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

Audit de la sécurité et de la disponibilité de l'exploitation GEVER

Chancellerie fédérale et Centre de services informatiques du Département fédéral de l'économie, de la formation et de la recherche

CDF-20385 | Prises de position incluses | 16 février 2021 | DélFin D2/2021

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Contrôle fédéral des finances (CDF) Monbijoustrasse 45 3003 Berne Suisse
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.20385.104.00060
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

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

Table des matières

Audit de la sécurité et de la disponibilité de l'exploitation GEVER

Chancellerie fédérale et Centre de services informatiques du Département fédéral de l'économie, de la formation et de la recherche

L'essentiel en bref

Avec le programme GENOVA, la Chancellerie fédérale (ChF) veut introduire un seul produit de gestion électronique des affaires (GEVER) pour toutes les unités de l'administration fédérale. Planifié entre novembre 2015 et septembre 2021, le programme est devisé à plus de 68 millions de francs. Le Centre de services informatiques du Département de l'économie, de la formation et de la recherche (ISCeco) assume la responsabilité principale de l'exploitation de la plateforme. Plus de 22 000 utilisateurs travaillent avec ce nouveau système en automne 2020.

Dans cette révision, le Contrôle fédéral des finances (CDF) évalue si, sous l'angle de la sécurité et de la disponibilité, les mesures mises en œuvre au niveau de l'exploitation sont adéquates. Il examine aussi si le passage du statut de projet au statut d'exploitation est réglé et si le suivi des points en suspens est assuré. Enfin, cet audit effectue un suivi de quatre recommandations de révisions antérieures.

Le CDF est parvenu à une conclusion globalement satisfaisante, bien que l'architecture complexe du système impose des exigences élevées à l'exploitation et qu'un travail important doit encore être accompli.

Les exigences de sécurité sont définies, mais la démarche n'est pas entièrement aboutie

L'architecture de la solution est complexe, plusieurs intervenants sont impliqués dans son exploitation. Leurs prérogatives sont clairement définies, ils jugent la collaboration satisfaisante. Les postes de spécialistes sont pourvus, l'exploitation peut être considérée comme stable, le développement des incidents est favorable. Les processus de conduite, de planification et d'exploitation sont définis au sein de l'ISCeco. Un audit interne du fonctionnement de l'exploitation a été mené, d'autres sont prévus. Pour le CDF, les définitions de l'organisation, de la conduite et des processus de l'exploitation sont appropriées. Les exigences de sécurité au niveau de la solution technique et de l'exploitation sont documentées. Les risques résiduels sont reconnus et acceptés. Le CDF a toutefois constaté que la mise en œuvre de la protection de base n'est pas complètement documentée.

Du côté des bénéficiaires de prestations, le CDF n'a pas examiné de façon approfondie le statut des démarches de sécurité. Il a cependant trouvé un cas où la répartition des tâches entre département et offices n'était pas clairement réglée. Le CDF demande ici un nouvel effort de communication.

Protection de l'accès et de l'intégrité : des mécanismes appropriés et quelques points à finaliser

La plateforme GEVER est installée dans le nuage privé (« private cloud ») de l'administration fédérale hébergé à l'Office fédéral de l'informatique et de la télécommunication (OFIT). Elle est utilisée au sein du réseau informatique protégé de la Confédération. L'authentification à deux facteurs est assurée par le service TIC standard eIAM[1]. Les utilisateurs se voient assigner le système de leur département et des autorisations limitant les opérations et objets auxquels ils peuvent accéder. Un nombre limité d'administrateurs est défini, aux niveaux applicatif et technique. Les mécanismes en place sont globalement appropriés. Le CDF a toutefois constaté que les contrôles annuels des listes d'utilisateurs privilégiés n'étaient pas encore opérationnels.

Une solution du Groupement défense assure la confidentialité des documents jusqu'au niveau CONFIDENTIEL. Le règlement d'utilisation proscrit par contre le traitement des documents de niveau SECRET et le système bloque la définition d'un document dans cette catégorie de classification. Le risque de saisie de données sensibles dans les métadonnées subsiste et est reconnu par le donneur d'ordre.

Le processus de gestion des changements en place à l'ISCeco définit de manière adéquate les étapes à suivre (demande, validation, exécution, tests). En revanche, les changements ne sont pas systématiquement répertoriés dans toutes les composantes du système. Le CDF n'a donc pas pu contrôler l'efficacité du processus de gestion des changements. Des outils contrôlent régulièrement l'intégrité des serveurs. Des mécanismes de hachage[2] sont disponibles sur la plateforme, mais pas encore utilisés. Le CDF a demandé de clarifier ce point.

Gestion de la continuité : la démarche n'est pas entièrement aboutie

Pour répondre aux besoins accrus en termes de disponibilité du système, l'infrastructure est conçue de manière redondante dans des centres de calcul séparés. Les tests ont montré que les bascules fonctionnent en cas de défaillance. Un système de surveillance des composantes de la plateforme est en place à l'ISCeco, des alertes sont émises et des tickets d'incident sont automatiquement générés en cas de grave dysfonctionnement. Ceux-ci sont alors traités selon les procédures en vigueur. Le CDF souligne que des composantes ne sont pas sous le contrôle de l'ISCeco. Celui-ci doit alors s'appuyer sur d'autres fournisseurs de prestations pour la résolution des incidents.

Sur le plan de la gestion de la récupération, le CDF constate que des aspects ne sont pas encore documentés. Diverses mesures sont certes définies, des sauvegardes régulières et des tests de restauration sont effectués, mais il manque une vue d'ensemble structurée dans ce domaine (« policy »). Des scénarios de défaillance, des plans de récupération actuels et des tests de reconstruction plus étendus doivent également être préparés.

La transition vers l'organisation permanente est réglée

Diverses activités et instances sont définies pour traiter la transition vers le statut d'exploitation. Des groupes de travail aux niveaux du pilotage, de la conduite et de l'exécution se réunissent régulièrement et impliquent les différents acteurs concernés. Le transfert de

[1] Service TIC standard de gestion de l'identité et des accès, géré par l'UPIC.
[2] Fonction cryptographique utilisée à des fins de vérification.

connaissance est ainsi facilité. Des listes de suspens sont gérées à ces niveaux. Le CDF estime que ces mécanismes sont adéquats, même s'il attend quelques incertitudes liées à la reprise des fonctions de l'UPIC par la Chancellerie fédérale dès janvier 2021.

Les recommandations émises précédemment par le CDF sont largement mises en œuvre.

Prüfung der Sicherheit und Verfügbarkeit im Betrieb GEVER

Bundeskanzlei und Information Service Center des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung

Das Wesentliche in Kürze

Die Bundeskanzlei (BK) möchte mit dem Programm GENOVA ein einheitliches elektronisches Geschäftsverwaltungsprodukt (GEVER) für die gesamte Bundesverwaltung einführen. Die Einführung des auf über 68 Millionen Franken veranschlagten Programms ist zwischen November 2015 und September 2021 geplant. Das Information Service Center des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung (ISCeco) trägt für den Betrieb der Plattform die Hauptverantwortung. Im Herbst 2020 arbeiten über 22 000 Benutzer mit dem neuen System.

Die Eidgenössische Finanzkontrolle (EFK) evaluiert im Rahmen dieser Prüfung, ob die umgesetzten betrieblichen Massnahmen unter dem Aspekt der Sicherheit und der Verfügbarkeit angemessen sind. Sie prüft auch, ob der Übergang vom Projekt- zum Betriebsstatus geregelt und die Weiterverfolgung offener Fragen sichergestellt ist. Schliesslich führt sie eine Nachprüfung der Umsetzung von vier Empfehlungen aus früheren Revisionen durch.

Die EFK ist zum Schluss gekommen, dass das Ergebnis insgesamt zufriedenstellend ist, obwohl die komplexe Systemarchitektur hohe Anforderungen an den Betrieb stellt und noch viel zu tun ist.

Die Sicherheitsanforderungen sind definiert, aber der Prozess ist nicht vollständig abgeschlossen

Die Systemarchitektur ist komplex, da mehrere Akteure am Betrieb beteiligt sind. Ihre Befugnisse sind klar definiert und die Zusammenarbeit wird von ihnen als zufriedenstellend bezeichnet. Die Stellen konnten mit Fachleuten besetzt werden, der Betrieb kann als stabil angesehen werden, die Anzahl an Störungen nimmt ab. Die Führungs-, Planungs- und Betriebsprozesse werden im Rahmen des ISCeco definiert. Eine erste interne Prüfung des Betriebs wurde durchgeführt, weitere sind geplant. Aus Sicht der EFK sind die Definitionen der Organisation, der Führung und der Betriebsprozesse angemessen. Die Sicherheitsanforderungen an die technische Lösung und den Betrieb sind dokumentiert. Die Restrisiken sind erkannt und akzeptiert. Die EFK hat allerdings festgestellt, dass die Umsetzung des Basisschutzes nicht vollständig dokumentiert ist.

Seitens der Leistungsbezüger hat die EFK keine vertiefte Prüfung des Status der Sicherheitsmassnahmen vorgenommen. Sie stiess jedoch auf einen Fall, bei dem die Aufgabenteilung zwischen dem Departement und den Ämtern nicht klar geregelt war. Die EFK fordert weitere Anstrengungen im Bereich Kommunikation.

