



# **Führung und Betrieb der Informatik nach Integration des Lösungszentrums**

Zentrale Ausgleichsstelle



## **Impressum**

<b>Bestelladresse</b>	Eidgenössische Finanzkontrolle (EFK)
<b>Adresse de commande</b>	Monbijoustrasse 45, CH - 3003 Bern
<b>Indirizzo di ordinazione</b>	<a href="http://www.efk.admin.ch/">http://www.efk.admin.ch/</a>
<b>Order address</b>	
<b>Bestellnummer</b>	1.14504.602.00191.11
<b>Numéro de commande</b>	
<b>Numero di ordinazione</b>	
<b>Order number</b>	
<b>Zusätzliche Informationen</b>	Fachbereich 4
<b>Complément d'informations</b>	E-Mail: <a href="mailto:cornelia.simmen@efk.admin.ch">cornelia.simmen@efk.admin.ch</a>
<b>Informazioni complementari</b>	Tel. 0041 58 464 10 83
<b>Additional information</b>	
<b>Originaltext</b>	Deutsch
<b>Texte original</b>	Allemand
<b>Testo originale</b>	Tedesco
<b>Original text</b>	German
<b>Zusammenfassung</b>	Deutsch (« Das Wesentliche in Kürze »)
<b>Résumé</b>	Français (« L'essentiel en bref »)
<b>Riassunto</b>	Italiano (« L'essenziale in breve »)
<b>Summary</b>	English (« Key facts »)
<b>Abdruck</b>	Gestattet (mit Quellenvermerk)
<b>Reproduction</b>	Autorisée (merci de mentionner la source)
<b>Riproduzione</b>	Autorizzata (indicare la fonte)
<b>Reproduction</b>	Authorized (please mention the source)

## **Führung und Betrieb Informatik nach Integration des Lösungszentrums Prüfung Zentrale Ausgleichsstelle**

### **Das Wesentliche in Kürze**

---

Die Zentrale Ausgleichsstelle (ZAS) ist für das reibungslose Funktionieren aller Sozialversicherungen der ersten Säule (AHV, IV und EO) von grundlegender Bedeutung. Sie weist zwei Besonderheiten auf: Erstens ist sie kein unabhängiges Bundesamt, sondern eine Abteilung der Eidgenössischen Finanzverwaltung (EFV); hierarchisch ist sie deren Direktion unterstellt. Zweitens wurde sie im März 2012 vom Bundesrat ermächtigt - in Abweichung von der Bundesinformatikverordnung - einen Teil ihrer Informatikdienste zu reintegrieren. Dies war mit der Schaffung der neuen Abteilung Unternehmensgovernance und Informationstechnologie (GETI) verbunden, die 70 Angestellte umfasst.

Die EFK hat die Umsetzung dieser jüngsten Reform einer Prüfung unterzogen. Mit der Reform wird längerfristig eine Verbesserung der Kommunikation zwischen der ZAS und ihren Informatikmitarbeitenden, der Qualität der Dienstleistungen wie auch der Sicherheit der Operationen und der Informatiksteuerung der ZAS angestrebt.

Die Prüfungsarbeiten haben ergeben, dass die 2012 gesetzten Ziele noch nicht erreicht wurden. Die Priorität ist zu Recht auf die Aufrechterhaltung des laufenden Betriebes gelegt worden, die Modernisierungsprojekte sind in Verzug geraten. Die Prüfung von fünf im Jahre 2013 durchgeführten oder abgeschlossenen Schlüsselprojekten hat zudem Lücken in der Definition der Arbeitsergebnisse, der Budget- und Projektüberwachung sowie insbesondere der Validierung der Resultate zu Tage gebracht. Sowohl die Verantwortlichen GETI als auch das Informatiksteuerungsorgan der ZAS (ComInf) müssen ihre Aufsichtsaufgaben korrekt wahrnehmen können. Dazu sind sie auf Informationen über die Ressourcenplanung und die Arbeitsfortschritte angewiesen; solche Informationen fehlen bisher.

Auch das Risikomanagement muss im Bereich der Sicherheit sowie der Kontinuität der Operationen und des Schutzes der Fachanwendungen verbessert werden. Die EFK sieht Risiken, die ungenügend beherrscht werden.

Im Bereich der Beschaffung von Informatikgütern und -dienstleistungen hat die EFK festgestellt, dass die ZAS seit Jahren Beschaffungen vornimmt, ohne über eine entsprechende Beschaffungsdelegation des Bundesamtes für Bauten und Logistik zu verfügen. Die Beschaffungen wurden externen Mitarbeitenden übertragen und sind nicht nach den Vorschriften zum öffentlichen Beschaffungswesen durchgeführt worden.

Sowohl die leitenden Organe der ZAS als auch die Direktion der EFV sind sich des Ernstes der Lage bewusst und haben sich verpflichtet, Abhilfe zu schaffen. Es wurden Administrativuntersuchungen durchgeführt und seit anfangs 2014 verschiedene andere Massnahmen getroffen. Die Ernennung eines neuen Verantwortlichen an der Spitze der ZAS soll zu einer Verbesserung des derzeit sehr schlechten Arbeitsklimas beitragen.

Schlussendlich hat die EFK die Empfehlung abgegeben, das interne Inspektorat der ZAS direkt dem Direktor der EFV zu unterstellen, um der Besonderheit der Unterstellung der ZAS Rechnung zu tragen und deren Führungsinstrumente zu verstärken.



Die EFK hat die Stellungnahmen der ZAS beziehungsweise der EFV zu ihren Empfehlungen zur Kenntnis genommen. Da im Rahmen der Prüfung die Wirksamkeit der getroffenen Massnahmen noch nicht spürbar war, hält sie an ihren Feststellungen und Beurteilungen fest. Für die zweite Jahreshälfte 2015 ist eine weitere Kontrolle der getroffenen Massnahmen geplant.

**Originaltext in französisch.**

## **Conduite et exploitation de l'informatique après l'intégration du Centre de solutions**

### **Révision de la Centrale de Compensation**

#### **L'essentiel en bref**

---

La Centrale de compensation (CdC) est une institution essentielle au bon fonctionnement de toutes les assurances sociales du premier pilier (AVS, AI et APG). Elle présente la particularité de ne pas être un office fédéral autonome, mais une division de l'Administration fédérale des finances (AFF) à laquelle sa direction est soumise hiérarchiquement. Autre particularité, elle a été autorisée en mars 2012 par le Conseil fédéral – en dérogation à l'Ordonnance sur l'informatique dans l'administration fédérale – à réintégrer une partie de ses services informatiques. Ceci a conduit à la création de la nouvelle division Gouvernance d'entreprise et technologies de l'information (GETI), forte de 70 personnes.

Le Contrôle fédéral des finances (CDF) a souhaité examiner la mise en place de cette dernière réforme, qui devrait à terme améliorer la communication entre la CdC et ses informaticiens, impacter positivement tant la qualité des prestations que la sécurité des opérations et finalement améliorer la gouvernance informatique de la CdC.

Les travaux ont montré que les objectifs fixés en 2012 ne sont pas encore atteints. La priorité a été mise à juste titre dans la continuité des opérations et les projets de modernisation ont pris du retard. L'examen de 5 projets-clés conduits ou achevés en 2013 montre en outre des lacunes dans la définition des livrables, la gestion des budgets, la surveillance des projets et en particulier la validation des résultats. Tant les responsables de la GETI que l'organe de pilotage informatique de la CdC (ComInf) doivent assumer correctement leurs tâches de surveillance. Pour ce faire, elles ont également besoin d'informations sur la planification des ressources et l'avancement des travaux, informations qui font aujourd'hui encore défaut.

La gestion des risques informatiques doit également être améliorée, tant au niveau de la sécurité et de la continuité des opérations que de la protection de certaines applications métier, qui présentent des risques insuffisamment maîtrisés selon le CDF.

Dans le domaine des achats, le CDF a constaté que la CdC procède depuis des années à des achats de biens et prestations de services informatiques sans être au bénéfice d'une délégation de l'Office fédéral des constructions et de la logistique. Ces opérations ont été confiées à des collaborateurs externes et n'ont pas été faites selon les règles de la législation sur les marchés publics.

Tant les organes dirigeants de la CdC que la direction de l'AFF sont conscients de la gravité de la situation et s'engagent pour remédier à cette situation. Des enquêtes administratives ont été menées et d'autres mesures ont été prises depuis le début de l'année 2014. Le choix d'une nouvelle personne à la direction de la CdC devra contribuer à améliorer le climat de travail, aujourd'hui très maussade.

Pour tenir compte de la subordination particulière de la CdC au directeur de l'AFF et renforcer les moyens de ce dernier, le CDF a finalement recommandé de rattacher l'inspectorat interne de la CdC directement au directeur de l'AFF.



Le CDF a pris connaissance de la prise de position de la CdC, respectivement de l’AFF à ses recommandations. Comme les effets des mesures prises n’ont pas encore pu être constatés lors de son audit, le CDF confirme ses constatations et son appréciation de la situation. Un suivi des mesures prises sera réalisé dans la seconde moitié 2015.

## **Gestione ed esercizio dell'informatica dopo l'integrazione del Centro soluzioni Verifica del Ufficio centrale di compensazione**

### **L'essenziale in breve**

---

L'Ufficio centrale di compensazione (UCC) è un'istituzione fondamentale per il buon funzionamento di tutte le assicurazioni sociali del primo pilastro (AVS, AI e IPG). Ha la particolarità di non essere un ufficio federale autonomo, ma una Divisione dell'Amministrazione federale delle finanze (AFF), alla quale la sua direzione è subordinata. Inoltre, in deroga all'ordinanza sull'informatica nell'Amministrazione federale, nel mese di marzo del 2012 è stata autorizzata dal Consiglio federale a reintegrare una parte dei suoi servizi informatici. Questo ha portato alla creazione della nuova divisione Governo d'impresa e tecnologie dell'informazione (GETI), che comprende 70 persone.

Il Controllo federale delle finanze (CDF) ha espresso la volontà di esaminare l'attuazione di quest'ultima riforma che, a termine, dovrebbe migliorare la comunicazione tra l'UCC e i suoi informatici, influenzare in modo positivo sia la qualità delle prestazioni che la sicurezza delle operazioni e migliorare infine il governo informatico dell'UCC.

