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

Audit de la sécurité de la base de données INFOSTAR

Office fédéral de la justice et Centre de service informatique du Département fédéral de justice et police

CDF-21135 | Prises de position incluses | 14 juillet 2022 | DélFin D5/2022

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	402.21135
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

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 Constatations et appréciations 15

2.1 Pour l'application actuelle, la gouvernance de la sécurité est en place, mais la documentation de sécurité est périmée 15

2.2 Infostar est intégré dans les standards du CSI-DFJP, la maintenance applicative est réduite à un minimum 16

2.3 Les défis de l'organisation du projet Infostar NG 18

2.4 Le projet est dans une passe délicate 19

2.5 L'architecture de sécurité de la nouvelle version est solide, mais les tests doivent être améliorés 20

2.6 Traitement des cyberincidents : les bases sont en place, l'opérationnalisation doit être renforcée 22

2.7 La gestion de la continuité des activités doit être exercée de bout en bout 23

Annexe 1 : Bases légales 25

Annexe 2 : Abréviations 26

Annexe 3 : Glossaire 27

Audit de la sécurité de la base de données INFOSTAR
Office fédéral de la justice et Centre de service informatique du Département fédéral de justice et police

L'essentiel en bref

Infostar est le registre centralisé pour la saisie électronique des événements d'état civil (naissance, mariage, décès, etc.), mis à disposition des cantons par la Confédération depuis 2005. Il compte près de 1200 utilisateurs répartis dans 142 offices de l'état civil. L'application est exploitée par l'Unité Infostar de l'Office fédéral de la justice (OFJ) et le Centre de service informatique du Département fédéral de justice et police (CSI-DFJP). Un projet de modernisation à hauteur de quelque 23,7 millions de francs est en cours, son achèvement était initialement prévu pour 2023.

Dans cet audit, le Contrôle fédéral des finances (CDF) examine si la sécurité de l'information est assurée dans le cadre de l'exploitation de l'application actuelle. Il vérifie aussi si les lacunes de sécurité sont corrigées dans le projet de modernisation et si la collaboration dans le processus de traitement des cyberincidents fonctionne.

Les bases de la sécurité de l'information sont globalement posées dans le cadre de l'exploitation de l'application actuelle et du projet de modernisation, notamment par leur intégration dans l'infrastructure standard du CSI-DFJP. Des lacunes sont toutefois constatées : la documentation de sécurité et l'analyse des risques de l'application doivent être mises à jour. Le projet « Infostar New Generation » est dans une passe difficile, des aménagements dans l'organisation et la planification sont à apporter et la démarche de test est à améliorer. Enfin, les bases du processus de traitement des cyberincidents sont posées, mais une opérationnalisation renforcée et une meilleure communication sont nécessaires.

Application actuelle : une exploitation stable mais une documentation de sécurité périmée

Par son intégration dans l'infrastructure standard du CSI-DFJP, l'application actuelle bénéficie d'une architecture de sécurité éprouvée. L'authentification des utilisateurs, des droits d'accès, un trafic crypté des informations, des redondances sont, entre autres, mis en œuvre. Des comités d'architecture en suivent l'évolution de manière continue.

Les activités d'exploitation applicative et technique sont décrites et appliquées adéquatement. La gestion des utilisateurs, des protections contre les logiciels malveillants, des sauvegardes de sécurité, la surveillance de l'infrastructure et des tests périodiques de sa solidité sont notamment assurés par des experts en la matière. L'exploitation de la solution actuelle est stable, mais sa maintenance est rendue difficile par la complexité de ses programmes.

La gouvernance de la sécurité est en place, les rôles sont définis, pourvus, et clairement délimités entre intervenants. Toutefois, alors qu'Infostar a des besoins accrus en termes de protection de l'information, la documentation de sécurité est largement périmée. Les responsables peuvent ainsi être amenés à sous-estimer les risques auxquels la solution fait face. Les documents de sécurité doivent être mis à jour et une analyse des risques résiduels doit être entreprise et validée.

Une modernisation en difficulté, une organisation de projet et des tests à améliorer

Lancé en 2018, le projet de modernisation d'Infostar est en cours. Les travaux doivent permettre de bénéficier des évolutions techniques et d'apporter des réponses aux difficultés rencontrées dans les activités de maintenance. Le projet est mené selon une méthodologie agile sous la responsabilité de l'OFJ, qui assure notamment la définition des besoins métier. Le CSI-DFJP est en charge de la réalisation.

Le projet fait face depuis plusieurs mois à des difficultés, un fort taux de rotation du personnel est constaté et le poste de chef de projet est pourvu ad interim. Les responsables ont conscience de la situation délicate et ont défini des mesures immédiates. Une nouvelle organisation a été mise en place, des profils sont recherchés sur le marché de l'emploi. Des retards et des dépassements de coûts sont ainsi prévisibles. Le CDF renonce à émettre une recommandation sur ce point, mais demande que la nouvelle organisation prévoie une intégration renforcée des spécialistes de la sécurité et de l'exploitation.

La nouvelle application est réalisée dans le cadre de l'architecture standard du CSI-DFJP. Elle bénéficie donc des solides composantes de sécurité qui y sont mises en œuvre. Le CDF note toutefois que la démarche de test au sein du projet n'est pas encore entièrement aboutie. Il demande en particulier que la profondeur des tests, leur automatisation, les non-régressions et le traitement des défauts soient repensés.

Traitement des cyberincidents et gestion de la continuité : une intégration à renforcer

Les bases du traitement des cyberincidents sont adéquatement définies. Les rôles et responsabilités dans ce domaine sont exercés activement au CSI-DFJP. Les processus sont décrits, mais les bénéficiaires de prestations ne sont pas assez impliqués dans la mise en œuvre de ces processus. Le Centre de service doit améliorer ce point. Il doit aussi réexaminer s'il est opportun d'élaborer des modèles de réponse selon les types d'incidents. Lors de l'audit, les modalités de la gestion de crise étaient en cours de mise à jour, le CDF renonce donc à émettre une recommandation.

Les systèmes de gestion et de remontée des incidents sont mis en œuvre, de même que les points de contact et les voies de signalement. Lors du déroulement d'un incident, les actions et décisions sont documentées. Les outils de surveillance sont en place, les événements sont journalisés et peuvent être analysés au moyen d'utilitaires.

Les modalités de la gestion de la continuité des activités sont définies dans le giron de chaque unité administrative, mais le CDF voit le risque qu'elles soient insuffisamment intégrées. Il conseille à l'OFJ d'organiser pour Infostar des exercices de gestion de la continuité intégrant bénéficiaires et fournisseurs de prestations. Le but est d'améliorer la coordination entre les parties prenantes et de reconnaître les éventuelles faiblesses dans le processus.

Prüfung der Sicherheit der Datenbank INFOSTAR

Bundesamt für Justiz und Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements

Das Wesentliche in Kürze

Infostar ist das zentrale Register für die elektronische Erfassung von Zivilstandsereignissen (Geburt, Ehe, Tod usw.), das der Bund den Kantonen seit 2005 bereitstellt. Rund 1200 Benutzer in 142 Zivilstandsämtern sind daran angeschlossen. Betrieben wird die Anwendung vom Fachbereich Infostar des Bundesamts für Justiz (BJ) und dem Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD). Derzeit läuft ein Modernisierungsprojekt im Umfang von rund 23,7 Millionen Franken, dessen Abschluss ursprünglich für 2023 geplant war.

