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

Nachprüfung der Informatik Führung und Betrieb

Zentrale Ausgleichsstelle

EFK-15381 / inkl. Stellungnahmen / 26. Februar 2016

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH-3003 Bern http://www.efk.admin.ch
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.15381.602.00191.07
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. +41 58 463 11 11
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung **Résumé** **Riassunto** **Summary**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») Italiano (« L'essenziale in breve ») English (« Key facts »)

Nachprüfung der Informatik: Führung und Betrieb
Zentrale Ausgleichsstelle

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hat bei der Zentralen Ausgleichsstelle (ZAS) nach 2014 eine weitere Prüfung im Informatikumfeld durchgeführt. Im Vordergrund standen die bei der Vorjahresprüfung abgegebenen Empfehlungen zur Behebung von zahlreichen festgestellten Mängeln[1]. Insgesamt hat die EFK eine wesentlich verbesserte Situation vorgefunden. Die Probleme wurden angegangen, die Führung zeigt Flagge. Die Empfehlungen der EFK sind insgesamt umgesetzt worden. Trotz aller Anstrengungen wird es jedoch noch Zeit und den notwendigen Willen der Führungskräfte brauchen, bis alle Mitarbeitenden an Bord des Schiffes sind, dass sich auf einem neuen Kurs befindet.

In den vergangenen 18 Monaten hat es die ZAS geschafft, feststellbare Verbesserungen zu realisieren. Für die EFK sind Ansätze einer neuen, positiven Unternehmenskultur spürbar. Dies ist vor allem auf die Zusammensetzung der Geschäftsleitung (GL) zurückzuführen. Drei von sieben Abteilungen haben neue Leiter/-innen erhalten. Seit Amtsantritt des Direktors am 1. August 2014 sind wichtige Reglemente und Weisungen erstellt bzw. überarbeitet worden. Vorarbeiten dazu hatten bereits vorgängig stattgefunden. Reorganisationen bei den Abteilungen „Centrale de compensation“ (CENT) und „Systèmes d’information“ (SI) bringen positive Entflechtungen bzw. Bündelungen.

Informatik und Beschaffungswesen: Die Grundlagen sind vorhanden

Bei der Informatik sind grosse Anstrengungen unternommen worden. Sowohl bei der Erfassung und Überwachung von Projekten wie auch bei deren Führung und Einbindung in die Unternehmensarchitektur konnten Fortschritte festgestellt werden. Die bisherige Praxis, für jede Änderung an einer Anwendung ein Projekt zu eröffnen, wurde aufgegeben. Ein Projekt muss heute definierte Kriterien erfüllen. Alle anderen Entwicklungstätigkeiten der SI laufen nun über das Änderungsmanagement ab, was zu wesentlich mehr Transparenz beiträgt. Die „Commission Informatique“ (ComInf) wird stärker in die Pflicht genommen. Nachholbedarf besteht bei den vertraglichen Regelungen zwischen der SI und deren Leistungsbezügern. Die Kundenzufriedenheit muss systematischer abgeholt und die IT-Strategie noch an die neuen Gegebenheiten angepasst werden.

Das Beschaffungswesen wurde grundlegend reorganisiert. Die dem stellvertretenden Direktor unterstellte zentrale Beschaffungsstelle sorgt in enger Zusammenarbeit mit den Abteilungen und Finanzdiensten für rechtmässige Beschaffungen. Die Weisungen zum Beschaffungswesen der ZAS und der dazu eingeführte Prozess geben den Verantwortlichen die notwendigen Kompetenzen. So verfügen nun auch die externen Mitarbeitenden der SI, deren Anzahl auf ein Minimum reduziert wurde, über korrekte Verträge.

[1] „Prüfung der Informatik, Führung und Betrieb (Integration des Lösungszentrums BIT Genf)“, PA 14504.

Das Absenzenmanagement funktioniert, die Geschäftsfortführung ist zu dokumentieren

Im Personalbereich hat das Absenzenmanagement der ZAS überzeugt. Es wird professionell gehandhabt. Die Personalumfrage 2014 hat auf Stufe GL zu Massnahmen geführt, um die Situation zu verbessern. Weiter sind die von der EFK geforderten Personensicherheitsprüfungen durchgeführt worden. Der bisher fehlende Austrittsprozess ist ebenfalls erarbeitet und vor Kurzem in Kraft gesetzt worden.

Beim Business Continuity Management (BCM) sind prozessorientiert die Risiken aufgenommen worden. Damit ist nur der Anfang gemacht, alle weiteren Grundlagen sollen bis Ende 2016 vorliegen. Insbesondere müssen sich die operationellen Risiken auch in den Informationssicherheits- und Datenschutzkonzepten (ISDS) widerspiegeln. Dies ist heute nicht systematisch der Fall. Die Überwachung der Schutzobjekte muss somit grundsätzlich verbessert werden.

Audit de suivi de l'informatique: gestion et exploitation Centrale de compensation

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a réalisé un deuxième audit de l'environnement informatique de la Centrale de compensation (CdC), après celui mené en 2014. Il s'agissait avant tout d'examiner la mise en œuvre des recommandations qui avaient été émises lors de l'audit précédent en vue de combler les nombreuses lacunes constatées[2]. Dans l'ensemble, le CDF a noté des progrès considérables. Grâce à la détermination de la direction, les problèmes ont été affrontés, et les recommandations du CDF ont globalement été mises en œuvre. Malgré les efforts déployés, les cadres devront encore faire preuve de patience et de suffisamment de volonté jusqu'à ce que tous les collaborateurs aillent dans la même direction.

Au cours des 18 derniers mois, la CdC a réalisé des progrès notables. Le CDF a pu observer les prémices d'une nouvelle culture d'entreprise positive, que l'on doit avant tout à la nouvelle composition de la direction. En effet, trois des sept divisions ont un nouveau responsable à leur tête. Par ailleurs, depuis l'entrée en fonction du directeur, le 1er août 2014, d'importants règlements et directives ont été établis ou modifiés sur la base des travaux préparatoires qui avaient déjà été entrepris. Enfin, la réorganisation des divisions Centrale de compensation (CENT) et Systèmes d'information (SI) permettent des séparations ou des regroupements positifs.

Informatique et acquisitions: les bases sont maintenant posées

Dans le domaine informatique, des efforts considérables ont été fournis. Le CDF a constaté des progrès tant aux niveaux de la saisie et de la surveillance des projets que de leur gestion et de leur intégration dans l'architecture d'entreprise. La pratique consistant à lancer un projet pour chaque changement apporté à une application a été abandonnée. Aujourd'hui, un projet doit remplir des critères définis. Toutes les autres activités de développement de la division SI passent par la gestion des changements, ce qui garantit nettement plus de transparence. La Commission Informatique (ComInf) est quant à elle davantage mise à contribution. Un retard doit être comblé en ce qui concerne les règles contractuelles entre la division SI et ses bénéficiaires de prestations. De plus, la satisfaction de la clientèle doit être vérifiée de façon plus systématique, et la stratégie informatique doit encore être adaptée aux nouvelles circonstances.