I lavori hanno mostrato che gli obiettivi fissati nel 2012 non sono ancora raggiunti. La priorità è stata giustamente data alla continuità delle operazioni e i progetti di rinnovamento hanno comunque subito dei ritardi. Inoltre, l'esame dei 5 progetti chiave condotti o conclusi nel 2013 mostra lacune nella definizione delle consegne, nella gestione dei budget, nella sorveglianza dei progetti e in particolare nella convalida dei risultati. Sia i responsabili del GETI che l'organo di direzione informatica dell'UCC (ComInf) devono poter svolgere correttamente i propri compiti di sorveglianza. A questo fine necessitano di informazioni sulla pianificazione delle risorse e sull'avanzamento dei lavori, che ancora oggi non sono disponibili.

La gestione dei rischi informatici deve parimenti essere migliorata, sia a livello della sicurezza e della continuità delle operazioni sia a livello della protezione di determinate applicazioni tecniche che, secondo il CDF, presentano dei rischi padroneggiati in misura insufficiente.

Nel settore degli acquisti, il CDF ha constatato che da anni l'UCC effettua acquisti di beni e prestazioni di servizi informatici senza essere in possesso di una delega da parte dell'Ufficio federale delle costruzioni e della logistica. Queste operazioni sono state affidate a collaboratori esterni e non sono state effettuate secondo la normativa sugli acquisti pubblici.

Sia gli organi direttivi dell'UCC che la direzione dell'AFF sono consapevoli della gravità della situazione e si impegnano per porre rimedio a questa situazione. Sono state condotte inchieste amministrative e dall'inizio del 2014 sono state introdotte ulteriori misure. La scelta di una nuova persona alla direzione dell'UCC dovrà contribuire a migliorare il clima di lavoro attualmente sgradevole.

Per tenere conto della particolare subordinazione dell'UCC al direttore dell'AFF e rafforzare i mezzi di quest'ultimo, il CDF ha raccomandato di aggregare l'ispettorato interno dell'UCC direttamente al direttore dell'AFF.

Il CDF ha preso atto della presa di posizione dell'UCC e di quella dell'AFF sulle sue raccomandazioni. Visto che gli effetti delle misure adottate non hanno ancora potuto essere constatati al momento del suo audit, il CDF conferma le sue constatazioni e la sua valutazione della situazione. Un controllo delle misure adottate sarà effettuato nella seconda metà del 2015.



**Testo originale in francese**



## **IT management and operation following Solution Centre integration Audit of Central Compensation Office**

### **Key facts**

---

The Central Compensation Office (CCO) is an institution which is crucial to the smooth running of all first-pillar social security funds (old age and survivor's insurance, disability insurance and compensation for loss of earnings). It has the specific feature of not being an independent federal office, but rather a division of the Federal Finance Administration (FFA), to which it is subordinate hierarchically. Furthermore, the Federal Council authorized the CCO in March 2012 – by derogation from the Federal Information Technology Ordinance – to restore some of its IT services. This led to the creation of the new division Corporate Governance and Information Technology (CGIT), which employs 70 people.

The Swiss federal audit office (SFAO) wanted to review the implementation of this last reform which aims to improve communication between the CCO and its IT specialists, have a positive impact on both service quality and the safety of operations, and enhance the CCO's IT governance.

The audit has shown that the objectives set in 2012 have not yet been achieved. Priority has correctly been given to business continuity, and the modernization projects have picked up delays. Furthermore, the review of five key projects carried out or completed in 2013 revealed gaps in the definition of the deliverables, budget management, project supervision and particularly the validation of results. Both the heads of the CGIT and the CCO's IT steering body (ComInf) must properly assume their supervision tasks. To do this, however, they need information on resource planning and work progress, which is still lacking at the moment.

IT risk management is also in need of improvement in terms of both the security and continuity of operations and the protection of certain business applications, which present risks that are insufficiently managed in the SFAO's opinion.

In the procurement area, the SFAO has found that the CCO has been procuring IT services and goods for years without a delegation from the Federal Office for Buildings and Logistics. These operations were assigned to external workers and were not carried out in accordance with the provisions of public procurement legislation.

Both the CCO's steering bodies and the FFA management are aware of the seriousness of the situation and are committed to rectifying it. Since the start of 2014, administrative investigations have been conducted and other measures have been taken. The appointment of a new head of the CCO will help to improve the working atmosphere, which is currently very gloomy.

In order to take account of the CCO's specific subordination to the Director of the FFA and to strengthen the latter's resources, the SFAO has ultimately recommended directly subordinating the CCO's Internal Inspectorate to the Director of the FFA.

The SFAO has acknowledged the position adopted by the CCO and the FFA in response to its recommendations. As it was not possible to observe the effects of the measures taken during its audit, the SFAO confirms its observations and assessment of the situation. A follow-up of the measures taken will be carried out in the second half of 2015.



**Original text in French**

## **Generelle Stellungnahme der [Zentralen Ausgleichsstelle] zur Prüfung:**

L'audit mené par le Contrôle fédéral des finances (CDF) au sujet de la gestion IT de la Centrale de compensation (CdC) a mis en évidence d'importantes lacunes ainsi qu'un non-respect de la loi fédérale sur les marchés publics (LMP). La CdC est consciente de cette situation et de la nécessité d'y remédier.

La création de l'unité Gouvernance d'entreprise et technologies de l'information (GETI) trouve son origine dans un réalignement stratégique au sein de l'administration fédérale (NOVE-IT) suivi d'une succession de réorganisations qui – dans le cas de la CdC – n'ont pas permis de réaliser les gains escomptés et de maîtriser l'obsolescence avérée des applications informatiques-clef nécessaires à l'accomplissement de ses tâches. En conséquence, le Conseil fédéral a approuvé le 28 mars 2012 une dérogation à l'Ordonnance sur l'informatique de l'administration fédérale (OIAF) autorisant la CdC à fournir elle-même les prestations informatiques dans le domaine des applications spécialisées propres à son domaine d'activité.

La mise sur pied d'un service informatique – la GETI – et l'intégration d'une part du personnel transféré de l'OFIT, avec tout le cortège de mesures d'ordre organisationnel, technique et financier qui l'accompagne, a eu lieu dans l'urgence et devait assurer le bon fonctionnement des applications informatiques sans lesquelles la CdC ne peut accomplir ses nombreuses missions. Cette situation, alliée à un manque de données fiables dans le domaine de technologies spécifiques et à une diminution importante de l'effectif de personnel suite à la réorganisation, a contraint la CdC à avoir provisoirement recours à des collaborateurs externes. Dans la foulée, il lui a également fallu conclure des contrats de gré à gré afin de ne pas stopper les projets et maintenances en cours, nécessaires pour l'accomplissement de ses objectifs. La CdC était toujours en mesure d'assurer l'exploitation du système informatique dont le paiement ponctuel des rentes.

Rendu attentive à diverses irrégularités en particulier par un audit mené par son Inspectorat interne, la direction ad intérim de la CdC a, dès novembre 2013, en coopération étroite avec la direction de l'AFF, mis en oeuvre une série de mesures en vue de remédier à la situation qui vient d'être évoquée. Ainsi fut-il décidé :

- de renforcer le processus d'internaliser le personnel temporaire dont la mission est pérenne et de limiter les engagements temporaires aux missions ponctuelles,
- de confier aux seuls collaborateurs internes des fonctions d'encadrement,
- de soumettre à l'OFCL tous les projets de contrat,
- de soumettre au Directeur de l'AFF tous les projets de contrats dont le montant nécessite de procéder à un appel d'offre OMC pour transmission à l'OFCL,
- d'assurer une gestion rigoureuse des projets informatiques, entre autres en renforçant les instances de surveillance et leurs instruments de pilotage,
- de mettre en vigueur une nouvelle réglementation concernant les compétences et signatures,
- que le Directeur de l'AFF participe jusqu'à nouvel avis aux séances du comité de direction ainsi que de la Commission informatique de la CdC,



- d'établir au sein du Comité de direction et de la Commission informatique une gestion transparente, participative et collégiale et de mettre en place ainsi une culture d'entreprise fondée sur la concertation et la participation aux décisions.

Ces mesures commencent maintenant à déployer leurs effets. De concert avec la mise en oeuvre des recommandations de l'audit en question et des enquêtes administratives, elles permettront d'éliminer les lacunes et irrégularités de façon durable.

## **Inhaltsverzeichnis**

<b>1</b>	<b>Auftrag und Vorgehen</b>	<b>14</b>
1.1	Ausgangslage	14
1.2	Prüfungsziel und -fragen	15
1.3	Prüfungsumfang und -grundsätze	16
1.4	Unterlagen und Auskunftserteilung	16
<b>2</b>	<b>Die Steuerung der Informatik</b>	<b>16</b>
2.1	Eine grundlegende IT-Strategie und das Steuerungsorgan existieren	16
2.2	Der Leistungserbringer GETI bekundet Mühe mit dem Erfüllen der Anforderungen	17
2.3	Die IT-Architektur kommt spät und ist noch unvollständig	17
2.4	Der Prozess IKT-Portfoliomanagement existiert, das Zusammenspiel der involvierten Stellen muss verbessert werden	18
2.5	Verschiedene Kontrollinstanzen sind in der ZAS vorhanden, können sich jedoch nicht durchsetzen	18
<b>3</b>	<b>Risikomanagement</b>	<b>19</b>
3.1	Das Risikomanagement muss verbessert werden	19
3.2	Hohe Risiken bestehen bei den Rentenzahlungssystemen	20
3.3	Arbeitsklima: mit Kritik muss offener und konstruktiver umgegangen werden	21
3.4	Fehlende Unterschriftenregelungen	21
3.5	Personensicherheitsprüfungen fanden bisher nicht statt	22
3.6	Die geprüften Finanzvorschriften wurden eingehalten	23
<b>4</b>	<b>Realisierung von IT-Projekten</b>	<b>24</b>
4.1	Die Abwicklung von IT-Projekten ist unbefriedigend	24
4.2	Ein funktionierendes Controlling bringt mehr Transparenz	25
<b>5</b>	<b>IT-Beschaffungen werden rechtswidrig durchgeführt</b>	<b>26</b>
5.1	Die ZAS verfügt über keine Beschaffungsdelegation für IT und braucht diese nicht	26
5.2	Temporär angestellte Mitarbeitende schulden nur die Arbeitszeit	27
5.3	Bei den getätigten IT-Beschaffungen gab es zahlreiche Ungereimtheiten	27
<b>6</b>	<b>Pendenzen aus der Prüfung der Schweizerischen Ausgleichskasse (Jahresrechnung 2013)</b>	<b>29</b>
<b>7</b>	<b>Schlussbesprechung</b>	<b>30</b>
	<b>Anhang 1: Rechtsgrundlagen</b>	<b>31</b>
	<b>Anhang 2: Abkürzungen, Priorisierung der Empfehlungen</b>	<b>32</b>



