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

Umsetzung der Weisungen der Querschnittsämter

Informatiksteuerungsorgan des Bundes

EFK-15562 / inkl. Stellungnahmen / 11. April 2016

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.15562.608.00184.008
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. +41 58 463 11 11
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung **Résumé** **Riassunto** **Summary**	Deutsch (« Das Wesentliche in Kürze ») Français (« L'essentiel en bref ») Italiano (« L'essenziale in breve ») English (« Key facts »)

Umsetzung der Weisungen der Querschnittsämter Informatiksteuerungsorgan des Bundes

Das Wesentliche in Kürze

Das Informatiksteuerungsorgan des Bundes (ISB) sorgt für die Umsetzung der Strategie zur Informations- und Kommunikationstechnik (IKT) in der Bundesverwaltung (BVerw). Es erlässt hierzu Vorgaben für die Verwaltungseinheiten (VE) und führt die IKT-Standarddienste. Die Steuerung und Führung des Einsatzes von IKT in der Bundesverwaltung sind im Jahr 2012 verstärkt worden. Das ISB nimmt nun Steuerungsaufgaben wahr. Diese Veränderungen beeinflussen die Aufsicht gegenüber den VE. Der vorliegende Bericht konzentriert sich auf die Aufsicht im Sinne der Überwachung der Umsetzung der Weisungen und Vorgaben in den Departementen. Die Eidgenössische Finanzkontrolle (EFK) hat geprüft, ob die Aufgaben, Kompetenzen und Verantwortungen definiert sind und die Aufsicht auch wahrgenommen wird.

Als Kontroll- bzw. Aufsichtsinstanz sieht sich das ISB nicht, dennoch nimmt es teilweise Aufsichtsaufgaben wahr. Regelkreise sind definiert, inhaltlich funktionieren sie beim IKT-Portfolio Bund und bei den Standards, wenn diese Produktbeschaffungen oder die Standarddienste betreffen. In den übrigen Bereichen entfalten sie aber keine oder zu wenig Wirkung. Verbesserungspotenzial besteht bei den Grundlagen bezüglich der Durchsetzungs- und Eskalationsinstrumente, beim Nachweis von Kontrollen und bei der Aufsicht über die Mängelbehebung.

Ansätze zu Kontrollen bestehen

Die Notwendigkeit der Querschnittsämter ist aus Sicht der EFK klar ausgewiesen. Sie stellen in Kernbereichen ein einheitliches Vorgehen in der BVerw sicher. Dafür sind Weisungs-, Aufsichts- und Durchsetzungskompetenzen unverzichtbare Grundlagen. Wer die Kontroll- und Aufsichtspflicht hat, geht aus den bestehenden Rechtsgrundlagen aber zu wenig deutlich hervor. Die Departemente bzw. die Leistungserbringer und -bezüger sind für die Umsetzung von Vorgaben in ihren Aufgabengebieten verantwortlich.

Dem ISB muss zuhanden des Bundesrates regelmässig in unterschiedlicher Weise rapportiert werden. Diese Selbstdeklarationen werden vom ISB nur partiell plausibilisiert. Die Zuverlässigkeit der Informationen an den Bundesrat z. B. beim Strategischen Controlling ist somit nicht umfassend sichergestellt.

Im IKT-Sicherheitsbereich stellt die EFK bei ihren Prüfungen immer wieder fest, dass IKT-Sicherheitsvorgaben nicht eingehalten werden. Dies ist ein Indiz, dass der Regelkreis nicht wirksam ist. Eine stärkere Rolle des ISB bei diesem Thema drängt sich auf.

Dem ISB stehen ausser der Eskalation innerhalb des eigenen Departementes keine Durchsetzungsinstrumente zur Verfügung.