Le domaine des acquisitions a connu une profonde réorganisation. Subordonné au directeur suppléant, le service d'achat central garantit, en étroite collaboration avec les divisions et les services financiers, des acquisitions conformes aux dispositions légales. Les directives sur les acquisitions de la CdC et les procédures introduites dans ce cadre octroient les compétences nécessaires aux personnes responsables. Ainsi, les collaborateurs externes de la division SI, dont le nombre a été limité au strict nécessaire, disposent eux aussi de contrats en bonne et due forme.

[2] „Prüfung der Informatik, Führung und Betrieb (Integration des Lösungszentrums BIT Genf)“, PA 14504.

La gestion des absences fonctionne, mais la poursuite de l'activité doit encore être documentée

Appliquée de manière professionnelle, la gestion des absences de la CdC a fait ses preuves dans le domaine du personnel. A la suite de l'enquête menée auprès du personnel en 2014, des mesures ont été prises à l'échelon de la direction afin d'améliorer la situation. Par ailleurs, des contrôles de sécurité relatifs aux personnes ont été effectués, comme l'avait demandé le CDF. Le processus de départ, qui manquait jusqu'à présent, a été élaboré et est récemment entré en vigueur.

En matière de gestion de la continuité (Business Continuity Management), les risques ont été pris en considération axés sur les processus. Il ne s'agit là que du début. Toutes les autres bases seront créées d'ici à la fin 2016. Les risques opérationnels doivent en particulier se refléter dans les concepts de sûreté de l'information et de protection des données (SIPD), ce qui n'est pas systématiquement le cas à ce jour. D'une manière générale, la surveillance des objets à protéger doit être améliorée.

Texte original en allemand

Verifica successiva dell'informatica: gestione ed esercizio
Ufficio centrale di compensazione

L'essenziale in breve

Nel 2014 il Controllo federale delle finanze (CDF) ha effettuato un'ulteriore verifica dell'ambiente informatico presso l'Ufficio centrale di compensazione (UCC). L'attenzione si è focalizzata sulle raccomandazioni formulate in occasione della verifica dell'anno precedente e intese a colmare le numerose lacune accertate[3]. In generale il CDF ha incontrato una situazione nettamente migliore. Grazie alla convinzione della Direzione i problemi sono stati affrontati e le raccomandazioni del CDF sono state nel complesso attuate. Nonostante gli sforzi profusi occorrerà ancora del tempo ma anche la volontà dei dirigenti affinché tutti i dipendenti remino nella stessa direzione.

Negli ultimi 18 mesi l'UCC è riuscito a concretizzare miglioramenti accertabili. Secondo il CDF, grazie principalmente alla composizione della Direzione si percepisce una nuova e positiva cultura aziendale. Tre divisioni su sette hanno un nuovo capo. Dal 1° agosto 2014, data di entrata in carica del direttore, sono state allestite o rielaborate importanti istruzioni e regolamenti, che si basavano su precedenti lavori preparatori. Le riorganizzazioni nelle divisioni Centrale di compensazione (CENT) e Sistemi d'informazione (SI) comportano districamenti o raggruppamenti con effetti positivi.

Informatica e acquisti: le basi sono disponibili

Nel settore informatico sono stati profusi grossi sforzi. Infatti, nella rilevazione e nella sorveglianza di progetti così come nella loro gestione e integrazione nell'architettura aziendale si sono constatati notevoli progressi. La prassi che prevedeva l'avvio di un progetto ogniqualvolta fosse stata necessaria la modifica di un'applicazione è stata abbandonata. Oggigiorno ogni progetto deve soddisfare determinati criteri. Tutte le altre attività di sviluppo della divisione SI passano dalla gestione delle modifiche, ciò che contribuisce ad aumentare la trasparenza. La Commissione informatica è viepiù coinvolta. Un fabbisogno di recupero sussiste nell'ambito delle regolamentazioni contrattuali tra SI e i rispettivi beneficiari di prestazioni. La soddisfazione dei clienti deve essere sistematicamente verificata e la strategia informatica deve essere adeguata alle nuove realtà.

Il settore degli acquisti è stato completamente riorganizzato. La legalità degli acquisti è garantita, dato che il servizio centrale d'acquisto – che sottostà al direttore sostituto – lavora in stretta collaborazione con le divisioni e i servizi finanziari. Le istruzioni per gli acquisti dell'UCC e la relativa prassi forniscono ai responsabili le necessarie competenze. Attualmente anche i collaboratori esterni della divisione SI, il cui numero è stato ridotto al minimo, dispongono di contratti corretti.

La gestione delle assenze funziona, la continuità aziendale deve essere documentata

Nel settore del personale, la gestione delle assenze ad opera dell'UCC è convincente ed è effettuata in modo professionale. L'inchiesta sul personale del 2014 ha portato a livello di Direzione all'adozione di misure per migliorare la situazione. Inoltre sono stati eseguiti i controlli di sicurezza relativi

[3] „Prüfung der Informatik, Führung und Betrieb (Integration des Lösungszentrums BIT Genf)", PA 14504.

alle persone richiesti dal CDF. D'altra parte, il processo d'uscita sinora mancante è stato elaborato e introdotto di recente.

Per quanto riguarda il piano di continuità operativa (BCM) sono stati integrati i rischi legati ai processi. Tutte le altre basi devono essere completate entro fine 2016. In particolare i rischi operativi dovranno essere considerati nei progetti riguardanti la sicurezza dell'informazione e la protezione dei dati (SIPD), cosa che oggi non è fatta sistematicamente. La sorveglianza degli oggetti da proteggere deve essere migliorata in modo sostanziale.

Testo originale in tedesco

Follow-up audit on IT: management and operations
Central Compensation Office

Key points

The Swiss Federal Audit Office (SFAO) conducted another audit on the IT environment at the Central Compensation Office (CCO) after 2014. The focus was on the recommendations made during the previous year's audit for remedying the various shortcomings identified.[1] Overall, the SFAO found a much-improved situation. The problems were tackled and management has asserted itself. The SFAO's recommendations have been implemented on the whole. Despite all the efforts, it will still take time and the necessary willpower from managers to ensure that all employees are on board and support the new direction set.

Over the past 18 months, the CCO has succeeded in making noticeable improvements. The SFAO has observed the beginnings of a new, positive business culture. This is primarily due to the composition of the Executive Board. Three of the seven divisions were assigned new leaders. Since the director took up his position on 1 August 2014, important regulations and directives have been drawn up or revised. Preparatory work for this had already been carried out beforehand. The reorganisation of the Central Compensation ("CENT") and Information Systems ("SI") divisions has resulted in positive bundling or unbundling.

IT and procurement: the basis now exists

Considerable efforts have been made in the area of IT. It is clear that progress has been made in both the reporting and monitoring of projects and in their management and integration into the enterprise architecture. The previous practice of initiating a project for every adjustment to an application has been abandoned. Today, a project has to fulfil specific criteria. All other information systems development activities now go through change management, which ensures considerably greater transparency. The IT Commission (ITCom) has been assigned more responsibility. There is a lot of catching up to do with regard to the contractual provisions between the SI and their service procurers. Customer satisfaction must be improved systematically and the IT strategy must be adjusted to the new circumstances.