## 1 Auftrag und Vorgehen

### 1.1 Ausgangslage

Die Zentrale Ausgleichsstelle (ZAS) hatte bis zur Reorganisation der Informatik und Telekommunikation in der Bundesverwaltung (Projekt NOVE-IT) ein eigenes Rechenzentrum in Genf. Danach wurden die Systeme grundsätzlich beim Bundesamt für Informatik und Telekommunikation (BIT) zentralisiert. Physisch sind durch das BIT jedoch nur jene Systeme übernommen worden, welche Bundesstandard entsprachen. Rund die Hälfte an Anwendungen blieb weiterhin am Standort Genf. Um den Betrieb der Systeme in Genf und den Unterhalt sowie die Neu-/Weiterentwicklung der zahlreichen Anwendungen sicherzustellen, befand sich ein Team von rund 70 Spezialisten des BIT im Lösungszentrum (LZ) Genf mit Arbeitsplatz am Hauptsitz der ZAS. Als Leistungsbezüger wurde per 2002 das Gremium „Coordination et Controlling Informatique (CCI)“ geschaffen, per 2004 erweitert als „Conduite Informatique et Organisation (CIO)“ mit den Zielen: „piloter et coordonner les activités informatiques en lien avec les directions métier de la CdC et l'OFIT“. Zusätzlich bestand gemäss Reglement ab Januar 2004 die „Commission informatique de la Centrale de compensation (ComInf)“, welche bis heute mit Führungsaufgaben (Strategie, Planung, Budget, Controlling usw.) betraut ist.

Die ZAS zeigte sich in der Folge zunehmend unbefriedigt bezüglich der Leistungserbringung seitens des Lösungszentrums Genf. Die damalige Direktorin erteilte daher im Herbst 2007 einer Firma den Auftrag, ein „Schéma Directeur SI de la CdC“ zu erstellen. Dabei wurden die Informationssysteme, die Strukturen und die Steuerung der Informatik einer vertieften Analyse unterzogen. In ihrem Prüfbericht vom 22. Dezember 2008 „Zentrale Ausgleichsstelle IT-Governance“ stellte die EFK fest, *„dass die Informatik in der ZAS weitgehend effektiv und effizient funktioniert. Positiv zu erwähnen ist, dass sich die Direktion der ZAS der Abhängigkeit von der Informations- und Kommunikationstechnologie (IKT) bewusst ist und mit einem Projekt die Führung der Informatik neu definieren will. Die EFK erwartet, dass die Reorganisation des Bereiches CIO durch das Projekt DSI wie kommuniziert Ende 2009 umgesetzt sein wird.“*

Aufgrund der Feststellungen ist ab 1. November 2009 die „Direction des Systèmes d'information (DSI)“, also eine Informatikabteilung der ZAS, aufgebaut worden. Diese hatte zusammengefasst die Aufgaben: Weiterentwicklung und Umsetzung der IT-Strategie, operationelle Führung der IT-Projekte, Budget- und Kostenkontrolle, Qualitätssicherung und IT-Risikomanagement.

Mit diesem Vorgehen wurden erste Anzeichen sichtbar, dass daraufhin gearbeitet wurde, die Leistungserbringung vom BIT zu steuern und zu verbessern. Bereits im April 2010 wird in einem Rapport DSI an das Generalsekretariat EFD konkret auf die Frage „comment la CdC va-t-elle mettre en place et conduire son projet de sourcing“ eingegangen. Dabei wird das Jahr 2012 als Zeitpunkt für das Ende des IT-Bezugszwangs der ZAS beim BIT genannt. Diesem Rapport kann entnommen werden, dass die Anforderungen der ZAS an das BIT durch dieses unbefriedigend erfüllt wurden.

Ebenfalls im 2010 hat die ZAS die bestehenden SLA für die Fachanwendungen mit dem BIT mittels Letter of intent aufgekündigt mit dem Ziel, die SLA neu auszuhandeln. Mit Bundesratsbeschluss vom 28. März 2012 wurde schlussendlich der ZAS auf Antrag des Eidg. Finanzdepartements eine Ausnahmegewilligung erteilt, damit sie ihre IKT-Leistungen im Bereich der Fachanwendungen wieder selber erbringen kann. Im April 2012 hat die EFK im Prüfbericht „Informatikführung und Anwendungsbetrieb – Prüfung bei der ZAS“ festgehalten, dass die Direktorin ihre Verantwortung erkannt und die notwendigen Führungsinstrumente geschaffen hat. Die EFK stellte fest, dass sich die ZAS selbstkritisch mit den Risiken, den eigenen Stärken und Schwächen auseinandersetzt. Sie stellte eine positive Entwicklung der IT-Governance bei der ZAS fest und erwähnte, dass heute ein gutes und motiviertes Team vorhanden ist. Mit der Übernahme des LZ Genf durch die ZAS im Mai 2012 wurde aus der damaligen DSI und rund zwei Dritteln der ehemaligen BIT-Mitarbeitenden die neue Abteilung „Gouvernance d'entreprise et technologies de l'information (GETI)“ geschaffen. Damit ist die Struktur eines eigenen Leistungserbringers zusätzlich zur Rolle als Leistungsbezüger geschaffen worden.

Die EFK stellt in den nachfolgenden Kapiteln dar, in welcher Situation sich die ZAS zwei Jahre nach dieser grundlegenden Entscheidung befindet, und wie die vorgängig definierten, langjährigen Ziele bisher erreicht worden sind.

## **1.2 Prüfungsziel und -fragen**

Ziel der Prüfung war, den aktuellen Stand der Arbeiten nach Übernahme des LZ Genf durch die ZAS zu beurteilen. Dabei standen folgende Fragen im Vordergrund:

- Wird die Informatik zielführend und entsprechend den Vorgaben des Bundes geführt und betrieben?
- Sind die Strategie, Organisation und Prozesse angemessen und klar?
- Sind die finanziellen und personellen Ressourcen ausreichend?
- Sind die Leistungsbezüger mit den Dienstleistungen zufrieden?
- Welche Risiken bestehen?
- Erfolgen die Beschaffungen gemäss den entsprechenden Vorschriften?

Weiter interessierte die EFK, welche Herausforderungen es bei der Übernahme im Jahr 2012 gab und welche Vor-/Nachteile die neue Organisation hat.

Die Prüfung der IT-Governance wurde auf der Basis des Audit-Leitfadens des französischen Vereins für Informatik Audit und Beratung (Association française de l'audit et du conseil informatique, AFAI) durchgeführt. Dieser Leitfaden beinhaltet Fragen zur guten Praxis in 12 Bereichen der IT-Governance. Die EFK legte die Schwerpunkte auf die IT-Strategie, die Architektur, das IKT-Portfoliomanagement, das Risikomanagement, die IT-Projektleitung und das IT-Controlling.



### **1.3 Prüfungsumfang und -grundsätze**

Die Prüfung wurde von Peter König, André Stauffer, Markus Wüst und Cornelia Simmen (Revisionsleiterin) durchgeführt. Zur Erfüllung des Prüfauftrages wurden Interviews mit Schlüsselpersonen aus allen Hierarchie-Stufen der ZAS geführt, ergänzt mit der Beurteilung gelieferter Dokumente.

Verschiedene Berichte des Internen Inspektorats haben ebenfalls als Grundlage für weitere Abklärungen gedient. Gleichzeitig mit der Prüfung der EFK erfolgten zwei parallel laufende Administrativuntersuchungen, welche durch die Eidg. Finanzverwaltung (EFV) an eine externe Firma vergeben wurden. Die Arbeiten wurden zwischen dieser und der EFK koordiniert und die Resultate wurden gegenseitig ausgetauscht.

### **1.4 Unterlagen und Auskunftserteilung**

Die notwendigen Auskünfte wurden in offener Weise erteilt. Dagegen konnten nicht alle angeforderten Unterlagen fristgerecht geliefert werden. Es fehlten die Zusammenstellung der effektiven Kosten für die einzelnen IT-Verträge und die Absenzenliste für 2013 und 2014. Im Anschluss an die Schlussbesprechung vom 11. April 2014 sind die verlangten effektiven Abrechnungen zu den 59 IT-Dienstleistungsverträgen (Vertragsausschöpfung) durch die ZAS geliefert worden. Diese wurden durch die EFK nicht mehr geprüft und beurteilt.

## **2 Die Steuerung der Informatik**

### **2.1 Eine grundlegende IT-Strategie und das Steuerungsorgan existieren**

Eine Informatikstrategie liegt in Form des Dokumentes „Symphonie – Schéma directeur des systèmes d'information de la CdC“ vor. Diese stellt die Verbindung zwischen den fachlichen Aspekten und der Informatik sowie deren Prioritäten dar. Sie enthält zum grössten Teil diejenigen Informationen, welche in einem solchen Dokument erwartet werden, und die Ausführungen sind plausibel. Projekte zur Umsetzung der Strategie sind bereits 2011 identifiziert worden, die Strategie wurde jedoch erst im November 2012 durch die Direktorin validiert. Eine regelmässige Überprüfung und Aktualisierung der Strategie ist seither nicht erfolgt, obschon dies explizit vorgesehen ist. Der systematische Vergleich der strategischen Vorgaben mit dem effektiv erreichten Umsetzungsfortschritt ist für die Steuerung der Informatik zentral. Zur Steuerung der Informatik besteht, wie in Kapitel 1.1 dargelegt, das Gremium ComInf. Die Führung der regelmässigen Sitzungen obliegt dem Direktor a.i. der ZAS, Mitglieder sind alle Abteilungsleiter, der Leiter des internen Inspektorats und die Leiterin HR, sowie andere Spezialisten nach Bedarf. Eine überarbeitete Version des Reglements von 2004, in welchem die Aufgaben, Verantwortlichkeiten und Kompetenzen präzisiert sind, besteht seit September 2010, ist aber bisher nicht in Kraft gesetzt worden. Die EFK hält fest, dass aufgrund der Zusammensetzung der ComInf alle Fachbereiche und die Informatik vertreten sind, so dass die Steuerung und Priorisierung der Informatiktätigkeiten in der ZAS korrekt erfolgen könnten.



