements n'ont pas d'impact sur d'autres applications. Lorsque les changements sont mis en production, ils sont validés par toutes les parties prenantes et ensuite ils sont déployés dans plusieurs environnements avec différents types de tests et de validations (p. ex., des tests d'intégration, des tests unitaires et des tests fonctionnels). En cas de changements d'urgence, ceux-ci sont gérés par un processus formalisé.

Afin d'augmenter la sécurité, des analyses de vulnérabilité sont effectuées en interne et des tests d'intrusion sont réalisés par une entreprise tierce. Les tests d'intrusion sont normalement effectués [redacted], mais il n'y en a pas eu [redacted], car l'OFIT a corrigé tous les problèmes du rapport 2022, et les analyses de vulnérabilité effectuées [redacted] n'ont rien révélé de critique. [redacted] aura lieu [redacted].

Si des vulnérabilités sont détectées, elles sont reproduites, la criticité est réévaluée, et un ticket est créé sur un système interne de gestion des tickets pour la traçabilité. Ensuite, en fonction de la criticité, les vulnérabilités sont programmées pour être résolues dans les incréments futurs. Pour rester à jour, à chaque modification de l'application, les différentes bibliothèques utilisées sont mises à jour.

Il existe également [redacted] pour détecter d'éventuels problèmes avec [redacted] (p. ex., [redacted]). L'OFIT a mis en place des systèmes de surveillance des serveurs utilisés par le portail, ainsi que de l'application elle-même.

Chaque application doit définir où et comment les rôles des utilisateurs sont gérés. Il existe deux types de rôles pour les utilisateurs : le premier concerne les rôles que l'utilisateur a pour toutes les applications métier (p. ex., un utilisateur technique). Le second type de rôle concerne les rôles que l'utilisateur a par application métier. L'implémentation des rôles se fait dans le système d'autorisation. Au sein de l'équipe du portail, les droits d'accès sont limités et documentés. Par contre, il existe un manque de surveillance [redacted].

Ceux-ci devraient être vérifiés chaque année par l'unité administrative en charge. A l'heure actuelle, les contrôles se font [redacted].

Appréciation

L'OFIT a mis en place un processus d'intégration et de décommissionnement pour les unités administratives, ce qui est essentiel pour assurer une transition sûre eux tout au long de leur cycle de vie dans le portail.

L'OFIT utilise de manière appropriée des méthodes modernes telles que Scrum, DevOps et SAFe pour effectuer des modifications sur les systèmes productifs. La documentation et la validation des modifications sont appropriées, ce qui réduit la probabilité que les modifications introduisent des faiblesses ou des erreurs dans le système. L'utilisation de différents environnements avec différents types de tests renforce la confiance dans la robustesse du processus de gestion des changements. Des tests d'intrusion sont effectués, [redacted]. Le CDF renonce donc à formuler une recommandation à ce sujet.

La mise à jour régulière des bibliothèques utilisées est une excellente pratique pour s'assurer que le portail est mis à jour avec les dernières corrections de sécurité. La surveillance des serveurs et de l'application elle-même est une étape cruciale pour identifier rapidement les comportements anormaux ou suspects et y répondre.

La gestion des utilisateurs se fait manuellement. Afin de minimiser le risque d'erreur, un processus automatique moins sujet aux erreurs pourrait être étudié. Une demande d'automatisation du processus devrait toutefois émaner du comité technique, au sein duquel tous les clients du portail sont représentés. Le CDF n'ayant pas eu l'occasion, dans le cadre de cet audit, de clarifier de manière approfondie le potentiel d'utilité, respectivement les coûts qui y sont liés, il renonce à formuler une recommandation à ce sujet.

3 Office fédéral de la douane et de la sécurité des frontières

Chez l'OFDF le CDF a examiné les questions d'audit sur la base des exemples concrets des applications « Via » et « Transparenza ». Ces applications ont été choisies en concertation avec l'OFDF lors de la réunion de lancement de l'audit, car ce sont les applications les plus complètes dont ils disposent sur le portail.

L'application « Via » est une boutique en ligne qui permet la perception de la RPLP (redevance forfaitaire sur les poids lourds) pour les véhicules étrangers et l'achat de la vignette électronique pour les véhicules immatriculés en Suisse et à l'étranger. L'application « Transparenza », quant à elle, est un système centralisé de suivi des données pour l'ensemble des applications de l'OFDF. Elle rassemble toutes les opérations sur les données et gère le cycle de vie des données. « Transparenza » n'est utilisée qu'au sein de l'OFDF.