Procurement has been completely reorganised. The central procurement office, which reports to the deputy director, works closely with the divisions and financial services to ensure that procurements comply with the law. The directives on CCO procurement and the process introduced for this give the managers the necessary authority. In this way, the contracts of the SI external staff, who have been reduced in number to a minimum, are now correct.

Effective management of absenteeism, business continuation to be documented

In the personnel area, the CCO's management of absenteeism is convincing and is managed professionally. The 2014 personnel survey resulted in measures at the executive management level to improve the situation. In addition, the personnel security screening requested by the SFAO has

[1] „Prüfung der Informatik, Führung und Betrieb (Integration des Lösungszentrums BIT Genf)", PA 14504.

been performed. The departure process that was previously non-existent was developed and has recently come into force.

In business continuity management, the risks have been mapped in a process-oriented manner. This is just the beginning; all further groundwork should be completed by the end of 2016. In particular, the operational risks should also be reflected in the information security and data protection (ISDP) plan, which is not systematically the case currently. The monitoring of protected objects must be improved significantly.

Original text in German

Generelle Stellungnahme der Zentralen Ausgleichsstelle zur Prüfung:

La CdC est satisfaite de constater que les mesures prises pour mettre en place les améliorations recommandées par le CDF dans son rapport d'audit d'avril 2014 sont reconnues. Elle est déterminée à poursuivre son effort d'amélioration, en particulier dans le domaine de la gestion des risques (SCI et BCM) et de la sécurité informatique. Par ailleurs, elle est tout autant déterminée à assurer que les améliorations mises en place au cours des années 2014 et 2015 soient durables.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die EFK hat bei der ZAS im Frühjahr 2014 die Führung und den Betrieb der Informatik geprüft. Es mussten schwerwiegende Mängel festgestellt werden: Die Steuerung der Informatik sowie das Risikomanagement waren ungenügend und bei den Beschaffungen war gegen Bundesvorschriften verstossen worden. Parallel geführte, durch die Eidgenössische Finanzverwaltung (EFV) in Auftrag gegebene Administrativuntersuchungen kamen zu gleichen Resultaten. Die von der EFK abgegebenen Empfehlungen wurden von der ZAS mehrheitlich akzeptiert. Verbesserungsmassnahmen waren teilweise bereits eingeleitet worden, zeigten jedoch zum Zeitpunkt der damaligen Prüfung noch keine Wirkung. Die EFK hat daher entschieden, die Situation im Herbst 2015 erneut zu prüfen.

1.2 Prüfungsziel und -fragen

Grundsätzliches Ziel der Prüfung war, die aktuelle Situation im Bereich Führung und Betrieb der Informatik zu beurteilen. Dabei waren folgende Fragen zu beantworten:

- Wurden die von der EFK festgestellten Mängel behoben, d. h. die Empfehlungen umgesetzt?
- Hat sich die Reorganisation der Informatikabteilung positiv ausgewirkt?
- Kann die Informatik sicher und effizient betrieben werden sowie zukünftige Herausforderungen bewältigen?
- Wie sieht die zukünftige Informatikstrategie aus?
- Sind die Kunden der ZAS mit deren IT-Leistungen zufrieden?

Weiter war zu klären, ob das Beschaffungswesen nun den gesetzlichen Vorschriften entspricht und die Anzahl der externen Mitarbeitenden reduziert werden konnte. Aufgrund von vorjährigen Feststellungen war zu prüfen, wie mit Langzeitabwesenheiten bei der ZAS umgegangen wird.

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Cornelia Simmen (Revisionsleitung), Peter König, Stéphane Kury und André Stauffer durchgeführt. Zur Erfüllung des Prüfauftrages sind Interviews mit Schlüsselpersonen geführt und Dokumente beurteilt worden. Weiter wurde mit der Internen Revision zusammengearbeitet. Ergänzend erfolgten Auswertungen im Finanz- und Personalbereich.

1.4 Unterlagen und Auskunftserteilung

Die Prüfung vor Ort fand in der Zeit vom 2. bis 19. November 2015 statt. Die EFK hat von allen Beteiligten in offener und konstruktiver Weise Auskunft erhalten. Die verlangten Dokumente sind termingerecht und vollständig geliefert worden.

2 Organisation

2.1 Wichtige Grundlagen sind erarbeitet worden

Nach dem Amtsantritt des neuen Direktors ZAS per 1. August 2014 sind für die Abteilungen AHV-Leistungen und SI neue Leiter/-innen ernannt worden. Diese Posten wurden durch externe Personen besetzt. Der seit Februar 2014 ebenfalls neue Leiter CENT wurde zum stellvertretenden Direktor gewählt. Mit der erneuerten Geschäftsleitung (GL) konnten Veränderungen rasch herbeigeführt werden.

Die GL hat als Erstes bei zentralen Grundlagen gehandelt. Vorarbeiten dazu waren schon vorgängig geleistet worden. Die Dokumente „Geschäftsordnung der ZAS“ und „Règlement de la Commission Informatique“ wurden überarbeitet. Mit der Geschäftsordnung wird die Organisation der ZAS in den Grundsätzen auf Stufe GL, aber auch in Bezug auf eingesetzte Ausschüsse und Kommissionen geregelt. Eine der wichtigsten Änderungen betrifft das interne Inspektorat (INSP). Es ist weiterhin dem Direktor ZAS unterstellt, stellt aber seine Berichte auch dem Direktor der Eidgenössischen Finanzverwaltung zu. Die Selbständigkeit und Unabhängigkeit dieser Instanz wird damit gestärkt. Entsprechend ist der Leiter INSP bei Sitzungen der GL und der ComInf nur noch rapportierend eingeladen, jedoch nicht mehr stimmloses Mitglied. Der Direktor nimmt dafür nach Möglichkeit an Schlussbesprechungen zu internen Revisionsberichten teil. Die EFK beurteilt diese Entwicklung positiv. Einerseits ist Distanz zwischen den Führungsgremien und dem INSP geschaffen worden; andererseits erhält das INSP mehr Aufmerksamkeit der GL und insbesondere des Direktors. Damit sind die hauptsächlichen Anliegen aus der Empfehlung der EFK umgesetzt worden.

Weitere Grundlagen zum Beschaffungswesen und zum BCM der ZAS sind in Kraft gesetzt worden. Im Sinne der Empfehlung der EFK ist die „Weisung über die Unterschriftsberechtigungen in der ZAS“ ergänzt worden. Die inhaltliche Prüfung von Kreditoren-Rechnungen ist nun von der formellen Beurteilung strikt getrennt und bei den richtigen Stellen angesiedelt.

