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

Prüfung des IKT-Schlüsselprojekts IAM Bund

Informatiksteuerungsorgan des Bundes ISB

EFK-15479/ inkl. Stellungnahme / 07. Mai 2015

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**	1.15479.608.00184.08
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. 058 463 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 »)
Abdruck **Reproduction** **Riproduzione** **Reproduction**	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention the source)

IKT-Schlüsselprojekt-Prüfung: IAM Bund

Das Wesentliche in Kürze

Anfang 2015 prüfte die Eidgenössische Finanzkontrolle EFK beim Informatiksteuerungsorgan des Bundes (ISB) das Programm Identity und Access Management (IAM Bund). Ziel der Prüfung war es, den Projektstand und die Risiken hinsichtlich der Zielerreichung zu beurteilen.

Das Programm IAM Bund ist ausreichend begründet und terminlich wie auch finanziell auf Kurs

Das Programm IAM Bund orientiert sich an den bzw. unterstützt direkt die übergeordneten Strategien des Bundes. Der massiv steigende Umfang der organisationsübergreifenden Nutzung von Informationen und die damit einhergehenden Anforderungen an Schutz und Funktionalitäten können nur noch mit übergreifend koordinierten Leistungen effizient gewährleistet werden. Dies gilt insbesondere wenn Identitäten, Berechtigungen / Attribute bzw. Rollen und Daten über Organisationsgrenzen hinweg national und international vertrauensvoll verwendet werden sollen. Um diese Services für die bundesweite Verwendung zu entwickeln, wurde das Programm IAM Bund gestartet.

Eine Wirtschaftlichkeitsbetrachtung im herkömmlichen Return on Investment (ROI) orientierten Sinne wurde nicht gemacht, was die EFK nachvollziehen kann, da die dazu nötigen Grundlagen nicht erhoben werden können.

Das Programm ist zum Prüfzeitpunkt sowohl terminlich wie auch finanziell auf Kurs. Die definierten Meilensteine wurden erreicht und die Finanzierung ist bis Programmende sichergestellt. Die Finanzierung der bewilligten 11,4 Millionen Franken erfolgte mit 10,7 Millionen Franken über einen Verpflichtungskredit. Der Rest wurde zur Beschleunigung der Startphase über departementale Mittel des GS-EFD beigesteuert.

Das Programm IAM Bund ist politisch herausfordernd und auf breite Akzeptanz angewiesen

In diesem Kontext ist es mitentscheidend, dass das Marktmodell Version 2 vollständig erarbeitet wird und insbesondere folgende Punkte darin verbindlich geregelt sind:

- Welcher Leistungserbringer erbringt welchen Service und wie grenzen sich diese untereinander und gegenüber potentiellen Leistungsbezügern ab?
- Wie sind die Migrationswege, welche Ausnahmen sind möglich und was wird durch wen finanziert?

Daneben ist es unerlässlich, die Bereiche Compliance, Governance und standardisierte Prozesse klar und verbindlich zu regeln.

Grosse Herausforderungen in der Kommunikation und im Stakeholder-Management

Die Kommunikation und das Stakeholder-Management beeinflussen massgeblich die Akzeptanz von IAM Bund und tragen folglich wesentlich zur erfolgreichen Umsetzung bei. Die Beziehungen zu den künftigen Leistungserbringern, jedoch auch zum künftigen Standardservice-Owner, sollten intensiviert werden. Die Kommunikation muss strukturierter erfolgen, wobei die Leistungsbezüger ebenso einbezogen werden. In diesem Kontext spielt der Projektbegleiter eine wichtige Rolle, der dem Programm allerdings nur noch kurze Zeit zur Verfügung steht. Es ist daher wichtig, dass diese

möglichst schnell wieder kompetent besetzt wird. Auch muss das Programm einen Weg finden, damit Projekte mit erhöhten IAM-Anforderungen automatisch auf dem «Radar von IAM Bund erscheinen.

In der Führungsunterstützungsbasis (FUB) wurde mit dem Projekt «Identity, Credential and Access Management» (ICAM) ebenfalls ein IAM-Projekt gestartet. Auch wenn ein solches separates Projekt aus Sicht der FUB ausreichend begründet ist, muss konsequent darauf geachtet werden, dass ein Maximum an Synergien genutzt wird. Das Projekt ICAM sollte nur wo nicht anders möglich eigene Services entwickeln und sonst auf die Standardservices von IAM Bund zurückgreifen.

Die Qualitätssicherung (QS) und das Risikomanagement (RM) müssen angepasst werden

Obwohl QS und RM im Programm gewährleistet sind, entspricht das Gelebte nicht dem Geschriebenen. Die Vorgaben müssen überarbeitet (QS) bzw. erweitert (RM) und in der Folge konsequent durchgesetzt werden. Der Qualitäts- und Risikomanager (QSRM) muss sich gegenüber der Führungs- und operativen Stufe klar abgrenzen und auf die steuernden Aufgaben konzentrieren. Aktuell besteht kein Prüfplan, dieser ist unbedingt zu erstellen.

Mehrfachrollen belasten die Qualität

Zum Prüfzeitpunkt wird das Projektoffice, die Stellvertretung des Programmleiters und die Projektleitungen IAMB sowie ABA/MIAMI durch eine einzige Person wahrgenommen. Dadurch entstehen Einbussen in der Qualität, welche seitens der EFK in Form einer nicht aktuellen Projektablage und einem nicht konsequent durchgesetzten Dokumenten- und Lifecycle-Management erkannt wurden. Weiter existiert ein Rollenkonflikt, da das Controlling durch das Projektoffice durchgeführt wird. Das Projektcontrolling und die Projektführung dürfen nicht in Personalunion erfolgen. Die Mehrfachrolle muss beseitigt werden.

Das Programm erfordert viel externes Expertenwissen

Für notwendige Folgebeschaffungen muss frühzeitig mit einer regelkonformen Beschaffungsplanung begonnen werden. Des Weiteren sollten geeignete Massnahmen für den Knowhow-Transfer von extern zu intern definiert werden.

Ein WTO-Verfahren zu Beginn des Programms hätte mehrere Vertragsverlängerungen unnötig gemacht

Aus Sicht der EFK sind die Initialbeschaffungen im Einladungsverfahren zwar korrekt abgelaufen. Eine realistische Aufwandsabschätzung zu Beginn des Programms hätte allerdings gezeigt, dass von Anfang an ein WTO-Verfahren angezeigt gewesen wäre. Mit der Auslösung von Folgeverträgen und der Einlösung von Optionen wurden jeweils die Schwellenwerte und somit die vom BBL delegierte Beschaffungskompetenz des ISB überschritten. Mit den getätigten WTO-Ausschreibungen für die Ersatzbeschaffungen der externen Dienstleistungsressourcen hat die Programmleitung zielführende Massnahmen zur Einhaltung der Compliance getroffen.

Audit du projet informatique clé: IAM de la Confédération

L'essentiel en bref

Au début de l'année 2015, le Contrôle fédéral des finances (CDF) a examiné le programme de gestion des identités et des accès (Identity and Access Management, IAM) de la Confédération auprès de l'Unité de pilotage informatique de la Confédération (UPIC). Il s'agissait d'apprécier l'état d'avancement du projet et les risques susceptibles de compromettre l'atteinte des objectifs.

Le programme IAM de la Confédération est suffisamment fondé et suit son cours sous l'angle des délais et du financement

Le programme IAM de la Confédération s'inspire des stratégies transversales de la Confédération, auxquelles il apporte un soutien direct. On ne peut plus répondre efficacement à l'utilisation croissante d'informations provenant de différentes organisations et aux exigences qui en découlent en matière de protection et de fonctionnalités sans services coordonnés. Cela vaut en particulier lorsque les identités, autorisations, attributs, rôles et données doivent être utilisés de manière fiable au-delà des organisations, sur les plans national et international. Le programme IAM de la Confédération développe ces services pour l'ensemble de la Confédération.

Une analyse économique en termes de retour sur investissement (ROI) au sens habituel du terme n'a pas été entreprise. Le CDF peut le comprendre dans la mesure où les données nécessaires ne peuvent être collectées.