## **2.2 Der Leistungserbringer GETI bekundet Mühe mit dem Erfüllen der Anforderungen**

Mit der Zusammenlegung von bestehenden Informatikbereichen in der Abteilung GETI bestand seit Mai 2012 eine Struktur mit genügenden Ressourcen, die den Anforderungen der ZAS mehrheitlich hätte entsprechen können. Aufgrund der jahrelangen Bemühungen, wieder eigener Leistungserbringer für die Fachanwendungen zu sein, konnte erwartet werden, dass GETI rasch in der Lage gewesen wäre, eine bessere Leistung zu erbringen als vorgängig das BIT. Dies umso mehr als zentrale Anwendungen immer noch auf den Systemen des BIT installiert sind und somit deren Betrieb weiterhin durch diesen Leistungserbringer gewährleistet ist. Es muss jedoch zwei Jahre später festgestellt werden, dass weder bei der Weiter-/Neuentwicklung von Fachanwendungen, noch bei den Kosten und auch nicht bei der Kundenzufriedenheit spürbare Verbesserungen eingetreten sind. GETI hat zwar technisch notwendige Erneuerungen (z. B. Virtualisierung) vorgenommen, dieses Vorgehen scheint jedoch durch die Fachabteilungen bzw. auch die ComInf nicht verstanden worden zu sein. Gemäss der ZAS liegen die Prioritäten auch heute mehrheitlich auf dem Bau eines neuen Datacenters wegen stark operativen Risiken in Bezug auf den IT-Betrieb beim Bau der neuen Gebäude, der Integration der Fachanwendungen der ZAS in das Bundesnetzwerk sowie der Realisierung von unumgänglichen Projekten aufgrund von gesetzlichen Vorgaben. Dagegen ist bei der Umsetzung von konkreten Modernisierungs-Projekten wenig Fortschritt erkennbar (siehe Kapitel 4).

GETI hat bei der Übernahme des LZ BIT die Priorität bei der Aufrechterhaltung des laufenden Betriebes gesetzt. Gemäss verschiedenen Auskünften konnte dieser mit wenigen Ausnahmen stabil gehalten werden. In diesem Bereich ist es für die EFK verständlich, dass temporär Spezialisten zur kurzfristigen Überbrückung von fehlendem Wissen herbeigezogen wurden. Für zahlreiche andere externe Ressourcen konnten dagegen keine stichhaltigen Erklärungen gefunden werden, auch nicht dafür, dass zahlreiche Externe seit über zwei Jahren weiterbeschäftigt worden sind, obschon deren ursprüngliches Tätigkeitsfeld mittlerweile mit internen Mitarbeitenden besetzt ist. Aus Sicht der EFK bestand ein Risiko darin, dass zahlreiche Schlüssel- und teilweise auch Führungsfunktionen mit externen Kräften über sehr grosse Zeiträume hinweg besetzt waren (siehe Kapitel 5.2).

Obwohl in der Strategie die Verbindung zu den fachlichen Anforderungen besteht, wurde eine mittelfristige Planung des Ressourceneinsatzes für Projekte erst 2013 durchgeführt. Für GETI ist eine solche Planung erst im Aufbau, insbesondere im Bereich Informatik. Die Kopplung zwischen Strategie und Planung besteht damit erst in Ansätzen. Insbesondere bestehen Divergenzen bei der Berechnung von verfügbaren Ressourcen und bei deren Bedarf. Die unterschiedlichen Resultate und Aussagen sind für die EFK nicht nachvollziehbar.

## **2.3 Die IT-Architektur kommt spät und ist noch unvollständig**

Seit einigen Monaten wird aktiv an der IT-Architektur gearbeitet. Verschiedene Kartographien der Informationssysteme sowie Datenbeschreibungen sind erstellt worden. In der Strategie werden die Architektur-Schemata verwendet, um den Weg zwischen dem Ist-Zustand und der zukünftigen Ausrichtung der Informationssysteme bei der ZAS aufzuzeigen. Die Resultate werden auch als Kommunikationswerkzeug verwendet, um den Fachabteilungen die zukünftigen Instrumente oder auch technisch notwendigen Modernisierungen verständlich zu machen.

Die EFK beurteilt diese Aktivitäten als positiv und zielführend. Sie betont jedoch, dass die Aufgaben nicht beendet sind. Die Kartographien müssen mit technischen Beschrieben vervollständigt und die

Kommunikation vor allem in der ComInf institutionalisiert werden. Ausserdem wird nach Ansicht der EFK die Problematik der veralteten Mainframe-Plattform mit zahlreichen kritischen Anwendungen zur Rentenberechnung/-zahlung in den Architekturüberlegungen nicht mit der notwendigen Priorität angegangen. Die genauen Termine und Optionen für die Ausserbetriebsetzung dieser Infrastruktur und damit verbunden die Migration der entsprechenden Anwendungen müssen jetzt geklärt werden.

#### **2.4 Der Prozess IKT-Portfoliomanagement existiert, das Zusammenspiel der involvierten Stellen muss verbessert werden**

Der Prozess des IKT-Portfoliomanagements basiert auf der IT-Strategie. Projekte mit einer IT-Komponente werden von der ComInf priorisiert und in ein jährliches Portfolio integriert, was nachvollziehbar ist. Die Fachabteilungen sind über die Teilnahme ihrer Abteilungsleiter an der ComInf bei der Priorisierung der Projekte involviert. Es wurde dennoch mehrfach bemängelt, dass GETI ungenügend auf fachliche Fragestellungen und Bedürfnisse reagiert. Dieser Widerspruch wirft Fragen einerseits bezüglich der Priorisierung seitens ComInf, andererseits über die Qualität der Realisierung von Projekten und der Kommunikation von Projektergebnissen seitens GETI auf.

Zudem muss festgestellt werden, dass Risikoüberlegungen ungenügend im Priorisierungsprozess integriert sind. So waren zum Prüfungszeitpunkt beispielsweise Projekte zur Modernisierung der Prozesse und Systeme beim Zahlungssystem der Renten („chaîne de paiement“) im Portfolio 2014 nicht enthalten, obwohl seit längerem Anforderungen definiert sind und diese aus Sicht EFK mit höchster Priorität zu realisieren wären. Eine Prüfung des Internen Inspektorats hat zu den gleichen Feststellungen geführt.

Das Werkzeug Changepoint unterstützt die Aktivitäten des IKT-Portfoliomanagements, wird aber von den Benutzenden mehrheitlich als unbefriedigend beurteilt. Es müssten entweder am bestehenden Werkzeug weitere Verbesserungen bezüglich Benutzerfreundlichkeit, Datenextraktion und Transparenz ausgeführt oder einfach die vorhandenen Werkzeuge der Bundesverwaltung eingesetzt werden.

#### **2.5 Verschiedene Kontrollinstanzen sind in der ZAS vorhanden, können sich jedoch nicht durchsetzen**

Die ZAS verfügt über ein eigenes internes Inspektorat, welches prüft, ob die Vorgaben des Bundes und auch die internen Weisungen der ZAS eingehalten werden. Die EFK hat auf Verlangen die entsprechenden Berichte erhalten. Der Bericht „Prestataires externes de la Confédération mandats par la GETI: respect des dispositions légales et réglementaires en matière de marchés publics et d'acquisitions“ vom 4. März 2013 hat unter anderem dazu geführt, dass die EFK bereits im August 2013 die IT-Beschaffungen einer ersten Sichtung unterzogen hat. Auch weitere im Jahr 2013 erstellte Berichte im Umfeld der Informatik haben gezeigt, dass einige Bereiche problematisch sind. Obschon alle gesichteten Berichte von guter Qualität sind und in diesen auf bestehende Probleme hingewiesen werden (z. B. nicht gesetzeskonforme IT-Beschaffungen), sind die entsprechenden Empfehlungen im IT-Bereich durch die Linie mehrheitlich nicht umgesetzt worden. Das Inspektorat war der Direktorin bzw. ist heute dem Direktor a.i. unterstellt. Ohne Unterstützung dieser Stelle konnte es seine Empfehlungen jedoch nicht durchsetzen.

Dasselbe gilt für den Dienst „contrôle de gestion“, welche mit seinen systematischen Analysen dafür sorgen sollte, dass die Finanzmittel korrekt und nachvollziehbar verwendet werden. Auch diese Stelle hat die Direktion mehrfach über Missstände aufzuklären versucht. So wurde dargelegt, dass

die Produktivität der GETI inkl. der externen Mitarbeitenden bedenklich tief ist oder IT-Projekte trotz laufenden Zahlungen an externe Firmen keinen nachvollziehbaren Fortschritt aufweisen. Verbesserungsvorschläge (z. B. zur Führung der Kasse, zu einem zentralen Zahlungssystem, zur Unterschriftenregelung) sind alle abgelehnt worden oder blieben unbearbeitet. Die EFK hat begrüsst, dass dieser Dienst im Herbst 2013 nicht mehr der Abteilung Zentralen Ausgleichsstelle (ZENT) sondern der Direktorin als Stabsstelle unterstellt worden ist. Während der Revision der EFK ist dieser Schritt jedoch rückgängig gemacht worden. Damit besteht für die Leiterin dieses wichtigen Organes der Führungsunterstützung kein direkter formeller Zugang mehr zum Direktor a.i. der ZAS, und ihre Möglichkeiten, sich Gehör zu verschaffen, sinken. Insbesondere bestehen wenige Chancen, dass Feststellungen bezüglich der GETI überhaupt zur Kenntnis genommen werden. Vielmehr bestehen Bestrebungen, dass GETI ein eigenes IT-Controlling aufziehen will, was aufgrund der bestehenden Kontrollorgane weder sinnvoll ist, noch sich finanziell rechtfertigen lässt.