2.2 Reorganisation von zwei zentralen Abteilungen führt zu Entflechtungen

Mit der Reorganisation der CENT sind die Finanzen der ZAS und die der AHV voneinander getrennt worden. Die Aufgaben werden nun in zwei Bereichen wahrgenommen. Die ehemalige „contrôle de gestion“ ist bei den Finanzen ZAS integriert worden. Durch die Unterstellung beim stellvertretenden Direktor ist gewährleistet, dass der direkte Zugang zur GL besteht. Die zugewiesenen Aufgaben umfassen Analysen und Berichterstattung, das Erstellen des Finanzplans und Voranschlags der ZAS, das Führen der Staatsrechnung und die Kosten-/Leistungsrechnung. Demzufolge findet eine enge Zusammenarbeit mit allen Bereichen der ZAS statt. Dies entspricht weitgehend den in der Bundesverwaltung üblichen Tätigkeiten einer Controlling-Stelle. Die EFK beurteilt dieses Vorgehen als zielführend und akzeptabel. Die dahingehende Empfehlung ist somit umgesetzt.

Die Abteilung SI ist in einem ersten Schritt von allen nicht konformen Bereichen befreit worden. Die Bereiche „Risques et sécurité d’entreprise“ (RSE) und „Qualité d’entreprise“ (QE) sind heute ihren übergreifenden Aufgaben entsprechend als Stabsstellen dem Direktor unterstellt. Damit erhalten sie wesentlich mehr Gewicht als in der vormals untergeordneten Stellung bei der SI. Die SI verfügt seit dem 1. August 2015 über ein neues Organisationsreglement. Dieses regelt die Grundsätze, nach

welchen die SI funktionieren soll. Unter anderem wurde die bisherige Praxis aufgegeben, für Unterhaltstätigkeiten an Anwendungen ein Projekt zu führen. Anhand von finanziellen und personellen Ressourcen sowie von Risikofaktoren ist nun festgelegt, ab wann ein Projekt eröffnet wird. Alle anderen Änderungen/Entwicklungen erfolgen unter normalem Änderungsdienst, d. h. unter „Change and Request Management“ (CRM).

Der zweite Schritt ist mit einer Reorganisation der SI per 1. Dezember 2015 erfolgt. Die bisher wenig homogenen Geschäftsbereiche sind konsequent aufgeteilt und logisch zusammengeführt worden. Dadurch ergeben sich fünf Bereiche:

- Querschnittsfunktionen,
- Projekte/Architektur,
- drei auf die Technik der Anwendungen ausgerichtete Kompetenzzentren.

Die letztgenannten sind grundsätzlich für den Support und die Weiterentwicklung der entsprechenden Anwendungen verantwortlich. Die vom Fach stammenden Anwendungsverantwortlichen sind diesen zugeteilt. Damit soll eine bessere Zusammenarbeit zwischen Fach und Informatik erreicht werden.

Eingeführt worden ist per Juni 2015 der „Informatik Controllingbericht des finanziellen Informatikportfolios“ (ICOP). Dieser richtet sich an das Direktionskomitee der ZAS, an den Direktor der EFV und das Generalsekretariat des Eidgenössischen Finanzdepartementes. Mit diesem Instrument wird alle drei Monate über alle wichtigen Belange der Informatikabteilung rapportiert.

Aufgrund der prioritären Reorganisation sind bezüglich IKT-Strategie noch keine Anpassungen erfolgt. Für den Leiter SI ist klar, dass dieses Dokument in absehbarer Zeit überarbeitet und auf die neuen Strukturen sowie Zielsetzungen der GL ausgerichtet werden muss.

Beurteilung:

Die EFK begrüsst die von der Geschäftsleitung unternommenen Schritte. Die erarbeiteten Grundlagen sowie die verschiedenen Reorganisationen scheinen geeignet, um die ZAS insgesamt und die SI im Speziellen systematischer zu steuern und zu führen. Damit sind aber nicht alle Altlasten beseitigt worden. Führungs- und Schlüsselpositionen sind mehrheitlich von denselben Personen besetzt, was nicht von allen Mitarbeitenden positiv aufgenommen wurde. Die Umsetzung der Ziele und damit der Erfolg der Reorganisation vor allem in der SI müssen sich in der Zukunft erst noch zeigen.

Die von der GL gewünschten Veränderungen sind spürbar, aber die angestrebte neue Amts- und Führungskultur wird noch nicht von allen Mitarbeitenden akzeptiert bzw. mitgetragen. Die Segel sind gesetzt, der eingeschlagene Weg erscheint der EFK als sinnvoll und erfolgversprechend. Es wird allerdings Zeit und Überzeugungskraft brauchen, um die ZAS auf den neuen Kurs zu bringen.

3 Informatikführung

3.1 Das Projektportfolio basiert auf vorhandenen Bundeswerkzeugen

La gestion du portefeuille des projets informatiques de la Centrale de compensation (CdC) suit un processus bien défini sous la direction d'un Portfolio Manager expérimenté et se base sur l'application Cockpit IKT (outil de gestion du portefeuille et de contrôle de gestion informatiques à l'échelle de la Confédération) de l'Unité de pilotage informatique de la Confédération (UPIC). Les responsabilités du processus sont établies. La CdC se conforme à la directive concernant les projets informatiques de l'administration fédérale.

Les projets du portefeuille sont identifiés, suivis et évalués selon une méthode homogène et clairement définie. Les dérives identifiées sont présentées à la ComInf suivant un processus d'escalade défini dans le règlement.

Pour les projets en cours, les chefs de projets sont responsables de l'actualisation mensuelle des informations dans le Cockpit IKT et le contrôleur de gestion informatique de celle des informations financières. La mise à jour des informations est supervisée par le Portfolio Manager, qui vérifie mensuellement, à l'aide d'une liste de contrôle, que les données concernant la planification, les coûts ainsi que les documents de projets importants ont été actualisées.

Le processus et les outils de gestion du portefeuille des projets IT de la CdC seront encore complétés par des référentiels additionnels, qui seront mis en œuvre avec la mise en place de la nouvelle organisation des SI.

Le choix des projets en portefeuille et leur priorisation sont effectués par la ComInf sur une base annuelle dans le cadre de la planification financière de la CdC. Le processus et les critères de hiérarchisation sont clairement établis. La priorisation des projets est réalisée selon trois critères d'évaluation (importance stratégique, rentabilité et risques), adaptés de la norme « IT–Portfolio Methode » de l'UPIC décrivant la méthode de gestion du portefeuille IT. Le portefeuille de projets est en outre mis en regard des ressources disponibles. La proposition résultant de l'évaluation est finalement validée de manière collégiale par la ComInf.

Appréciation :

Le Contrôle fédéral des finances (CDF) considère que les outils et processus en place garantissent un suivi efficace du portefeuille des projets IT sur la base de données dont la qualité est contrôlée. Le processus de construction du portefeuille des projets IT répond à des critères clairs et est maîtrisé. Les responsabilités sont également clairement définies.

3.2 Bei der Projektführung/-steuerung sind Fortschritte sichtbar

Pour procéder à son contrôle, le CDF a sélectionné quatre projets et une étude. Le choix s'est porté sur des projets qui ont une importance pour le bon fonctionnement de la CdC. Parmi les projets, un a été finalisé dans le courant de l'année 2015, et les trois autres étaient encore en cours. Les projets suivants ont été examinés :

- ISO20022
- Echanges de Données eAVS - AI
- Migration Application Métier dans l'ADR (Active Directory)
- Modernisation Sumex,

ainsi que l'étude suivante:

- Fonctions standard Paiement et Comptabilité (FSPC).