Au moment de l'audit, le programme suivait son cours sous l'angle des délais et du financement. Les étapes prévues ont été atteintes et le financement est assuré jusqu'à l'achèvement du programme. Le financement des 11,4 millions de francs alloués a fait l'objet d'un crédit d'engagement de 10,7 millions de francs. La différence a pu être comblée grâce à des ressources départementales mises à disposition par le Secrétariat général du Département fédéral des finances afin d'accélérer la phase de lancement.

Le programme IAM de la Confédération est exigeant du point de vue politique et tributaire d'une large acceptation

Dans ce contexte, il est essentiel que la version 2 du modèle de marché soit intégralement développée et qu'on y règle en particulier les points suivants:

- Quel fournisseur de prestations procure quel service, et comment ces fournisseurs se démarquent-ils les uns de autres et vis-à-vis des bénéficiaires de prestations potentiels?
- Quelles sont les voies de migration, quelles exceptions sont admissibles et qui finance quoi?

De plus, il faut impérativement régler de façon claire et contraignante les domaines de la conformité, de la gouvernance et des processus standardisés.

Les défis sont considérables pour la communication et la gestion des parties prenantes

La communication et la gestion des parties impliquées conditionnent de manière décisive l'acceptation du programme IAM. Ils sont des éléments importants pour le succès du programme. Dès lors, il convient d'intensifier les relations avec les futurs bénéficiaires de prestations et le futur responsable du service standard. La communication doit être plus structurée qu'au moment de

l'audit et associer les bénéficiaires de prestations. A cet égard, le responsable du suivi du projet joue un grand rôle, mais ce dernier ne se tient plus à disposition du programme. Il est donc important que cette fonction soit à nouveau occupée rapidement par une personne compétente. Dans le cadre du programme, il faut également trouver un moyen de faire apparaître automatiquement sur le «radar IAM de la Confédération» les projets qui présentent des exigences accrues dans le domaine de la gestion des identités et des accès.

La Base d'aide au commandement (BAC) a aussi lancé un projet de gestion des identités et des accès qui s'intitule «Identity, Credential and Access Management» (ICAM). Même si du point de vue de la BAC, un projet séparé se justifie, il faut veiller à utiliser un maximum de synergies. Le projet ICAM ne devrait développer ses propres services que lorsqu'une autre solution n'est pas envisageable, et dans le cas contraire recourir aux services standard de l'IAM de la Confédération.

Il faut améliorer l'assurance de la qualité et la gestion des risques

Bien que l'assurance de la qualité et la gestion des risques soient assurées dans le cadre du programme, la réalité ne correspond pas aux intentions. Les exigences doivent être revues (assurance de la qualité) ou élargies (gestion des risques), puis être respectées. Le gestionnaire de la qualité et des risques doit se distancer clairement de la direction du programme et du secteur opérationnel, et se concentrer sur ses tâches de pilotage. Il n'existe actuellement aucune planification des contrôles et il faut y remédier au plus vite.

Les rôles multiples grèvent la qualité

Lors de l'audit, une personne unique était chargée du bureau de projet, de la suppléance du responsable du programme et de la direction des projets IAM de la Confédération et ABA/MIAMI. La qualité s'en ressent, ce qui se traduit aux yeux du CDF par des archives de projet incomplètes et une gestion incohérente des documents et du cycle de vie. De plus, il existe un conflit de rôles car le contrôle de gestion relève du bureau de projet. Le contrôle de gestion et la direction du projet ne peuvent incomber à la même personne. Ce cumul de fonctions doit être éliminé.

Le programme nécessite une expertise externe considérable

Pour les acquisitions subséquentes nécessaires, on doit établir à temps une planification des marchés publics conforme aux règles. De plus, des mesures adéquates doivent être prises en matière de transfert de connaissances de l'extérieur à l'intérieur.

Une procédure OMC au début du programme aurait évité plusieurs prolongations de contrats

De l'avis du CDF, les acquisitions initiales par la procédure sur invitation se sont déroulées correctement, mais une évaluation réaliste des charges au début du programme aurait montré que des procédures OMC auraient été indiquées dès le départ. En concluant des contrats subséquents et en exerçant des options, les valeurs seuils et de ce fait la compétence en matière de marchés publics déléguée par l'OFCL à l'UPIC ont été dépassées. Par les appels d'offres OMC concernant l'acquisition alternative des ressources externes dans le domaine des services, la direction du programme a pris les mesures qui s'imposaient pour respecter la conformité.

Texte original en allemand

Verifica del progetto chiave TIC: IAM Confederazione

L'essenziale in breve

All'inizio del 2015 il Controllo federale delle finanze (CDF) ha esaminato il programma IAM Confederazione presso l'Organo direzione informatica della Confederazione (ODIC). La verifica mirava a valutare lo stato del progetto e i rischi in relazione al raggiungimento degli obiettivi.

Il programma Identity & Access Management (IAM) Confederazione è sufficientemente giustificato e rispetta le scadenze e i requisiti finanziari

Il programma IAM Confederazione si orienta alle strategie sovraordinate della Confederazione e le sostiene direttamente. Il notevole aumento dell'utilizzo di informazioni trasversali alle organizzazioni e le conseguenti esigenze in materia di protezione e funzionalità possono essere soddisfatti in modo efficace solo con servizi coordinati trasversalmente. Questo vale in particolare nei casi in cui identità, autorizzazioni / attributi o ruoli e dati devono poter essere utilizzati in modo fidato anche a livello nazionale e internazionale. Il programma IAM Confederazione è stato avviato per sviluppare questi servizi per l'intera Confederazione.

Non è stata effettuata alcuna valutazione della redditività nel senso abituale (Return of Investment, ROI), cosa che il CDF può comprendere, poiché non è possibile rilevare le basi necessarie.

Al momento della verifica, il programma rispettava le scadenze e i requisiti finanziari. Le tappe definite sono state raggiunte e il finanziamento è garantito fino alla fine del programma. L'importo stanziato di 11,4 milioni di franchi è stato finanziato attraverso un credito d'impegno di 10,7 milioni. Il resto è stato messo a disposizione dalle risorse dipartimentali della SG-DFF allo scopo di accelerare la fase iniziale.

Il programma IAM Confederazione costituisce una sfida dal punto di vista politico e richiede un ampio consenso

In questo contesto è decisivo che la versione 2 del modello di mercato sia elaborata interamente e, in particolare, che siano disciplinati in maniera vincolante i punti seguenti:

- Quale fornitore di prestazioni fornisce quale servizio e come si distinguono i vari fornitori tra di loro e dai potenziali beneficiari di prestazioni?
- Quali sono le modalità della migrazione e le possibili eccezioni e chi finanzia cosa?

È inoltre indispensabile disciplinare in modo chiaro e vincolante gli ambiti della compliance, della governance e dei processi standardizzati.

Grandi sfide per la comunicazione e la gestione degli stakeholder

La comunicazione e la gestione degli stakeholder influiscono molto sul consenso nei confronti di IAM Confederazione e contribuiscono quindi in maniera determinante alla buona riuscita dell'attuazione. Occorre intensificare le relazioni con in futuri fornitori di prestazione, ma anche con i futuri proprietari dei servizi standard. La comunicazione deve avvenire in maniera più strutturata e includere anche i beneficiari di prestazioni. In questo contesto l'accompagnatore del progetto, che ha a sua disposizione il programma solo per un breve periodo, riveste un ruolo importante. È fondamentale che questo ruolo sia occupato da una persona competente il più rapidamente

possibile. Il programma deve pure essere impostato in modo che i progetti con elevate esigenze IAM appaiano automaticamente sul «radar di IAM Confederazione».

Con il progetto «Identity, Credential and Access Management» (ICAM), è stato avviato un progetto IAM pure nella Base d'aiuto alla condotta (BAC). Anche se secondo la BAC un progetto IAM separato è sufficientemente giustificato, occorre sistematicamente vigilare affinché venga sfruttato il massimo delle sinergie. Il progetto ICAM dovrebbe sviluppare servizi propri soltanto laddove è inevitabile e, a parte questo, ricorrere ai servizi standard di IAM Confederazione.