Zugriffs- und Integritätsschutz: Zweckmässige Mechanismen und punktueller Klärungsbedarf

Die GEVER-Plattform befindet sich in der «Private Cloud» der Bundesverwaltung und ist im Bundesamt für Informatik und Telekommunikation (BIT) gehostet. Die Plattform wird innerhalb des geschützten Informatiknetzwerks des Bundes genutzt. Die Zwei-Faktor-Authentifizierung erfolgt über den IKT-Standarddienst eIAM[1]. Die Nutzer werden dem System ihres jeweiligen Departements zugewiesen und erhalten nur Zugriff auf die Geschäfte und Inhalte, für die sie zugangsberechtigt sind. Auf der Anwendungsebene und in technischer Hinsicht wird eine beschränkte Anzahl an Administratoren definiert. Die geschaffenen Mechanismen sind insgesamt angemessen. Die EFK hat jedoch festgestellt, dass die jährlichen Überprüfungen der Listen der privilegierten Nutzer noch nicht betriebsbereit sind.

Eine Lösung der Gruppe Verteidigung gewährleistet die Vertraulichkeit der Dokumente bis zur Stufe VERTRAULICH. Das Nutzungsreglement untersagt hingegen die Verarbeitung von Dokumenten der Stufe GEHEIM und das System blockiert die Definition eines Dokuments in dieser Klassifizierungskategorie. Das Risiko, schützenswerte Daten in den Metadaten zu erfassen, besteht und wird vom Auftraggeber anerkannt.

Der beim ISCeco eingeleitete Change-Management-Prozess legt die zu befolgenden Schritte angemessen fest (Antrag, Validierung, Ausführung, Tests). Die Änderungen werden jedoch nicht systematisch in allen Systemkomponenten erfasst. Die EFK konnte somit die Wirksamkeit des Change-Management-Prozesses nicht überprüfen. Die Serverintegrität wird regelmässig mit entsprechenden Tools kontrolliert. Auf der Plattform sind Hashmechanismen[2] verfügbar, sie werden aber noch nicht genutzt. Die EFK bat um Klärung dieses Punktes.

Kontinuitätsmanagement: Der Prozess ist nicht vollständig abgeschlossen

Um den erhöhten Anforderungen an die Systemverfügbarkeit gerecht zu werden, ist die Infrastruktur redundant in getrennten Rechenzentren ausgelegt. Die Tests haben ergeben, dass die Ausfallsicherung bei Störungsfällen funktionieren. Im ISCeco ist ein Überwachungssystem der Plattformkomponenten installiert, das Alarm auslöst und im Falle ernsthafter Störungen automatische Fehlertickets generiert. Diese werden nach den geltenden Verfahren bearbeitet. Die EFK weist darauf hin, dass manche Komponenten nicht der Kontrolle des ISCeco unterstehen. In solchen Fällen muss das ISCeco andere Leistungserbringer für die Problemlösung beiziehen.

Die EFK stellt hinsichtlich des Wiederherstellungsmanagements fest, dass gewisse Aspekte noch nicht dokumentiert werden. Es wurden zwar verschiedene Massnahmen definiert, regelmässige Backups und Wiederherstellungstests werden durchgeführt, doch es fehlt eine strukturierte Gesamtsicht in diesem Bereich («Policy»). Auch Ausfallszenarien, aktuelle Wiederherstellungspläne und umfassendere Wiederherstellungstests sind vorzubereiten.

Der Übergang zur ständigen Organisation ist geregelt

Für den Übergang zum Betriebsstatus wurden verschiedene Aktivitäten und Instanzen definiert. Arbeitsgruppen, die die verschiedenen betroffenen Akteure einbeziehen, befassen sich regelmässig mit Fragen rund um die Steuerung, die Führung und die Ausführung. Dies

[1] IKT-Standarddienst für das Zugriffs- und Berechtigungssystem, das vom ISB verwaltet wird.
[2] Verschlüsselungsfunktion, die zu Überprüfungszwecken verwendet wird.

erleichtert den Wissenstransfer. Pendenzenlisten werden auf diesen Ebenen geführt. Die EFK hält zwar diese Mechanismen für angemessen, rechnet aber mit gewissen Unsicherheiten im Zusammenhang mit der Übernahme der Funktionen des ISB durch die Bundeskanzlei ab Januar 2021.

Die bisherigen Empfehlungen der EFK sind weitgehend umgesetzt.

Originaltext auf Französisch

Verifica della sicurezza e della disponibilità del sistema GEVER

Cancelleria federale e centro dei servizi informatici del Dipartimento federale dell'economia, della formazione e della ricerca

L'essenziale in breve

Con il programma GENOVA, la Cancelleria federale (CaF) vuole introdurre un unico prodotto per la gestione elettronica degli affari (GEVER) destinato a tutte le unità dell'Amministrazione federale. Pianificato tra novembre del 2015 e settembre del 2021, il programma ha un valore di oltre 68 milioni di franchi. Il centro dei servizi informatici del Dipartimento federale dell'economia, della formazione e della ricerca (ISCeco) è il principale responsabile del funzionamento della piattaforma. Nell'autunno del 2020, già più di 22 000 utenti lavorano con il nuovo sistema.

Con la presente revisione, il Controllo federale delle finanze (CDF) valuta se le misure attuate a livello dell'uso del sistema sono adeguate dal punto di vista della sicurezza e della disponibilità. Controlla anche se la transizione dallo stato di progetto a quello operativo è regolamentata e se le questioni in sospeso vengono monitorate. Infine, questa verifica effettua il monitoraggio di quattro raccomandazioni formulate in occasione di revisioni precedenti.

Il CDF è giunto a una conclusione soddisfacente a livello globale, anche se la complessa architettura del sistema impone esigenze elevate alla gestione e una parte importante del lavoro rimane ancora inconclusa.

I requisiti per la sicurezza sono definiti, ma il processo non è ancora stato completato

L'architettura della soluzione è complessa, diversi attori sono coinvolti nella sua gestione. Le loro prerogative sono definite in maniera chiara ed essi giudicano la collaborazione soddisfacente. Le cariche specialistiche sono ricoperte, il sistema può essere considerato stabile, l'evoluzione degli incidenti è favorevole. Le linee guida, i processi di pianificazione e di gestione sono definiti all'interno dell'ISCeco. Un controllo interno del funzionamento del sistema è stato effettuato e altri sono previsti. Per il CDF, le definizioni dell'organizzazione, delle linee guida e dei processi di gestione sono appropriate. I requisiti per la sicurezza, per quanto riguarda la soluzione tecnica e la gestione, sono documentati. I rischi residui sono riconosciuti e accettati. Tuttavia, il CDF ha constatato che l'attuazione della protezione di base non è pienamente documentata.

Per quanto riguarda i beneficiari delle prestazioni, il CDF non ha esaminato in dettaglio lo stato delle procedure di sicurezza. Ciononostante, ha trovato un caso in cui la ripartizione delle mansioni tra il dipartimento e gli uffici non era stabilita in modo chiaro. Il CDF chiede, in questo caso, un nuovo sforzo di comunicazione.

Protezione dell'accesso e dell'integrità: meccanismi appropriati e alcune questioni da finalizzare

La piattaforma GEVER è installata nel cloud privato («private cloud») dell'Amministrazione federale, ospitata dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT).

Essa viene utilizzata all'interno della rete informatica protetta della Confederazione. L'autenticazione a due fattori è fornita dal servizio TIC standard eIAM[1]. Agli utenti viene assegnato il sistema del loro dipartimento e con esso le autorizzazioni che limitano le operazioni e gli oggetti a cui possono accedere. Viene definito un numero limitato di amministratori, sia a livello di applicazione che tecnico. I meccanismi in atto sono appropriati a livello globale. Tuttavia, il CDF ha constatato che i controlli annuali delle liste di utenti privilegiati non erano ancora operativi.

Una soluzione dell'Aggruppamento Difesa assicura la riservatezza dei documenti fino al livello CONFIDENZIALE. Il regolamento d'uso vieta però il trattamento di documenti di livello SEGRETO e il sistema blocca la definizione di un documento classificato in questa categoria. Il rischio di inserire dati sensibili nei metadati rimane ed è noto al committente.

Il processo di gestione dei cambiamenti in atto presso l'ISCeco definisce adeguatamente le fasi da seguire (richiesta, convalida, esecuzione, test). D'altra parte, i cambiamenti non sono sistematicamente registrati in tutti i componenti del sistema. Il CDF non è stato quindi in grado di controllare l'efficacia del processo di gestione dei cambiamenti. Sono predisposti strumenti che controllano regolarmente l'integrità dei server. Alcune funzioni hash[2] sono disponibili nella piattaforma, ma non ancora in uso. Il CDF ha chiesto dei chiarimenti su questo punto.