Mit risikobasiertem Aufsichtskonzept zu systematischen Kontrollen

Die EFK empfiehlt, die Aufsichtspflicht klar der weisungsgebenden Instanz zu übertragen und die Bundesinformatikverordnung entsprechend anzupassen. Anhand eines risikobasierten Aufsichtskonzepts sollte nachfolgend festgelegt werden, welche IKT-Bereiche wesentlich sind. Der daraus abgeleitete Kontrollbedarf muss sicherstellen, dass eine Gesamtsicht ohne Doppelspurigkeiten

resultiert. Das ISB soll im Rahmen seiner Querschnittsaufgaben über die Amts- und Departementsgrenzen hinweg intervenieren und eskalieren können. Die entsprechenden Durchsetzungsinstrumente müssen daher definiert werden, festgestellte Mängel oder Schwachstellen über den Regelkreis systematisch weiterverfolgt bzw. eliminiert werden. Die stärkere zentrale Aufsicht sollte möglichst effizient und automatisiert umgesetzt werden.

Mise en œuvre des directives des offices transversaux
Unité de pilotage informatique de la Confédération

L'essentiel en bref

L'Unité de pilotage informatique de la Confédération (UPIC) veille à la mise en œuvre de la stratégie en matière de technologies de l'information et de la communication (TIC) dans l'administration fédérale. Elle édicte à cet effet des directives à l'intention des unités administratives et gère les services standard TIC. En 2012, le pilotage et la gestion du recours aux TIC ont été renforcés au sein de l'administration fédérale. L'UPIC assume désormais aussi des tâches de pilotage. Ces changements influencent la surveillance exercée sur les unités administratives. Le présent rapport se focalise ainsi sur la surveillance de la mise en œuvre des directives et normes dans les départements. Le Contrôle fédéral des finances (CDF) a vérifié si les tâches, les compétences et les responsabilités sont définies et si la surveillance est assurée.

L'UPIC ne se voit pas comme une instance de contrôle et de surveillance, mais elle assume néanmoins partiellement des tâches en la matière. Des mécanismes de régulation sont définis et fonctionnent au niveau du portefeuille TIC de la Confédération et des normes lorsqu'elles concernent l'acquisition de produits et les services standard. Ils ne produisent pas ou peu d'effets dans les autres domaines. Un potentiel d'amélioration existe en ce qui concerne les bases relatives aux instruments permettant de faire appliquer les mesures et remonter les problèmes à l'échelon hiérarchique supérieur, la preuve de l'existence des contrôles et la surveillance de l'élimination des lacunes.

Les approches pour mener les contrôles existent

Selon le CDF, la nécessité des offices transversaux est incontestable. En effet, ils assurent l'uniformisation des procédures dans les domaines clés de l'administration fédérale. Dans ce but, ils doivent absolument disposer de compétences pour édicter des directives, les mettre en œuvre et contrôler leur application. Malheureusement, les bases légales ne précisent pas assez clairement qui exerce ce devoir de contrôle et de surveillance. Les départements ainsi que les fournisseurs de prestations et leurs bénéficiaires sont responsables de la mise en œuvre des directives dans leurs domaines de compétence.

L'UPIC doit recevoir régulièrement des rapports sous différentes formes à l'intention du Conseil fédéral. Elle ne soumet que partiellement ces déclarations à un contrôle de vraisemblance. La fiabilité des informations que le Conseil fédéral reçoit, par exemple au niveau du contrôle de gestion stratégique, n'est donc pas totalement garantie.

Régulièrement, le CDF constate lors de ses audits que les directives de sécurité informatique ne sont pas respectées. C'est un indice de l'inefficacité du mécanisme de régulation. L'UPIC doit jouer un rôle plus important dans ce domaine.

L'UPIC ne dispose pas d'instruments pour faire appliquer les directives et doit se contenter de faire remonter les problèmes au sein de son département.