La garanzia della qualità e la gestione dei rischi devono essere adeguati

Benché la garanzia della qualità e la gestione dei rischi sono effettuati dal programma, la realtà non sempre corrisponde alla teoria. Le direttive devono essere rielaborate (garanzia della qualità) ed estese (gestione dei rischi) e successivamente attuate sistematicamente. Il gestore della qualità e dei rischi deve distinguersi chiaramente dal livello direzionale e da quello operativo e concentrarsi sui compiti di gestione. Attualmente non esiste alcun piano di verifiche. È quindi assolutamente necessario allestirne uno.

I ruoli multipli incidono sulla qualità

Al momento della verifica l'amministrazione del progetto, la supplenza del capo del programma e la direzione dei progetti IAM Confederazione e ABA/MIAMI erano svolti da una sola persona. In tal modo risultano perdite di qualità. Il CDF constata queste perdite nell'archiviazione dei progetti non aggiornata e nella gestione incoerente dei documenti e del ciclo di vita. Esiste inoltre un conflitto tra ruoli, dato che il controlling viene effettuato dall'amministrazione del progetto. Non è infatti opportuno che il controlling e la gestione del progetto siano svolti dalla stessa persona. Di conseguenza è necessario eliminare questi ruoli multipli.

Il programma richiede molte conoscenze specialistiche esterne

Per i necessari acquisti successivi, è indispensabile iniziare per tempo con una pianificazione degli acquisti conforme alle norme. Occorre inoltre definire misure adeguate per il trasferimento delle conoscenze dall'esterno all'interno.

Una procedura OMC all'inizio del programma avrebbe evitato diverse proroghe del contratto

Il CDF è del parere che gli acquisti iniziali effettuati secondo la procedura mediante invito si siano svolti correttamente. Una stima realistica delle spese all'inizio del programma avrebbe però mostrato che sarebbe stato più sensato effettuare una procedura OMC sin dal principio. In seguito ai contratti successivi e all'utilizzo di opzioni sono stati superati i valori soglia e quindi la competenza in materia di acquisti concessa dall'UFCL all'ODIC. Con i bandi OMC effettuati per gli acquisti sostitutivi delle risorse di prestazioni di servizi esterne, la direzione del programma ha adottato misure mirate per rispettare la compliance.

Testo originale in tedesco

Key ICT project audit: IAM Bund

Key facts

At the start of 2015, the Swiss Federal Audit Office (SFAO) audited the IAM Bund programme at the Federal IT Steering Unit (FITSU). The audit's aim was to assess the project status and risks with regard to the achievement of targets.

Identity and access management (IAM) programme is duly justified and its budget and schedule are on track

The IAM Bund programme is geared toward and directly supports the Confederation's overriding strategies. The massive increase in the extent to which information is used on a cross-organisational basis and the demands this entails in terms of protection and functionalities can only be efficiently guaranteed with comprehensively coordinated services. This is particularly true whenever identities, authorisations, attributes, profiles and data are intended for trusted use above and beyond organisational limits in Switzerland and abroad. The IAM Bund programme was launched to develop these services for use by the entire Federal Administration.

A cost-efficiency analysis conventionally geared toward return on investment was not performed, which is something the SFAO understands given that it is not possible to determine the basis required for the analysis.

At the time of the audit, the programme's schedule and budget were on track. The milestones defined were reached and the financing was secured up to the end of the programme. The approved CHF 11.4 million was financed with a guarantee credit of CHF 10.7 million. The difference was contributed from GS-FDF department resources to speed up the launch phase.

IAM Bund programme is politically challenging and depends on a broad acceptance

A decisive factor in this context is that the market model version 2 is fully developed and, in particular, contains binding regulations on the following points:

- Which service providers provide which services and how do the service providers create a distinction between themselves and for potential service procurers?
- What are the migration paths, what exceptions are possible and who will finance what?

In addition, it is essential to set clear and binding regulations for the areas of compliance, governance and standardised processes.

Major challenges in communication and stakeholder management

Communication and stakeholder management significantly influence the acceptance of IAM Bund and therefore contribute to its successful implementation considerably. Relations with both the future service providers and the future owner of the standard service ought to be strengthened. Communication must be more structured in that the service providers are also included. In this context, an important role is played by the project officer, who is available to the programme for a short time only. It is important that this role is filled with a skilled professional as quickly as possible. The programme must also find a way to ensure that projects with higher IAM demands automatically appear on the IAM Bund radar.

An IAM project has been launched in the Armed Forces Command Support Organisation (AFCSO) with the "Identity, Credential and Access Management" (ICAM) project. Even if the AFCSO sees a separate IAM project as duly justified, attention must be paid consistently to exploiting a maximum of synergies. The ICAM project should rely on IAM Bund standard services and should only develop its own services as a last resort.

Modifications to quality assurance (QA) and risk management (RM) required

Despite the fact that QA and RM are included in the programme, the actual situation does not correspond to what's on paper. The guidelines need to be revised (QA) or expanded (RM) and then implemented consistently. The quality assurance and risk manager (QARM) must be kept clearly separate from the management and operational levels and must focus on control tasks. At present, there is no inspection plan, but one must be drawn up.

Multiple roles putting a strain on quality

At the time of the audit, one person was taking care of the project office, deputising for the programme manager and managing the IAMB and ABA/MIAMI projects. This reduces quality, evidence of which the SFAO saw in an outdated project filing system and document and lifecycle management that is not being implemented consistently. Furthermore, there is a conflict of roles in that the project office is attending to control system duties. The project control system and project management should not be carried out by the same person. Multiple roles must be eliminated.

Programme requires a lot of external expertise

Work on a procurement plan that complies with the regulations must be started at an early stage for necessary follow-up procurements. Moreover, appropriate measures for the external-to-internal transfer of knowledge ought to be defined.

A WTO procedure at the start of the programme would have rendered several contract extensions unnecessary

In the SFAO's view, the initial procurements in the invitation to tender procedure were undertaken correctly. However, a realistic cost estimate at the start of the programme would have shown that a WTO procedure was advisable from the very beginning. The awarding of successive contracts and the exploitation of options resulted in the thresholds and the FITSU's procurement authority as delegated by the FOBL being exceeded. By carrying out WTO tenders to procure replacements of external service resources, the programme management took effective measures to ensure compliance.

Original text in German

Generelle Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB) zur Prüfung:

Das ISB bedankt sich bei der EFK für die Prüfung des Schlüsselprojekts Programm IAM Bund und die wertvollen Hinweise zur Verbesserung der Projektabwicklung. Mit Befriedigung nimmt das ISB zur Kenntnis, dass auch gemäss der Beurteilung der EFK das Programm zum Prüfzeitpunkt sowohl terminlich wie auch finanziell auf Kurs ist.

Speziell im Bereich der Qualitätssicherung und des Risikomanagements wird das ISB angeregte Verbesserungen umsetzen, die die Transparenz erhöhen werden. Auch wurden und werden die empfohlenen Rollenentflechtungen im Rahmen der verfügbaren Personalressourcen vorgenommen.

Es liegt in der Natur einer Prüfung während eines laufenden Programms (ausserhalb eines Phasenabschlusses), dass verschiedene Massnahmen bereits geplant bzw. in Erarbeitung waren. In diesem Sinne wurden auch die Beschaffungen einschliesslich von WTO von Anfang an geplant. Allerdings ging man von den damaligen Erfahrungswerten für die Durchlaufzeiten aus, die im Verlaufe der Projektarbeiten aufgrund der Umfeldentwicklung leider mit bedeutenden Verzögerungen überholt wurden. Seit dem Prüfungszeitpunkt der EFK wurden mehrere im Rahmen der Prüfung formulierte Massnahmen bereits umgesetzt oder ausgelöst. Die Prüfungsanalysen unterstützen diese Massnahmen.