*Empfehlung 1 (Priorität 1)*

*Um dem vorhandenen Kontrollorgan mehr Gewicht zu geben, soll das Interne Inspektorat der Zentralen Ausgleichsstelle direkt dem Direktor der Eidg. Finanzverwaltung unterstellt werden. Die Führung der Zentralen Ausgleichsstelle als organisatorischer Bestandteil der EFV kann mit dieser Massnahme verbessert werden.*

Stellungnahme der [EFV]:

Die EFV wird die Empfehlung vertieft prüfen. Mit Blick auf eine zielführende und administrativ einfache Lösung wird sie dazu in den kommenden Monaten verschiedene Varianten evaluieren.

*Empfehlung 2 (Priorität 2)*

*Der Dienst „contrôle de gestion“ soll direkt dem Direktor oder der Direktorin der ZAS unterstellt werden, um diesen in seinen Führungstätigkeiten direkt unterstützen zu können.*

Stellungnahme der [ZAS]:

La recommandation du CDF sera examinée. D'autres possibilités sont également envisageables.

### **3 Risikomanagement**

#### **3.1 Das Risikomanagement muss verbessert werden**

Ein funktionierendes Risikomanagement sollte fachliche und IT-Risiken verbinden, sie in einen globalen Rahmen auf Stufe Gesamtunternehmung integrieren und damit eine Übersicht über die Risiken auf strategischer, organisatorischer und operationeller Ebene ermöglichen. Bei der ZAS wird die Methodik R2C der Bundesverwaltung eingesetzt, was die EFK positiv beurteilt. Trotz ergriffener Massnahmen bei den definierten strategischen IT-Risiken bleiben diese hoch eingestuft. Weitere Massnahmen zur Reduktion der Restrisiken sind allerdings nicht definiert worden. Es bestehen Mängel im Risikomanagement. So ist beispielsweise die Liste der 10 wichtigsten Risiken GETI unvollständig. Weiter wurde festgestellt, dass bei den definierten operationellen Risiken von GETI keinerlei Massnahmen definiert sind und dadurch auch keine Kontrolle erfolgen kann, ob

diese wirksam sind. Ausserdem sind die IT-Prozesse und die darin integrierten Kontrollen (Internes Kontrollsystem) im dafür vorgesehenen Werkzeug MEGA ungenügend dokumentiert. Wie der EFK dargelegt wurde, ist die ZAS bestrebt, eine Zertifizierung für ein Qualitätsmanagementsystem nach Standard ISO9001 zu erhalten. Grundlegende Basis für ein solches Vorhaben ist die detaillierte Dokumentation aller vorhandenen Kernprozesse. Da bereits Voraudits für die Zertifizierung durchgeführt worden sind, müsste GETI seine Prozesse seit längerer Zeit ausreichend dokumentiert haben. Die EFK zweifelt daran, ob hier die richtigen Prioritäten gesetzt wurden.

### **3.2 Hohe Risiken bestehen bei den Rentenzahlungssystemen**

Die EFK sieht einerseits technische Risiken und andererseits ein sehr hohes Unternehmensrisiko bei den Prozessen und Systemen der Rentenzahlungen. Mit der „chaîne de paiement“ werden monatlich Zahlungen von rund einer halben Milliarde Franken an beinahe 900'000 Empfänger in der ganzen Welt getätigt. Einerseits besteht die Problematik der Verfügbarkeit der eingesetzten Mainframe-Systeme. Diese sind „end-of-life“ und es wird immer schwieriger, die personellen Ressourcen für die Betreuung dieser veralteten Technologie zu finden.

Andererseits ist die gesamte systemische Abwicklung der Rentenzahlungen kaum nachvollziehbar. Kontrollen über die ausgeführten Zahlungen können nur sehr rudimentär durchgeführt werden und es finden mehrfache Medienbrüche mit manuellen Eingriffsmöglichkeiten statt. Der Gesamtbetrag an bezahlten Renten kann für eine einzelne Person nicht automatisiert berechnet werden. Die Zahlungsdaten werden zudem auf verschiedenen Systemen verarbeitet und gelagert, die den bundesweiten Sicherheitsanforderungen nicht genügen.

Die Systeme für die Abwicklung der Zahlungen (verantwortliche Sektion „Trafic des paiements internationaux - TPI“) müssen modernisiert werden. Um prioritär die monatlichen Zahlungen auf den neuen von PostFinance ab 2016 verwendeten und anerkannten Standard zu bringen, wurde TPI selber aktiv. Die fehlende Definition der Bedürfnisse in diesem Bereich führte allerdings zu verschiedenen internen Problemen mit der GETI und Schwierigkeiten mit einer externen Firma. Die EFV hat dazu eine Administrativuntersuchung angeordnet. Die EFK hat den entsprechenden Bericht zur Kenntnis genommen und keine weiteren Abklärungen vorgenommen.

In der Risikomatrix von GETI wird die „chaîne de paiement“ zwar in den 10 Toprisiken geführt, aber nur global mit „incident majeur“ und mit wenig Priorität. Die EFK sieht nicht nur beim Ausfall der Systeme Risiken, sondern auch darin, dass Datenmanipulationen bei den Zahlungen oder der Abfluss von besonders schützenswerten Personendaten erfolgen könnten. Da die nötige Dokumentation (Know-How Verlust) nicht vollständig zur Verfügung steht, sowie kein wirksames internes Kontrollsystem aufgesetzt ist, beurteilt die EFK die „chaîne de paiement“ sowie die damit verbundene Datenhaltung als intransparent, nicht nachvollziehbar und sieht darin ein hohes Risiko.

#### *Empfehlung 3 (Priorität 1)*

*Die Risiken im Zusammenhang mit den Systemen und Anwendungen der Rentenzahlungen sind vollständig zu adressieren und notwendige Massnahmen zur Reduktion dieser Risiken zu definieren und umzusetzen. Die Nachvollziehbarkeit muss über den gesamten Zahlungsprozess gewährleistet werden können.*

Stellungnahme der [ZAS]:

La recommandation est acceptée.

Les mesures de mitigation des risques sont listées dans le cadre de l'audit de l'Inspectorat sur la chaîne de paiement INAR et seront définies dans l'Etude de modernisation des applications financières.

L'ensemble des risques ainsi qu'un plan d'action seront présentés à la ComInf et au Directeur de la CdC pour approbation.

### **3.3 Arbeitsklima: mit Kritik muss offener und konstruktiver umgegangen werden**

Die EFK stellt fest, dass das Arbeitsklima in der ZAS verbessert werden muss, um die notwendigen Veränderungen und Weiterentwicklungen auch in der Informatik zu ermöglichen. Für die anstehenden Veränderungen ist eine bereichsübergreifende Zusammenarbeit ohne „Silodenken“ nötig, ebenso ist ein ausreichend offener und konstruktiver Umgang mit Kritik essenziell.

Auffallend waren in der Vergangenheit krankheitsbedingte Abwesenheiten von Mitarbeitenden der ZAS, die als kritisch eingestellt bekannt sind. Ob diese als Reaktion auf zu hohen Druck seitens der Führung gedeutet werden muss, kann nicht abschliessend beurteilt werden. Die Leiterin des Personaldienstes versichert, dass man überdurchschnittliche Abwesenheiten systematisch im Auge behalte und auffällige bzw. hilfeschuchende Mitarbeitende professionell begleite. Die angeforderten Abwesenheitslisten hat die EFK bis zum Abschluss der Revision nicht erhalten. Von der EFK eingesehene Kreditorenrechnungen belegen, dass in Einzelfällen tatsächlich Mitarbeitende eine externe Unterstützung erhielten.

In einigen Bereichen konnten Anzeichen für einen Kulturwandel festgestellt werden. Es wird die Aufgabe der neuen Führung der ZAS sein, diesen Weg zu einer von gegenseitigem Vertrauen geprägten Unternehmenskultur konsequent fortzuführen und wo nötig auch durchzusetzen.

### **3.4 Fehlende Unterschriftenregelungen**

In der ZAS existierte jahrelang lediglich eine Liste der Mitarbeitenden, welche über die Berechtigung zur Rechnungsfreigabe verfügten. Wer Verträge abschliessen oder Einkäufe tätigen durfte und bis zu welcher Höhe die Kompetenzen der Unterschriftsberechtigten gingen, war bis September 2013 unregelt. Dies hat in der Vergangenheit zu verschiedensten Ungereimtheiten geführt. So hat die Direktorin zumindest mit einer Firma Verträge mit Einzelunterschrift abgeschlossen (Vertrag aus dem Jahr 2008) und die nachfolgenden Rechnungen in der Höhe von 750'000 Franken alleine zur Zahlung freigegeben. Weiter haben bis ins Frühjahr 2013 temporär angestellte Mitarbeitende die Fakturen von ebenfalls externen Mitarbeitenden zur Zahlung freigegeben, teilweise sogar von Firmen, in denen sie vorgängig selber Angestellte waren. Die Weisung, welche weitergehende Regelungen beinhaltet, lag mehrere Monate unbeantwortet in der Direktion und wurde erst dann in Kraft gesetzt, als die EFK bereits vor Ort die IT-Beschaffungen einer ersten Sichtung unterzogen hatte.



Die nun seit 1. Oktober 2013 geltende „Directive sur les compétences et les droits de signature du personnel de la CdC pour les achats, les transactions et les engagements financiers“ mit ihren vier Anhängen regelt einiges, erfüllt aber die Anforderungen gemäss Finanzhaushaltverordnung (FHV), Art. 37 noch nicht. Gemäss diesem Artikel wird mit der Unterschrift auf Rechnungsbelegen die formelle und materielle Richtigkeit bestätigt. Im Anhang 3 der ZAS-Weisung ist geregelt, wer externe Fakturen validiert. Sowohl für die Freigabe von Rechnungen temporärer Angestellter wie auch für solche von IT-Mandaten sind untergeordnete Angestellte aufgeführt, welche nicht in der Lage sind, die fakturierten Stunden mit der tatsächlich erbrachten Leistung zu prüfen. Das Überprüfen der materiellen Richtigkeit liegt normalerweise bei IT-Projekten in der Verantwortung des Projektleiters. Bei temporären Angestellten müsste eine Freigabe durch den für die Person verantwortlichen Linienvorgesetzten stattfinden. In allen Fällen muss die Freigabe durch interne Mitarbeitende und nicht durch externes Personal stattfinden.