In der vorliegenden Prüfung untersucht die Eidgenössische Finanzkontrolle (EFK), ob die Informationssicherheit beim Betrieb der aktuellen Anwendung gewährleistet ist. Des Weiteren prüft sie, ob die Sicherheitslücken mit dem Modernisierungsprojekt behoben sind und ob die Zusammenarbeit im Prozess zur Behandlung von Cybervorfällen funktioniert.

Die Grundlagen für die Informationssicherheit im Rahmen des Betriebs der aktuellen Anwendung und des Modernisierungsprojekts sind insgesamt gelegt, u. a. durch ihre Integration in die Standardinfrastruktur des ISC-EJPD. Allerdings sind Lücken festzustellen: Die Sicherheitsdokumentation und die Risikoanalyse der Anwendung müssen aktualisiert werden. Das Projekt «Infostar New Generation» befindet sich in einer schwierigen Phase, Anpassungen in der Organisation und Planung sind vorzunehmen und der Testansatz muss verbessert werden. Schliesslich sind die Grundlagen für den Prozess zur Behandlung von Cybervorfällen gelegt, aber eine stärkere Operationalisierung und eine bessere Kommunikation sind erforderlich.

Aktuelle Anwendung: stabiler Betrieb, aber veraltete Sicherheitsdokumentation

Durch die Integration in die Standardinfrastruktur des ISC-EJPD profitiert die aktuelle Anwendung von einer bewährten Sicherheitsarchitektur. Die Benutzerauthentifizierung, Zugriffsrechte, ein verschlüsselter Informationsverkehr und Redundanzen sind unter anderem implementiert. Architekturboards verfolgen die Entwicklung fortlaufend.

Die Aktivitäten im Anwendungs- und technischen Betrieb werden zweckmässig beschrieben und umgesetzt. Die Benutzerverwaltung, der Schadsoftwareschutz, Sicherheitsbackups, die Infrastrukturüberwachung und periodische Stabilitätstests werden durch Fachpersonen sichergestellt. Der Betrieb der aktuellen Lösung ist stabil, ihre Wartung wird jedoch durch die Komplexität der Programme erschwert.

Eine Security-Governance ist vorhanden, die Rollen sind definiert, besetzt und unter den Beteiligten klar abgegrenzt. Obwohl Infostar einen erhöhten Bedarf an Informationsschutz aufweist, ist die Sicherheitsdokumentation weitgehend veraltet. Dies kann dazu führen, dass die Verantwortlichen die Risiken, denen die Lösung ausgesetzt ist, unterschätzen. Die Sicherheitsdokumente müssen aktualisiert und eine Restrisikoanalyse muss durchgeführt und validiert werden.

Die Modernisierung sieht sich mit Schwierigkeiten konfrontiert, die Projekt- und Testorganisation müssen verbessert werden

Das 2018 lancierte Projekt zur Modernisierung von Infostar ist im Gang. Die Arbeiten sollen technische Entwicklungen nutzen und Antworten auf die Schwierigkeiten finden, die bei den Wartungstätigkeiten auftreten. Das Projekt wird nach einer agilen Methode unter der Leitung des BJ geführt, das insbesondere die Fachbedürfnisse definiert. Das ISC-EJPD ist für die Umsetzung verantwortlich.

Das Projekt ist seit mehreren Monaten mit Schwierigkeiten konfrontiert, die Personalfluktuation ist hoch und die Projektleitungsstelle ist ad interim besetzt. Die Verantwortlichen sind sich der heiklen Situation bewusst und haben Sofortmassnahmen festgelegt. Eine neue Organisation wurde eingeführt, Profile werden auf dem Arbeitsmarkt gesucht. Verzögerungen und Kostenüberschreitungen sind somit absehbar. Die EFK verzichtet auf eine Empfehlung, fordert aber eine verstärkte Integration von Fachpersonen für Sicherheit und Betrieb in die neue Organisation.

Die neue Anwendung wird im Rahmen der Standardarchitektur des ISC-EJPD realisiert. Damit profitiert sie von deren soliden Sicherheitskomponenten. Die EFK stellt aber fest, dass der Testansatz des Projekts noch nicht ausgereift ist. Sie fordert insbesondere, dass die Tiefe der Tests, ihre Automatisierung, die Nichtregression und die Fehlerbehandlung neu überdacht werden.

Behandlung von Cybervorfällen und Kontinuitätsmanagement: Die Integration muss gestärkt werden

Die Grundlagen für die Behandlung von Cybervorfällen sind angemessen definiert. Die Rollen und Zuständigkeiten werden im ISC-EJPD aktiv wahrgenommen. Die Prozesse sind beschrieben, die Leistungsbezüger sind aber nicht genügend in deren Umsetzung eingebunden. Diesen Punkt muss das ISC verbessern. Es sollte auch prüfen, ob es sinnvoll ist, Reaktionsmodelle für verschiedene Arten von Vorfällen zu entwickeln. Zum Prüfungszeitpunkt wurden die Modalitäten des Krisenmanagements aktualisiert, die EFK verzichtet deshalb auf eine Empfehlung.

Die Vorfallsmanagement- und Eskalationssysteme sind implementiert, ebenso die Kontaktstellen und die Meldewege. Bei der Abwicklung eines Vorfalls werden die Handlungen und Entscheide dokumentiert. Die Überwachungsinstrumente sind vorhanden, die Ereignisse werden protokolliert und können mit Hilfsmitteln analysiert werden.

Die Modalitäten des Business Continuity Management werden in den einzelnen Verwaltungseinheiten festgelegt, die EFK sieht jedoch die Gefahr, dass sie nicht ausreichend integriert werden. Die EFK rät dem BJ, Übungen zum Infostar-Continuity-Management mit Einbezug der Leistungsbezüger und -erbringer durchzuführen. Dies mit dem Ziel, die Koordination unter den Beteiligten zu verbessern und allfällige Schwachstellen im Prozess zu erkennen.

Originaltext auf Französisch

Verifica della sicurezza della banca dati INFOSTAR

Ufficio federale di giustizia e Centro servizi informatici del Dipartimento federale di giustizia e polizia

L'essenziale in breve

Infostar è il registro centralizzato per la registrazione elettronica degli eventi relativi allo stato civile (nascita, matrimonio, decesso ecc.) che la Confederazione mette a disposizione dei Cantoni dal 2005. Conta quasi 1200 utenti ripartiti in 142 uffici dello stato civile. L'applicazione è gestita dal Settore Infostar dell'Ufficio federale di giustizia (UFG) e dal Centro servizi informatici del Dipartimento federale di giustizia e polizia (CSI-DFGP). Attualmente è in corso un progetto di modernizzazione i cui costi ammontano a circa 23,7 milioni di franchi e che inizialmente si prevedeva di concludere nel 2023.

Nell'ambito della presente verifica, il Controllo federale delle finanze (CDF) esamina se la sicurezza delle informazioni è garantita quando viene utilizzata l'applicazione corrente. Verifica inoltre se il progetto di modernizzazione è in grado di colmare le lacune a livello di sicurezza e se la collaborazione nel trattamento dei ciberincidenti è efficace.