Gestione della continuità: il processo non è ancora stato completato

Per soddisfare le crescenti richieste di disponibilità del sistema, l'infrastruttura è progettata in modo ridondante in centri di calcolo separati. I test hanno dimostrato che i dispositivi di memoria funzionano in caso di guasto. Un sistema di monitoraggio dei componenti della piattaforma è attivo presso l'ISCeco, in caso di un grave malfunzionamento vengono emessi avvisi e vengono generate automaticamente richieste di risoluzione dell'incidente. Queste sono poi trattate secondo le procedure in vigore. Il CDF sottolinea che ci sono componenti che non sono sotto il controllo dell'ISCeco. In questi casi, l'ISCeco deve appoggiarsi ad altri fornitori di servizi per la risoluzione degli incidenti.

In termini di gestione del recupero, il CDF constata che ci sono aspetti che non sono ancora stati documentati. Anche se sono state definite diverse misure e si effettuano backup regolari e test di ripristino, manca una visione d'insieme strutturata in questo settore («policy»). Devono essere preparati anche scenari per affrontare guasti, piani di recupero attuali e test di ricostruzione più estesi.

Il passaggio all'organizzazione permanente è regolamentato

Varie attività e istanze sono state definite per affrontare la transizione verso lo stato operativo. Dei gruppi di lavoro a livello direttivo, gestionale ed esecutivo si incontrano regolarmente e coinvolgono le varie parti interessate. In questo modo il trasferimento delle conoscenze viene facilitato. Le questioni in sospeso sono gestite a questi livelli. Il CDF ritiene questi meccanismi adeguati, anche se si aspetta qualche incertezza in relazione alla ripresa delle funzioni dell'ODIC da parte della Cancelleria federale a partire dal mese di gennaio del 2021.

Le precedenti raccomandazioni emesse dal CDF sono state ampiamente attuate.

Testo originale in francese

[1] Servizio TIC standard per la gestione dell'identità e dell'accesso, gestito dall'ODIC.
[2] Funzione crittografica usata per la verifica.

Audit of the security and availability of the GEVER system

Federal Chancellery and IT Service Centre of the Federal Department of Economic Affairs, Education and Research

Key facts

With the GENOVA programme, the Federal Chancellery (FCh) aims to introduce a single electronic business management product (GEVER) for all units of the Federal Administration. The programme is planned to run from November 2015 to September 2021 and is expected to cost more than CHF 68 million. The IT Service Centre of the Department of Economic Affairs, Education and Research (ISCeco) is primarily responsible for running the platform. By autumn 2020, more than 22,000 users were working with the new system.

In this audit, the Swiss Federal Audit Office (SFAO) assessed whether the measures implemented at the operational level are adequate from the point of view of security and availability. It also examined whether the transition from project status to operational status has been completed and whether outstanding issues are being followed up. Finally, this audit follows up on four recommendations from previous audits.

Overall, the SFAO reached a satisfactory conclusion, although the complex system architecture places high demands on operations and a significant amount of work remains to be done.

Security requirements are defined but process is not yet complete

The architecture of the solution is complex, with several players involved in its operation. Their prerogatives are clearly defined, they judge the collaboration to be satisfactory. Specialist positions are filled, operations can be regarded as stable, and the development of incidents is favourable. The management, planning and operational processes are defined within ISCeco. An internal audit of operations was conducted and more are planned. The SFAO considered the definitions of the organisation, management and processes of operations to be appropriate. The security requirements for the technical solution and operations are documented. Residual risks are recognised and accepted. However, the SFAO found that the implementation of basic protection is not fully documented.

As regards the service procurers, the SFAO did not examine the status of the security measures in detail. It did, however, find one case where the division of tasks between departments and offices was not clearly defined. The SFAO calls for further effort in terms of communication here.

Access and integrity protection: mechanisms are appropriate, some points need to be finalised

The GEVER platform is installed in the Federal Administration's private cloud at the Federal Office of Information Technology and Telecommunication (FOITT). It is used within the Confederation's secure IT network. Two-factor authentication is provided by the standard ICT

service eIAM[1]. Users are assigned their department's system and permissions limiting the operations and objects they can access. A limited number of administrators are defined, both at application and technical levels. The mechanisms in place are generally appropriate. However, the SFAO found that the annual checks on the lists of privileged users were not yet operational.

A Defence Group solution ensures the confidentiality of documents up to CONFIDENTIAL level. However, the user regulations prohibit the processing of documents at SECRET level and the system blocks the definition of a document in this classification category. The risk of entering sensitive data in the metadata remains and is recognised by the client.

The change management process in place at ISCeco adequately defines the steps to be followed (request, validation, execution, testing). However, changes are not systematically logged in all the system's components. The SFAO was therefore unable to check the effectiveness of the change management process. Tools regularly check the integrity of the servers. Hash[2] mechanisms are available in the platform, but not yet in use. The SFAO asked for clarification on this point.

Continuity management: approach is not fully developed

To meet the increased need for system availability, the infrastructure is designed with redundancy in separate computer centres. Tests have shown that the failovers work in case of failure. A monitoring system for the platform components is in place at ISCeco, alerts are issued and incident tickets are automatically generated in the event of a serious malfunction. These are then processed according to the procedures in force. The SFAO points out that some components are not under ISCeco's control. In such cases, ISCeco has to rely on other service providers to resolve incidents.

In terms of recovery management, the SFAO noted that some aspects had not yet been documented. Although various measures are defined and regular backups and recovery tests are carried out, there is no structured overview of this area (policy). Failure scenarios, up-to-date recovery plans and more extensive reconstruction tests also need to be prepared.

Transition to the permanent organisation is regulated

Various activities and bodies are defined to deal with the transition to operational status. Working groups at the steering, management and implementation levels meet regularly and involve the various players concerned. This facilitates the transfer of knowledge. Pending lists are managed at these levels. The SFAO considered these mechanisms to be adequate, although it expects some uncertainty in connection with the takeover of the FITSU's functions by the Federal Chancellery from January 2021.

The SFAO's previous recommendations have largely been implemented.

Original text in French

[1] Standard ICT service for identity and access management, managed by the FITSU.
[2] Cryptographic function used for verification purposes.

Prise de position générale de la Chancellerie fédérale et du Centre de services informatiques du Département de l'économie, de la formation et de la recherche

> La Chancellerie fédérale et l'ISCeco remercient le CDF pour le présent audit de la sécurité et de la disponibilité de l'exploitation GEVER. Nous avons apprécié l'esprit constructif de cet audit, axé sur la recherche d'améliorations tangibles, qui apportent une plus-value à l'exploitation de GEVER. Nous avons aussi apprécié que nos retours soient compris et intégrés. L'amélioration continue de la sécurité et de la disponibilité sont les priorités absolues de l'exploitant ISCeco, et cet audit y contribue grandement.

1 Mission et déroulement

1.1 Contexte

Depuis le 1er janvier 2013, la Chancellerie fédérale (ChF) pilote et dirige les activités liées à la gestion électronique des affaires (GEVER, en allemand « Geschäftsverwaltung ») dans l'administration fédérale. Le programme GENOVA vise à introduire un seul et unique produit (Acta Nova) pour les unités des sept départements et la ChF. Ce programme, conduit par la ChF, est en cours au moment de la révision. Il est prévu de s'étaler entre novembre 2015 et septembre 2021 et est devisé à plus de 68 millions de francs, dont près de 34 millions avec incidence financière (sans les projets départementaux).

La gestion électronique des affaires se fait de manière centralisée comme service TIC standard[3] pour toute l'administration fédérale. Ce rôle est assumé par l'Unité de pilotage informatique de la Confédération (UPIC) jusqu'à fin 2020. Dès 2021, et suite à la réorganisation de la transformation numérique et de la gouvernance de l'informatique, la gestion des services standards sera rattachée à la ChF. Le Centre de services informatiques du Département fédéral de l'économie, de la formation et de la recherche (ISCeco) assume le rôle de fournisseur de prestations pour la plateforme GEVER. Un premier volet de l'exploitation a démarré en avril 2020. A l'automne 2020, près de 22 000 utilisateurs dans toute l'administration fédérale travaillent déjà avec le système. A ce stade, la priorité est de gérer l'introduction de la solution dans les unités administratives restantes. Il s'agit aussi de migrer la plateforme vers la version 3.0 et de continuer d'accompagner le passage vers l'organisation permanente prévue pour son exploitation.

1.2 Objectif et questions d'audit

Dans cette révision, le Contrôle fédéral des finances (CDF) évalue si les mesures mises en œuvre au niveau de l'exploitation sous l'angle de la sécurité et de la continuité du service sont adéquates. Il vise en particulier à répondre aux questions suivantes :

- L'infrastructure et l'exploitation de l'application GEVER sont-elles conçues de manière à assurer une sécurité (confidentialité, disponibilité, intégrité) et une résilience appropriées ?
- Des mesures adéquates sont-elles en place pour assurer le maintien et la restauration de la disponibilité du système ?
- Le passage du statut de projet au statut d'exploitation est-il réglé et la répartition des éventuels points ouverts est-elle assurée ?
- Suivi de diverses recommandations de révisions antérieures du CDF (voir l'annexe 2 pour le détail).

[3] Prestation informatique gérée de manière centralisée.