Inhaltsverzeichnis

1	**Auftrag und Vorgehen**	**13**
1.1	Ausgangslage	13
1.2	Prüfungsziel und -fragen	13
1.3	Prüfungsumfang und -grundsätze	13
2	**Was ist IAM und wieso ist ein Programm IAM Bund notwendig?**	**14**
3	**Das Programm ist gut strukturiert und aktuell auf Kurs**	**15**
4	**Die Programmgrundlagen wurden erarbeitet, müssen aber verfeinert werden**	**16**
5	**Das Programm ist gut geführt, die Dokumentation und Detailaspekte der Programmführung bieten noch Möglichkeiten zur Verbesserung**	**18**
5.1	Programmführung und Steuerung entsprechen den Erwartungen, Herausforderungen bestehen bei weiteren Rollenbesetzungen	18
5.2	Die Kommunikation hat einen grossen Stellenwert, das entsprechende Konzept fehlt noch	19
5.3	Es arbeiten überwiegend externe Ressourcen im Programm	20
6	**Die Qualitätssicherung und das Risikomanagement müssen angepasst werden**	**21**
6.1	Qualitätssicherung und Risikomanagement auf der Steuerungs-Stufe	21
6.2	Qualität auf Führungs- und operativer Stufe	22
7	**Informations- und Datensicherheit müssen aus einer übergeordneten Sicht geregelt werden**	**23**
8	**Das Programm IAM vergibt Folgeaufträge zur Überbrückung bis zum WTO-Zuschlag freihändig**	**24**
8.1	Ein WTO-Verfahren zu Beginn des Programms hätte mehrere Vertragsverlängerungen unnötig gemacht	24
8.2	Nach der Initialisierungsphase erfolgten die weiteren Beschaffungen der Dienstleistungsaufträge nach einem WTO-Verfahren	25
9	**Schlussbesprechung**	**26**
Anhang 1: Rechtsgrundlagen, Priorisierung der Empfehlungen		**27**
Anhang 2: Abkürzungen		**28**

1 Auftrag und Vorgehen

1.1 Ausgangslage

Im März 2013 hat der Bundesrat Weisungen für IKT-Schlüsselprojekte erlassen. Darauf gestützt prüfte die Eidgenössische Finanzkontrolle (EFK) das Programm Identity und Access Management Bund (IAM Bund) des Informatiksteuerungsorgans des Bundes (ISB).

1.2 Prüfungsziel und -fragen

Ziel der Prüfung war es, den Projektstatus und die Risiken hinsichtlich der Zielerreichung von IAM Bund zu beurteilen. Dazu sollten folgende Fragestellungen dienen:

- Unterstützen Projektauftrag und Projektvorgehen die übergeordneten Ziele?
- Entspricht die Architektur der Lösung dem Stand der Technik, sowie internen und externen Richtlinien?
- Erlauben die Rahmenbedingungen eine erfolgreiche Umsetzung des Projekts?
- Ist das Projektmanagement (Planung, Organisation, Controlling, Steuerung) dazu geeignet, die gesetzten Ziele erreichen zu können?
- Werden die Ressourcen (Finanzen, Personal) zielführend eingesetzt?
- Sind die Risiken bezüglich Einhaltung von Terminen und Budget unter Kontrolle?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Martin Schwaar (Leitung) und Markus Wüst im Zeitraum von Januar bis März 2015 durchgeführt. Sie basiert auf Interviews mit Schlüsselpersonen auf allen Stufen der Projektorganisation, ergänzt durch eine kritische Beurteilung der Projektdokumentation und ausgewählter Lieferergebnisse.

Der Prüffokus beschränkt sich auf das Programm und ein durch dieses direkt geführtes und verantwortetes Projekt vom Typ I gemäss Projekt-Typologie des Programms. Da das Projekt IAMB die Kern-Ergebnisse des Programms erbringt, wird für die Prüfung auf Projektstufe auf dieses fokussiert.

2 Was ist IAM und wieso ist ein Programm IAM Bund notwendig?

Das Programm IAM Bund weist nicht die typische finanzielle Dimension eines IKT-Schlüsselprojekts auf. Es wurde vom Bundesrat aufgrund seiner Bedeutung auf die Liste der Schlüsselprojekte gesetzt. Die Lieferergebnisse des Programms tangieren jede Verwaltungseinheit und sind Teil der Enterprise Security Architecture Bund (ESAB).

Zur Wahrnehmung ihrer Geschäftsaufgaben betreibt die Bundesverwaltung zahlreiche Informationssysteme. Bei den meisten ist es entscheidend, wer welchen Zugriff auf welche Informationen, Anwendungen und Systeme hat. Aktuell wird dies über die einzelnen Anwendungen selbst oder über räumlich oder organisatorisch beschränkte Identity und Access Management Lösungen (IAM-Lösungen) sichergestellt.

Durch den massiv steigenden Umfang der organisationsübergreifenden Nutzung von Informationen können die Anforderungen an Schutz und Funktionalitäten nur noch mit übergreifend koordinierten Services effizient gewährleistet werden. Auch muss über die sogenannte «Föderation» sichergestellt werden, dass Identitäten, Berechtigungen / Attribute bzw. Rollen und Daten über Organisationsgrenzen hinweg national und international vertrauensvoll verwendet werden können.

In einem Vorprojekt wurden strategische Grundsätze, strategische Ziele und die notwendigen strategischen Massnahmen zum IAM in der Bundesverwaltung erarbeitet. Diese Resultate sind Grundlage zur IKT-Teilstrategie IAM, welche eine Massnahme der Stossrichtung «S02 - Organisations-übergreifende Kooperation» der Informatikstrategie Bund darstellt.

Auch für eCH (Verein für die Festlegung von Standards für das eGovernment) spielt das IAM Bund eine zentrale Rolle und ist eine priorisierte Massnahme im e-Government Aktionsplan 2015 (B2.06 Dienste für die Identifikation und Berechtigungsverwaltung).

Beurteilung

Aus Sicht der EFK ist das Programm IAM Bund begründet und auf die übergeordneten Strategien des Bundes ausgerichtet.

Ein übergreifendes gemeinsames Verständnis von IAM und dessen Implementierung sind notwendig, um organisationsübergreifend den richtigen Personen schnell, sicher und vertrauenswürdig die korrekten Zugriffsrechte auf Ressourcen zu gewähren.

3 Das Programm ist gut strukturiert und aktuell auf Kurs

Das Programm wurde von August 2013 bis Ende 2013 initialisiert und ist seit Anfang 2014 in der Durchführungsphase. In dieser Phase wird es bis zu den Abschlussarbeiten bleiben, da die Umsetzung nicht im Programm enthalten ist.

Die Kernleistungen des Programms werden im Projekt IAMB erbracht. Dieses wurde Anfang 2014 mit der Initialisierung gestartet und ist seit November 2014 in der Konzeptphase.

Das Projekt MIAMI ist ein weiteres zentrales Projekt in welchem die Grundlagen sowie erste Umsetzungen zugunsten des zukünftigen Standarddienstes IAMv2 erarbeitet werden. Das Projekt ist in der Initialisierung und wird gemäss Planung noch vor den Sommerferien in die nächste Phase wechseln.

Das Programm ist zum Prüfzeitpunkt sowohl terminlich wie auch finanziell auf Kurs. Die definierten Meilensteine wurden erreicht und die Finanzierung ist bis Programmende sichergestellt. Von 11,4 Millionen Franken sind 10,7 Millionen Franken über einen Verpflichtungskredit finanziert. Um die Startphase zu beschleunigen wurden vom GS EFD departementale Mittel zur Finanzierung des Restes beigesteuert.

Die Programm- und Projektaufträge wurden erstellt. Im Programmauftrag sind die Ziele aufgrund von IRB-Empfehlungen zu Beginn des Programms nicht durchgängig messbar definiert.

Das Programm hat auch die Aufgabe, Projekte von Leistungserbringern wie Leistungsbezügern zu begleiten. Das Projekt Identity, Credential und Access Management (ICAM) des VBS hat dieselben Projektziele wie IAM Bund, beinhaltet jedoch auch die Phase Umsetzung bei der FUB. Aus Sicht EFK ist ICAM ein Projekt, welches durch das Programm zu berücksichtigen ist. Die Diskussionen über die Art der Zusammenarbeit dauern jedoch noch an und es finden erst langsam Annäherungen statt.

Beurteilung

Aus Sicht der EFK ist die Strukturierung des Programms zielführend und der aktuelle Programmstand wie auch die finanzielle Situation gut.

Die Ziele im Projektauftrag sollten messbar definiert sein, damit die Feststellung der Zielerreichung keinen Interpretationsspielraum bietet.

Die Begründungen für ein eigenständiges IAM-Projekt in der FUB sind für die EFK schwer nachvollziehbar. Die EFK hat den Eindruck gewonnen, dass wenig Interesse an einer Zusammenarbeit/Abstimmung zwischen der FUB und dem Programm IAM Bund besteht.