De la stratégie de surveillance basée sur les risques aux contrôles systématiques

Le CDF recommande de confier clairement le devoir de surveillance à l'instance qui fixe les directives et de modifier en conséquence l'ordonnance sur l'informatique dans l'administration fédérale. Une

stratégie de surveillance basée sur les risques devrait ensuite définir quels secteurs informatiques sont essentiels. Les contrôles nécessaires qui en découlent doivent assurer une vue d'ensemble sans doubles emplois. Dans le cadre de ses tâches transversales, l'UPIC doit pouvoir intervenir et faire remonter les problèmes au-delà d'un office et d'un département. Il faut dès lors définir les instruments d'application ainsi que rechercher et éliminer systématiquement les lacunes ou les points faibles constatés par le biais des mécanismes de régulation. La surveillance centralisée renforcée devrait être mise en œuvre de manière efficace et automatisée.

Texte original en allemand

Attuazione delle istruzioni degli uffici trasversali
Organo direzione informatica della Confederazione

L'essenziale in breve

L'Organo direzione informatica della Confederazione (ODIC) provvede all'attuazione della strategia in materia di tecnologie dell'informazione e della comunicazione (TIC) nell'Amministrazione federale. A questo proposito emana direttive per le unità amministrative (UA) e gestisce i servizi standard TIC. Nel 2012 la gestione e la direzione dell'impiego delle TIC nell'Amministrazione federale sono state rafforzate. L'ODIC svolge ora anche compiti gestionali. Questi cambiamenti influenzano la vigilanza delle UA. Il presente rapporto è incentrato sulla vigilanza intesa quale verifica dell'attuazione delle istruzioni e delle direttive nei dipartimenti. Il Controllo federale delle finanze (CDF) ha verificato se i compiti, le competenze e le responsabilità sono definiti e se la vigilanza è assicurata.

L'ODIC non vede se stesso come un'autorità di controllo o di vigilanza, nonostante eserciti in parte anche compiti in questo ambito. I meccanismi di controllo sono definiti e risultano efficaci nell'ambito del portafoglio TIC della Confederazione e degli standard se questi riguardano acquisti di prodotti o servizi standard. Negli altri settori non esplicano però effetti o i loro effetti sono troppo contenuti. Un potenziale di miglioramento esiste nell'elaborazione delle basi per gli strumenti che permettono di far applicare le istruzioni e trasmettere i problemi al livello gerarchico superiore, nella prova dell'esecuzione dei controlli e nella vigilanza sull'eliminazione delle lacune.

Gli approcci per l'esecuzione dei controlli esistono

Il CDF ritiene evidente la necessità di uffici trasversali, dal momento che garantiscono processi uniformi nei settori chiave dell'Amministrazione federale. È quindi indispensabile che dispongano della competenza di emanare istruzioni e di competenze in materia di vigilanza e di applicazione. Le basi legali vigenti, tuttavia, non definiscono abbastanza chiaramente a chi spetta l'obbligo in materia di controllo e di vigilanza. I dipartimenti, come pure i fornitori e i beneficiari di prestazioni sono responsabili dell'attuazione delle direttive nei loro settori di compiti.

L'ODIC deve ricevere regolarmente rapporti sotto forme diverse da presentare al Consiglio federale. Poiché l'ODIC esamina soltanto in parte la plausibilità di queste autodichiarazioni, l'affidabilità delle informazioni fornite al Consiglio federale, ad esempio in ambito di controlling strategico, non è pienamente garantita.

In occasione delle sue verifiche il CDF ha più volte constatato che le direttive sulla sicurezza TIC non vengono rispettate. Questo denota che i meccanismi di controllo non sono efficaci. L'ODIC deve quindi rivestire un ruolo più importante in questo ambito.

Oltre a strumenti che permettono di trasmettere i problemi al livello gerarchico superiore all'interno del proprio dipartimento, l'ODIC non dispone di strumenti che consentono di far applicare le istruzioni.