1.3 Etendue de l'audit et principe

L'audit a été mené du 29 septembre au 27 novembre 2020 par André Stauffer (responsable de révision) et Hans Ulrich Wiedmer. Il a été conduit sous la responsabilité de Bernhard Hamberger. Les travaux se sont appuyés sur les exigences de sécurité des TIC de l'administration fédérale, les normes de la série ISO 27000 (Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information) et la norme ISO 27031 (Technologies de l'information – Techniques de sécurité – Lignes directrices pour la préparation des technologies de l'information et de la communication à la continuité des activités). Le présent rapport ne prend pas en compte les développements ultérieurs à l'audit.

1.4 Documentation et entretiens

Les informations nécessaires ont été recueillies lors d'entretiens avec les spécialistes de la ChF, de l'ISCeco, de l'UPIC et de l'Office fédéral de l'informatique et de la télécommunication (OFIT). Des évidences documentaires étayent les éléments discutés. Les interlocuteurs ont fourni ces informations au CDF de manière exhaustive et compétente. 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 28 janvier 2021. La ChF était représentée par le vice-chancelier, les chefs de programme GEVER et un responsable de service standard. L'ISCeco était représenté par son directeur, le responsable de la sécurité informatique, le responsable d'unité commerciale GEVER et le chef de département Exploitation GEVER. Les participants du CDF étaient deux responsables de mandat, le responsable de centre de compétence et le responsable de révision.

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

CONTRÔLE FÉDÉRAL DES FINANCES

2 Constats et appréciations

2.1 L'organisation de l'exploitation est globalement adéquate

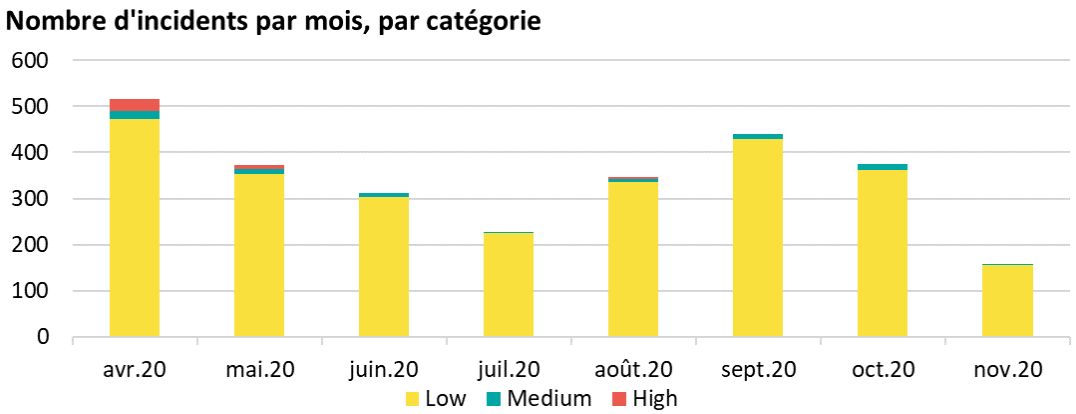
La plateforme GEVER est constituée de plusieurs couches dont la responsabilité incombe à des acteurs différents. Pour les couches matérielles (serveurs, virtualisation, réseau, stockage) jusqu'à et y compris les systèmes d'exploitation, l'OFIT est en charge. Les logiciels fournissant les fonctionnalités et les service communs (« middleware ») sont généralement du ressort de l'ISCeco. Des exceptions existent telles que le service TIC standard eIAM (Identity and Access Management) gérant les accès aux applications Web (UPIC), ou encore Sedex pour l'échange de données asynchrone sécurisé (Office fédéral de la statistique). L'exploitation de la couche applicative (notamment l'application Acta Nova) est sous la responsabilité de l'ISCeco. Une convention signée entre l'OFIT et l'ISCeco règle les modalités de la collaboration entre ces deux unités dans le domaine GEVER. Une matrice décrit dans le détail les droits et responsabilités de chacun des fournisseurs de prestations. Les premières expériences de la collaboration sont considérées comme positives par les intervenants.

Le domaine de l'exploitation GEVER à l'ISCeco emploie seize personnes à l'interne et sept personnes externes. Elles sont actives au sein de trois unités couvrant le support de l'application, l'exploitation des bases de données et du système et l'ingénierie applicative. A l'exception d'un poste, les douze équivalents temps pleins supplémentaires prévus ont pu être engagés et sont opérationnels. Les rôles opérationnels définis selon le modèle ITIL (Information Technology Infrastructure Library) sont occupés dans l'organisation. Les compétences sont considérées comme suffisantes, mais elles continuent de faire l'objet d'approfondissements, notamment pour assurer les suppléances.

Sur le plan de la sécurité, un poste de délégué à la sécurité de l'information est défini pour tout l'ISCeco. Ce spécialiste s'occupe des questions de gouvernance de la sécurité pour toute l'unité. Il n'est donc pas subordonné aux responsables de l'exploitation des applications GEVER, ce qui est un gage d'indépendance.

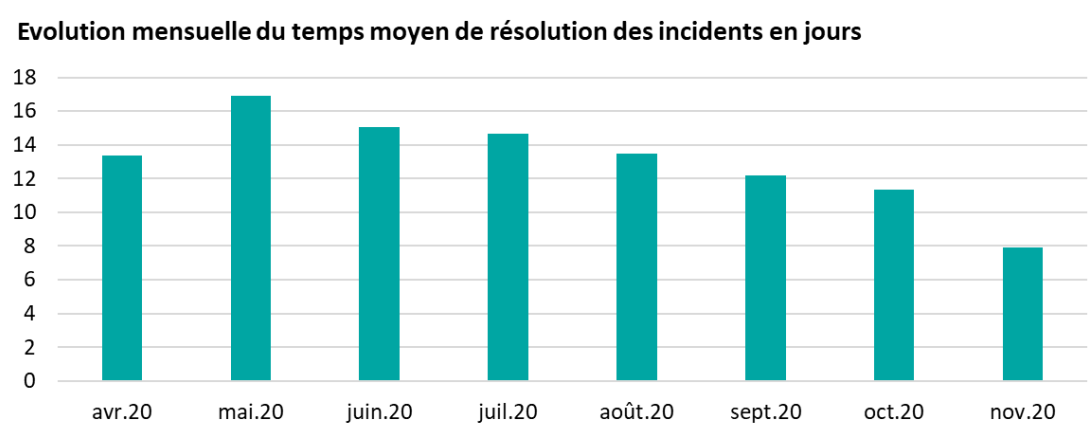
Pour l'exploitation 2021, les responsables ne voient pas de goulet d'étranglement au niveau des ressources personnelles. La majorité des introductions dans les offices, qui peuvent être gourmandes en ressources, ont eu lieu en 2020 et le calendrier 2021 prévoit moins de telles activités. D'autre part, l'industrialisation se poursuit, avec notamment l'automatisation des tests et des déploiements. Ces nouveautés contribuent à diminuer la charge de travail. Les responsables de l'exploitation de GEVER ne voient pas pour eux d'impact de l'interruption de certains appels d'offres de l'ISCeco pour des prestations de services.

L'exploitation de GEVER est considérée comme stable par plusieurs intervenants différents et par le programme. Les données des incidents ne laissent pas supposer d'une capacité personnelle insuffisante de l'exploitation : le nombre mensuel des incidents enregistrés depuis le mois d'avril 2020 pour la plateforme GEVER suit une tendance à la baisse et aucun incident critique n'a été détecté.



Graphique 1 : Evolution mensuelle du nombre d'incidents de la plateforme GEVER depuis avril 2020, par catégorie d'incident (Source : système de gestion des incidents de l'ISCeco).

Sur la même période, le temps de résolution mensuel moyen des incidents suit une courbe descendante. Les valeurs moyennes sont toutefois encore à des niveaux élevés, plus de deux cents incidents ont un temps de résolution supérieur à 30 jours :



Graphique 2 : Evolution mensuelles du temps moyen de résolution des incidents de la plateforme GEVER en jours depuis avril 2020 (Source : système de gestion des incidents de l'ISCeco).

La planification des travaux de l'exploitation est basée sur un calendrier des principaux événements (plan des fenêtres de maintenance), qui comprend, entre autres, les maintenances planifiées, les montées de version, les jours fériés, les votations et les séances du Conseil fédéral. Un plan journalier détaillé par collaborateur est également tenu.

Les processus d'exploitation de l'ISCeco suivent un modèle de type ITIL. Pour les applications GEVER, un concept d'exploitation a d'abord été édité par le fournisseur de prestations sous l'égide du programme GENOVA. Le concept a présidé ensuite à la réalisation du projet de constitution de l'exploitation. Il se matérialise enfin dans le manuel d'exploitation et la description des processus, disponibles sur la page intranet de l'unité.

Le domaine Consulting et Gouvernance de l'ISCeco prévoit des audits réguliers de l'exploitation GEVER. En mars 2020, le délégué à la sécurité de l'information de l'unité a procédé à un premier examen de son fonctionnement et identifié des faiblesses auxquelles il faut remédier.