Projets

Le CDF a constaté que les projets sélectionnés sont gérés en utilisant la méthode HERMES conformément à la directive concernant les projets informatiques de l'administration fédérale. Pour les quatre projets, l'organisation a été clairement définie. Les rôles importants comme le mandant sont occupés au niveau hiérarchique correspondant. Les décisions de libération de phase ont été prises par ce dernier durant les séances de Comité de Pilotage (CoP). Un suivi régulier des résultats du projet est donc assuré.

Pour les projets passés en revue où une solution technique n'était pas imposée, la sélection des variantes de solutions possibles a été réalisée durant la phase d'initialisation à travers l'élaboration d'une étude. Un concept de solution a été rédigé, contenant les choix réalisables en tenant compte des contraintes de l'architecture d'entreprise.

La mise à jour mensuelle des informations dans le Cockpit IKT par les chefs de projet permet de réaliser un suivi, en particulier des coûts et délais. Lors de réunions périodiques, le CoP et le mandant sont informés de l'avancement du projet et de l'évolution des coûts. Lorsqu'un écart important est identifié, le mandant peut décider d'escalader l'information à la ComInf en expliquant les déviations et les mesures prises. Tout changement de périmètre ou de planification qui a un impact sur le budget est validé par le mandant et documenté. Ce processus permet de garder le contrôle sur les dépassements de délai et de coût grâce à un suivi régulier. Le CDF a par ailleurs constaté que les initialisations et clôtures de projets sont validées par la ComInf.

Une analyse de risques est effectuée pour chaque projet. Celle-ci est discutée et validée pendant les séances du CoP. Une réévaluation régulière des risques et des mesures est réalisée durant l'avancement du projet. Les mesures de réduction de ces risques sont clairement identifiées. Ces informations sont enregistrées dans le Cockpit IKT.

Etude Fonctions standard Paiement et Comptabilité (FSPC)

La pré-étude Fonctions standard Paiement et Comptabilité (FSPC) est basée sur la méthode TOGAF (The Open Group Architecture Framework) en utilisant des documents et certains éléments proposés par la méthodologie HERMES comme l'organisation, la gestion des risques et la fixation d'objectifs clairement définis. La pré-étude, réalisée en collaboration étroite entre l'informatique et les métiers, s'est concentrée sur les risques associés aux processus financiers et aux plateformes de paiement, y compris le système « Chaîne de paiement ». Une analyse de la situation actuelle a

montré les forces et faiblesses du système en place. Des variantes de solutions ont pu être développées et sont maintenant en cours d'évaluation.

L'évaluation de l'architecture existante a permis d'identifier toutes les applications et les interfaces concernées dans le processus. Avec le soutien des architectes d'entreprise, l'architecture cible a ensuite été définie. Les différentes solutions ont été analysées et évaluées en fonction d'une grille de critères validée par le mandant.

Appréciation :

Le CDF considère que des améliorations ont été apportées au niveau de la gestion de projet. La méthode de gestion de projet HERMES est appliquée. Le mandant est impliqué dans chaque projet et prend les décisions nécessaires à sa bonne conduite. Les projets sont suivis et la communication est définie de manière adéquate. Un processus d'escalade a été mis en œuvre lors de déviations constatées. Le CDF juge également appropriée la démarche d'analyse utilisée pour l'étude.

3.3 Die Unternehmensarchitektur wird kontinuierlich durchgesetzt

En matière de gestion de l'architecture d'entreprise, la CdC adopte le référentiel TOGAF, préconisé par l'UPIC. Les principes, normes et standards d'architecture de la CdC sont définis, tout comme les contraintes architecturales (traitant par exemple des technologies qui ne sont plus supportées par l'OFIT). Les cartographies des applications, des données et de l'infrastructure supportant les processus métiers sont établis avec la participation conjointe de l'informatique et des divisions métier.

Un Comité d'Architecture d'Entreprise est en place et prend position sur la feuille de route technologique, les principes d'architecture et les décisions impactant l'informatique de la CdC. Ce comité verra sa composition étendue aux départements métier et aura en outre pour mission de vérifier la conformité des architectures proposées dans les projets. Les architectures cibles sont élaborées dans le cadre des projets informatiques, auxquels les architectes participent et dont ils valident la conformité architecturale. Les principes d'architecture et les décisions relatives aux technologies ont permis de préciser les critères de remplacement des applications et les choix des technologies.

Les capacités et l'alignement de l'architecture avec la stratégie d'entreprise ont été actualisés avec les départements métier pour aboutir à une liste de projets, priorisés au travers des méthodes de construction du portefeuille. Les grandes étapes de l'évolution architecturale, les éléments de l'architecture-cible et les projets correspondants sont identifiés, notamment pour la modernisation des applications métiers et la problématique du cycle de vie des applications. Le remplacement du mainframe « Host » fait l'objet d'une étude. Celle-ci comprend une analyse de faisabilité d'une bascule sur des serveurs utilisant la technologie UNIX. Les risques liés à ce grand projet, particulièrement les besoins importants de ressources financières et personnelles, sont identifiés.

Appréciation :

Le CDF considère que la thématique de l'architecture d'entreprise est maîtrisée. Les activités d'architecture d'entreprise et la stratégie d'entreprise sont intégrées logiquement, et les divisions métier participent à la démarche. L'architecture actuelle est décrite en détail, l'architecture cible est élaborée au sein des projets IT métier et techniques, et validée par les architectes. Les grandes évolutions architecturales et les projets correspondants sont identifiés de manière appropriée. La CdC devra veiller à intégrer dans ses réflexions architecturales l'évolution prévue de la stratégie IT.

3.4 Die Kundenzufriedenheit wurde punktuell eingeholt, vertragliche Vereinbarungen fehlen

Aufgrund einer Empfehlung der IR wurde im zweiten Semester 2015 eine Zufriedenheitsumfrage innerhalb der ZAS für die Anwendung „Aide au Calcul et Octroi de Rentes“ (ACOR) durchgeführt. Diese Anwendung ist eine der meistbenutzten. Die Resultate zeigen eine mehrheitlich hohe Zufriedenheit mit dem vorhandenen Werkzeug, aber dennoch auch Verbesserungsmöglichkeiten. Umfragen bei externen Partnern, z. B. den verschiedenen AHV-Kassen, haben bisher nicht stattgefunden.

Service Level Agreement bestehen für alle Dienstleistungen, die das Bundesamt für Informatik und Telekommunikation (BIT) für die ZAS erbringt. Diese entsprechen den üblichen Vertragswerken zwischen Leistungserbringer und -bezüger in der Bundesverwaltung. Keine speziellen vertraglichen Vereinbarungen existieren dagegen für die Dienste, welche der Leistungserbringer SI gegenüber internen und externen Kunden erfüllt. Das ComInf hat an seiner Sitzung vom 24. November 2015 das Thema „Operational Level Agreement“ (OLA) auf der Traktandenliste gehabt. Es wurde aufgezeigt und diskutiert, welche Dienstleistungen die SI für die internen Leistungsbezüger, d. h. die verschiedenen Bereiche der ZAS, ausführt. Da alle Abteilungsleiter der ZAS Mitglieder der ComInf sind, wurde damit ein einheitliches Verständnis erreicht. Diese sollte nun noch schriftlich zwischen den Partnern vereinbart werden.