*Empfehlung 4 (Priorität 1)*

*Gemäss Finanzhaushaltverordnung müssen sowohl materielle wie formelle Kontrollen stattfinden, bevor Auszahlungen durchgeführt werden. Die Prüfung und Freigabe (Valideur 1) der Kreditorenrechnungen hat ausschliesslich durch die für das Vertragsobjekt verantwortlichen Projektleiter bzw. Linienvorgesetzten zu erfolgen (materielle Würdigung). Eine Delegation an den Finanz- oder Personaldienst ist nicht zulässig, weil diese Stellen keine materiellen Prüfungen vornehmen können.*

Stellungnahme der [ZAS]:

La recommandation est acceptée.

La CdC vérifie que les approbateurs disposent de tous les éléments et compétences nécessaires à une approbation formelle et matérielle correcte.

### **3.5 Personensicherheitsprüfungen fanden bisher nicht statt**

Im Anhang 1 der Verordnung über die Personensicherheitsprüfungen (PSPV) sind die Mitarbeitenden der ZAS von solchen Prüfungen ausgenommen. Dies gilt jedoch nicht für bestimmte Funktionen. Daher müssen Datenschutz- und Informationssicherheitsverantwortliche, Verantwortliche für Informationsschutz, Informatiksicherheit und Objektschutz sowie Direktorinnen/Direktoren von Gruppen und Ämtern sowie deren Stellvertreter/innen dieser Prüfung unterzogen werden.

Die ZAS betreibt als Leistungserbringer für die Fachanwendungen seit Mai 2012 ein eigenes Rechenzentrum und beschäftigt mittlerweile rund 100 Informatikspezialisten bei GETI. Bei allen departementalen IT-Leistungserbringern müssen sämtliche Mitarbeitende eine Personensicherheitsprüfung durchlaufen, bevor eine Anstellung stattfindet. Die EFK empfiehlt daher der ZAS, dass bei Mitarbeitenden mit sicherheitsrelevanten Funktionen mindestens überprüft wird, ob das Betreibungs- und Strafregister einwandfrei ist.

*Empfehlung 5 (Priorität 2)*

*Funktionsträger gemäss Anhang 1 der Verordnung über die Personensicherheitsprüfung müssen zwingend überprüft werden.*

Stellungnahme der [ZAS]:

La recommandation est acceptée.

Les personnes occupant à la CdC une fonction figurant à l'annexe 1, chiffre 1 de l'OCSP (RS 120.4) seront soumises à un contrôle de sécurité. En outre, toute personne exerçant une fonction présentant un lien avec la sécurité, et pour qui l'ordonnance ne prévoit pas de contrôle, voire ne le permet pas, subira un contrôle périodique. Pour ces personnes, dont la liste sera établie, la CdC exigera un extrait de l'office des poursuites ainsi qu'un extrait du casier judiciaire.

Parallèlement, une réflexion sera menée quant aux fonctions que la CdC annoncera au titre de l'annexe 1, chiffre 2 de l'OCSP qui est actuellement en révision.

### **3.6 Die geprüften Finanzvorschriften wurden eingehalten**

Die Kreditorenbuchhaltungen der Geschäftsjahre 2012 bis 2014 wurden mit einem Standardreport auf mögliche Doppelzahlungen hin untersucht. Es konnte nur eine wahrscheinliche Doppelzahlung festgestellt werden, welche zudem nicht aus der Informatik stammte. Für die EFK liegt dies klar im tolerierbaren Fehlerbereich.

Durch den Personaldienst der ZAS wurden die Rechnungen für die externen temporären Angestellten des Jahres 2012 geprüft. Dabei wurde festgestellt, dass Abrechnungen angewandt wurden, die nicht den vertraglichen Vereinbarungen entsprachen. Gemäss den Berechnungen des Personaldienstes wurde dadurch verschiedenen Kreditoren rund 55'000 Franken zu viel vergütet. Grundsätzlich können solche Differenzen vermieden werden, wenn in den Verträgen festgehalten ist, dass nur aufgrund der im Zeiterfassungssystem der ZAS erfassten Stunden abgerechnet werden kann. Anderweitig verrechnete Stunden (Dienstreisen, externe Sitzungen, etc.) bedürfen der ausdrücklichen Genehmigung der für die Führung von externen Mitarbeitenden verantwortlichen Linie. Die EFK stellt dazu fest, dass in den Verträgen keine Angaben zu finden sind, wer die Führungsverantwortung für diese externen Mitarbeitenden seitens ZAS trägt.

#### *Empfehlung 6 (Priorität 2)*

*Die Verträge für temporäre Mitarbeitende sollten künftig so abgefasst werden, dass eine Abrechnung nur nach den im Zeiterfassungssystem ZAS erfassten Stunden erfolgt. Die Behandlung der Kosten für Aus- und Weiterbildung ist gemäss den gültigen Vertragsklauseln zu handhaben. In den Verträgen sollte zudem die für die Führung verantwortliche Person der ZAS aufgeführt werden.*

Stellungnahme der [ZAS]:

La première partie de la recommandation concernant la saisie du temps de travail dans SAP PT est appliquée depuis le 01.01.2013. Depuis cette date, les factures sont payées selon les heures badgées dans SAP PT.

Dans tous les nouveaux contrats, la CdC précisera la clause spécifique aux coûts de formation et mentionnera le nom du responsable de la ligne auquel le temporaire rapporte.

## 4 Realisierung von IT-Projekten

### 4.1 Die Abwicklung von IT-Projekten ist unbefriedigend

Die EFK hat 5 Projekte gewählt (von insgesamt 22), die im 2013 am Laufen waren oder abgeschlossen wurden. Sie stellen eine besondere Wichtigkeit (projets-clé) in Bezug mit der IT-Governance und dem Betrieb der ZAS dar, und ihre Aufwände und internen Kosten überschreiten 150'000 Franken. Namentlich wurden folgende Projekte ausgewählt:

- Datacenter
- Migration ADR
- Datamatrix
- Tableau de bord GETI
- Changepoint.

Die EFK hat festgestellt, dass bei vier der analysierten Projekte die beim Bund vorgegeben Methodik „HERMES“ zur Führung von IT-Projekten angewandt wurde. Entsprechende Dokumente wurden geliefert. Allerdings werden bei allen fünf Projekten der Status der Dokumente und deren Gültigkeit nicht systematisch gehandhabt. Phasenfreigaben und Produktabnahmen, die seitens Projektauftraggeber oder durch ComInf stattfanden, sind in den Dokumenten nicht nachgeführt. Der überwiegende Teil der Unterlagen befindet sich im Status „in Arbeit“ obwohl die Projekte bereits abgeschlossen sind. Beim Projekt „Tableau de bord GETI“ entspricht das ganze Vorgehen nicht dem Bundesstandard.

Bei drei der fünf analysierten Projekte wurden Nachprojekte (z. B. Datacenter, Migration ADR als Nachfolger des Projektes ALExSI) oder eine zweite Version desselben Projektes (Datamatrix) gestartet, obschon die ursprünglich definierten Ergebnisse nur partiell erreicht worden waren. Eine genaue Definition von Lieferobjekten liegt nicht systematisch vor. Die Spezifikationen werden teilweise laufend anstatt zu Beginn des Projektes erstellt, und der Projektumfang wird oft bedeutend erweitert. Die Kontrolle der Lieferobjekte ist ungenügend, was beim Projekt Datamatrix dazu führte, dass schwerwiegende Fehler und mangelhafte Leistungen des Lieferanten viel zu spät bemerkt wurden. Massive Termin- und Kostenüberschreitungen sowie ein Lieferantenwechsel im laufenden Projekt waren die Folge.

Die Auswahl von möglichen Lösungen bzw. der Lieferanten ist nicht immer nachvollziehbar. Sie erfolgt teilweise vor einer Projektinitialisierung, d. h. bevor die Spezifikationen erarbeitet waren, so z. B. bei Changepoint, oder ist überhaupt nicht dokumentiert, wie bei Tableau de bord GETI. Budgets werden nicht systematisch in der ersten Phase der Projekte aufgestellt oder fehlen gänzlich wie bei ALExSI. Die Einhaltung der Budgets und des Projektfortschritts sind aufgrund von Projektsplitting oder fehlender Dokumentation schwer bis gar nicht nachvollziehbar. Auch Projektrisikoplanungen werden nicht systematisch durchgeführt, womit auch keine Massnahmen zur Risikoverminderung umgesetzt werden können.

Aufgrund der durchgeführten Analysen bezweifelt die EFK, dass die Führung und Steuerung von IT-Projekten bei GETI und bei der ComInf wirksam ausgeübt wird. Die ZAS hat sicherzustellen, dass alle IT-Projekte gemäss den Bundesvorgaben (HERMES, IKT-Cockpit, Vertragsmanagement) abgewickelt werden, damit die Nachvollziehbarkeit und der ordnungsgemässe Ablauf sichergestellt sind. Projektinitialisierungen, Phasenfreigaben und Produktabnahmen müssen entsprechend do-



kumentiert bzw. validiert werden. In den Projektorganisationen muss die fachliche Seite mit dem Projektauftraggeber vertreten sein. Bei der Definition, Planung und Kontrolle von Projektergebnissen, Kosten, Terminen und Risiken besteht hoher Handlungsbedarf.

Die EFK hält auch fest, dass bei der ZAS in einigen Bereichen Eigenentwicklungen (z. B. Change-point) gemacht oder angestrebt werden, obschon bereits gute und langjährige Lösungen in der BVerw vorhanden sind, die ohne grössere Aufwände sofort eingesetzt werden könnten.