Appréciation

L'architecture de la solution est complexe, nécessitant une bonne orchestration des différents services la constituant. Le partage des responsabilités pour l'exploitation de GEVER entre plusieurs fournisseurs de prestations est un facteur supplémentaire de complexité. Les temps de résolution des incidents sont encore élevés. Les mises en service de plusieurs départements et le démarrage du modèle d'exploitation partagé l'expliquent en partie. Le règlement dans les détails des prérogatives de chaque fournisseur de prestations facilite la prise en charge des problèmes d'exploitation. L'efficacité de la collaboration devra toutefois augmenter au fur et à mesure des expériences engrangées. Le CDF souligne à cet égard les processus d'amélioration continue, partie intégrante du modèle ITIL.

Au niveau de l'ISCeco, le CDF estime que la définition de l'organisation, de la conduite et des processus d'exploitation des applications GEVER est appropriée. Il relève la volonté d'organiser des audits internes réguliers du fonctionnement de l'exploitation et encourage l'ISCeco à finaliser une planification de ces examens. Le CDF n'a pas évalué en détail l'organisation de l'exploitation du côté des autres fournisseurs de prestations dans cet audit. Il renvoie au rapport de la révision 18484[4] de février 2019 pour des détails sur les aspects économiques et sécuritaires de la solution Atlantica Cloud.

2.2 Les exigences en matière de sécurité de l'information sont définies, des aspects formels doivent être finalisés

Le programme GENOVA a produit la documentation de sécurité de l'information de l'application Standard GEVER. Le document de mise en œuvre de la protection informatique de base traite les points incombant au fournisseur de prestation et au mandant. Dans l'analyse des besoins de protection, des besoins accrus sont constatés en matière de confidentialité, de disponibilité, d'intégrité et de traçabilité. Un concept de sécurité de l'information et de protection des données (SIPD) est édité en conséquence, une de ses annexes détaille les risques résiduels. Les solutions à mettre en œuvre pour couvrir ces exigences sont décrites dans le document d'architecture technique du système.

Sur un plan formel, le CDF note que le concept de sécurité de l'information a été passé en revue par de nombreuses instances de contrôle et est signé par le mandant du programme. Les risques résiduels sont ainsi identifiés et acceptés. Les autres documents de sécurité sont également validés par le mandant. La mise en œuvre de la protection informatique de base est quant à elle signée par le délégué au pilotage informatique de la Confédération. La règle veut en outre que le fournisseur de prestations documente par écrit la mise en œuvre de la protection de base. Le CDF n'a pas reçu d'évidence en ce sens.

Le programme GENOVA prévoit également que les bénéficiaires de prestations éditent des documents de sécurité pour l'utilisation du service standard GEVER. Une directive de l'UPIC détaille la marche à suivre, des modèles de documents (notamment concept SIPD et règlement de traitement) sont également mis à disposition. La responsabilité de l'édition de ces documents incombe aux unités administratives dans le cadre de leur projet d'introduction de GEVER. Les concepts SIPD et les risques résiduels au niveau des bénéficiaires de prestations doivent être validés par les directions des offices utilisateurs. Dans un cas au moins,

[4] Rapport 18484 du CDF du 22 février 2019 «Prüfung der Informatikanwendung ʻAtlantica Cloudʼ».

la répartition des tâches entre département et unités administratives n'était pas claire et les documents pas encore finalisés, même plusieurs mois après l'introduction de la solution.

Appréciation

La définition et le traitement des exigences en matière de sécurité de l'information sont globalement appropriés pour ce qui est de la solution standard. Le CDF relève toutefois sur le plan de la mise en œuvre de la protection de base, la démarche n'est pas aboutie (documentation par le fournisseur de prestations) et demande au projet de prendre les mesures pour y remédier.

Le CDF apprécie la mise à disposition par le programme des modèles de documents de sécurité pour les offices utilisateurs. Il n'a par contre pas vérifié le statut de la documentation de sécurité des plus de 80 bénéficiaires de la prestation GEVER. Il voit le risque que des retards soient encourus dans l'édition de ces documents et qu'un standard minimum de qualité ne soit pas respecté. Les directeurs des offices ne seraient alors pas à même de pleinement apprécier et d'accepter les risques résiduels liés à l'utilisation du service standard GEVER.

Recommandation 1 (Priorité 2)

Le CDF recommande à la Chancellerie fédérale de finaliser le volet de la protection informatique de base pour le standard fédéral en faisant documenter la mise en œuvre par le fournisseur de prestations informatiques.

Prise de position des audités

Il existe des documents de sécurité valables et signés pour SD GEVER de l'année 2020. La Chancellerie fédérale révisera à nouveau les documents de sécurité centraux, les mettra à jour et les fera signer par les responsables d'ici à la fin du programme GENOVA prévu pour septembre 2021).

Recommandation 2 (Priorité 1)

Le CDF recommande à la Chancellerie fédérale de renforcer la visibilité et la communication au sein du programme GENOVA sur les obligations des bénéficiaires de prestations en matière de documents de sécurité. L'état des travaux de mise en œuvre des mesures de sécurité incombant aux bénéficiaires de prestations devra aussi être consigné dans le rapport de clôture du programme.

Prise de position des audités

Dans le passé, la Chancellerie fédérale a rappelé aux Départements, à plusieurs reprises, leurs obligations concernant leurs documents de sécurité. En vue du rapport final du programme GENOVA, la Chancellerie fédérale rassemblera l'état des documents de sécurité chez les bénéficiaires du service et consignera les résultats dans ce rapport de clôture.

2.3 L'architecture complexe impose des exigences élevées à l'exploitation

La conception de l'infrastructure de la solution GEVER a fait l'objet de nombreux travaux spécialisés et d'études et a impliqué de nombreux intervenants. Une description détaillée de l'architecture système est disponible, elle se concentre sur les aspects des données, des applications et de la technologie. Parmi les caractéristiques de la plateforme technique, le

CDF note l'utilisation de l'infrastructure en nuage privé Atlantica Cloud, de serveurs physiques dédiés pour les bases de données et de serveurs de stockage en réseau, conçus de manière redondante. Les plateformes sont organisées en huit instances séparées, une pour chaque département et la ChF. Au plan applicatif, le CDF relève les multiples services logiciels mis en œuvre, tels que serveurs frontaux et arrières, bases de données et serveurs web. De nombreux services applicatifs externes à GEVER tels que eIAM, Sedex (voir ci-dessus), SAP (gestion des finances et de la logistique) ou SecureCenter (chiffrage de documents) sont invoqués par la plateforme au moyen d'interfaces.

Les nombreuses composantes mises en œuvre et leurs interactions font que l'architecture est complexe. Une première version de la documentation de l'architecture est validée en février 2018 par un large panel de spécialistes de l'UPIC et des fournisseurs de prestations informatiques. Les travaux architecturaux se sont poursuivis après cette date, en particulier avec l'évolution des versions du logiciel. Une version actuelle de l'architecture système est éditée en continu par les spécialistes de la solution.

Le document décrit en particulier les solutions techniques touchant la sécurité de l'information, apportant ainsi une réponse aux exigences évoquées ci-dessus. Le rapport du CDF va évaluer ces solutions dans les chapitres suivants, en les rapportant aux différents enjeux de la sécurité de l'information (sécurisation des accès, confidentialité, disponibilité, intégrité et traçabilité).

Appréciation

De manière générale, le CDF relève que la complexité de la solution et les nombreuses interactions entre ses composantes peuvent exacerber les risques liés à la sécurité de la plateforme et impacter les performances du système. Il note également la dépendance du système envers des services exploités par d'autres fournisseurs de prestations informatiques. L'évolution continue des travaux architecturaux et l'implication d'un large panel de spécialistes dans la validation de leurs résultats peuvent contribuer à garder ces risques sous contrôle. L'orchestration des activités d'exploitation n'en reste pas moins un défi.

2.4 Sécurisation des accès : des mécanismes appropriés et quelques points à finaliser

Une majorité de composantes de la plateforme GEVER fonctionne sur l'infrastructure hébergé à l'OFIT, au sein du réseau de la Confédération. Les fonctionnalités de réseau informatique sont assurées par le biais du service TIC standard DAKO (Datenkommunikation). Le matériel et les services sont donc abrités derrière l'infrastructure de sécurité réseau (pare-feux, zones de réseaux, procédures de connexion) standard. Les accès à la solution par des utilisateurs utilisant le protocole https sont canalisés de manière standard au travers des points d'accès situés sur la zone d'accès commun. Le CDF n'a pas examiné le niveau de sécurité des fonctionnalités d'accès au réseau informatique.

L'identification et l'authentification auprès du service GEVER est assurée par le service eIAM, pour les utilisateurs internes comme externes. La connexion est établie par un mécanisme d'authentification à deux facteurs (mot de passe et carte à puce ou appareil mobile enregistré). Le CDF relève des problèmes périodiques de disponibilité de eIAM, service TIC standard de l'UPIC exploité techniquement par l'OFIT. L'ISCeco n'est pas responsable de ce service, l'accès à la plateforme GEVER est quand même impacté.

Divers types d'interfaces sont disponibles pour l'accès au service GEVER par des applications tierces. Les descriptions de ces accès sont encore en cours de finalisation dans le document d'architecture, notamment pour les services Web.