Beurteilung:

Die SI gilt gemäss der erhaltenen Ausnahmeregelung seit 2012 als Leistungserbringer mit internen und externen Leitungsbezügern. Daher sollten die Dienstleistungen der SI mit ihren Kunden schriftlich vereinbart werden. Regelmässige Kundenzufriedenheitsumfragen tragen zudem dazu bei, dass Schwachstellen und Verbesserungspotenzial erkannt werden können. Aufgrund der Zertifizierung nach internationalem Qualitätsmanagement Standard ISO9001 müssten Umfragen regelmässig im Rahmen dieses Regelwerks stattfinden. Daher geht die EFK davon aus, dass dadurch zukünftig die SI ebenfalls abgedeckt sein wird.

Empfehlung 1 (Priorität 1):

Die EFK empfiehlt der ZAS, prioritär mit den institutionellen externen Leistungsbezügern vertragliche Vereinbarungen für die Dienstleistungen der Abteilung Informatiksysteme abzuschliessen. Diese Vereinbarungen sollten insbesondere die Verfügbarkeit, Vertraulichkeit, Integrität, Sicherheit und Verantwortlichkeiten regeln.

Stellungnahme der ZAS:

La CdC accepte la recommandation. Les bénéficiaires des services proposés par la CdC sont les organes d'exécution du 1er pilier.

Ces services sont: 1) le module ACOR, 2) les registres centraux, 3) le module d'augmentation des rentes, 4) SUMEX, et 5) la mise à disposition de token d'identifications.

Pour ces services, qui ne sont pas facturés, la CdC examinera – outre la possibilité des accords contractuels – d'autres variantes, afin d'aller dans le sens de la recommandation.

3.5 Beschaffungen erfolgen unter Einhaltung der gesetzlichen Vorgaben

Das Beschaffungswesen ist in der ZAS grundlegend geändert worden. Das Bundesamt für Bauten und Logistik (BBL) hat die ZAS bei der Erarbeitung der Grundlagen und Prozesse unterstützt. Die „Weisung zum Beschaffungswesen der ZAS“ regelt alle notwendigen Grundsätze. Die zentrale Beschaffungsstelle ZAS ist dem Stellvertretenden Direktor unterstellt und besteht zurzeit aus zwei Personen. Die Leiterin hat die spezifische BBL-Ausbildung bereits absolviert, ihr Mitarbeiter wird diese per 2016 besuchen. Verstärkt wird das Beschaffungswesen durch zwei spezialisierte Koordinatoren, welche im Rechtsdienst tätig sind. Für die technische Abwicklung wird einerseits das Vertragsmanagement Bund und andererseits SAP verwendet. Die aufgesetzten Prozesse gewähren grundsätzlich, dass die Beschaffungsstelle nicht mehr umgangen werden kann. Entsprechend bestehen keine Hinweise, dass die ZAS seit der letzten Prüfung der EFK Einkäufe getätigt hat, die nicht in ihrer Kompetenz lagen.

Die Beschaffungsstelle überprüft des Weiteren auch alle bisherigen z. T. langjährigen Verträge der ZAS. Es wird angestrebt, dass diese entsprechend den Weisungen inhaltlich und formell neu abgeschlossen werden können. Diese Arbeiten werden noch einige Zeit beanspruchen und führen zu hoher Arbeitsbelastung der Beschaffungsstelle.

Mit der bereits 2014 eingeleiteten Zentralisierung des Beschaffungswesens wurde die Anzahl von externen Mitarbeitenden bei der SI bereits erheblich reduziert. Nachfolgend konnten in Zusammenarbeit mit der EFV durch die Aufstockung des Personalbestandes bisherige Externe unter Arbeitsvertrag ZAS genommen werden. Die noch für die ZAS tätigen externen IT-Spezialisten sind mehrheitlich aufgrund einer durchgeführten öffentlichen Ausschreibung für Personalverleih ausgewählt worden. Die Leistungen werden gemäss den Empfehlungen der EFK aufgrund der gestempelten Präsenzzeit vom Fach kontrolliert und im Vieraugenprinzip durch einen Finanzverantwortlichen formell überprüft sowie zur Zahlung freigegeben.

Beurteilung:

Das aktuelle Beschaffungswesen der ZAS hinterlässt einen guten Eindruck. Die Prozesse sind so aufgestellt, dass Beschaffungen nun rechtmässig erfolgen und zentral überwacht werden. Aufgrund des raschen und noch nicht vollständig abgeschlossenen Aufbaus des Beschaffungswesens wird ein abschliessendes Urteil erst nach einiger Zeit im stabilen Regelbetrieb möglich sein. Positiv beurteilt die EFK auch die Reduktion an externen IT-Spezialisten.

4 Risikomanagement

4.1 Die Risiken sind erfasst worden, die Geschäftsfortführung im Katastrophenfall ist damit noch nicht sichergestellt

Die ZAS erfasst jährlich die strategischen Risiken gemäss Bundesprozess. Zusätzlich wurden per 2015 ausgehend von den operativen Prozessen die Verfügbarkeitsanforderungen definiert. Ebenfalls erfasst wurden dabei die für den Prozess notwendigen Anwendungen. Dieses Dokument stellt die Grundlage für eine weiterführende Business Impact Analyse (BIA) dar. Mit dieser muss nun aufgezeigt werden, welche Auswirkungen der Ausfall der IT auf die Kernprozesse haben könnte. Nachfolgend müssen die Massnahmen definiert werden, um die Risiken minimieren zu können.

Im Sinn einer Business Continuity Strategy (BCS) hat der Direktor per 1. Juni 2015 die „Directive relative à la gestion de la continuité des activités (directive BCM de la CdC)“ in Kraft gesetzt. In dieser werden die Ziele und Leitplanken des BCM festgelegt. Die Verantwortung für die Überarbeitung der Unterlagen BCM aus dem Jahr 2009 sind dem Bereichsleiter Risiko und Unternehmenssicherheit übertragen worden. Dieser muss nun sicherstellen, dass die BIA in Zusammenarbeit mit den Fachabteilungen erarbeitet wird. Alle weitergehenden Dokumente wie der Business Continuity Plan (BCP) und die nachfolgenden regelmässigen Testszenarien sind ebenfalls zu erstellen. Die Erkenntnisse aus der BIA müssen sich bezüglich IT-Risiken in den Informationssicherheits- und Datenschutzkonzepten der Anwendungen widerspiegeln (siehe Kapitel 4.2). Schlussendlich gilt es auch die Mitarbeitenden für das Thema zu sensibilisieren und fit zu machen.