#### **4.2 Ein funktionierendes Controlling bringt mehr Transparenz**

Die abgelieferten Projekt-Dokumente und Finanzzahlen weichen teilweise von einer Quelle zur anderen ab. Änderungen über den gleichen Sachverhalt von einer Dokumentenversion zur nächsten sind nicht nachvollziehbar, die budgetierten Kosten auf Kostenstellen – wie auch auf Projektebene – weichen teilweise massiv von den Ist-Werten ab. So wurde z. B. bei ALExSI das Projekt nach Erreichen von 35% der Ziele mit 50% der Kosten geschlossen. Unter solchen Prämissen kann kein aussagekräftiges Projektcontrolling durchgeführt werden und eine zuverlässige Sicht über den Projektverlauf ist unmöglich.

Ein ordnungsgemässes IT-Controlling existiert bei der ZAS nicht. Damit ist es sehr schwierig bzw. unmöglich zu beurteilen, wie die Lage und Entwicklung von GETI heute ist, sowohl vom Standpunkt der Revision aus wie auch bezüglich Entscheidungen. Das Projekt „Tableau de bord“ zur Realisierung eines IT-Leistungs-Cockpits weist noch keine Resultate auf. Es muss aber dringend ein von allen Involvierten akzeptiertes Instrumentarium zur verbesserten Steuerung der GETI konzipiert und realisiert werden. Eine wichtige Voraussetzung dazu ist, dass die Kompetenzen, Aufgaben und Verantwortungen für die GETI und auch das Unternehmenscontrolling (contrôle de gestion) definiert und eingehalten werden.

Insgesamt beurteilt die EFK die GETI als intransparent und deren Leistungen mehrheitlich als nicht nachvollziehbar. Die Prioritätensetzung bei den IT-Projekten erfolgt nicht risikoorientiert. Die fachlichen und zum Teil langjährigen Forderungen werden nur schleppend oder gar nicht in Angriff genommen. Es ist zwar in den letzten zwei Jahren durch die Virtualisierung der Systeme ein Schritt Richtung Modernisierung der Informatik gemacht worden. Auch der laufende Betrieb konnte bisher befriedigend sichergestellt werden. Der Bau eines neuen Datacenters innerhalb der ZAS ist jedoch fragwürdig. Es hätte auch Lösungen ausserhalb der ZAS gegeben, z. B. bei bereits bestehenden Rechenzentren des Bundes oder bei kantonalen Partnern, die über entsprechendes Fachwissen verfügen. Trotz hohem Finanzverbrauch – 5,5 Mio. Franken IT-Mandate, rund 7,5 Mio. Franken temporäre Externe per 2013 und weitere Millionen interne Kosten – ist kein durchschlagender Erfolg sichtbar.

##### *Empfehlung 7 (Priorität 1)*

*Die IT Projekte müssen durch das zuständige Comité Informatique beurteilt und gesteuert werden, (risikoorientierte Priorisierung, Budgetierung, Planung sowie die Überwachung von bewilligten IT-Projekten). Die IT-Projektleiter müssen entsprechend eine regelmässige, stufengerechte und transparente Rapportierung sicherstellen.*

Stellungnahme der [ZAS]:

La recommandation est acceptée.

Les statuts de la ComInf sont en cours de révision avec comme but de renforcer l'efficacité et l'efficience de cette dernière.

En parallèle, le reporting sera étoffé selon les normes de la Confédération.

## **5 IT-Beschaffungen werden rechtswidrig durchgeführt**

### **5.1 Die ZAS verfügt über keine Beschaffungsdelegation für IT und braucht diese nicht**

Die ZAS ist weder durch eine Beschaffungsdelegation des BBL noch durch die gesetzlichen Grundlagen zum öffentlichen Beschaffungswesen (BöB/VöB/Org-VöB) ermächtigt, selbständig IT-Beschaffungen (insbesondere IK-Technologie, Informatikdienstleistungen und Personalverleih im Bereich IKT gemäss Org-VöB Anhang Art. 9, Ziff. 14, 15 + 20) zu tätigen. Alle bisher getätigten IT-Beschaffungen sind mit einer Ausnahme ausserhalb des gesetzlichen Rahmens abgelaufen. Der Einkauf wurde zudem seit 2011 durch einen externen temporären Mitarbeitenden mit nicht adäquatem Anforderungsprofil, d. h. kein Zertifikat des BBL als Beschaffer, durchgeführt. Seit über einem halben Jahr ist zudem eine weitere externe Mitarbeitende im Einkauf tätig, ohne ausreichende Ausbildung im Einkaufsbereich. Die ZAS hat Handlungsbedarf gesehen und aktuell eine neue Einkaufsorganisation aufgebaut. Deren Ansiedlung bei GETI gewährleistet jedoch die notwendige Unabhängigkeit nicht.

Grundsätzlich benötigt die ZAS auch keine Einkäufer, sondern einen vom BBL ausgebildeten Beschaffungskoordinator, welcher für die korrekte Abwicklung aller Beschaffungen sorgt. Die ZAS hat allen Bedarf über die „zentralen und weiteren Beschaffungsstellen“ abzuwickeln. Als Bedarfsstelle hat die ZAS gemäss Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB), Art 9 und 10 die Erstellung der Pflichtenhefte zu verantworten sowie bei der Erstellung der Ausschreibungsunterlagen massgeblich mitzuarbeiten. Ebenso ist sie verpflichtet die Erfassung der Angaben gemäss Org-VöB, Art. 6, Abs 2, lit a und b „Vertragsmanagement“ und Art. 8, Abs. 1 und 2 „Monitoring nachhaltige Beschaffung“ sicherzustellen.

Die deklarierten IT-Dienstleistungsverträge von GETI von Mai 2012 bis März 2014 dürfen mit etwas mehr als 5.5 Mio. Franken Beschaffungsvolumen im Bundesumfeld als marginal betrachtet werden. Dieser Umstand lässt den Schluss zu, dass die zentralen Beschaffungsstellen die entstehenden Arbeitsaufwände organisatorisch ohne Einschränkungen bewältigen können. Mit entsprechender Beschaffungsplanung seitens ZAS kann den Vorhaben der dringliche Charakter genommen und damit auch die Beanspruchung von Art. 13, VöB reduziert werden. Dadurch ergeben sich eine erhöhte Rechtssicherheit und minimierte Beschaffungsrisiken. Zudem wird mit einer zentralen Beschaffung auch das Einhalten von Bundesstandards besser sichergestellt.

## **5.2 Temporär angestellte Mitarbeitende schulden nur die Arbeitszeit**

Der Einkauf über Personalleihverträge für temporäres Personal ist grundsätzlich als geeignete Massnahme zu beurteilen, um kurzfristige Engpässe bzw. Vakanzen oder fehlendes Know-how zu überbrücken. Davon ausgenommen sind jedoch Führungs- und Schlüsselpositionen. Die bei der ZAS entstandenen Kosten in dieser Personalkategorie sind zu hoch, insbesondere wenn berücksichtigt wird, dass sich unter den extern beschafften Ressourcen nicht nur IT-Spezialisten, sondern auch rein administrative Profile (z. B. Assistenten, Mitarbeitende im Finanz- und Personalbereich) befinden. Beschaffungen über Personalleihverträge sind zudem nicht nachhaltig. Besonders kritisch ist der Umstand, dass durch die vertraglichen Bestimmungen über Personalverleih durch den Auftragnehmer keine Erfolge oder Lieferobjekte geschuldet werden, sondern nur die Arbeitszeit. Dies bedeutet die vollständige Risikoübernahme durch den Auftraggeber. Festgestellt wurde auch, dass Firmen im Mandatsverhältnis zugleich auch als Personalverleiher auftreten.

Die Kosten dieser Personalkategorie betragen rund 7.9 Mio. Franken im Jahr 2013 für 52 Personen bzw. 33.8 FTE, was einem durchschnittlichen Jahressalar pro FTE von 233'346 Franken entspricht. Im Vergleich zur fehlenden Erfolgsschuld ist dieser Betrag zu hoch. Begründete vakante Stellen sollten daher rasch möglichst intern besetzt werden.

## **5.3 Bei den getätigten IT-Beschaffungen gab es zahlreiche Ungereimtheiten**

Insgesamt wurden von Mai 2012 bis März 2014 59 Beschaffungsgeschäfte durch die ZAS getätigt. Davon hat die EFK deren 19 aufgrund von bestimmten Kriterien ausgewählt und im Detail geprüft. Sie musste mehrfache Verstösse gegen die gültigen Regeln sowie teilweise grundlegende Mängel feststellen. Solange die ZAS eine ordnungsgemässe Beschaffungspraxis mittels geeignet festgelegter Prozesse und Strukturen nicht gewährleisten kann, kommt für die EFK eine Beschaffungsdelegation des BBL an die ZAS nicht in Frage.

Alle deklarierten Geschäfte wurden im freihändigen Verfahren nach VöB, Art 13 getätigt. Nur eine Beschaffung der ZAS für die EAK wurde durch das BBL ordnungsgemäss abgewickelt. Ausser bei drei Verträgen fehlen alle Begründungen für die freihändigen Vergaben. Die drei vorhandenen Begründungen sind auf unvollständig ausgefüllten Formularen erfasst und genügen den Anforderungen ebenfalls nicht.

Bei 27 Verträgen der ZAS mit Umfang von insgesamt 2'280'076 Franken muss eine tranchierte Beschaffung festgestellt werden. Mit freihändigen Verfahren sind 24 Verträge im Gesamtbetrag von 2'496'156 Franken abgeschlossen worden, obwohl ein höherwertiges Verfahren hätte angewendet werden müssen; in 13 Fällen mindestens ein Einladungsverfahren und in 11 Fällen eine öffentliche Ausschreibung. Dieser Umstand steht in direktem Zusammenhang mit den tranchierten Beschaffungen bzw. ist eine Folge davon.

Bei den 19 ausgewählten Beschaffungsgeschäften fehlt als letzte Referenz in der Rangfolge der Vertragsbestandteile die Offerte des Auftragnehmers, was nicht der üblichen Berufspraxis entspricht. Für keine der Stichproben ist eine standardisierte Offertanfrage vorhanden, aus welcher die einzuladenden Firmen hervorgehen. Die Nutzwertanalysen zur Zuschlagsbewertung und die dazugehörenden Verfügungen konnten nicht vorgelegt werden.