Un concept décrit le fonctionnement des autorisations au niveau applicatif. Les utilisateurs se voient attribuer un profil d'autorisation correspondant à un poste (« Stelle ») dans une instance donnée (un département) et un mandant (un office). Le poste lui-même contient les droits d'accès aux différents objets applicatifs du mandant. Sans accès spécifique, un utilisateur pourra se connecter à un autre mandant que son office, mais ne pourra y afficher que les objets communs (tels que la structure des dossiers, mais pas leur contenu).

En plus des profils assignés aux utilisateurs finaux, des postes spéciaux aux droits étendus, tels qu'administrateur système (réservé aux collaborateurs des fournisseurs de prestations informatiques), administrateurs, gestionnaires des utilisateurs, etc. sont définis dans l'application. Certains profils permettent de s'attribuer des droits supplémentaires, mais le système protocole ces modifications. Le concept d'autorisation règle la gestion de ces profils spéciaux, une nouvelle version est d'ailleurs en cours d'élaboration pour différencier plus finement les postes d'administration. Dans les listes de contrôles des utilisateurs possédant des droits d'administration, le CDF a constaté une inconsistance (utilisateur d'un département dans le système d'un autre).

L'accès aux composantes de la couche de services communs est réservé à un nombre limité de spécialistes des fournisseurs de prestations informatiques, selon la répartition des tâches évoquée plus haut. Les administrateurs des bases de données sont par exemple membres d'un groupe restreint de l'ISCeco, des mécanismes de contrôle des modifications assurent que l'entrée dans le groupe soit protocolée. L'accès aux fonctions d'administration sur les serveurs GEVER se fait par l'intermédiaire d'un système de passerelle au moyen d'un compte d'administrateur.

Appréciation

Les mécanismes de contrôle mis en place pour les accès et les autorisations aux fonctions d'utilisation et d'administration de la plateforme GEVER sont fondamentalement appropriés. En particulier, le niveau d'assurance élevé de l'identification est adéquat et ne devrait pas être baissé malgré les demandes de certaines unités dans ce sens. La description des modalités de l'accès aux services Web doit être finalisée. Un contrôle périodique et documenté des listes d'utilisateurs possédant des droits d'administration doit aussi être instauré aux niveaux applicatifs et logiciels communs (middleware).

Recommandation 3 (Priorité 2)

Le CDF recommande à l'ISCeco de s'assurer que des listes d'utilisateurs possédant des profils d'administration dans des systèmes productifs GEVER soient périodiquement éditées et validées pour les niveaux applicatifs (Acta Nova) et des logiciels communs (middleware, notamment les systèmes de gestion de bases de données).

Prise de position des audités

Une plateforme donnant une vue d'ensemble des accès de chaque utilisateur ISCeco est actuellement en préparation.

2.5 Confidentialité : l'essentiel est assuré, les erreurs humaines restent possibles

L'article 11 de l'ordonnance GEVER[5] décrit les modalités de traitement des informations classifiées dans les systèmes de gestion des affaires. Il prescrit le chiffrage des informations classifiées CONFIDENTIEL, le traitement d'informations classifiées SECRET est proscrit. Si un utilisateur tente d'assigner la catégorie de classification SECRET à un document, le système bloque le traitement et informe le chargé de sécurité de l'information de l'unité. La solution SecureCenter, produit standard de l'administration fédérale, est utilisée pour le chiffrage de documents dans la plateforme GEVER. Les documents traités sont transmis et stockés encryptés, le déchiffrage n'intervient que sur le poste de travail de l'utilisateur et présuppose qu'il soit autorisé à le faire. Des métadonnées, partiellement définies par les utilisateurs, sont associées aux documents stockés et sauvegardées dans les bases de données de la plateforme. Les règlements d'utilisation prescrivent de ne pas gérer d'informations confidentielles dans les métadonnées.

Les instances de systèmes GEVER productifs sont parfois copiées dans d'autres environnements, par exemple des systèmes de formation ou de contrôle qualité (« Cloning »). Le fournisseur de prestations a proposé un concept de solution, les travaux de mise en œuvre sont en cours.

Appréciation

Une solution technique éprouvée est en place pour assurer la confidentialité des documents. Le CDF relève que pour le traitement des métadonnées, un risque d'erreur humaine ou de malveillance subsiste. Celui-ci est explicitement identifié dans la liste des risques résiduels.

Le CDF attend par ailleurs que les travaux de mise en place de la solution de clonage soient finalisés.

2.6 Gestion de la continuité : la démarche n'est pas aboutie

Des besoins accrus en termes de disponibilité sont identifiés pour le Standard fédéral du service GEVER. Une classe de disponibilité 3 est définie. Diverses mesures ont été mises en place par le programme GENOVA et l'ISCeco pour satisfaire aux exigences de la continuité informatique du service. Elle dépend toutefois du fonctionnement d'autres éléments qui ne sont pas sous le contrôle de l'SCeco (eIAM, infrastructure matérielle, autres services tels que Sedex). Les relations entre ISCeco et les bénéficiaires de prestations sont décrites dans des accords de niveau de service (Service Level Agreements, SLA). La gestion de la continuité des affaires (en anglais Business Continuity Management, BCM) est du ressort des bénéficiaires de prestations, elle n'a pas été examinée dans cette révision.

La gestion de la continuité du fonctionnement informatique du service est dans les mains de l'ISCeco. Un responsable est défini et rattaché au domaine des applications GEVER. Divers documents décrivent les modalités de la gestion de la continuité du service (organisation de crise, méthodologie en cas de crise). Le CDF remarque pourtant l'absence d'un standard (« policy ») actuel en la matière. Il n'a pas non plus trouvé de plan de récupération

[5] RS 172.010.441 : Ordonnance sur la gestion électronique des affaires dans l'administration fédérale, 3 avril 2019.

en cas de catastrophe (Disaster recovery plan, DRP), qui en indiquerait les étapes en fonction de scénarios de défaillance.

Sur le plan de l'infrastructure, la principale mesure contribuant à la disponibilité du service est la redondance des systèmes GEVER de production et de validation dans deux centres de calcul distincts de l'OFIT. Les tests de bascule entre les systèmes montrent que le mécanisme fonctionne. Ces deux centres sont situés en ville de Berne, leur proximité est un risque reconnu dans de nombreuses révisions antérieures du CDF. La migration des centres de calculs de l'OFIT (Migration CC CAMPUS OFIT 2020), dont les travaux ont commencé, contribuera à atténuer ce risque.

Pour surveiller le bon fonctionnement de la plateforme, un système de monitorage est en place, couvrant autant les aspects logiciels que matériels. L'application Acta Nova comporte également des fonctions de suivi de sa bonne marche. Le monitorage analyse en temps réel le fonctionnement de diverses composantes critiques, par instance. Il présente les résultats de manière synthétique dans un tableau de bord, mais permet aussi l'affichage détaillé de l'état des composantes. Enfin, il émet des alarmes qui peuvent, selon leur gravité, automatiquement générer des tickets dans la solution de gestion des incidents. Ils sont alors suivis et traités selon la procédure en vigueur.

En cas de défaillance, certaines mesures de récupération sont définies. Pour les documents et les bases de données notamment, des sauvegardes sont régulièrement effectuées. Des essais de restauration à partir des sauvegardes sont également effectuées dans le cadre de copies de systèmes. Le CDF note cependant l'absence de tests plus systématiques de récupération. Il relève par ailleurs que des incertitudes subsistent quant aux modalités des sauvegardes de documents. Des discussions à ce sujet sont encore en cours.

Appréciation

Plusieurs éléments de la gestion de la continuité sont en place. Le CDF note par exemple que le système de monitorage offre de bonnes possibilités de suivre le fonctionnement du système et de réagir à temps en cas de problème. Par contre, la démarche est encore incomplète et ne correspond que partiellement aux bonnes pratiques telles qu'elles sont décrites par exemple dans les normes ISO 27031 ou les librairies ITIL. Le CDF pointe particulièrement l'absence d'exercices de récupération selon différents scénarios et la documentation incomplète. Ces manques peuvent prétériter le degré de préparation de l'exploitation en cas de défaillance étendue des systèmes. Les départements et offices utilisateurs bénéficieraient aussi d'une démarche mieux définie pour la mise en place de leur propre gestion de la continuité des affaires.

Le CDF voit aussi un risque dans les incertitudes sur les modalités des sauvegardes. Il rejoint l'estimation des exploitants d'une très faible probabilité mais d'un impact majeur en cas de problème de récupération des données. Le CDF attend que les discussions à ce sujet soient finalisées.

Recommandation 4 (Priorité 1)

Le CDF recommande à l'ISCeco de définir à l'aide d'un cadre structuré le degré de maturité à atteindre en matière de gestion de la continuité du service informatique pour la plateforme GEVER et de planifier la mise en place de mesures dans ce sens.

Prise de position des audités

Un projet interne ISCeco est démarré en janvier 2021 pour définir les scénarios possibles de pertes de données et les mesures adéquates à implémenter, y compris les plans de récupération (DRP). La normes et standards ISO 27031 et ITIL seront considérés. Les orientations possibles seront présentées avant la fin 2021.