3.1 Les interactions avec le portail sont conformes aux directives et la mesure supplémentaire pour l'accès aux données sensibles est un point fort

En principe, les applications métier doivent être enregistrées dans le système d'autorisation [redacted]. « Via » est un cas particulier, car cette application est accessible sans authentification.

« Transparenza » n'est pas directement accessible via le portail, car cette application auxiliaire est utilisée entre autres par « Via » pour la journalisation.

L'application « Via » est accessible via la passerelle API en tant qu'utilisateur anonyme ou authentifié à l'aide du système d'authentification [redacted]. Pour les utilisateurs anonymes, certaines demandes sont protégées par un mécanisme de sécurité.

Les applications « Via » et « Transparenza » utilisent des interfaces et des bibliothèques standardisées pour la sécurité et la gestion des rôles. Cette standardisation est obligatoire et spécifiée dans les directives.

Afin d'augmenter la sécurité lors de l'authentification des utilisateurs, une clé de preuve pour l'échange de code (PKCE) est utilisée pour garantir que l'application qui démarre le flux d'authentification est la même que celle qui le termine. De plus, la gestion des secrets tels que, par exemple, les mots de passes et les certificats sont gérés dans un coffre-fort externe aux applications. Les applications récupèrent les secrets lorsque celles-ci sont lancées. Ces mécanismes de sécurité sont aussi obligatoires et spécifiés dans les directives.

Un concept de rôle a été mis en place et celui-ci est appliqué à l'OFDF ainsi que pour les partenaires externes. Il existe un processus semestriel au cours duquel tous les chefs d'équipe doivent confirmer les rôles attribués aux utilisateurs.

En cas d'accès à des données très sensibles, par exemple des données de recherches, un système d'authentification supplémentaire à [redacted] est demandé.

Appréciation

La communication entre les applications métier et les différents composants de l'environnement tels que le système d'autorisation [redacted] et la passerelle API est mise en œuvre conformément à l'architecture du portail. Les mesures de sécurité sont conformes aux directives. En outre, l'authentification supplémentaire est utile pour les données sensibles.

La définition et la gestion des rôles sont clairement formalisées. L'implémentation des rôles dans les applications métier est mise en œuvre conformément aux directives.

3.2 Le cycle de vie des applications est bien structuré mais le concept de suppression des données doit être étendu

L'OFDF a défini et formalisé un processus pour le cycle de vie des applications. Un outil interne permet de suivre le cycle de vie des projets informatiques. Ceux-ci sont lancés en fonction d'un budget. Une fois le budget validé, un planning est établi pour l'application concerné. Lorsque celui-ci est finalisé et que les différents documents de sécurité sont en place et validés par la direction de la conformité, la mise en œuvre peut commencer.

Au cours de la vie de l'application, des modifications peuvent être planifiées et mises en œuvre par l'OFIT. Celles-ci sont documentées et suivies dans un outil interne de gestion de tickets selon un processus défini. L'OFDF communique régulièrement avec l'OFIT au cours de ce processus. Tous les changements sont gérés de manière contrôlée, y compris les normes et procédures de changement, l'évaluation de l'impact, la hiérarchisation et l'approbation des changements. Après validation, chaque modification passe par plusieurs environnements et une série de tests tels que des tests d'intégration, unitaire, de sécurité et de qualité du code avant d'atteindre l'environnement de production. Les tests sont documentés et contrôlés. Les changements d'urgence suivent aussi une procédure standardisée et sont contrôlés afin de réduire au minimum les perturbations. Pour ces derniers, l'approbation et les tests sont documentés ultérieurement dans un délai raisonnable.

Pour renforcer la sécurité, l'OFDF a mis en place des tests d'intrusion et des analyses de vulnérabilité OWASP. Il n'y a pas de planification pour la réalisation de tests d'intrusion ni de fréquence fixe, mais l'OFDF adopte une approche basée sur les risques pour déclencher la réalisation de ces tests. De plus, les tests sont effectués lorsqu'une application est mise en production ou lorsque des modifications importantes sont apportées. En cas d'alerte de sécurité, une communication rapide est établie avec les personnes concernées et un ticket est créé. La catégorisation et la résolution des vulnérabilités et autres problèmes de sécurité sont de la responsabilité du gestionnaire de l'application concernée. Les vulnérabilités sont surveillées via l'intermédiaire d'un outil interne. Les mises à jour des composants utilisés dans une application sont planifiées en collaboration avec l'OFIT mais les mises à jour de sécurité sont appliquées rapidement. De plus, il existe une vérification active manuelle et automatique des différents composants utilisés dans la conception des applications mé-

tier. Pour renforcer les tests et la sécurité, un système de monitoring a été mis en place par l'OFIT pour vérifier, par exemple, la disponibilité des applications.