Beurteilung:

Die wichtigsten Grundlagen sind mit der Erfassung der operativen Prozessrisiken und der Weisung zum BCM vorhanden. Die daraus abzuleitenden weitergehenden Pläne für die Aufrechterhaltung der wichtigsten Kernprozesse im Katastrophenfall müssen noch abgeleitet werden. Die Aktivitäten sind richtig aufgesetzt, aber es braucht noch Zeit bis zu einem formell korrekt aufgesetzten und operativ sichergestellten BCM. Die EFK erwartet, dass gemäss Planung bis Ende 2016 die noch fehlenden Teile erarbeitet und kommuniziert sind.

4.2 Die Informatiksicherheit muss systematischer überwacht werden

La sécurité de l’information à la CdC dépend du domaine RSE, indépendante de la division SI. Le délégué à la sécurité informatique de l’organisation (DSIO) participe aux réunions hebdomadaires du comité opérationnel des SI, le chef du domaine RSE est lui intégré à la Commission Informatique. Durant l’année, plusieurs activités de formation et de sensibilisation des collaborateurs à la sécurité de l’information ont été menées par le DSIO.

Les objets de protection pour les applications sont documentés dans le catalogue des applications et services. Pour les projets, le DSIO réalise un suivi de l’avancement de la rédaction des documents relatifs à la sécurité avec les informations disponibles dans le Cockpit IKT. Il soutient les chefs de projets dans l’élaboration de ces documents. Les outils permettant au DSIO de suivre la mise en œuvre des documents liés à la sécurité de l’information pour les applications ainsi que les projets ont été remis au CDF.

Suivi de la sécurité de l'information des projets

Le CDF a constaté que le document de suivi pour les projets a été créé au milieu du mois de septembre 2015. Celui-ci comporte un tableau comprenant la liste des projets, extraite du portefeuille IKT. Le contrôle réalisé est basé sur l'existence ou non d'une analyse des besoins de protection (ABP) validée et du concept de sûreté de l'information et de la protection des données (SIPD). Par contre, aucune indication n'est disponible sur la nécessité de l'élaboration d'un concept SIPD suite aux résultats de l'ABP ni sur la présence des documents relatifs à la protection de base. Lorsqu'un suivi doit être entrepris, les actions à réaliser sont bien décrites mais aucune indication n'est donnée sur le délai de leur mise en œuvre.

Suivi de la sécurité de l'information des applications

Les documents relatifs au suivi de la sécurité des applications comportent une référence à une base Lotus Note du catalogue des applications de la CdC, dans laquelle division SI maintient une liste des ABP et des concepts SIPD. Par contre, le document de suivi ne comprend pas de liste détaillée montrant l'état de la documentation de la sécurité des applications et ne permet pas de garantir que le contrôle effectué couvre l'intégralité des applications.

Durant cette révision, le CDF n'a pas procédé à un contrôle étendu de l'existence et de la validité des documents de sécurité des objets de protection de la CdC. Un exemple de preuve a été demandé pour une application considérée comme critique. Le document ABP reçu est daté du 18 novembre 2015 et est en version 0.1. Le CDF a constaté que ce document n'était pas validé formellement par le responsable du processus d'affaires. Le résultat de l'ABP a conclu à la nécessité de l'élaboration d'un concept SIPD. Celui-ci n'a pourtant pas été remis au CDF, ni le document contenant les indications relatives à la protection de base.

Appréciation :

Le CDF estime que les principes de l'organisation de la sécurité de l'information sont appropriés. Il juge par contre que l'outil utilisé pour le contrôle des documents de sécurité des projets et applications de la CdC ne garantit pas un suivi efficace et systématique de ces documents. Du point de vue du CDF, l'outil de contrôle doit contenir la liste complète des objets de protection (projets et applications). Pour chaque objet de protection, les indications suivantes sont au minimum nécessaires :

- existence, date et résultat de l'ABP,
- existence et date du concept SIPD,
- date du contrôle de la mise en œuvre des mesures de protection de base,
- date prévue du prochain contrôle de la conformité des documents de sécurité.

Le CDF n'a pas procédé à un contrôle étendu de l'existence des documents relatifs à la sécurité de l'information, mais constate que ces documents ne sont pas à jour pour au moins une des applications critiques de la CdC.

Recommandation 2 (Priorité 1):

Le CDF recommande à la CdC de revoir et systématiser la démarche de contrôle de l'existence et de la validité des documents relatifs à la sécurité de l'information pour ses objets de protection. Un inventaire de la situation de ces documents, un processus de contrôle périodique ainsi qu'un plan d'action pour leur actualisation doivent notamment être établis pour garantir un suivi efficace et systématique.

Stellungnahme der ZAS:

La CdC accepte cette recommandation et confirme les éléments suivants:

– La démarche de contrôle a été systématisée en 2015. Une feuille de route et un inventaire de la situation ont été fournis au CDF. Ces documents seront améliorés afin de tenir compte des commentaires du CDF au sous-chapitre „appréciation" du suivi de la sécurité de l'information.

– Le document de suivi fourni au CDF mentionne la nécessité ou non de l'élaboration d'un concept SIPD (colonne Concept SIPD) disponible (oui/non/pas nécessaire).

– Un mandat formel sera préparé par le DSIO à l'attention du chef de l'unité SI afin de rendre prioritaire cette action de mise-à-jour auprès notamment des chefs de projet et des responsables d'application, selon les jalons indiqués dans la feuille de route.

5 Personelles

5.1 Das Absenzenmanagement hat überzeugt

Die ZAS verfügt über zwei Mitarbeitende im Bereich Ressources Humaines (RH), welche für das Absenzenmanagement verantwortlich sind. Die Systematik und Werkzeuge werden seit drei Jahren kontinuierlich auf- und ausgebaut. Die Kader sind ausgebildet worden, damit diese ihre Verantwortung bei wiederkehrenden oder langfristigen Absenzen von Mitarbeitenden wahrnehmen. Alle drei Monate werden rollende Auswertungen über die Absenzen erstellt, d. h. es werden immer die letzten zwölf Monate erfasst. Überschreiten Absenzen 10 % der Sollzeit eines Mitarbeitenden wird der für den Bereich zuständige RH-Betreuer aktiv. Dieser tauscht sich mit dem entsprechenden Linienvorgesetzten aus. Die ZAS will möglichst früh die Gründe für Absenzen erfassen und wo notwendig Gegenmassnahmen ergreifen können. Die Vorgesetzten haben auch die Pflicht nach vier kleineren Absenzen mit dem betroffenen Mitarbeitenden ein Gespräch zu führen.

Der gesamte Prozess stellt sicher, dass bei Langzeitabwesenheiten die notwendigen externen Stellen rechtzeitig informiert und beigezogen werden (ärztlicher Dienst, Publica, Invalidenversicherung usw.). Die nach einer gewissen Zeit notwendige Kürzung von Ferienguthaben und Lohn läuft ebenfalls systematisch ab. Die betroffenen Mitarbeitenden werden darüber monatlich schriftlich informiert. Kehrt jemand von einer längeren Abwesenheit an den Arbeitsplatz zurück, so haben der Vorgesetzte wie auch die RH die Aufgabe, die Person in der ersten Zeit eng zu begleiten. Damit soll sichergestellt werden, dass allfälligen Einschränkungen Rechnung getragen wird.