2.7 Maintien de l'intégrité : quelques lacunes

Diverses mesures organisationnelles et techniques sont en place pour assurer l'intégrité des systèmes et des données. Un processus de gestion des changements est décrit pour la plateforme GEVER à l'ISCeco, comprenant la création obligatoire d'une demande dans un système de suivi des tickets, sa validation, sa mise en œuvre technique, des tests et une validation avant sa mise en production. Les aspects contextuels de ce processus sont les suivants :

- Les environnements de production sont séparés de ceux de référence et de validation.
- Dans l'état actuel du programme, où des montées de version du logiciel sont encore en cours, une majorité de modifications sont appliquées à la production au travers d'un processus de gestion des versions (voir ci-dessous). Celui-ci implique la définition d'un paquet de changements, des tests documentés, une validation explicite et un déploiement automatisé. Dans ce cas, le système édite un protocole technique des modifications.

Le CDF relève toutefois que tous les objets constituant un développement dans la plateforme GEVER n'obéissent pas à la même logique. Certains d'entre eux, par exemple les configurations métier, les corrections urgentes (« hot fixes ») ou certains paramètres de fonctionnement, ne sont pas déployés de manière automatisée. Les autorisations doivent également être transportées manuellement par les spécialistes de l'exploitation. Enfin, les modifications dans les bases de données peuvent être faites manuellement directement dans les systèmes de production. Ces modifications ne peuvent bien sûr être effectuées que par le personnel autorisé, mais toutes ne laissent pas systématiquement de trace technique (protocole ou autre).

Sur le plan de l'intégrité des documents, des mécanismes existent dans Acta Nova pour calculer une valeur de hachage (« hash ») des fichiers, permettant ainsi une vérification de leur intégrité. Ces mécanismes ne sont pas encore mis en œuvre dans la version actuellement en place à la Confédération.

L'intégrité des systèmes est contrôlée périodiquement à l'aide d'outils d'analyse (« scan »). Ces analyses s'appliquent aux serveurs du Cloud Atlantica, aux serveurs de bases de données et aux programmes Web de la plateforme GEVER. Elles en mettent en lumière les éventuelles vulnérabilités. L'OFIT édite régulièrement les rapports de ces analyses et met en œuvre les éventuelles mesures correctives. Des audits sous forme de tests de pénétration sont également exécutés afin de vérifier l'intégrité et la solidité de la plateforme.

Appréciation

Le processus de gestion des changements comporte les points de contrôle et de validation attendus. L'automatisation des déploiements est à même d'assurer un transport ordonné des modifications dans l'environnement de production. Le CDF relève pourtant qu'un ré-

pertoire central et automatisé des changements n'est pas disponible pour tous les composantes de la plateforme GEVER. En conséquence, il n'a pas pu tester l'efficacité du processus de gestion des changements.

Le CDF relève qu'une partie des mesures visant à vérifier l'intégrité des documents (valeur de hachage) n'est pas encore mise en œuvre et n'a pas relevé d'entrée à ce sujet dans la liste des suspens.

Recommandation 5 (Priorité 1)

Le CDF recommande à l'ISCeco d'examiner les possibilités permettant la traçabilité de toutes les modifications apportées dans les composantes techniques de la plateforme productive GEVER (par ex. dans les bases de données). Les mesures améliorant la traçabilité des modifications doivent être mises en œuvre tout en tenant compte de leur faisabilité et de leur rapport coûts/utilité.

Prise de position des audités

Le service d'exploitation GEVER examinera les solutions permettant de répondre à cette recommandation.

Recommandation 6 (Priorité 2)

Le CDF recommande à l'ISCeco de finaliser les mesures de travaux de mise en place des mesures visant à la vérification de l'intégrité des documents (valeur de hachage).

Prise de position des audités

Le hachage est prévu dans la version 3.5 TZ1 du produit ActaNova. Le rollout de cette version sera réalisé jusqu'à mi 2022.

2.8 Traçabilité : les accès sont journalisés dans l'application

L'application Acta Nova journalise les accès en mode lecture et écriture aux documents contenus dans le système, ainsi qu'aux métadonnées. Les événements système sont également journalisés. Un profil d'autorisation spécifique permet l'affichage de ces accès. Le CDF a pu consulter ces protocoles. Toutefois, la vérification de l'efficacité de leur protection contre d'éventuelles manipulations aurait dépassé le cadre temporel fixé à cet audit.

2.9 Les mises en service s'effectuent de manière contrôlée

Un processus de mise en service des versions de la solution est décrit et mis en œuvre dans le cadre du programme GENOVA. Plusieurs contrôles sont en place pour assurer la qualité des livraisons du logiciel de la plateforme GEVER. Les mises en service sont planifiées et effectuées au sein d'un processus de gestion des versions. Au moment de la révision, la montée de version 3.0 est par exemple en cours, les activités à cet effet sont définies dans un plan de fenêtres de maintenance.

Avant une mise en service, des tests sont exécutés. Les critères de tests sont définis dans un outil. Ils assurent une large couverture des exigences fonctionnelles et non-fonctionnelles posées à l'application, par exemple des aspects relatifs à la sécurité. Des cas de tests sont décrits pour ces critères. Plusieurs cycles de tests se déroulent pour une livraison, leurs résultats et les défauts sont consignés dans l'outil. Les demandes de corrections sont alors assignées et suivies selon un processus établi. Lorsque les exigences sont suffisamment

couvertes, les tests sont considérés comme réussis. Dans le cas contraire, un cycle supplémentaire peut être organisé, ou la validation peut être ajournée. Les résultats des cycles de tests sont consignés dans un rapport.

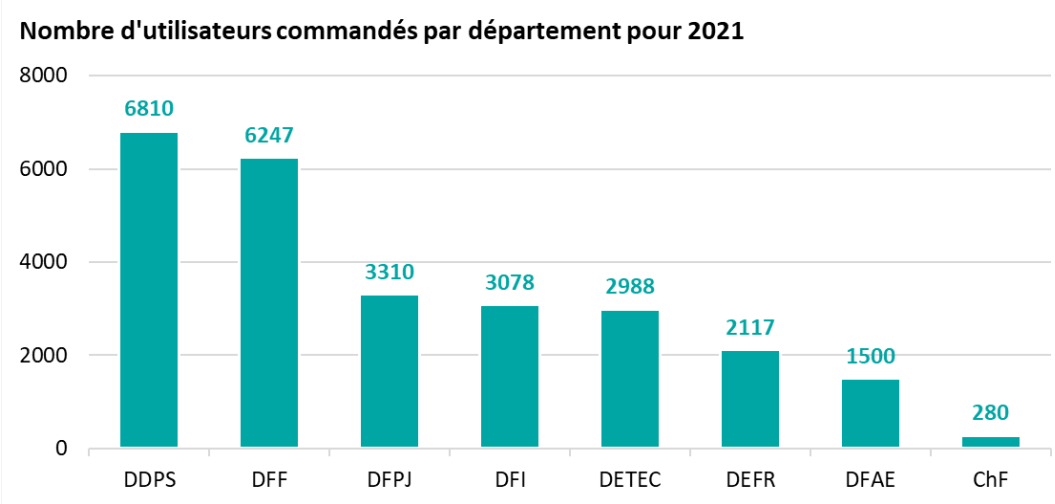
Le processus de validation d'une version est constitué de trois étapes. Si les résultats des tests sont suffisants, la direction du programme GENOVA, d'entente avec les départements, la ChF, l'ISCeco et le mandant, peut décider d'une préréception. Cette décision est prise pour chacun des deux projets du programme et documente notamment les réserves émises sur les défauts constatés. En parallèle, des tests sont effectués dans les projets départementaux, menant à la décision de mise en service. Après un mois d'exploitation de la nouvelle version, la validation peut intervenir.

Appréciation

Des contrôles suffisants sont définis et mis en œuvre dans le processus de mise en service des versions de la plateforme. Leurs résultats sont adéquatement documentés et les principaux intervenants (programme, fournisseurs de prestations, bénéficiaires de prestations) sont consultés.

2.10 La transition vers l'organisation permanente est réglée et en cours

Le programme GENOVA est encore en cours au moment de la révision, sa fin est prévue pour l'automne 2021. Une partie des tâches de l'exploitation du service GEVER a toutefois déjà été transférée à l'organisation permanente. A ce stade, l'introduction a eu lieu dans tous les départements, près de 20 000 utilisateurs travaillent déjà avec la solution. Depuis avril 2020, l'UPIC a repris la gestion des exigences pour la future version 4.0 de la plateforme. L'ISCeco est déjà en charge de l'exploitation informatique de la solution, près de 29 000 utilisateurs sont prévus pour 2021. Le passage de témoin vers l'organisation permanente s'opère au travers de différents canaux.



Graphique 3 : Nombre d'utilisateurs commandés par département pour 2021 (source : Programme GENOVA).

Un projet de mise en place de l'exploitation est explicitement défini au sein du programme GENOVA. Il vise à mettre en œuvre l'environnement et l'organisation de l'exploitation chez les fournisseurs de prestations désignés. Les processus et outils de l'exploitation ont notamment été définis et mis en service pour la plateforme GEVER, l'équipe en charge a été

constituée. Actuellement, diverses activités d'optimisation de l'exploitation sont en cours, portant notamment sur la gouvernance des configurations métiers et le déploiement. Les possibilités d'optimisation du support sont également examinées. Les responsables du programme GENOVA jugent satisfaisante la marche du projet de mise en place de l'exploitation, sa clôture est prévue pour décembre 2020.