Nel complesso, le basi per la sicurezza delle informazioni sono state gettate nel quadro dell'utilizzo dell'applicazione corrente e del progetto di modernizzazione, in particolare tramite la loro integrazione nell'infrastruttura standard del CSI-DFGP. Tuttavia, sono state constatate delle lacune: la documentazione di sicurezza e l'analisi dei rischi dell'applicazione devono essere aggiornate. Il progetto «Infostar New Generation» si trova in una fase difficile: si devono apportare modifiche all'organizzazione e alla pianificazione come pure migliorare il processo di test. Infine, vi sono le basi per trattare i ciberincidenti, ma occorre rafforzare l'operatività e perfezionare la comunicazione.

Applicazione corrente: il funzionamento è stabile ma la documentazione di sicurezza è datata

Grazie alla sua integrazione nell'infrastruttura standard del CSI-DFGP, l'applicazione corrente beneficia di un'architettura di sicurezza comprovata. Questa comprende l'autenticazione degli utenti, i diritti di accesso, un traffico criptato delle informazioni e le ridondanze. I comitati di architettura seguono costantemente gli sviluppi.

Le attività di esercizio dell'applicazione e quelle tecnico-operative sono descritte e applicate in maniera adeguata. La gestione degli utenti, la protezione contro i malware, i backup di sicurezza, la sorveglianza dell'infrastruttura e i test periodici della sua stabilità sono assicurati da esperti. Il funzionamento della soluzione corrente è stabile, ma la sua manutenzione è difficile a causa della complessità dei programmi.

Esiste una governance della sicurezza, i ruoli sono definiti e assunti dai collaboratori nonché chiaramente delimitati l'uno dall'altro. Tuttavia, benché le esigenze di Infostar in termini di protezione delle informazioni siano maggiori, la documentazione di sicurezza è in gran parte datata. Ciò potrebbe portare i responsabili a sottovalutare i rischi cui è esposta la soluzione. La documentazione di sicurezza deve essere aggiornata e deve essere svolta e convalidata un'analisi dei rischi residui.

La modernizzazione incontra alcune difficoltà, l'organizzazione del progetto e dei test deve essere migliorata

Il progetto di modernizzazione di Infostar, lanciato nel 2018, è in fase di realizzazione. I lavori dovrebbero permettere di sfruttare gli sviluppi tecnici e fornire delle soluzioni alle difficoltà riscontrate nelle attività di manutenzione. Il progetto è condotto secondo una metodologia agile e sotto la responsabilità dell'UFG, che definisce le esigenze specifiche. Il CSI-DFGP è responsabile della realizzazione.

Da diversi mesi il progetto deve far fronte ad alcune difficoltà. Il ricambio di personale è molto frequente e il posto di capoprogetto è occupato ad interim. I responsabili sono consapevoli di questa situazione delicata e hanno definito misure immediate. È stata introdotta una nuova organizzazione e si cercano i profili necessari sul mercato del lavoro. Pertanto, si prevedono ritardi e sforamenti dei costi. Il CDF rinuncia a formulare una raccomandazione al riguardo, ma chiede alla nuova organizzazione di coinvolgere maggiormente gli specialisti della sicurezza e dell'esercizio.

La nuova applicazione viene realizzata nel quadro dell'architettura standard del CSI-DFGP e beneficia quindi delle sue solide componenti di sicurezza.

Tuttavia, il CDF ha constatato che la preparazione del processo di test non è ancora terminata. In particolare, chiede di rivalutare la profondità dei test e la loro automazione, la non regressione e il trattamento delle lacune.

Trattamento dei ciberincidenti e gestione della continuità: la collaborazione deve essere rafforzata

Le basi per il trattamento dei ciberincidenti sono definite in modo adeguato. I ruoli e le responsabilità in questo ambito sono assunti attivamente in seno al CSI-DFGP. I processi sono descritti, ma i beneficiari delle prestazioni non sono coinvolti a sufficienza nella loro attuazione. Il CSI deve migliorare questo aspetto. Deve inoltre rivalutare l'opportunità di elaborare dei modelli di risposta in base al tipo di incidente. Siccome al momento della verifica le modalità di gestione delle crisi erano in fase di aggiornamento, il CDF ha rinunciato a formulare una raccomandazione al riguardo.

I sistemi di gestione degli incidenti e le procedure di escalation sono implementati, come pure i servizi di contatto e i canali di comunicazione. Durante il trattamento degli incidenti, le azioni e le decisioni vengono documentate. Sono disponibili strumenti di monitoraggio e gli eventi vengono registrati e possono essere analizzati tramite appositi ausili.

Le modalità di gestione della continuità operativa sono definite all'interno di ciascuna unità amministrativa, ma il CDF teme che non siano sufficientemente integrate. Consiglia all'UFG di organizzare per Infostar degli esercizi di gestione della continuità che coinvolgano i beneficiari e i fornitori di prestazioni allo scopo di migliorare il coordinamento tra le parti interessate e individuare eventuali punti deboli nel processo.

Testo originale in francese

Security audit of the INFOSTAR database

Federal Office of Justice and IT Service Centre of the Federal Department of Justice and Police

Key facts

Infostar is the centralised register for the electronic registration of civil status events (births, marriages, deaths, etc.), made available to the cantons by the Confederation since 2005. It has almost 1,200 users across 142 civil register offices. The application is managed by the Infostar Unit of the Federal Office of Justice (FOJ) and the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP). A modernisation project costing some CHF 23.7 million is currently under way, with completion originally planned for 2023.

In this audit, the Swiss Federal Audit Office (SFAO) examined whether information security is guaranteed when the application is currently used. It also examined whether the security vulnerabilities in the modernisation project have been remedied and whether the cooperation in the process of handling cyberincidents is working.

The fundamentals of information security are broadly in place for the operation of the current application and the modernisation project, including their integration into the standard infrastructure of the ISC-FDJP. However, there are shortcomings: the application's security documentation and risk analysis need to be updated. The Infostar New Generation project is in a difficult phase: organisational and planning adjustments are required and the testing process needs to be improved. Finally, the foundations of the cyberincident handling process have been laid, but greater operationalisation and better communication are necessary.

Current application: stable performance but outdated security documentation

Through its integration into the standard infrastructure of the ISC-FDJP, the current application benefits from a tried and tested security architecture. User authentication, access rights, encrypted information traffic and redundancies are among the features that have been implemented. Architectural committees monitor the evolution of the system on an ongoing basis.

The application and technical operation activities are described and applied appropriately. User management, malware protection, security backups, monitoring of the infrastructure and periodic testing of its robustness are ensured by specialists. The current solution's performance is stable, but its maintenance is made difficult by the complexity of its programs.

Security governance is in place and roles are defined, staffed, and clearly defined between stakeholders. However, as Infostar's information protection needs have increased, the security documentation is largely out of date. This can lead those responsible to underestimate the risks the solution faces. The security documentation should be updated and a residual risk analysis undertaken and validated.

Modernisation in difficulty, project organisation and testing need improvement

Launched in 2018, the Infostar modernisation project is under way. The work should make it possible to benefit from technical developments and provide answers to the difficulties encountered during maintenance activities. The project is being carried out using agile methodology under the responsibility of the FOJ, which is in charge of defining the business requirements. The ISC-FDJP is in charge of implementation.