En cas de défaillances du portail, il est possible d'accéder aux différentes applications, mais avec des droits limités. Si les systèmes d'authentification [redacted] et d'autorisation [redacted] tombent en panne, dans ce cas, un plan d'urgence est activé.

La fin de vie d'un projet informatique est décidée en fonction du budget, afin de déterminer quelle application conserver, remplacer ou mettre hors service. Pour le démantèlement et la suppression des données, il y a un audit financier, technique et organisationnel. Tout cela est discuté avec les différentes équipes à tous les niveaux. Dans tous les cas, l'OFDF supprime les données après cinq ans. A l'heure actuelle, il existe un concept d'effacement des données pour « Transparenza » mais pas pour « Via ». L'OFDF y travaille.

Appréciation

L'OFDF a pris des mesures ciblées pour définir et formaliser le processus du cycle de vie des applications, ce qui est essentiel pour garantir la cohérence et la qualité tout au long du développement et de la maintenance des applications.

La communication régulière avec l'OFIT pendant le processus de gestion des changements est un signe positif, car elle garantit que toutes les parties prenantes sont informées et impliquées.

L'analyse et la gestion des problèmes de sécurité, la surveillance des applications par l'OFIT et la réaction aux pannes de portail semblent appropriées. La réalisation de tests d'intrusion axés sur les risques, en premier lieu lors de modifications, a permis jusqu'à présent d'atteindre une fréquence appropriée. L'OFDF n'a toutefois pas fixé de fréquence minimale pour les tests d'intrusion. Une telle fréquence pourrait éviter qu'aucun test d'intrusion ne soit effectué pendant une longue période lors de phases sans changement. Le CDF renonce toutefois à formuler une recommandation, car les tests d'intrusion sont effectués en fonction des risques.

Enfin, la suppression des données après cinq ans est demandée par la loi[5] pour garantir la confidentialité des données. Il est important de mettre en œuvre un concept de suppression pour toutes les applications afin de garantir que les données des applications soient supprimées de manière permanente et sécurisée lorsqu'elles ne sont plus nécessaires. L'OFDF souhaitait introduire des modifications sur ce thème dans le cadre de la révision totale de la loi sur les douanes[6]. La loi correspondante étant encore en discussion au Parlement, le CDF renonce à formuler une recommandation à ce sujet.

[5] https://www.fedlex.admin.ch/eli/cc/2017/535/de#art_10
[6] https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20220058

4 Administration fédérale des contributions

Chez l'AFC le CDF a examiné les questions d'audit sur la base des applications de l'AFC en général, en mettant l'accent sur l'application « Décompter la TVA ». Cette application a été choisie en concertation avec l'AFC lors de la réunion de lancement de l'audit, car il s'agit de l'application la plus complète dont ils disposent sur le portail.

Cette application se compose d'une version « Easy » et d'une version « Pro ». La version « Easy » est accessible en tant qu'invité avec un numéro de téléphone mobile. Cette version simplifie l'envoi des décomptes de TVA. La version « Pro », en revanche, est accessible avec un compte, ce qui permet à l'utilisateur d'avoir un aperçu de ses décomptes de TVA et d'effectuer des corrections.

4.1 Les interactions avec le portail sont conformes aux directives

L'application « Décompte de la TVA » fonctionne directement via le système d'autorisation [redacted] contrairement au schéma classique via le module supplémentaire entre les applications métier et [redacted]. Elle interagit avec différentes applications partagées dans le portail, comme [redacted] et [redacted]. De plus, [redacted]. Pour les applications qui utilisent la passerelle API, il existe des mesures de sécurité sur celle-ci.

Chaque application et les réseaux logiques sont déployés [redacted]. Afin d'augmenter la sécurité [redacted] par l'application « Décompter la TVA » sont [redacted].

[redacted] pour l'application « Décompter la TVA » [redacted].

Un concept de rôles et une matrice d'autorisation ont été mis en place. L'application « Décompter la TVA » récupère les rôles de ses différent profiles via le système d'autorisation.