Beurteilung:

Das vorgestellte Absenzenmanagement wird als vollständig und wirkungsvoll beurteilt. Die Prozesse sind dokumentiert, ergänzende schriftliche Weisungen vorhanden. Das Kader und die RH verstehen ihre Aufgaben und Pflichten, sie werden entsprechend gelebt. Die von der EFK festgestellte Häufung von Absenzen in bestimmten Bereichen ist rein zufällig durch schwere Krankheiten und unvorhergesehene Unfälle entstanden. Sie steht in keinem Zusammenhang mit dem beruflichen Umfeld der betroffenen Personen.

5.2 Die Resultate der Personalumfrage 2014 werden ernst genommen

Die vom Eidgenössischen Personalamt durchgeführte Personalumfrage ergab für die ZAS in einigen Punkten unterdurchschnittliche Werte im Vergleich zur übrigen Bundesverwaltung. Dies hat auf Stufe GL zu Massnahmen geführt. Danach wurde im Sommer 2015 eine erneute interne Umfrage durchgeführt. Diese zeigt, dass in vielen Bereichen bereits Verbesserungen erreicht worden sind. Allerdings sind viele Massnahmen, die sich in der Arbeitszufriedenheit auswirken, noch am Laufen oder wurden gerade erst abgeschlossen (z. B. Reorganisation SI). Die EFK hat daher keine vertiefte Prüfung zur angewandten Methodik durchgeführt.

5.3 Notwendige Personensicherheitsprüfungen wurden durchgeführt

Die EFK hat bei der vorjährigen Prüfung festgestellt, dass Funktionsträger in der ZAS nicht gemäss der Verordnung über die Personensicherheitsprüfung (PSPV) geprüft waren. Dies wurde in der Zwischenzeit nachgeholt, die entsprechenden Nachweise sind vorgelegt worden. Zusätzlich wird der Direktor ZAS voraussichtlich am 1. Februar 2016 die „Directive sur les conditions d'engagement et de contrôle du personnel de la CdC" in Kraft setzen. Darin ist u. a. geregelt, für welche Funktionen

zukünftig Straf- und Betreibungsregisterauszüge verlangt werden. Momentan findet zudem eine Überarbeitung der PSPV statt, welche für die ZAS Erweiterungen zur Folge haben kann.

5.4 Ein einheitlicher Prozess bei Personalaustritten ist nun vorhanden

Die EFK hat in der Vergangenheit bei zwei austretenden Kadern feststellen müssen, dass diese am letzten offiziellen Arbeitstag nicht alle von der ZAS zur Verfügung gestellten Hilfsmittel abgegeben hatten. Es lagen zwar Checklisten bei den verschiedenen im Austrittsprozess beteiligten Organisationseinheiten vor. Diese waren jedoch nicht vollständig und wurden nicht zentral überwacht. Dies hat zu unerwünschten Pannen geführt. Die RH hat dies nun in Form eines einheitlichen Austrittsprozesses geregelt. Bei Eingang einer Kündigung löst die RH den Prozess aus, sodass alle involvierten Stellen wie Vorgesetzte, IT, Gebäudesicherheit usw. über Checklisten einbezogen werden. Am Austrittstag stellt wiederum die RH sicher, dass alle Checklisten unterzeichnet vorliegen. Damit sollte zukünftig sichergestellt sein, dass niemand mehr mit Zugangsbadges oder geschäftlichen iPhones das letzte Mal das Gebäude der ZAS verlässt. Da der Prozess erst vor kurzem aufgesetzt wurde, hat die EFK lediglich die Änderungen zur Kenntnis genommen, jedoch keine weiteren Prüfungen durchgeführt.

6 Umsetzung der Empfehlungen aus der Vorjahresprüfung

Die EFK stellt fest, dass gemäss den Ausführungen in den obigen Kapiteln die Empfehlungen aus der Prüfung 2014 insgesamt umgesetzt worden sind.

7 Schlussbesprechung

Die Schlussbesprechung fand am 20. Januar 2016 statt. Teilgenommen haben seitens ZAS alle Mitglieder des „Comité de Direction“ sowie die Leiter INSP und RSE. Seitens EFK waren Herr Eric-Serge Jeannet und Frau Cornelia Simmen anwesend.

Sie ergab Übereinstimmung mit den Beurteilungen und Empfehlungen der EFK.

Eine weitere Besprechung fand mit der Eidgenössischen Finanzverwaltung am 28. Januar 2016 statt.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen

Finanzkontrollgesetz (FKG, SR 614.0)

Finanzhaushaltgesetz (FHG, SR 611.0)

Finanzhaushaltverordnung (FHV, SR 611.01)

Bundesinformatikverordnung (BinfV, SR 172.010.58)

Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB)

Geschäftsordnung der Zentralen Ausgleichskasse vom 17.12.2014

Règlement de la Commission Informatique de la Centrale de Compensation du 11.11.2014

Règlement d'organisation des systèmes d'information du 1er août 2015

Weisung zum Beschaffungswesen der ZAS (V2.0)

Directive relative à la gestion de la continuité des activités (directive BCM de la CdC, V1.4)

Directive sur les conditions d'engagement et de contrôle du personnel de la CdC du 1.11.2015

Weisung über Unterschriftsberechtigungen in der ZAS (V2.1)

Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen

Abkürzungen

ABP	Analyse des besoins de protection
ACOR	Aide au Calcul et Octroi de Rentes
BBL	Bundesamt für Bauten und Logistik
BCM	Business Continuity Management
BCP	Business Continuity Planning
BCS	Business Continuity Strategy
BIA	Business Impact Analysis
BIT / OFIT	Bundesamt für Informatik und Telekommunikation / Office fédéral de l'informatique et de la télécommunication
CdC / ZAS	Centrale de compensation / Zentrale Ausgleichsstelle
CDF / EFK	Contrôle fédéral des finances / Eidgenössische Finanzkontrolle
CENT	Centrale de compensation
ComInf	Commission informatique de la CdC
CoP	Commission de pilotage
CRM	Change and Request Management
DSIO	Délégué à la sécurité informatique
FSPC	Fonctions standard Paiement et Comptabilité
GL	Geschäftsleitung
INSP	Inspectorat interne
ISDS / SIPD	Informationssicherheit und Datenschutz / Sûreté de l'information et de la protection des données
OLA	Operational Level Agreement
QE	Qualité d'entreprise
RH	Ressources humaines
RSE	Risques et Sécurité d'Entreprise
SI	Systèmes d'Information (Informatikabteilung der ZAS)
UPIC	Unité de pilotage informatique de la Confédération

Glossar

HERMES	Projektmanagementmethode für alle Projekte in der Bundesverwaltung
IKT Cockpit	Werkzeug der Bundesverwaltung zur Erfassung und Kontrolle aller IKT-Anwendungen und -Projekte
TOGAF	Methodik und Industriestandard zur Entwicklung der Unternehmensarchitektur

Priorisierung der Empfehlungen

Die EFK priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).