The project has been experiencing difficulties for several months, with high staff turnover and the project manager's position being filled on an interim basis. Those in charge are aware of the delicate situation and have defined some immediate measures. A new organisational structure has been put in place and profiles are being sought on the job market. As a result, delays and cost overruns are to be expected. The SFAO decided not to make a recommendation in this regard, but it did ask that the new organisational structure provide for closer integration of the security and operational specialists.

The new application is being implemented within the framework of the standard architecture of the ISC-FDJP. It therefore benefits from the strong security components already in place. The SFAO noted, however, that the project's testing process is not yet fully developed. In particular, the SFAO requested that the depth of the tests, their automation, the non-regression and the handling of defects be rethought.

Cyberincident response and continuity management: integration needs to be improved

The basis for handling cyberincidents is well defined. Roles and responsibilities in this area are actively pursued at the ISC-FDJP. The processes are described, but service users are not sufficiently involved in the implementation of these processes. The Service Centre needs to improve this. It should also reconsider whether it is appropriate to develop response models for different types of incidents. At the time of the audit, the crisis management procedures were being updated, which is why the SFAO refrained from issuing a recommendation.

Incident management and reporting systems are in place, as are contact points and reporting channels. Actions and decisions taken during an incident are documented. Monitoring instruments are in place, and events are logged and can be analysed using tools.

Business continuity management procedures are defined within each administrative unit, but the SFAO found that there is a risk that they are not sufficiently integrated. It has advised the FOJ to organise continuity management exercises for Infostar that include users and service providers. The aim is to improve coordination between the parties involved and to identify any weaknesses in the process.

Original text in French

Prise de position générale des audités

Prise de position de l'Office fédérale de la justice

Die Prüfung der Sicherheit des Systems Infostar durch die EFK widerspiegelt die Bedeutung, welche Infostar als zentrale Datenquelle für das Zivilstandswesen zukommt. Die Sicherheit des Systems ist ein zentraler Aspekt. Insofern erachtet es das BJ als erfreulich, dass das Resultat der Untersuchung zeigt, dass keine wesentlichen Schwachstellen erkannt wurden und die Sicherheit von Infostar gewährleistet ist. Die punktuellen Empfehlungen der EFK werden als sinnvoll erachtet und durch das BJ umgesetzt.

Prise de position du Centre de service informatique du Département fédéral de justice et police

Das ISC-EJPD bedankt sich bei der Eidgenössischen Finanzkontrolle für die konstruktive Durchführung der Prüfung. Die positiv ausgefallene Beurteilung der durch das ISC-EJPD zur Verfügung gestellten und betriebenen Standardinfrastruktur nehmen wir mit Befriedigung zur Kenntnis.

1 Mission et déroulement

1.1 Contexte

Depuis 2005, tous les événements d'état civil (par ex. naissance, mariage, décès, etc.) sont enregistrés par voie électronique dans le registre centralisé Infostar (de l'allemand INFOrmatisiertes STAndesRegister), auquel tous les offices de l'état civil suisses sont raccordés. La solution a pour objectif de gérer efficacement les données, sans perte de qualité et avec une sécurité garantie. Son fonctionnement est jugé stable et ses utilisateurs sont majoritairement satisfaits. Le système est sous la responsabilité de l'Office fédéral de la justice (OFJ), son exploitation technique est assurée par le Centre de service informatique du Département fédéral de justice et police (CSI-DFJP).

Le registre Infostar permet la saisie et l'enregistrement d'événements d'état civil et la production d'actes prouvant ces événements. Il compte près de 1200 utilisateurs, répartis dans 142 offices de l'état civil. Un total de quelque 10,5 millions de personnes, 1,7 millions de naissances, 800 000 mariages et 1,2 millions de décès sont enregistrés dans le système[1].

Le système a migré sur une plateforme Java en 2008, mais sa technologie ne correspond plus à plusieurs égards aux critères et aux possibilités actuels. La maintenance et la mise en œuvre de nouvelles fonctionnalités sont devenues difficiles à assurer, alors que les bases légales évoluent. Pour ces raisons, l'OFJ a lancé en avril 2018 un projet de modernisation de l'application (Infostar New Generation, Infostar NG). Le projet est doté d'un budget de près de 23,7 millions de francs (y compris les dépenses de personnel interne), son terme était initialement prévu pour fin 2023.

1.2 Objectif et questions d'audit

Dans cette révision, le Contrôle fédéral des finances (CDF) examine la sécurité de l'information dans le cadre de l'exploitation de l'application Infostar actuelle et future, et le remplacement en cours dans le cadre du projet Infostar NG. Il vise en particulier à répondre aux questions suivantes :

- La sécurité de l'information (confidentialité, disponibilité et intégrité des données) est-elle assurée conformément aux standards et aux instructions en vigueur ?
- Les lacunes identifiées en termes de sécurité de l'information sont-elles adressées dans le projet Infostar NG et est-il assuré que la sécurité de l'information de la nouvelle application est garantie ?
- Le flux d'information et la collaboration dans le processus de traitement de cyberincidents fonctionnent-ils pour Infostar entre tous les niveaux fédéraux et à l'intérieur de l'administration fédérale ?

[1] Chiffres au 31 mai 2022, source : OFJ.

1.3 Etendue de l’audit et principe

L’audit a été mené du 28 mars au 25 mai 2022 par André Stauffer (responsable de révision), Warren Paulus et Elizabeth O’Sullivan. 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’OFJ et le CSI-DFJP. 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 16 juin 2022. L’OFJ était représenté par le chef du domaine de direction Droit privé et par le chef de l’unité Infostar. Le CSI-DFJP était représenté par le chef des Services centraux. Pour le CDF, le directeur, un responsable de mandat et le responsable de révision ont participé.

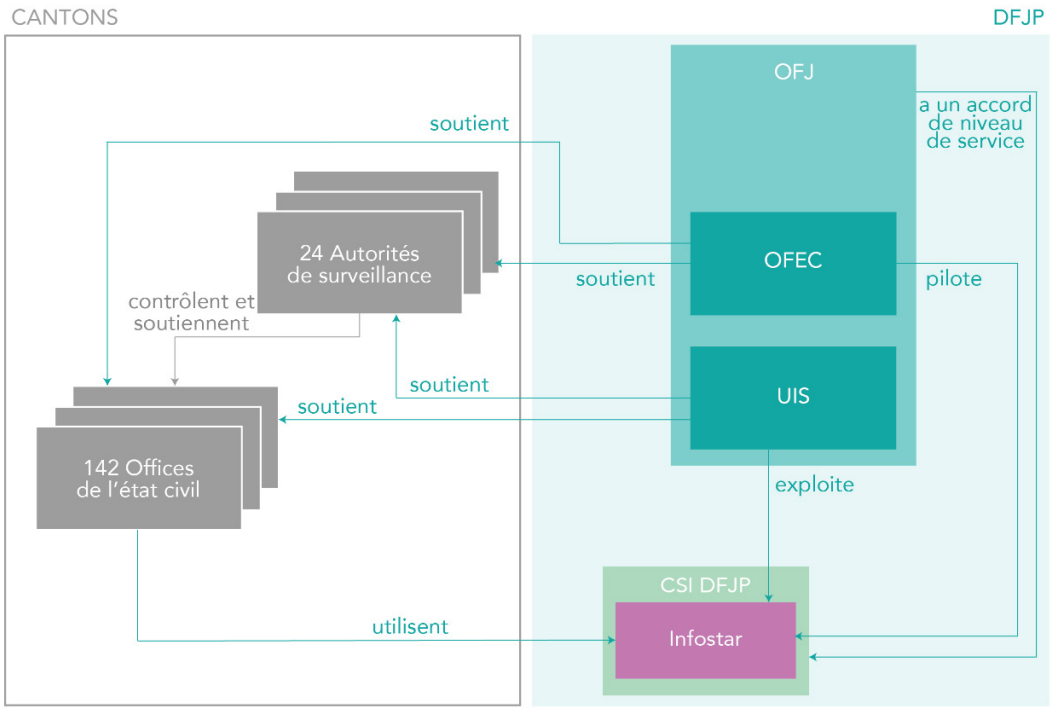
Le CDF remercie l’attitude coopérative et rappelle qu’il appartient aux directions d’office, respectivement aux secrétariats généraux de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 Constatations et appréciations