Von der FUB wird vor allem die Degradationsfähigkeit[1] als Grund für eine eigene IAM-Lösung genannt. Aus Sicht EFK gibt es, auch unter Berücksichtigung der Degradationsfähigkeit, Lösungsteile von IAM Bund, welche seitens FUB verwendet werden können. Deshalb sollte der Austausch zwischen dem Programm IAM Bund und dem Projekt ICAM bei der FUB intensiviert werden.

---

[1] Nach einem Ausfall von Teilen des Netzes / von übergeordneten Systemen ist die Funktionalität einzelner Systeme noch immer sichergestellt

Das ISB sollte darauf hinwirken, dass im Projekt ICAM dieselben Sprachen, Notationen und Standards (z. B. SABSA, Archimate, etc.) wie bei IAM Bund verwendet werden.

Empfehlung 1 (Priorität 1)
Die EFK empfiehlt dem ISB, dass der Status des Projekts ICAM der FUB und die Art der Zusammenarbeit von IAM Bund und ICAM geklärt und Synergien konsequent genutzt werden. Bei fehlender Kooperation seitens ICAM oder dem Programm IAM Bund muss frühzeitig eine Eskalation aus dem Projekt ICAM bzw. dem Programm IAM Bund erfolgen.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):
Das ISB hat den Prozess zur Zusammenarbeit und Integration des Projekts ICAM in das Programm (auf Basis der bestehenden Sofort-Governance "IAM Bund") gestartet. Die endgültige Einstufung des Projekts ICAM in die Programmstruktur erfolgt in Q2/2015, die Empfehlung wird in diesem Rahmen umgesetzt.

4 Die Programmgrundlagen wurden erarbeitet, müssen aber verfeinert werden

Die Programm- und Projektmanagementpläne wurden erarbeitet. In gewissen Bereichen fehlt es jedoch am erforderlichen Detaillierungsgrad. Im Programmmanagementplan fehlt das Kapitel, welches die Beziehung zwischen dem Programm und der Abteilung Standarddienste im ISB beschreibt.

Die Architektur ist aktuell in Erarbeitung. Die Rahmenarchitektur ist bereits erarbeitet und praktisch abgeschlossen und aktuell sind die Architekturprinzipien in der Vernehmlassung. Die EFK hat festgestellt, dass die einzuführende Lösung mit der Architektur der Zielsysteme (soweit zu diesem Zeitpunkt beurteilbar) sowie der IT Strategie des Bundes kompatibel ist.

Die Stakeholder wurden aktiv in die Erarbeitung der Anforderungen eingebunden und abgeholt. Es ist jedoch aktuell noch keine Strategie für das Stakeholder-Management erkennbar.

Die Rechtsgrundlagenanalyse des Programms stellte fest, dass die bestehenden gesetzlichen Grundlagen für ein föderatives IAM im Bund nicht genügen. Das Programm hat bereits einen Vorschlag für die notwendigen Gesetzesanpassungen im Bundesgesetz für die Informationssicherheit (ISG) vorbereitet. Da diese Anpassungen voraussichtlich erst 2017 behandelt werden, hat das Programm die Erarbeitung einer Übergangsverordnung eingeleitet.

Es gibt keine übergreifende Governance im Bereich IAM im Bundesumfeld. Diese wird im Programm erarbeitet.

Für IAM Bund existieren keine Wirtschaftlichkeitsberechnungen. Kein Amt konnte die Kosten für Entwicklung, Unterhalt und Betrieb ihrer Identitäts- und Zugriffsinformationen in den einzelnen Programmen bzw. lokalen IAM-Lösungen benennen, welche für eine solche Berechnung notwendig wären.

Eine Schutzbedarfsanalyse (SchuBan) für das Programm IAM Bund wurde als nicht relevant eingestuft. SchuBan der IAM nutzenden Fachanwendungen werden vorausgesetzt. Ein Dokument «Überlegungen zu SchuBan IAM Bund» wurde erstellt. In diesem Dokument sind offene Fragen zur Klärung aufgeführt.

Die SchuBan für das Projekt ABA[2] wurde erstellt, diejenige für das Projekt MIAMI ist geplant.

In einem Eckwertpapier sind die folgenden Wertbeitrags- und Mehrwertbetrachtungen qualitativ ausgewiesen:

- Erhöhte Sicherheit
- Regelkonformität
- Verbesserte Interoperabilität
- Verbesserte Endbenutzerprozesse
- Vermeidung von Doppelspurigkeiten und verbesserte Wirtschaftlichkeit
- Schutzverbesserung von identifizierbaren, persönlichen Daten

Beurteilung

Aus Sicht der EFK decken die PM-Pläne die relevanten Themen ab, jedoch nicht überall in der geforderten Tiefe. Da die «Aussensicht» nicht zwischen dem Programm IAM Bund und der Abteilung Standarddienste (SD) im ISB unterscheidet, ist es für den Erfolg des Vorhabens wichtig, dass die Zusammenarbeit dieser beiden ISB-internen Player vertieft und im Programmmanagementplan festgehalten wird.

Aus Sicht der EFK wird die Architektur durch kompetente Experten sauber Top-Down basierend auf den Strategievorgaben des Bundes erarbeitet und ist mit den Leistungsbezügern und Leistungserbringern abgestimmt. Eine fachliche Prüfung ist zum jetzigen Zeitpunkt nicht möglich.

Die Einbindung der Stakeholder nur im Rahmen der normalen Programm-/Projektrapportierung IAM Bund genügt künftig nicht zur erfolgreichen Abstützung und Verankerung in den Stammstrukturen. Im Hinblick auf die nächsten Programm-Phasen von IAM Bund sollte das Stakeholder Management konzeptionell und zeitlich intensiviert und wo notwendig noch definiert werden. Die existierende Auflistung der Stakeholder in der Stakeholder Management-Prozessgestaltung ist in einem iterativen, terminierten Vorgehen zu berücksichtigen

Die fehlenden rechtlichen Voraussetzungen und die fehlende übergreifende Governance im Bereich IAM für den Bund sind starke Unsicherheitsfaktoren, welche jedoch im Programm adressiert sind.

Aufgrund der Natur des Programms ist es nachvollziehbar, dass auf Programmebene keine Schuban erstellt wird. Da die offenen Fragen im Dokument «Überlegungen zu SchuBan IAM Bund» grundlegend sind, müssen diese aus Sicht der EFK noch vor Fertigstellung des Marktmodelles Version 2 geklärt werden.

Die EFK kann nachvollziehen, dass eine Wirtschaftlichkeitsbetrachtung im herkömmlichen ROI-orientierten Sinn nicht möglich ist. Der nicht ausschliesslich wirtschaftliche Nutzen wird in der Verwendung des zu schaffenden Standarddienstes durch die Fachanwendungen entstehen. Um dies zu vermitteln, sollten gezielte und speziell auf dem nicht quantifizierbaren Nutzen aufbauende Kommunikationsaktivitäten für das Programm IAM Bund durchgeführt werden.

---

2 Das Projekt ABA war bis Ende 2014 ein eigenständiges Projekt im EPA und nur zu einem kleinen Teil über das Programm finanziert. Ab 1.1.2015 wurde das Projekt in das Programm integriert mit dem Programmleiter als Auftraggeber. Ziel von ABA ist der Aufbau eines zentralen Identity Store. Abschluss ist Ende April 2015 geplant.

Im Rahmen der Marktmodelleinführung IAM Version 2 erwartet die EFK zwingend, dass eine TCO-Betrachtung enthalten ist.

Empfehlung 2 (Priorität 1)
Die EFK empfiehlt dem ISB, dass die Zusammenarbeit zwischen dem Programm IAM Bund und der Abteilung Standarddienste, insbesondere in Bezug auf Ziele und Finanzen, schnellstmöglich geklärt und im Programmmanagementplan von IAM Bund dokumentiert wird.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):
Die Empfehlung wird insbesondere im Rahmen der Erarbeitung des Marktmodells für den Standarddienst IAM V2 umgesetzt.