Controlli sistematici grazie a un piano di vigilanza basato sui rischi

Il CDF raccomanda di affidare chiaramente l'obbligo di vigilanza all'autorità che emana le istruzioni e di modificare di conseguenza l'ordinanza sull'informatica nell'Amministrazione federale. Mediante un concetto di vigilanza basato sui rischi, si dovranno in seguito definire i settori TIC considerati essenziali. I controlli necessari che ne conseguono devono essere strutturati in modo da evitare un

doppio lavoro. Nel quadro dei suoi compiti trasversali, l'ODIC deve poter intervenire e trasmettere i problemi al livello gerarchico superiore in tutti gli uffici e i dipartimenti. È quindi necessario che i relativi strumenti di applicazione siano definiti e che le lacune e i punti deboli constatati siano sistematicamente monitorati ed eliminati tramite il meccanismo di controllo. La vigilanza centrale rafforzata dovrebbe essere realizzata nel modo più efficiente possibile e automatizzata.

Testo originale in tedesco

Implementation of cross-departmental office directives
Federal IT Steering Unit

Key points

The Federal IT Steering Unit (FITSU) ensures implementation of the information and communication technologies (ICT) strategy in the Federal Administration. For this purpose, it issues guidelines for the administrative units and manages the ICT standard services. Steering and managing the use of ICT in the Federal Administration was boosted in 2012. The FITSU now performs steering tasks. These changes influence supervision of the administrative units. This report concentrates on supervision in the sense of monitoring implementation of the directives and specifications in the departments. The Swiss Federal Audit Office (SFAO) checked whether or not the tasks, powers and responsibilities are defined and supervision is also carried out.

The FITSU does not see itself as an audit or supervisory body, but it nonetheless performs some supervisory tasks. Control cycles have been defined. In terms of content, they function in the federal ICT portfolio and in the standards if these involve product procurements or standard services. In the other areas, they have no or too little impact. There is room for improvement with regard to the basis for the enforcement and escalation instruments, proof of controls and supervision of the remedying of deficiencies.

Approaches to controls maintained

The SFAO believes the need for cross-departmental offices has been clearly identified. They guarantee a uniform approach in core areas of the Federal Administration. To this end, the authority to issue directives and supervisory and enforcement powers are an essential basis. However, it is not clear enough from the existing legal framework who is responsible for controls and supervision. The departments and service providers and procurers are responsible for the implementation of specifications in their task areas.

Regular reports must be made in various ways to the FITSU, and these are then submitted to the Federal Council. These self-declarations are only partially validated by the FITSU. The reliability of the information submitted to the Federal Council, e.g. on strategic controlling, is thus not fully guaranteed.

In its audits, the SFAO notes time and again that ICT security requirements are not adhered to in the field of ICT security. This is an indication that the control cycle is not effective. A stronger role for the FITSU in this area is essential.

Apart from escalation in its own department, the FITSU does not have any enforcement tools at its disposal.

Using a risk-based supervisory concept for systematic controls

The SFAO recommends clearly transferring the supervisory duty to the authority issuing the directives and amending the Federal Information Technology Ordinance accordingly. It should be subsequently determined by means of a risk-based supervisory concept which ICT areas are significant. The resulting monitoring requirement must ensure that an overview without duplication emerges. The FITSU should be able to intervene and escalate issues across offices and departments within the

scope of its cross-disciplinary tasks. The corresponding enforcement instruments must therefore be defined, and identified deficiencies and weaknesses must be systematically pursued and eliminated via the control cycle. Greater central supervision should be implemented in a manner that is as efficient and as automated as possible.