2.1 Pour l'application actuelle, la gouvernance de la sécurité est en place, mais la documentation de sécurité est périmée

L'application Infostar est exploitée par la Confédération pour les cantons et soutient les officiers de l'état civil dans l'exercice de leur fonction au sens du code civil suisse[2] et de l'ordonnance sur l'état civil[3]. Ces bases légales définissent les tâches, les compétences et les responsabilités des diverses parties prenantes. L'OFJ est responsable de la mise au point, du perfectionnement et de l'exploitation du système, et prend les mesures nécessaires pour garantir la protection et la sécurité des données. L'Office fédéral de l'état civil (OFEC) appartient au domaine de direction Droit privé de l'OFJ, il exerce la haute surveillance sur l'état civil suisse. Il élabore notamment des instructions concernant la tenue des registres de l'état civil et inspecte les offices de l'état civil ainsi que les autorités de surveillance et des archives cantonales de l'état civil. L'Unité Infostar (UIS) fait partie du même domaine de direction, elle est responsable des aspects métier de l'exploitation, du développement et de la formation, ainsi que du support aux utilisateurs. Elle gère aussi les droits d'accès. Le CSI-DFJP, fournisseur de prestations pour applications à exigences élevées, assure l'exploitation technique de la solution. Un accord de niveau de service en régit l'hébergement. Au niveau cantonal les autorités de surveillance veillent à l'exacte exécution des tâches de l'état civil dans leur canton.



Infographie 1 : offices et autorités impliqués (Source OFJ, illustration CDF).

[2] Code civil suisse du 10 décembre 1907 (CC, RS 210), notamment les articles 33 et 39 à 49 ainsi que les articles 90 ss.
[3] Ordonnance sur l'état civil du 28 avril 2004 (OEC, RS 211.112.2).

Pour l'exploitation de l'application actuelle, les rôles liés à la sécurité de l'information sont définis et pourvus: un délégué à la sécurité de l'information est en poste tant à l'OFJ qu'au CSI-DFJP. Le CDF relève que dans cette constellation, l'exploitation de l'application fonctionne de manière stable depuis des années et qu'aucun incident de sécurité significatif n'a été rapporté.

La classification des données de l'application est établie, des mesures de protection en relation avec le niveau déclaré sont documentés. Lors de la révision, le règlement de traitement était en cours d'actualisation. La documentation de sécurité de l'application existante est par contre largement périmée. Au Département fédéral de justice et police (DFJP), le concept de sécurité de l'information et de protection des données (SIPD) d'un objet regroupe les mesures de protection de base et celles répondant à un besoin accru. Pour Infostar, la dernière actualisation documentée de ce concept date de 2010 et la version remise au CDF n'est pas formellement validée.

Appréciation

Les rôles et responsabilités en matière de sécurité de l'information sont suffisamment établis et mis en œuvre pour la solution Infostar. La documentation de sécurité de l'application actuelle accuse cependant un retard important, alors qu'elle doit être actualisée tous les cinq ans. Avec le développement de la technologie et l'augmentation des menaces, les responsables de l'application pourraient être amenés à sous-estimer les risques de sécurité encourus. Au vu du retard prévisible du projet de modernisation, l'évaluation de la situation des risques et la documentation de la mise en œuvre des mesures de la protection de base doivent être mises à jour.

Recommandation 1 (Priorité 1)

Le CDF recommande à l'OFJ de mettre à jour la documentation de sécurité et de protection des données de l'application Infostar (Concept SIPD, règlement de traitement).

La recommandation est acceptée.

Prise de position de l'OFJ

Das BJ ist mit der Empfehlung einverstanden. Das BJ prüft in regelmässigen Abständen die ISDS-Konzepte für alle Fachapplikationen des BJ. Das vorliegend betroffene Infostar i13 wird in diesem Rahmen wie vorgesehen mit allen anderen ISDS-Konzepten noch dieses Jahr überarbeitet.

2.2 Infostar est intégré dans les standards du CSI-DFJP, la maintenance applicative est réduite à un minimum

L'application Infostar est hébergée par le CSI-DFJP. La conception de l'application est ancienne et la technologie client utilisée (client « lourd », installé sur le poste de travail de l'utilisateur) ne fait plus partie des produits stratégiques du centre de service. Néanmoins, l'application s'intègre dans le cadre de l'infrastructure et des procédures d'exploitation standard du centre de service et ne bénéficie d'aucune exception architecturale. Sous l'angle de la sécurité, les éléments architecturaux suivants ressortent:

- Les utilisateurs accèdent à l'application au travers du portail à signature unique (Single Sign On, SSO) du DFJP. Cette composante permet l'identification et l'authentification des utilisateurs et pilote les accès aux applications.

- Des droits d'accès spécifiques sont gérés en plus pour les utilisateurs d'Infostar.
- Les composantes de l'application sont localisées sur des zones sécurisées du réseau informatique, la communication entre les composantes est cryptée.
- Des serveurs applicatifs miroirs sont en service, permettant un fonctionnement redondant.
- L'environnement productif est séparé des environnements de développement, de test et d'intégration ; les environnements de développement et de test ne contiennent pas de copies de données productives. Les accès à l'environnement d'intégration, qui contient une copie des données productives, sont restreints.
- Des instances spécialisées (comité d'architecture au niveau du centre de service et du département) suivent en continu l'évolution de l'architecture. Des réunions périodiques sont organisées, les décisions sont dument documentées.

Les processus d'exploitation applicative sont décrits, autant chez le bénéficiaire que chez le fournisseur de prestations. Du point de vue de la sécurité de l'information, les points suivants ressortent :

- L'UIS gère le processus de création des nouveaux utilisateurs, de suppression des comptes utilisateurs obsolètes et l'assignation des droits spécifiques. Des listes d'utilisateurs et de leurs droits sont régulièrement éditées et contrôlées.
- Des outils de protection contre les logiciels malveillants sont mis en œuvre. Au moment de la révision, des compléments étaient encore prévus.
- Des sauvegardes de sécurité sont régulièrement effectuées, sur différents supports. La récupération des données est occasionnellement testée.
- Divers outils de surveillance de l'infrastructure sont en service, les journaux d'événements sont consolidés. Des mécanismes d'alertes sont mis en œuvre, divers rapports et tableaux de bord permettent un suivi des événements.
- L'installation et la configuration de logiciels se fait par les spécialistes du centre de service, selon un processus documenté et contrôlé.
- La solidité de l'infrastructure est suivie de manière continue. En cas de vulnérabilité, un processus est appliqué, dont les étapes et les intervenants varient selon la gravité. Les étapes de remédiation sont documentées. Le CDF relève que le document de traitement des vulnérabilités doit être actualisé sous peu.
- Des audits de la solidité de l'infrastructure sont occasionnellement commandés à des sociétés spécialisées, selon les besoins, et sont documentés.