5 Das Programm ist gut geführt, die Dokumentation und Detailaspekte der Programmführung bieten noch Möglichkeiten zur Verbesserung

5.1 Programmführung und Steuerung entsprechen den Erwartungen, Herausforderungen bestehen bei weiteren Rollenbesetzungen

Die Rollen des Programmleiters wie auch Auftraggebers sind kompetent und stufengerecht besetzt und die Rollenträger nehmen ihre Verantwortung aktiv wahr. Der Projektbegleiter nimmt eine Schlüsselrolle als Schnittstelle zu den Leistungserbringern und Leistungsbezügern ein. Für diese Rolle zeichnet sich eine Neubesetzung ab.

Die Planung auf Stufe Programm erfolgt über Projektaufträge und Arbeitspakete. Diejenige im Projekt IAMB über Arbeitspakete, welche vom Programm zugewiesen wurden. Die Planung der Ressourcen erfolgt auf Ebene der Arbeitspakete.

Der kritische Pfad (CPM-Methodik) wird weder im Programm noch im Projekt IAMB angewendet, womit eine Gesamtübersicht erst durch Konsolidierung der Einzelergebnisse möglich ist.

Die Projektleitung des zentralen Projekts IAMB und des Projekts ABA, bzw. nach dessen Ende des Projekts MIAMI, wird in Personalunion durch den Verantwortlichen für das PMO des Programms wahrgenommen. Gleichzeitig ist dieser Stellvertreter des Programmleiters. Das Controlling im Programm wird durch das PMO wahrgenommen.

Im PM-Plan ist definiert, welche Berichte in welcher Periodizität erstellt werden. Die Berichte waren jedoch zum Prüfzeitpunkt auf der Projektplattform nicht vollständig abgelegt.

PCO Berichte wurden bis Mitte 2014, PCOE Berichte bis Ende 2014 erstellt. Ab 2015 wurden die Informationen gemäss PMO direkt in das IKT Cockpit erfasst. Deshalb wurde auf die weitere Erstellung der PCO wie auch PCOE Berichte verzichtet.

Beurteilung

Nach Ansicht der EFK ist das Programm aus personeller (Programmleiter, Auftraggeber) wie auch methodischer Sicht (HERMES 5) gut aufgesetzt. Der Programmleiter ist sowohl fachlich wie auch methodisch in der Lage, das Programm erfolgreich zu führen.

Der Besetzung der Projektbegleitung muss hohe Bedeutung beigemessen werden. Diese Rolle nimmt eine wichtige Scharnierfunktion zwischen dem Programm und den Projekten in den Verwaltungseinheiten sowie den Leistungserbringern ein und muss kontinuierlich und kompetent besetzt sein.

Aus Sicht der EFK entspricht die Planung den Erwartungen an ein professionelles Projektmanagement. Die EFK zweifelt nicht am Wissen des Rollenträgers PMO über den kritischen Pfad bzw. über den Stand der Arbeitspakete. Jedoch sind diese Informationen für Dritte nicht ohne weiteres abrufbar. Betroffen sind hier insbesondere der Auftraggeber und der Projektausschuss. Der kritische Pfad sollte aufgrund seiner Vorteile visualisiert und eine Möglichkeit geschaffen werden, den Fertigstellungsgrad der Arbeitspakete bzw. Teil-Arbeitspakete auf einen Blick zu sehen.

Als ungünstig erachtet die EFK die Wahrnehmung von unterstützenden Funktionen im Programm (PMO), Führungsfunktionen in den Projekten ABA/Miami und IAMB sowie Steuerungsfunktion als Stellvertretender Programmleiter durch ein und dieselbe Person. Es können nicht alle diese Rollen ohne Qualitätseinbussen durch eine Person wahrgenommen werden. Dies hat sich bereits in der Aktualität der Projektablage verdeutlicht. Aus Sicht der EFK stellt die Personalunion der Controlling-Instanz (PMO) mit der Projektführungsinstanz ein hohes Risiko dar.

Die Erfassung der Daten im IKT-Cockpit entbindet beim aktuellen Entwicklungsstand des Tools nicht von der Erstellung der PCOE-Berichte gemäss herkömmlicher Vorlage. Diese werden gemäss Aussage des Programmleiters ab sofort wieder erstellt.

Empfehlung 3 (Priorität 1)
Die EFK empfiehlt dem ISB, dass im Programm IAM Bund das PMO und die Projektleitungen IAMB sowie ABA/MIAMI mit unterschiedlichen Personen besetzt werden und insbesondere das Controlling (PMO) von den Führungsaufgaben getrennt wird.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):

Die Empfehlung wird umgesetzt. Das Finanzcontrolling wurde planmässig mit der Schaffung einer internen Stelle im ISB noch im April von den Führungsaufgaben getrennt. Das Projekt ABA wurde im April abgeschlossen und für das Projekt MIAMI wird Personal für PL und darunterliegende TPLs bis Ende Juni ernannt.

5.2 Die Kommunikation hat einen grossen Stellenwert, das entsprechende Konzept fehlt noch

Die EFK hat festgestellt, dass kein Kommunikationsplan oder Kommunikationskonzept vorhanden ist und die Kommunikation mit den zukünftigen Anwendern und dem Topmanagement zu wenig empfängergerecht erfolgt.

Auf Seiten der bestehenden IAM-Leistungserbringer wird die Beziehung mit dem BIT viel intensiver gepflegt als beispielsweise diejenige mit dem ISC EJPD oder mit der FUB. Auch gelangen zum Prüfzeitpunkt Projekte mit erhöhten IAM-Anforderungen der Leistungsbezüger aktuell nicht automatisch «auf den Radar» der Projektbetreuung des Programms IAM Bund.

Beurteilung

Aufgrund des hohen Stellenwertes der Kommunikation für dieses Programm sollte unbedingt ein Kommunikationskonzept erstellt und die stufengerechte Kommunikation mit dem Topmanagement und den zukünftigen Benutzern im Sinne eines Erwartungsmanagements intensiviert werden.

Der Austausch zwischen dem Programm und den Leistungserbringern EJPD und FUB sollte intensiviert werden. Die EFK erachtet es auch als suboptimal, dass die Departemente für die Meldung von Projekten mit erhöhten IAM Anforderungen der Leistungsbezüger noch nicht konsequent den offiziellen Anforderungsprozess des ISB oder das IGT nutzen.

Empfehlung 4 (Priorität 1)
Die EFK empfiehlt dem ISB ein Vorgehen zu suchen, damit Projekte mit erhöhten IAM-Anforderungen, welche nicht über den Standard abgedeckt werden können, zwingend an das Programm (später an die Abteilung Standarddienste im ISB) gemeldet werden.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):

Das ISB wird neben den erwähnten Standardmechanismen (zentrales Anforderungsmanagement, IAM Governance Team) das Management für besonders kritische Stakeholder weiter intensivieren und über die Gremien hinaus IAM-relevante Aktivitäten abfragen. Dabei ist das ISB aufgrund der hohen Anzahl der Bundesämter auf Stichproben angewiesen und definiert kritische und weniger kritische Stakeholder, um dabei knappe Personalressourcen zu schonen.

Empfehlung 5 (Priorität 2)
Die EFK empfiehlt dem ISB, dass durch das Programm IAM Bund die Kommunikationsmassnahmen auf allen Stufen empfängergerecht intensiviert werden. Das Kommunikationskonzept inklusive Plan ist rasch zu entwickeln, insbesondere ist die Abstimmung mit den Leistungserbringern zu institutionalisieren.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):

Das empfohlene Kommunikationskonzept inklusive Kommunikationsplan für das System IAM Bund ist während der Prüflaufzeit in letzter Vernehmlassungsrunde und wird in Q2/2015 in Kraft und damit die Empfehlung umgesetzt.

5.3 Es arbeiten überwiegend externe Ressourcen im Programm

Die EFK hat festgestellt, dass im Programm überwiegend externe Ressourcen arbeiten. Die Mitarbeitenden sind teilweise über Rahmenverträge längerfristig an das Programm gebunden und stehen auch für die kommenden Programmphasen zur Verfügung. Eine mittel- bis langfristige Beschaffungsplanung fehlt jedoch.

Beurteilung

Bei den aktuellen Vertragsvolumen ist bei Folgebeschaffungen von Mitarbeitenden davon auszugehen, dass die Schwellenwerte für freihändige Verfahren wesentlich überstiegen werden. Die Ersatzbeschaffungen können nur bei frühzeitiger Initialisierung ordnungsgemäss durchgeführt werden.