Appréciation

La communication entre les applications métier et les différents composants de l'environnement tels que le système d'autorisation, les autres applications métier, et la passerelle API est mise en œuvre de manière appropriée et conformément à l'architecture du portail. Une amélioration possible de l'application « Décompter la TVA » [redacted]

[redacted]. Les mesures de sécurité sont conformes aux directives.

La définition, la gestion, et l'implémentation des rôles dans les applications métier sont ciblées. La définition et la gestion des rôles sont clairement formalisées. L'implémentation des rôles dans les applications métier est aussi mise en œuvre conformément aux directives.

4.2 La coordination dans le cycle de vie peut être amélioré

L'AFC documente toutes ces applications dans un outil interne de gestion de portefeuilles et établit les documents de sécurité correspondants, tels que la protection informatique de base dans l'administration fédérale, l'analyse des besoins de protection (Schuban) et le concept de sécurité de l'information et de protection des données (Concept SIPD).

Les demandes de changement ou les nouvelles exigences de l'AFC sont gérées par le biais d'un processus de gestion du changement. Les changements sont mis en œuvre par incréments, documentés et suivis en interne par l'AFC. Lorsque les changements sont déployés, ils passent par différents environnements et une série de tests sont effectués, tels que des tests fonctionnels et techniques (tests d'intégration, tests unitaires, etc.), avant qu'ils ne soient mis en production. En cas d'erreur de sécurité dans le code, l'OFIT est en contact [redacted], afin de vérifier les erreurs. Les changements d'urgence sont aussi formalisés à l'aide d'un processus. Les changements mineurs sont réalisés, en règle générale, [redacted] et les changements majeurs [redacted]. La difficulté réside dans la coordination entre les équipes pour s'assurer que les changements sont mis en œuvre au bon moment. Cette responsabilité est incluse dans le cahier des charges du Release Train Engineer (RTE) et le gestionnaire du portefeuille.

Pour renforcer la sécurité pendant le cycle de déploiement, un outil d'analyse des vulnérabilités des dépendances est disponible. L'OFIT vérifie les bibliothèques nouvelles et existantes, par exemple, le nombre de contributeurs et le nombre de mises à jour récentes des bibliothèques utilisées. Si une bibliothèque existante n'est plus mise à jour ou si des fonctions souhaitées par la communauté ne sont pas implémentées, des alternatives sont examinées. Le gestionnaire de l'application à l'AFC prend ensuite des mesures en fonction de la criticité des problèmes identifiés.

Des tests d'intrusion sont effectués dans l'environnement de test en collaboration avec l'OFIT. Ils sont effectués [redacted] pour les principales applications métier, une planification est en cours pour les autres applications. [redacted]. En cas de vulnérabilités, elles sont vérifiées et testées par l'OFIT. Après cela, elles sont classées par ordre de priorité sur la base d'évaluations de la criticité avec les différentes parties prenantes. Elles sont ensuite introduites dans un système interne de gestion de tickets avec une date de mise en œuvre. Les problèmes majeurs sont résolus dans l'environnement d'acceptation et introduits dans l'environnement de production. Des difficultés sont également rencontrées dans la coordination de la résolution des vulnérabilités.

En cas de problèmes de sécurité détectés par l'OFIT hors tests d'intrusion, si ceux-ci peuvent être résolus en interne, cela se fait [redacted]

[redacted]. Dans le cas contraire, [redacted] et accepte ou non les changements nécessaires pour résoudre les vulnérabilités.

En ce qui concerne la surveillance, les applications sont contrôlées par l'OFIT tels que, par exemple, la mémoire et l'accessibilité des applications grâce à un outil de surveillance interne. En outre, les journaux des applications métier sont stockés [redacted] dans un outil interne de gestion des journaux. Des alertes sont mises en place pour détecter les problèmes de sécurité. Elles contiennent le minimum d'informations nécessaires à une investigation ultérieure. Elles sont ensuite archivées.

Afin de renforcer la communication et l'échange d'informations concernant les applications métier sur le portail, une discussion a lieu [redacted] entre l'AFC et l'OFIT. Si le portail n'est plus accessible alors un processus de gestion des incidents est déclenché.

Finalement, le démantèlement des applications se fait en collaboration avec l'OFIT. Tout est défini et documenté dans un outil interne.

Appréciation

La gestion du portefeuille d'applications, la gestion des changements et le démantèlement des applications sont bien définis et documentés, ce qui permet de mieux s'aligner sur le cycle de vie des applications, d'assurer une utilisation optimale des ressources et de réduire les risques liés à l'obsolescence et à la non-conformité.