En 2008 dans le cadre d'une migration technique, un outil a traduit les programmes d'Infostar du langage de programmation COOL:Gen vers Java, le premier étant arrivé en fin de vie. L'opération a ajouté une couche de complexité dans le code de l'application et celui-ci est devenu moins lisible. Ceci a rendu la maintenance applicative d'Infostar plus difficile. La mise en œuvre de nouvelles fonctionnalités et de corrections peut occasionner de graves dysfonctionnements et présenter des risques importants pour la stabilité de l'application.

En cas de nécessité, un spécialiste interne du CSI-DFJP prend en charge les développements. Mais à chaque modification des programmes, des activités doivent être planifiées pour tester non seulement les nouvelles fonctionnalités mais aussi les éventuelles régressions. Une

batterie de tests métier doit être exécutée. Avant la mise en production des modifications, les tests sont documentés et une validation formelle est donnée par le métier. Dans l'environnement d'intégration, des copies de données productives sont disponibles pour effectuer des tests représentatifs. Ces copies ont été validées par le responsable applicatif.

Ces activités mobilisent d'importantes ressources chez les bénéficiaires de prestations. La maintenance applicative est réduite à un minimum, dans l'attente de la nouvelle génération de l'application.

Appréciation

Grâce à son intégration dans l'infrastructure standard du CSI-DFJP, Infostar bénéficie des nombreuses fonctionnalités de sécurité qui y sont mises en œuvre. Les procédures d'exploitation définies sont adéquates. Le CDF n'a toutefois pas vérifié qu'elles étaient systématiquement et intégralement appliquées.

De manière générale, les risques liés à la sécurité de l'information sont en augmentation. Dans ce contexte, une attention et une amélioration continue de l'architecture de sécurité et des procédures d'exploitation sont indispensables. Le CSI-DFJP satisfait à ces éléments. L'exploitation d'Infostar est suffisamment équipée pour faire face au courant normal.

Le CDF note les difficultés et les risques liés à la maintenance de l'application actuelle. Dans ce contexte, il juge compréhensible la réduction des activités de maintenance. Le CDF souligne la nécessité de la mise en œuvre rapide de la nouvelle génération d'Infostar.

2.3 Les défis de l'organisation du projet Infostar NG

En réponse aux difficultés rencontrées dans les activités de maintenance et pour bénéficier des évolutions techniques, l'OFJ a lancé en avril 2018 un projet de modernisation de l'application (Infostar NG – New Generation). La plateforme technique est actualisée et de nouveaux événements d'état civil sont ajoutés pour suivre l'évolution des bases légales.

Un des dirigeants de l'OFJ assure la fonction de mandant de projet, un comité de projet suit l'avance des travaux. Des spécialistes de l'office assurent la direction du projet et représentent les intérêts du domaine métier. La mise en œuvre de la nouvelle solution est prise en charge par le CSI-DFJP et repose en partie sur des spécialistes externes. L'organisation n'est toutefois pas au complet. Le poste de chef de projet est occupé ad interim par le responsable de l'UIS après le départ du titulaire en décembre 2021. Un spécialiste qualifié est recherché sur le marché de l'emploi. La rotation du personnel de projet est élevée et plusieurs postes clés viennent d'être repourvus (par ex. architecte du projet, chef de projet développement, responsable des tests).

En réponse à ces défis, une nouvelle organisation de projet a été mise en place au niveau de la réalisation : trois groupes de livraison de produit sont créés, composés chacun de représentants du métier, d'analystes métier et de développeurs. Cette nouvelle organisation n'inclut pas explicitement des spécialistes de la sécurité ou des représentants de l'exploitation. Ceux-ci sont impliqués en cas de besoin, mais ne participent par exemple pas régulièrement aux réunions de projet.

Appréciation

L'organisation de projet a subi des changements, le CDF note qu'ils doivent encore faire leurs preuves. Il partage les soucis de l'OFJ quant à la rotation du personnel et relève que des mesures sont définies, mais que l'assèchement du marché du travail pour les spécialistes qualifiés complique la donne. Sur ce point, le CDF renonce à émettre une recommandation.

Il estime par contre que le projet n'intègre pas suffisamment directement les spécialistes de la sécurité et de l'exploitation. Dans un contexte DevOps tel qu'il est pratiqué par le projet, une intégration renforcée est nécessaire.

Recommandation 2 (Priorité 1)

Le CDF recommande à l'OFJ d'intégrer de manière renforcée les spécialistes de la sécurité et de l'exploitation dans le projet Infostar NG. Il veillera notamment à modifier l'organigramme de projet en conséquence, définir les tâches et compétences de ces spécialistes dans le projet et les intégrer dans les réunions.

La recommandation est acceptée.

Prise de position de l'OFJ

Das BJ ist mit der Empfehlung einverstanden. Das BJ teilt die Einschätzung der EFK, dass für das Projekt Infostar NG der Einbezug von Sicherheits- und Betriebsspezialisten wichtig ist. Die Projektleitung wird die wiederkehrende Einbindung von beiden Spezialisten (Security und Betrieb) in die dafür nötigen Gefässe umgehend prüfen und mit dem ISC-EJPD abstimmen.

2.4 Le projet est dans une passe délicate

Le projet est mené selon une méthodologie agile. Une feuille de route a été élaborée, les étapes majeures du développement sont structurées en incréments de produit. Les exigences sont gérées au sein d'un backlog de produit et des sprints sont organisés. Divers rapports permettent le suivi d'avancement, dans le cockpit ICT, lors des réunions du comité de projet et à la clôture d'un incrément de produit. En 2021 déjà, ils pointent les difficultés du projet, par exemple celles liées à la gestion des équipes de développement ou à la communication entre fournisseur et bénéficiaire de prestations. Diverses mesures sont proposées et mises en œuvre, manifestement avec des résultats insuffisants jusqu'ici, puisque l'évaluation reste négative. Le rapport pour l'incrément de produit 9 du printemps 2022 laisse apparaître une situation mitigée : le travail avance, mais plus lentement que prévu, des défauts sont constatés dans les livraisons de logiciel. Malgré l'implication jugée encourageante des utilisateurs finaux, la maturité et les ressources du testing doivent être améliorées. Dans ce contexte, l'OFJ a décidé de poursuivre le projet mais met en œuvre des mesures immédiates. Outre le changement de l'organisation de la réalisation déjà évoqué ci-dessus, le CDF relève :

- Un poste de chef de projet a été ouvert à l'OFJ. Dans l'attente d'un engagement, le chef de projet ad interim a été relevé de certaines de ses fonctions pour se concentrer sur les missions prioritaires.
- Un comité exécutif ad hoc composé de dirigeants de l'OFJ et du CSI-DFJP a été créé, avec pour mission d'identifier les difficultés et de prendre les mesures rapides pour les résoudre.