Der hohe Anteil von externen Mitarbeitern stellt aus Sicht der EFK, angesichts des benötigten Spezialisten-Wissens, ein nicht unerhebliches Risiko für Know-how-Abfluss und externe Abhängigkeit dar.

6 Die Qualitätssicherung und das Risikomanagement müssen angepasst werden

6.1 Qualitätssicherung und Risikomanagement auf der Steuerungs-Stufe

Die EFK hat festgestellt, dass Aktivitäten zur Qualitätssicherung (QS) und zum Risikomanagement (RM) stattfinden. Der Qualitäts- und Risikomanager (QSRM) rapportiert direkt an den Auftraggeber. Die QS findet aber nicht strukturiert und gemäss den Vorgaben in den dafür vorgesehenen Dokumenten statt. Der Prozess für das RM ist zudem nicht ausreichend dokumentiert.

Der Qualitäts- und Risikomanager (QSRM) führt eine inhaltliche Qualitätssicherung durch bis auf die Ebene von einzelnen Dokumenten. Explizite Quality Gates sind nicht definiert, die Dokumente werden aber durch das IAM Governance Team (IGT) und die Führungsmeetings freigegeben.

Es gibt weder einen vollständigen Prüfplan auf Programm- noch auf Projektebene.

Restrisiken werden zwar zwischen QSRM und Auftraggeber besprochen, es wird aber kein Protokoll über dieses Gespräch geführt. Die Massnahmen zu den Risiken werden nicht terminiert, sondern jeweils vor der Projektausschuss-Sitzung (PAS) durch den QSRM neu geprüft.

Beurteilung

Aus Sicht der EFK entspricht die Definition der QS nicht der Realität, welche im Programm und den Projekten gelebt wird. Hier müssen allenfalls die Vorgaben in den Dokumenten angepasst und deren Einhaltung strikte eingefordert und überwacht werden.

Obwohl Quality Gates nicht explizit definiert sind, könnte die Freigabe durch das IGT und im Führungsmeeting als Quality Gate betrachtet werden. In diesem Fall müsste dies aber im dokumentierten QS-Prozess entsprechend definiert sein.

Dass der QSRM operativ in die Qualitätssicherung eingebunden ist, widerspricht dem Zweck dieser Rolle als Peer des Auftraggebers auf Steuerungsstufe. Er sollte eine neutrale und steuernde Sicht auf die Qualität im Programm haben, was in der aktuellen Konstellation nicht möglich ist.

Ein vollständiger Prüfplan ist für eine adäquate und verlässliche Qualitätssicherung unerlässlich.

Das Risikomanagement im Programm und den Projekten wird aus Sicht EFK «ad hoc» durchgeführt. Es gibt keine verbindlichen übergeordneten Vorgaben, wie Risiken erhoben und behandelt werden.

Der QSRM konsolidiert zwar die Risiken der Projekte in die Riskmap des Programms, fügt aber keine weiteren Risiken auf Stufe Steuerung hinzu, was eigentlich den Mehrwert seiner Rolle als «unbeteiligte» Stelle ausmacht.

Die Massnahmen zu den Risiken werden nicht terminiert und deren Überwachung erfolgt nicht proaktiv und aus Sicht der EFK in zu grossen Abständen. So kann das Programm nicht schnell genug auf veränderte Risiko-Situationen reagieren.

Empfehlung 6 (Priorität 1)
Die EFK empfiehlt dem ISB, dass der Qualitäts- und Risikomanager (QSRM) im Programm IAM Bund stufengerecht ausschliesslich auf der Steuerungsstufe des Programms eingesetzt wird und nicht in die operative Qualitätssicherung eingebunden ist. Das Risikomanagement muss er aktiver und in wesentlich kürzeren Kadenzen wahrnehmen, die Massnahmen müssen terminiert und überwacht werden und der QSRM ist auch zuständig für die Einbringung von Risiken auf Stufe Steuerung.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):

Der QSRM wird aus der operativen Qualitätssicherung gelöst und konzentriert sich auf die Stufe Steuerung.

Empfehlung 7 (Priorität 2)
Die EFK empfiehlt dem ISB, dass im Programm IAM Bund die Vorgaben für die Qualitätssicherung in den relevanten Dokumenten allenfalls angepasst und diejenigen für das Risikomanagement verbindlich definiert werden. Die Einhaltung muss durch die Programmleitung und den QSRM eingefordert und überwacht werden.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):

Die Programmleitung wird im Programmmanagementplan Massnahmen zur Sicherstellung des Risikomanagements definieren und überwachen. Die notwendige Qualitätssicherung wird über das IGT als Quality Gate erfolgen.

Empfehlung 8 (Priorität 2)
Die EFK empfiehlt dem ISB, dass im Programm IAM Bund ein vollständiger Prüfplan erstellt und die Protokollierung der Prüfungen einheitlich geregelt und vorgegeben wird.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):

Ein Prüfplan wird auf den Stufen Steuerung und Führung separat erstellt und entsprechend im Programmmanegementplan dokumentiert.

6.2 Qualität auf Führungs- und operativer Stufe

Die Programm- und Projektmanagementpläne (PM-Pläne) wurden nach deren initialen Erarbeitung in zu langen Zeitabständen aktualisiert. Die Logbücher, welche viele dynamische Informationen des Programms bzw. der Projekte enthalten, sind auf der Projektplattform (Sharepoint) nicht aktuell.

Auf der Projektplattform fehlen generell Dokumente und es sind auch viele nicht mehr gültige Dokumente abgelegt. Die Berichte sind auf der Ablage verstreut und nicht vollständig abgelegt.

Die EFK hat festgestellt, dass das Dokumenten- und Lifecyclemanagement für das Programm initial umfassend definiert wurde. Anhand einzelner Stichproben wurde jedoch festgestellt, dass die Vorgaben nicht immer durchgängig angewendet werden.

Beurteilung

Die PM-Pläne werden, gemessen an ihrer Bedeutung, nicht regelmässig genug aktualisiert und die Einhaltung der darin definierten Vorgaben wird nicht aktiv genug eingefordert.

Für die Nachvollziehbarkeit ist es wichtig, dass die Ablage auf der Projektplattform vollständig und aktuell ist und nicht nur ein Teil der Dokumente dort auffindbar sind. Auch sollten ungültige Dokumente entsprechend gekennzeichnet bzw. archiviert werden. Sich verändernde Dokumente wie Logbücher etc. müssen immer in der aktuellsten Version abrufbar sein.

Dass die Vorgaben gemäss Dokumenten- und Lifecyclemanagement im PM-Plan nicht eingehalten werden, erschwert es erheblich, den Status von Arbeiten nachzuvollziehen.

Empfehlung 9 (Priorität 2)
Die EFK empfiehlt dem ISB, die Programm- und Projekt-Ablage des Programms IAM Bund zu vervollständigen, auf den aktuellen Stand zu bringen und zukünftig aktuell zu halten. Für die PM-Pläne sind verbindliche Vorgaben betreffend Umfang und Aktualisierungs-Periodizität zu schaffen. Die Vorgaben für das Dokumenten- und Lifecyclemanagement im gesamten Programm IAM Bund sind zwingend einzuhalten.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):
Mit der Auflösung der Mehrfachrollen im PMO wird sowohl das Dokumenten- und Lifecycle-management als auch die Aktualisierungsperiodizität verbessert.

7 Informations- und Datensicherheit müssen aus einer übergeordneten Sicht geregelt werden

Für Schutzobjekte wurden Stammblätter erstellt und ein Vorgehen ISDS auf Stufe des ISB ist vorhanden. Viele der in den Stammblättern beschriebenen Massnahmen sind zum Prüfzeitpunkt noch nicht vorhanden bzw. noch nicht umgesetzt.

Es ist kein übergeordnetes ISDS-Konzept auf Programmstufe geplant, da das Programm keine Umsetzungsverantwortung trägt. Für das Projekt ABA existiert ein ISDS-Konzept.