Preisverhandlungen aufgrund der vorliegenden Offerten aus dem Stichprobenset lassen sich ausser bei einem Geschäft keine erkennen. Bei einem Vertrag muss ein höherer Tagessatz als der



offerierte festgestellt werden. In vier Fällen wurden Vorauszahlungen in der Höhe von 30 bis 40% vereinbart; teilweise bereits fällig bei der Bestellung. Solche Vereinbarungen bei Dienstleistungsverträgen entsprechen nicht der gängigen Praxis in der Bundesverwaltung.

Vertragsabschlüsse in Fremdwährungen sind nicht begründet und lassen sich auch nicht durch bessere Preiskonditionen erklären. Sie bedeuten die vollständige Übernahme des Währungsrisikos durch den Bund, was bei reinen Dienstleistungsverträgen unnötig ist.

Bis zum Abschluss der Revision wurden die verlangten effektiven Abrechnungen zu den 59 IT-Dienstleistungsverträgen (Vertragsausschöpfung) durch die ZAS nicht abgeliefert. Dieser Umstand lässt den Schluss zu, dass kein adäquates Vertragscontrolling geführt wird. Strategische Instrumente des Lieferantenmanagements (Bündelungen, Portfoliobildung, Lieferantenbeurteilung/-bewertung/-entwicklung, usw.) werden verunmöglicht oder erschwert. Zu hohe, wettbewerbslose Preise und qualitative Probleme können die Folgen sein.

Im Weiteren ist der korrekten Zuteilung der IT-Beschaffungen zu den richtigen Beschaffungskategorien (gemäss CPV-Klassifizierung) die notwendige Beachtung zu schenken. Das Beschaffungscontrolling des Bundes erwartet die IT-Beschaffungen der ZAS unter der Rubrik „Informatikdienstleistungen“ und nicht unter „Betriebswirtschaftliche Beratungsleistungen (Managementberatung, Organisation und Coaching)“.

Zu keiner der getätigten Beschaffung konnte die ZAS Vertraulichkeitserklärungen der vertraglich gebundenen Personen vorlegen. Hingegen wurden alle Verträge mit der standardisierten Vertragsklausel zur Vertraulichkeit gegenüber den vertragsnehmenden Firmen verfasst und unterschrieben.

Die von der EFV angeordnete zweite Administrativuntersuchung im Bereich von IT-Projekten und IT-Beschaffungen fand gleichzeitig mit der Revision der EFK statt. Die Arbeiten wurden koordiniert, um Doppelspurigkeiten zu vermeiden und einen effizienten Arbeitsansatz zu ermöglichen. In diesem Zusammenhang wurden die Stossrichtungen der beiden Untersuchungen und die Tendenz der Befunde zwischen der EFK und den Mitarbeitenden der durchführenden externen Firma besprochen. Die Untersuchungen kamen zu den gleichen Schlüssen.

#### *Empfehlung 8 (Priorität 1)*

*Die ZAS hat ab sofort sämtliche IT-Beschaffungsgeschäfte (insbesondere IK-Technologie, Informatikdienstleistungen und Personalverleih im Bereich IKT gemäss Org-VöB Anhang Art. 9, Ziff 14, 15 + 20) über die zentralen Beschaffungsstellen des Bundes abzuwickeln. Von einer Delegation der Beschaffungskompetenz an die ZAS ist bis auf weiteres abzusehen, da insbesondere die Bedingungen gemäss Org-VöB Art. 13-15 durch die ZAS als Delegationsempfängerin nicht gegeben sind. Funktionen und Stellen im Beschaffungsbereich sind zudem gemäss den Aufgaben und Zuständigkeiten von Bedarfsstellen nach Org-VöB Art. 16 und 17 zu gestalten und auf hoher Ebene in der Organisation ZAS anzusiedeln.*

Stellungnahme der [ZAS]:

La CdC a d'ores et déjà mis en conformité sa pratique des achats et collabore étroitement avec l'OFCL. Une juriste (formée par l'OFCL et certifiée) exerce le rôle de coordinateur des achats et contrôle le respect des procédures. L'acheteur (directement subordonné au chef de la division CENT) collabore avec la coordinatrice des achats selon les directives spécifiques. La nouvelle procédure des achats approuvée par la Direction de la CdC est actuellement mise en place avec l'objectif d'être opérationnelle à la fin du mois de juin 2014.

## 6 Pendenzen aus der Prüfung der Schweizerischen Ausgleichskasse (Jahresrechnung 2013)

Die EFK verweist pro Memoria auf die Empfehlungen aus dem Bericht vom 12. Dezember 2013 „Révision principale de l'exercice 2013 de la Caisse suisse de compensation“:

No	Recommandations
<b>2.1.2 Organisation pratique de la CSC</b>	
RP 2013 2102.1	Nous recommandons à la CdC de formaliser le Système de contrôle interne SCI pour la partie informatique. Nous notons l'existence de contrôle environnant afin de maîtriser les risques au niveau de la gestion des changements, gestion des accès utilisateurs et gestion de l'exploitation informatique. Néanmoins, ces derniers n'étant pas formalisés et centralisés dans une matrice SCI, il est difficile d'obtenir une vision synthétique des processus, des risques associés et des contrôles mis en place afin de réduire les risques inhérents à un niveau acceptable.
RP 2013 2102.2 (RP 2012 2102.1 et 2102.2)	Nous recommandons à la CdC de poursuivre les mesures nécessaires afin de disposer d'un site de secours. Le risque de continuité, en ce qui concerne l'infrastructure informatique gérée à Genève, est très élevé et nécessite une considération élevée de la part de la Direction de la CdC. Poursuivre l'analyse d'impact des processus critiques en cas de sinistre, finaliser la définition d'une stratégie de continuité et d'un plan de reprise des activités informatiques adéquat.
RP 2013 2102.3	Nous recommandons au département intégration et exploitation d'insister auprès des équipes en charge de contrôler les backups de bien documenter chaque événement dans l'outil de centralisation des incidents. Le référencement de cet événement est un élément important dans la gouvernance de l'exploitation informatique.
RP 2013 2102.4	Nous recommandons à la CSC de définir des SLA/OLA avec la GETI afin d'être en mesure d'évaluer le niveau de service fourni et de le comparer avec le niveau de service informatique attendu.
RP 2013 2102.5	Poursuivre le développement du Système de contrôle interne SCI et suivre les recommandations de l'Inspectorat interne plus particulièrement dans la Division Prestations-AVS.



## **7 Schlussbesprechung**

An der Schlussbesprechung vom 11. April 2014 haben folgende Personen teilgenommen:

Eidg. Finanzverwaltung:	Serge Gaillard, Direktor
	Marc Elsener, Stv. Sektionschef Grundlagen AP
	Sacha Stegmann, Leiter Leistungsbezug und Sicherheit
Zentrale Ausgleichsstelle:	Jean-Pierre Kuhn, Direktor a.i.
	Markus Odermatt, Direktionsadjunkt
	Pierre-Philippe Durussel, Leiter Internes Inspektorat
	Stéphane Brunner, Leiter GETI
Eidg. Finanzkontrolle:	Michel Huissoud, Direktor
	Eric-Serge Jeannet, Vizedirektor
	Walter Risler, Mandatsleiter
	Peter König, Revisionsexperte
	André Stauffer, IT-Revisionsexperte

Sie ergab eine konstruktive Diskussion über die erwähnten Feststellungen. Die von der ZAS und der EFV gelieferten Kommentare haben geholfen, ein gemeinsames Verständnis aufzubauen. Hinweise auf bereits eingeführte Verbesserungen oder Informationen, die während der Prüfung nicht verfügbar waren, können in der Stellungnahme der ZAS erwähnt werden. Diese Elemente wurden von der EFK nicht mehr überprüft.

Die EFK dankt für die gewährte Unterstützung.

Die Finanzdelegation der eidgenössischen Räte hat an ihrer ordentlichen Sitzung im Juni 2014 vom Bericht Kenntnis genommen.

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)

Bundesgesetz über das öffentliche Beschaffungswesen (BöB, SR 172.056.1)

Verordnung über das öffentliche Beschaffungswesen (VöB, SR 172.056.11)

Verordnung über die Organisation des öffentlichen Beschaffungswesens in der Bundesverwaltung (Org-VöB, SR 172.056.15)

Verordnung über die Personensicherheitsprüfungen (PSPV, SR 120.4)



## **Anhang 2: Abkürzungen, Priorisierung der Empfehlungen**

### **Abkürzungen**

AFAI	Association française de l'audit et du conseil informatique
BBL	Bundesamt für Bauten und Logistik
BIT	Bundesamt für Informatik und Telekommunikation
BVerw	Bundesverwaltung
CCI	Coordination et Controlling Informatique
CdC	Centrale de Compensation
CIO	Conduite Informatique et Organisation
ComInf	Comité Informatique
CSC	Caisse suisse de compensation
DSI	Direction des Systèmes d'information
EFD	Eidg. Finanzdepartement
EFV	Eidg. Finanzverwaltung
EFK	Eidg. Finanzkontrolle
FTE	Full-time equivalent (Vollzeitstelle)
GETI	Gouvernance d'entreprise et technologies de l'information
HERMES	Projektmanagementmethode der Bundesverwaltung
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikations-Technologie
LZ	Lösungszentrum
SCI	Système de contrôle interne
ZAS	Zentrale Ausgleichsstelle
ZENT	Zentrale Ausgleichsstelle (Abteilung innerhalb der ZAS)

### **Priorisierung der Empfehlungen**

Die EFK beurteilt die Wesentlichkeit der Empfehlungen nach Prioritäten (1 = hoch, 2 = mittel, 3 = klein). Sowohl der Faktor Risiko (z.B. Höhe der finanziellen Auswirkung, Wahrscheinlichkeit eines Schadeneintrittes usw.) als auch der Faktor Dringlichkeit der Umsetzung (kurzfristig, mittelfristig, langfristig) werden berücksichtigt. Dabei bezieht sich die Bewertung auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).