- Dans son sillage, plusieurs rapports d'experts sont produits pour analyser les causes de la situation et proposer des mesures correctives. Certains de ces rapports pointent une communication insuffisante entre le métier et les développeurs. Un spécialiste externe est mandaté pour faciliter la communication.
- L'analyse de la feuille de route conclut à un retard conséquent. Une adaptation de la planification est lancée et doit aboutir en août 2022 : les composantes du produit viable minimum (Minimum viable product, MVP) seront redéfinies, la date de fin de projet et l'impact sur les ressources et les coûts seront recalculés.

Appréciation

Le projet est dans une situation délicate. Le CDF relève que les difficultés sur le plan de la conduite du projet et des équipes ont été amplifiées du fait de la crise sanitaire. Les approches agiles et le travail à domicile peuvent être difficiles à concilier. Les mesures correctives prises initialement n'ont en tous cas pas suffi à redresser la situation. Dans ce contexte, l'adaptation de la planification du projet prévue pour août 2022 paraît indispensable. Des dépassements de coûts et de délais sont prévisibles.

Le CDF estime plausible le deuxième train de mesures en cours de mise en œuvre. Leur succès n'est toutefois pas garanti, il dépendra de la rigueur de leur suivi et de l'engagement des bonnes personnes pour les postes encore vacants. L'attention du management est donnée, des mesures sont en cours, le CDF renonce à ce stade à émettre une recommandation.

2.5 L'architecture de sécurité de la nouvelle version est solide, mais les tests doivent être améliorés

Un des objectifs affichés du projet est de gagner en flexibilité dans la maintenance future du système, en particulier de faciliter les évolutions fonctionnelles sans mettre en danger la stabilité du système. Dans le cadre du projet l'application est réécrite en utilisant les outils définis dans l'architecture logicielle de référence du CSI-DFJP. Des contrôles manuels et automatiques sont mis en œuvre dans le processus de développement pour s'assurer de la tenue des bonnes pratiques de codage. Des règles régissent le travail des développeurs et spécialistes externes.

La documentation de sécurité de la nouvelle application est disponible et validée. Les mesures de la protection de base sont décrites. Le concept SIPD identifie un besoin de protection accrue et énonce les mesures à prendre pour le satisfaire. Une majorité d'exigences de sécurité de l'information sont couvertes au travers de l'architecture de référence et de sécurité du CSI-DFJP. Celle-ci prévoit notamment l'utilisation du portail SSO pour l'accès aux applications, le cryptage des informations en transit, la segmentation du réseau en zones sécurisées et séparées par des pare-feux (firewalls), la redondance du matériel et la journalisation des modifications dans les applications. Des règles sont aussi définies pour la gestion des environnements de développement, de test et d'intégration, qui sont séparés des systèmes productifs. Le projet Infostar NG se base sur cette architecture, aucune exception n'est prévue. L'architecture de référence évolue constamment, des audits de sécurité sont organisés périodiquement et des mesures de protection additionnelles sont mises en œuvre en cas de besoin.

Un certain nombre d'exigences de sécurité spécifiques à l'application sont définies (par exemple les autorisations fines ou l'intégrité des données liées à la « bi-temporalité [4]»). Ces exigences sont documentées dans le backlog de produit, au titre des exigences non-fonctionnelles. Le CDF a constaté que leur définition était incomplète à certains égards, surtout les critères d'acceptation, qui ne sont pas décrits.

Un concept de test est défini, mais il n'est pas finalisé ni validé. Des cas de test existent, basés sur les processus dans le système actuel, mais des plans de tests n'ont pas pu être remis au CDF. Le rapport de l'incrément produit 9 du printemps 2022 soulève par ailleurs plusieurs faiblesses au niveau des tests : leur degré de profondeur est insuffisant, des erreurs constatées ne sont pas corrigées à temps, les tests de non-régression doivent être améliorés. L'automatisation des tests pour la partie métier n'en est qu'à ses débuts. C'est dans ce contexte qu'un nouveau responsable des tests externe vient de prendre ses fonctions dans le projet.

Appréciation

La faiblesse de l'application actuelle est identifiée, le projet s'est donné les moyens de l'éliminer. Des audits de réalisation ont toutefois montré que la qualité n'était pas toujours au rendez-vous. Le projet a identifié ce point, les mesures correctives sont définies mais doivent être mises en œuvre continuellement, notamment au travers de la démarche de test.

La documentation de sécurité est actuelle et validée. Pour le CDF, l'intégration de la nouvelle application au sein de l'architecture de référence et de sécurité contribue à lui assurer un degré adéquat de sécurité. Pour les exigences spécifiques à l'application, la définition des critères d'acceptation manque, ce qui pose problème pour l'opérationnalisation des tests. Les critères de détail qui permettent de juger si une fonction répond aux exigences font en effet défaut.

Le CDF souligne le degré de maturité encore insuffisant des tests. Les réflexions sur leur profondeur, les mécanismes assurant que les défauts identifiés soient traités dans les délais, l'exécution systématique de tests de non-régression et l'automatisation des tests utilisateurs par exemple, sont encore inabouties.

Recommandation 3 (Priorité 1)

Le CDF recommande à l'OFJ de renforcer l'opérationnalisation des tests dans le cadre du projet Infostar NG. Il veillera à finaliser et valider le concept de tests et à régler les aspects de la profondeur des tests, du traitement des erreurs constatées, des tests de non-régression et de l'automatisation. Le projet veillera aussi à ce que la démarche définie soit appliquée.

La recommandation est acceptée.

Prise de position de l'OFJ

Das BJ ist mit der Empfehlung einverstanden. In Absprache mit dem ISC-EJPD wird dessen Umsetzung bereits laufend in das Projekt Infostar NG integriert.

[4] Pour une même personne, les événements d'état civil sont soumis aux bases légales valables au moment de leur survenance. Des bases légales différentes peuvent ainsi s'appliquer aux événements d'une personne en fonction du temps où ils ont eu lieu.

2.6 Traitement des cyberincidents : les bases sont en place, l'opérationnalisation doit être renforcée

Les rôles et responsabilités du traitement des cyberincidents sont définis au sein du CSI-DFJP. Ils sont remplis et exercés activement. Le CDF relève que le document central régissant ces aspects va être actualisé en 2022. Une procédure de gestion des cyberincidents est définie, la description comprend les différents intervenants (fournisseurs de prestations, bénéficiaires de prestations, Centre national pour la cybersécurité (NCSC). Le CDF note que dans le cas d'Infostar, l'OFJ est peu informé des détails de ce processus. Il relève aussi que le CSI-DFJP n'a pas de modèles de réponse selon les types d'incidents *(playbooks)*, ils sont considérés comme trop peu flexibles et détachés du contexte des incidents.

Le système de gestion et de remontée des incidents est défini et mis en œuvre. Les points de contact et les voies de signalement sont décrits. Les actions à entreprendre sont définies en fonction de la gravité de l'incident, un délai est fixé pour la réponse. Au fur et à mesure du déroulement de l'incident et de la réponse, les actions et décisions sont consignées dans un formulaire.

Des outils de contrôle et de surveillance sont mis en œuvre pour l'environnement Infostar. Ils suivent en continu les paramètres de fonctionnement des composantes de l'infrastructure et le réseau. Les événements sont journalisés, des utilitaires permettent une exploitation de ces journaux. En cas d'anomalies, des alertes sont envoyées aux personnes en charge.

Le CDF relève que la description des rôles et responsabilités, les plans et procédures et les modalités de la communication en cas de crise étaient aussi en cours d'actualisation au moment de l'audit.