Divers groupes de travail se sont constitués sous l'égide du programme pour traiter de la transition vers l'organisation permanente et faciliter le transfert de connaissances. Le « Managementboard » regroupe des membres de la direction de la ChF, de l'ISCeco, du programme, le mandant et le responsable du service TIC standard pour décider des grandes lignes de la suite des événements. Une équipe étendue (« erweitertes Kernteam ») traite des problématiques au niveau de la conduite. Des représentants du programme, de la ChF (notamment le Service spécialisé GEVER de la Confédération), de l'UPIC et de l'ISCeco participent à ce groupe. Selon les besoins, des spécialistes peuvent être convoqués (notamment pour les aspects de la sécurité).

A un niveau opérationnel, différents groupes « horizontaux » sont définis pour impliquer les représentants des utilisateurs et assurer la continuité des travaux de détail et le transfert de connaissances. Les thèmes du changement organisationnel, de l'architecture, de la configuration, de la migration, des tests et de la formation font notamment l'objet des travaux de ces groupes horizontaux. Le service spécialisé GEVER de la Confédération, rattaché à la ChF, assure le lien vers les départements et les offices utilisateurs.

Le CDF a pu prendre connaissance des comptes rendus du « Management-Board » et de l' « erweitertes Kernteam ». Les réunions se tiennent régulièrement. Les points ouverts sont consignés et suivis dans des listes de suspens. Elles couvrent une large palette de thèmes, allant des erreurs à traiter jusqu'à la vue d'ensemble des activités techniques pour 2021.

Appréciation

Les activités et les instances pour traiter du passage de témoin vers l'organisation permanente sont définies de manière appropriée. Le CDF relève que l'entrée en vigueur de la nouvelle organisation de la transformation numérique et de la gouvernance de l'informatique (TNI) est prévue pour janvier 2021. Toute réorganisation engendre des incertitudes qui pourraient peser sur certains points du fonctionnement du Service TIC standard GEVER. Les mécanismes de transition décrits ci-dessus et le fait que la TNI est rattachée à la ChF devraient faciliter la recherche des réponses à apporter.

2.11 Des recommandations largement mises en œuvre

Le CDF a vérifié la mise en œuvre de quatre recommandations issues d'audits précédents (voir l'annexe 2 pour le détail). Deux d'entre elles (15628.006, 16650.002) concernent l'utilisation de l'application SecureCenter dans GEVER comme solution de chiffrage des documents de niveau de classification « CONFIDENTIEL ». Une première était adressée à la ChF, la seconde à l'UPIC. Toutes deux préconisaient de suivre de près et de faciliter la mise en œuvre de SecureCenter au sein de la plateforme. Le CDF constate aujourd'hui que la solution de chiffrage est intégrée à GEVER. Les tests de la fonctionnalité sont effectués à chaque montée de version. Le CDF considère donc que ces deux recommandations sont mises en œuvre.

Une autre recommandation examinée (15628.009) préconisait de ne donner la responsabilité de la plateforme à l'UPIC qu'une fois l'introduction du produit complètement terminée, afin d'assurer la continuité dans le suivi du service GEVER. Le CDF constate que le passage de témoin se fait de manière progressive. L'UPIC et l'ISCeco prennent leurs prérogatives de manière échelonnée, mais parallèlement, le programme est encore en cours et pilote l'introduction de la version 3.0. La bascule complète vers le modèle du service standard est prévue après l'introduction de la version 3.5 du produit et se déroulera jusqu'en septembre 2021. La transition est traitée au sein de différents groupes de travail, aux niveaux du pilotage, de la conduite et de l'exécution. Le CDF considère que cette recommandation est mise en œuvre.

Une dernière recommandation (17407.004) portait sur la gestion stratégique du risque et de la qualité au sein du programme. Elle préconisait de redéfinir le mandat du gestionnaire (externe) des risques et de la qualité pour une participation mensuelle aux séances de gestion des risques. Elle demandait également d'élargir son périmètre de l'analyse aux projets des départements et des offices et d'évaluer la gestion opérationnelle de la qualité. Le CDF constate que le rythme des passages en revue est resté trimestriel, mais que le champ d'action du gestionnaire des risques s'est élargi aux éléments mentionnés. La recommandation est donc partiellement mise en œuvre. Au vu du statut du programme (plus que deux unités administratives sont prévues pour l'introduction), le CDF ne voit plus de risque élevé lié à ces points et clora la recommandation.

Appréciation

Le CDF considère que les recommandations examinées sont suffisamment mises en œuvre et les clora.

Annexe 1 : Bases légales

Textes législatifs
Ordonnance sur la gestion électronique des affaires dans l'administration fédérale (Ordonnance GEVER) du 3 avril 2019, RS 172.010.441

Annexe 2 : Recommandations examinées

15628.006	Die EFK empfiehlt der BK, die Entwicklung der gewählten Secure Center Lösungsvariante eng zu führen und gegebenenfalls auch rechtzeitig Korrekturmassnahmen einzuleiten, um sicherzustellen, dass die Bearbeitung vertraulicher Geschäfte rechtzeitig für die GEVER Einführung in den Departementen und Verwaltungseinheiten zur Verfügung steht.
15628.009	Die EFK empfiehlt der BK, die Verantwortung an das ISB erst nach erfolgreichem Abschluss der Einführungen zu übergeben, damit die notwendige Kontinuität sichergestellt wird.
16650.002	Die EFK empfiehlt dem ISB, die Umsetzung des Einsatzes von Secure Center für die Bearbeitung vertraulicher Geschäfte mit dem neuen GEVER Bundesstandard zu forcieren.
17407.004	Die EFK empfiehlt der Bundeskanzlei, den Auftrag an den strategischen Qualitäts- und Risikomanager neu zu definieren. Die Risikobeurteilung sollte öfter als alle drei Monate stattfinden. Mindestens die Teilnahme an den monatlichen Risikositzungen muss sichergestellt sein. Der Fokus sollte auch die Departements- und Amtsprojekte umfassen. Neben den Risiken sollte der QSRM auch die operative QS beurteilen.

Annexe 3: Abréviations

CDF	Contrôle fédéral des finances
ChF	Chancellerie fédérale
C-SI	Comité de la sécurité informatique
DEFR	Département fédéral de l'économie, de la formation et de la recherche
ISCeco	Centre de services informatiques du DEFR
OFIT	Office fédéral de l'informatique et de la télécommunication
OFS	Office fédéral de la statistique
SIPD (concept)	Sécurité de l'information et protection des données
TIC	Technologies de l'information et des communications
UPIC	Unité de pilotage informatique de la Confédération

Annexe 4 : Glossaire

Acta Nova	Logiciel de l'entreprise Rubicon It Sàrl de gestion des opérations et des dossiers
Atlantica Cloud	Infrastructure en nuage exploitée par l'OFIT
Business Continuity Management	BCM, ensemble de pratiques visant à maintenir la continuité des affaires en cas de défaillance des ressources ou dans les processus
DAKO	En allemand Datenkommunikation, service TIC standard pour la communication des données, géré par l'UPIC
Disaster Recovery Plan	DRP. Plan détaillant les étapes permettant la récupération du fonctionnement de systèmes en cas de défaillance.
eIAM	Service TIC standard de gestion de l'identité et des accès, géré par l'UPIC
GENOVA	Programme géré par la Chancellerie fédérale visant à introduire un seul et unique produit pour la gestion des affaires dans l'administration fédérale
GEVER	Gestion des affaires (en allemand « Geschäftsverwaltung »), système, système de gestion des affaires proposé par le service TIC standardisé GEVER
Hachage	En anglais hash, fonction cryptographique de calcul d'une valeur numérique identifiant de manière unique un contenu informatique (par ex. fichier), utilisée à des fins de vérification
ISO 27301	Norme de l'organisation internationale des standards réglant les pratiques de gestion de la continuité du service informatique.
ITIL	Information technology infrastructure library, modèle de bonnes pratiques dans la gestion du système d'information
Nuage privé	En anglais « private cloud », modèle d'informatique en nuage dédiée à une organisation
Middleware	Couche de logiciels offrant des fonctionnalités communes dans une architecture de système d'information, par exemple les bus d'entreprise ou les systèmes de gestion de bases de données
SecureCenter	Solution de chiffrage du Groupement défense
Sedex	Service TIC pour l'échange sécurisé de données, géré par l'OFS

Service level agreement	SLA, accord entre un fournisseur et un bénéficiaire de prestations sur le niveau de service que celles-ci devraient maintenir
Service TIC standard	Prestation informatique dont les unités administratives de la Confédération ont besoin avec une fonctionnalité égale ou similaire et gérée de manière centralisée
TNI	Transformation numérique et gouvernance informatique, nouvelle unité au sein de la Chancellerie fédérale, active à partir de janvier 2021, reprenant en partie les fonctions de l'UPIC.

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).