L'implémentation des analyses et la gestion des problèmes de sécurité est ciblée. Il manque la définition d'une fréquence minimale des tests d'intrusion afin d'éviter qu'aucun test d'intrusion ne soit effectué pendant une longue période lors de phases sans changement. Un calendrier des tests d'intrusion pour l'année 2024 est disponible. Un calendrier pour 2025 est en préparation. Le CDF renonce donc à formuler une recommandation à ce sujet.

Finalement, la surveillance par l'OFIT des applications métier et la durée de conservation des journaux de [redacted] avant l'archivage sont des points forts qui renforcent la sécurité.

Annexe 1 : Bases légales

Textes législatifs
Loi fédérale sur le Contrôle fédéral des finances (Loi sur le Contrôle des finances, LCF) du 28 juin 1967 (État le 1er septembre 2023), SR 614.0
Loi fédérale sur la protection des données (LPD) du 25 septembre 2020 (État le 1er septembre 2023), SR 235.1
Ordonnance concernant la protection des informations de la Confédération (Ordonnance concernant la protection des informations, OPrI) du 4 juillet 2007 (État le 1er septembre 2023), SR 510.411
Ordonnance sur la protection des données (OPDo) du 31 août 2022 (État le 1er septembre 2023), SR 235.11
Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques, OPCy) du 27 mai 2020 (Etat le 1er avril 2021), SR 120.73

Annexe 2 : Abréviations

AFC	Administration fédérale des contributions
API	Interface de programmation d'application
B2B	Business to Business
CDF	Contrôle fédéral des finances
CIA	Confidentialité, Intégrité et Disponibilité
DFF	Département fédéral des finances
[redacted]	[redacted]
IdP	Fournisseurs d'identité
OFDF	Office fédéral de la douane et de la sécurité des frontières
OFIT	Office fédéral de l'informatique et de la télécommunication
OFC	Ordonnance sur les finances de la Confédération
[redacted]	[redacted]
PKCE	Clé de preuve pour l'échange de code
RPLP	Redevance forfaitaire sur les poids lourds
RTE	Release Train Engineer
SAFe	Scaled Agile Framework

Annexe 3 : Glossaire

DevOps	Mouvement en ingénierie informatique visant à l'unification du développement logiciel et de l'administration des infrastructures, notamment l'administration système.
[redacted]	[redacted] Il met à disposition différents fournisseurs d'identité (IdP) pour l'authentification des employés de l'administration fédérale et des utilisateurs de la cyberadministration et permet, si nécessaire, la connexion d'autres fournisseurs d'identité.
[redacted]	[redacted] qui contient un gros volume de données. Les informations concernant l'utilisateur, les autorisations, les groupes et les périodes sont incorporées dans [redacted].
OWASP	L'Open Web Application Security Project (OWASP) est une organisation à but non lucratif fondée en 2001, dans le but d'aider les propriétaires de sites Web et les experts en sécurité à protéger les applications Web contre les cyberattaques.
[redacted]	[redacted]. Il offre une solution [redacted] et dispose d'une gestion des droits et des utilisateurs.
PKCE	La clé de vérification pour l'échange de codes (PKCE) est une implémentation plus sûre du flux OAuth. La PKCE consiste à garantir que l'application qui démarre le flux d'authentification est la même que celle qui le termine.
Passerelle API	Une passerelle API est un outil de gestion d'API qui se situe entre un client et un ensemble de services backend. Une passerelle API agit comme un proxy inverse pour accepter tous les appels d'interface de programmation d'application (API), regrouper les différents services requis pour les exécuter et renvoyer le résultat approprié.
Release Train Engineer	Il est responsable de coordonner, faciliter et optimiser le processus de livraison de projets multiples interconnectés dans un cadre Agile à grande échelle.
SaFe	Le Scaled Agile Framework® est un ensemble de connaissances qui comprend des conseils structurés sur les valeurs, la planification et la gestion, les rôles et les responsabilités.

Scrum	Scrum est une approche basée sur l'équipe, comme un moyen pour créer de la valeur pour l'entreprise. Les membres de l'équipe travaillent ensemble pour atteindre un but commun. La méthodologie Scrum vise à encourager les échanges entre les membres de l'équipe pour qu'elle puisse apporter de la valeur à l'entreprise.
Widget	Une petite application qui s'intègre à un système d'exploitation, une page Web ou un blog (flux RSS, horloge, mini-jeu, par exemple).

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).