Appréciation

Les bases du traitement des cyberincidents sont adéquatement définies. Le CDF relève toutefois que les bénéficiaires de prestations sont insuffisamment impliqués dans sa mise en œuvre au sens de l'art. 14 de l'ordonnance sur la protection contre les cyberrisques[5]. Il s'interroge aussi sur le manque de modèles de réponse *(playbooks)*. Le CDF estime que s'ils sont définis au bon niveau de détail et pour les types d'incidents les plus fréquents, ils peuvent contribuer à améliorer la vitesse de réaction et à harmoniser les procédures de réponse entre les différents domaines spécialisés du CSI-DFJP.

Le CDF n'a pas constaté de faiblesse majeure dans la définition et le fonctionnement des systèmes de gestion et de remontée des incidents, ni dans les outils de contrôle et de surveillance.

Au vu des remaniements en cours, le CDF renonce à émettre une appréciation sur l'organisation, les processus et la communication en cas de crise. Il attend que ces documents soient finalisés rapidement.

Recommandation 4 (Priorité 1)

Le CDF recommande au CSI-DFJP de renforcer l'opérationnalisation des procédures de traitement des cyberincidents, en impliquant de manière accrue les bénéficiaires de prestations (OFJ, cantons) dans la définition du détail des étapes et des compétences

[5] Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale du 27 mai 2020 (OPCy, RS 120.73).

décisionnelles dont relèvent les mesures d'urgence. Le CSI-DFJP veillera aussi à réanalyser l'opportunité de définir des modèles de réponse pour les types d'incidents les plus fréquents.

La recommandation est acceptée.

Prise de position du CSI-DFJP

Bereits heute ist definiert, dass abhängig von der Kritikalität eines Vorfalls die Sicherheitsverantwortlichen bzw. die Anwendungsverantwortlichen der Leistungsbezüger in die Prozesse zur Bewältigung des Vorfalls miteinbezogen werden. Das ISC-EJPD wird bei der Weiterentwicklung der Grundlagen für die Behandlung von Cybervorfällen – wie von der Empfehlung gefordert – die Operationalisierung der Verfahren verstärkt berücksichtigen.

2.7 La gestion de la continuité des activités doit être exercée de bout en bout

Les exigences portant sur la gestion de la continuité des activités sont définies. L'OFJ a décrit les plans de continuité pour ses processus, les responsabilités et remplaçants sont définis, de même que les principes de la communication et la gestion du personnel en cas de crise. Le personnel clé est défini par prestation de l'office, notamment pour Infostar. Des listes de contrôle sont aussi à disposition, elles décrivent les étapes à suivre dans les cas où la continuité doit être assurée. Ces listes sont complétées par un plan de mesures spécifiques pour l'utilisation de solutions manuelles pour assurer la continuité du processus. Ces solutions mentionnent les éléments assurant la confidentialité des informations transmises manuellement. Pour Infostar, une plateforme redondante est exploitée.

Le CSI-DFJP a établi une stratégie et des plans de continuité pour ses processus, après avoir dûment identifié ses processus critiques. Les modalités de la reprise après sinistre sont décrites.

Pour Infostar, des exercices intégrés de gestion de la continuité (entre bénéficiaires et fournisseur de prestation) ne sont pas systématiquement organisés.

Appréciation

Les aspects de la gestion de la continuité sont définis dans le giron de chaque unité administrative (bénéficiaire et fournisseur de prestations), mais le CDF voit le risque que les mesures et les étapes définies soient insuffisamment intégrées entre elles. Des exercices en commun, entre tous les intervenants dans la production et l'utilisation de la prestation Infostar, font défaut. De tels exercices peuvent aider à mieux coordonner les étapes entre les différentes parties impliquées en cas de crise et à identifier les éventuelles faiblesses.

Recommandation 5 (Priorité 1)

Le CDF recommande à l'OFJ d'organiser des exercices intégrés de la gestion de la continuité des activités. Il veillera à mettre l'accent sur les aspects de la communication entre utilisateurs finaux (cantons), exploitant applicatif et fournisseur de prestations et sur la coordination entre activités métier et techniques (reprise du fonctionnement des systèmes).

La recommandation est acceptée.

Prise de position de l'OFJ

Das BJ erachtet integrierte Übungen zwischen den betroffenen Einheiten zum Kontinuitätsmanagement ebenfalls als sinnvoll und wird die Empfehlung umsetzen. Im jetzigen System existiert mit den «Notfallkoffer» ein technologieunabhängiges Instrument zur Verfügung, mittels dem eine verzugslose Weiterarbeit in den Zivilstandsämtern möglich ist. Eine grossflächige Übung des Business Continuity Management mit mehreren Bundesstellen und kantonalen Ämter erfolgt sinnvollerweise auf der Basis des neuen Systems.

Annexe 1 : Bases légales

Textes législatifs et stratégies
Code civil suisse (CC) du 10 décembre 1907, RS 210
Ordonnance sur l'état civil (OEC) du 28 avril 2004, RS 211.112.2
Ordonnance sur les cyberrisques dans l'administration fédérale (OPCy) du 27 mai 2020, RS 120.73
Stratégie numérique de la Confédération 2020-2023 (Stratégie de l'administration fédérale dans le domaine de la transformation et de l'informatique), septembre 2021

Annexe 2 : Abréviations

CDF	Contrôle fédéral des finances
CSI-DFJP	Centre de service informatique du Département fédéral de justice et police
DFJP	Département fédéral de justice et police
NCSC	Centre national pour la cybersécurité (« National Cyber Security Center »)
OFEC	Office fédéral de l'état civil
OFJ	Office fédéral de la justice
UIS	Unité Infostar

Annexe 3 : Glossaire

Backlog de produit	Dans une méthodologie agile, liste d'éléments ou de fonctionnalités nécessaires pour atteindre les objectifs, classés par ordre de priorité (anglais « product backlog »).
Bi-temporalité	Des bases légales différentes peuvent s'appliquer aux événements d'état civil d'une même personne, selon le moment où ils ont eu lieu. Le lien vers la base légale valable lors de la survenance de l'événement doit donc être conservé.
Cockpit ICT	Outil de suivi de portefeuille de projets en service à l'administration fédérale.
COOL:Gen	Langage de programmation de 4e génération, populaire dès la fin des années 90.
DevOps	Pratique en ingénierie informatique visant à l'unification du développement logiciel et de l'administration système.
Infostar	Registre centralisé de tenue des événements d'état civil (de l'allemand INFOrmatisiertes STAndesRegister).
Infostar NG	Infostar New Generation, projet de modernisation du registre Infostar.
Produit viable minimum	Version d'un produit rassemblant seulement les fonctionnalités élémentaires lors de son lancement (en anglais « Minimum viable product », MVP).
SIPD (concept)	Concept de sécurité de l'information et de protection des données, document décrivant les mesures à mettre en œuvre pour un objet ayant des besoins de protection accrue.
Sprint	Dans une méthodologie agile, phase séquentielle d'élaboration, de courte durée, durant laquelle des activités s'enchainent pour déboucher sur la livraison d'un incrément de produit qui fonctionne.
SSO (portail)	Portail à signature unique (« single sign-on ») permettant l'identification et l'authentification des utilisateurs et l'accès aux applications.

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).