Beurteilung

Der übergeordnete Bedarf eines ISDS-Rahmens auf Stufe Programm IAM ist aus Sicht EFK gegeben. Das Programm IAM Bund sollte im Hinblick auf die Schaffung des neuen Standarddienstes IAMv2 ein erhebliches Interesse haben, dass Schuban/ISDS-Konzepte der benötigten Teilservices vorhanden und greifbar sind. Das ISDS-Konzept für den neuen Standarddienst ist nach Erachten der EFK zur Feststellung allfälliger Lücken im Zusammenspiel der Teilservices notwendig. Da der Standarddienst IAM Bund in einem engen Kontext zum Thema «Schutz von Informationen des Bundes» steht, ist es eines der wichtigsten Werkzeuge zur Gewährleistung dieses Schutzes.

Das aktive Einfordern der fehlenden Punkte und Massnahmen durch das Programm-Management IAM Bund macht Sinn, obwohl die Verantwortung in der Linie liegt. Das Einbringen und Abholen über das IGT ist zielführend. Aus Sicht der EFK sollten die terminierten Massnahmen gemäss den erstellten Stammblättern zu den Services durch den Programmleiter IAM Bund überwacht und lückenlos eingefordert werden.

Empfehlung 10 (Priorität 2)
Die EFK empfiehlt dem ISB, das Zusammenspiel und die Abhängigkeiten der einzelnen bestehenden ISDS-Konzepte innerhalb des Standarddienstes IAM Bund zu analysieren und die nötigen Massnahmen abzuleiten. Die daraus abgeleiteten, übergeordneten Regelungen pro hierarchische Stufe des IAM Bund sind unbedingt zu erarbeiten. Die Erledigung dieser Empfehlung sollte vor Abschluss der Konzeptions-Phase der Projekte mit Umsetzungscharakter erfolgen.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):
Ein ISDS-Rahmenkonzept wird noch innerhalb der Konzeptphase des Kernprojekts etabliert und aktiv gesetzt.

8 Das Programm IAM vergibt Folgeaufträge zur Überbrückung bis zum WTO-Zuschlag freihändig

8.1 Ein WTO-Verfahren zu Beginn des Programms hätte mehrere Vertragsverlängerungen unnötig gemacht

Das ISB besitzt eine gültige Delegation des BBL vom 07. Mai 2012 für IT-Dienstleistungsbeschaffungen, die den massgebenden Schwellenwert für eine öffentliche Ausschreibung nicht erreichen.

Alle Beschaffungen der Initialisierungsphase wurden mittels Einladungsverfahren abgewickelt. In den Initialverträgen wurden bereits Optionen in Aussicht gestellt und auch abgerufen. Nach Ausschöpfen der Optionen wurden auf der Basis von drei Grundverträgen nahtlos weitere Folgeverträge abgeschlossen. Diese enthielten ebenfalls optionale Leistungen. Auch diese Optionen wurden vom Programm eingelöst. In zwei anderen Fällen wurden freihändige Folgeaufträge vergeben. Alle fünf Geschäfte überstiegen mit den Folgeleistungen jeweils den WTO-Schwellenwert. Parallel dazu wurde eine WTO-Ausschreibung vorbereitet und durchgeführt (siehe Kapitel 8.2). Nach dem nachfolgenden Mini-Tender-Verfahren konnten mit den gleichen Dienstleistungsfirmen ab dem 4. Quartal 2014 die vorherigen – auf den Einladungsverfahren basierenden – Verträge und Optionen vorzeitig oder nahtlos abgelöst werden.

Beurteilung

Aus Sicht der EFK sind die Initialbeschaffungen im Einladungsverfahren zwar korrekt abgelaufen. Eine realistische Aufwandabschätzung zu Beginn des Programms hätte aber gezeigt, dass von Anfang an ein WTO-Verfahren angezeigt gewesen wäre. Mit der Auslösung von Folgeverträgen und der Einlösung von Optionen wurden jeweils die Schwellenwerte und somit die vom BBL delegierte Beschaffungskompetenz des ISB überschritten.

Mit den getätigten WTO-Ausschreibungen für die Ersatzbeschaffung der externen Dienstleistungs-Ressourcen hat die Programmleitung zielführende Massnahmen zur Einhaltung der Compliance getroffen. Das ursprünglich erhöhte Risiko von Reputationsschäden wegen nicht gesetzeskonformer Beschaffungen, konnte damit im Programm IAM verringert werden.

8.2 Nach der Initialisierungsphase erfolgten die weiteren Beschaffungen der Dienstleistungsaufträge nach einem WTO-Verfahren

Es wurden keine Rekurse verzeichnet. Die Rahmenverträge wurden durch das BBL erstellt. Bei den vertraglich gebundenen Lieferanten besteht keine Bezugspflicht im Sinne von Mindestabnahmemengen. Die rahmenvertraglich abgerufen Beschaffungen wurden mit strukturierten Verfahren (Mini-Tender) abgewickelt.

Beschaffungsentscheide werden in den Protokollen «Koordination Programmführung» unter dem Traktandum Beschlüsse ggf. Pendenzen, jedoch nicht im Logbuch festgehalten.

Die EFK hat festgestellt, dass das Programm IAM Bund keine Beschaffungsplanung erstellt hat.

Beurteilung

Die bisher geführten WTO-Ausschreibungen (Dienstleistungen) bzw. die daraus abgerufenen ‚Mini-Tender'-Leistungen sind konform abgelaufen. Die Ausschreibungen wurden nach den geltenden Bestimmungen aufgesetzt und die Mini-Tender-Abrufe gemäss den rahmenvertraglichen Bestimmungen durchgeführt. Bei diesen Mini-Tender-Verfahren ist minutiös darauf zu achten, dass die zu erbringenden Leistungen genau spezifiziert sind und eine Beurteilung der vollendeten Leistungserbringung zweifelsfrei festgestellt werden kann. Damit kann eine klare Abgrenzung zu Leistungserbringungen im Rahmen von Personalverleihbestimmungen geschaffen werden.

Eine Protokollierung der Entscheide im Logbuch ist gemäss HERMES auf Stufe Steuerung und Führung vorgeschrieben. Aus Sicht der EFK sollten sämtliche Steuerungs- und Führungs-Entscheide im Programm IAM Bund im dafür vorgesehenen Dokument erfasst werden (im konkreten Fall im Logbuch).

Im Programm IAM Bund ist der Bund auf externes Wissen angewiesen. Für wirtschaftliche und WTO-konforme Beschaffungen ist eine mit dem Programmplan abgestimmte Beschaffungsplanung unabdingbar.

Empfehlung 11 (Priorität 1)
Die EFK empfiehlt dem ISB, umgehend eine Beschaffungsplanung zu erstellen und nötigenfalls mit der zentralen Beschaffungsstelle abzustimmen.

Stellungnahme des Informatiksteuerungsorgans des Bundes (ISB):
Eine Beschaffungsplanung ist während der Prüflaufzeit erstellt worden.

9 Schlussbesprechung

Die Schlussbesprechung fand am 23. April 2015 statt. Teilgenommen haben [redacted] (GS-EFD); [redacted], [redacted] und [redacted], ISB. Die EFK war vertreten durch Michel Huissoud, Bernhard Hamberger und Martin Schwaar.

Sie ergaben Übereinstimmung mit den wesentlichen Feststellungen und Empfehlungen.

Die EFK dankt für die gewährte Unterstützung.

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen, Priorisierung der Empfehlungen

Rechtsgrundlagen:

Finanzkontrollgesetz (FKG, SR 614.0)

Finanzhaushaltgesetz (FHG, SR 611.0)

Finanzhaushaltverordnung (FHV, SR 611.01)

Bundesinformatikverordnung (BinfV, SR 172.010.58)

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).

Anhang 2: Abkürzungen

Abkürzungen:

AKV	Aufgaben, Kompetenzen und Verantwortung
BöB	Bundesgesetz über das öffentliche Beschaffungswesen
IAM	Identity und Access Management (Identitäts- und Zugriffsverwaltung)
ICAM	Identity, Credential und Access Management
IGT	IAM Governance Team
IP	Internet Protokoll
ISDS	Informationssicherheit und Datenschutz
PA	Programm-/Projektausschuss
PAS	Programm-/Projektausschusssitzung
PCO	Projekt-Controlling
PCOE	Erweitertes Projekt-Controlling
PT	Personentage
QS	Qualitätssicherung
QSRM	Qualitäts- und Risikomanager
RM	Risikomanagement
SchuBan	Schutzbedarfsanalyse
VöB	Verordnung über das öffentliche Beschaffungswesen
WTO	World Trade Organization