Original text in German

Generelle Stellungnahme des ISB zur Prüfung:

Die Durchsetzung von Weisungen ist Teil der Führung. Gemäss Artikel 9 der Bundesinformatikverodnung (BinfV) führen die Departemente und die Bundeskanzlei beziehungsweise die Verwaltungseinheiten den IKT-Einsatz in ihren Bereichen. Sie regeln im Rahmen der gültigen Vorgaben die Steuerung und die Führung der IKT in ihrem jeweiligen Bereich (Artikel 5 Absatz 3 BinfV). Das Informatiksteuerungsorgan des Bundes (ISB) bereitet u.a. die IKT-Geschäfte des Bundesrates vor und vollzieht die sich daraus für das ISB ergebenden Aufträge. Dazu gehört auch das Strategische IKT-Controlling einschliesslich des Sicherheitscontrollings. Es führt die IKT-Standarddienste (Artikel 17 Absatz 1 Buchstabe c BinfV). Die Informatikrevision ihrerseits wird von der Eidgenössischen Finanzkontrolle (EFK) wahrgenommen (Artikel 28 Absatz 2 BinfV). Damit ist die Grundzuordnung für die Durchsetzung und Aufsicht betreffend die Weisungen im Informatikbereich gegeben. Das ISB nimmt seine Controlling- und Kontroll-Aufgaben gemäss den geltenden rechtlichen Grundlagen (BinfV sowie Weisungen des Bundesrates und des EFD) wahr. Eine Änderung dieser Grundzuordnung müsste durch den Bundesrat unter Berücksichtigung der übrigen Führungsorganisation der Bundesverwaltung und der entsprechenden Ressourcierung erfolgen. Wo möglich wird das ISB gestützt auf die Empfehlungen der EFK gerne Optimierungen bei der Durchsetzung in seinem Kompetenzbereich vornehmen.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

In der Bundesverwaltung (BVerw) haben der Bundesrat (BR) und die Departemente in den vergangenen Jahren eine Vielzahl neuer Weisungen erlassen bzw. bestehende Weisungen revidiert oder aufgehoben. Die Finanzdelegation der Eidgenössischen Räte (FinDel) hat sich im Bereich Informations- und Kommunikationstechnik (IKT)-Strategie des Bundes eingehend mit diesen Weisungen auseinandergesetzt. Dabei legte sie einen Schwerpunkt auf die Frage, ob die Aufgaben, Kompetenzen und Verantwortungen klar definiert sind und ob die Kontrolle über die Einhaltung und Umsetzung der Weisungen durch die Linienverantwortlichen ausreichend klar geregelt wurden. In ihrem Schreiben vom 5. März 2014 an den BR betreffend das Informatiksteuerungsorgan Bund (ISB) hält die FinDel Folgendes fest: „Die FinDel ist klar der Ansicht, dass es Aufgabe des ISB ist, die Umsetzung seiner Weisungen und Vorgaben in den Departementen zu kontrollieren." Diese Haltung ist bemerkenswert und klärt die Abgrenzung der Rollen der Querschnittsämter zu derjenigen des Aufsichtsamtes Eidgenössische Finanzkontrolle (EFK). Sie deckt sich mit der Ansicht der EFK, wonach trotz klarem Auftrag im Finanzkontrollgesetz (FKG) Kontrollen im Rahmen der Oberaufsicht gemäss FKG nicht *delegierte* Kontrollen oder Aufsichtsaufgaben der Querschnittsämter sein können. Die Prüfungsergebnisse der EFK dürfen und sollen durch die Querschnittsämter und Linienverantwortlichen genutzt werden, die Verantwortung für ausreichende Kontrollen bzw. die Aufsicht[1] über die Einhaltung der Weisungen bleibt jedoch beim Weisung erlassenden Querschnittsamt. Die FinDel ortete Handlungsbedarf und hat die EFK mit einer Prüfung bei den Querschnittsämtern Eidgenössisches Personalamt (EPA), Bundesamt für Bauten und Logistik (BBL), Eidgenössische Finanzverwaltung (EFV) und ISB beauftragt.

1.2 Prüfungsziel und -fragen

Abgeleitet aus dem Auftrag der FinDel hat die EFK folgende Fragen zu klären:

- Bestehen für die wesentlichen Querschnittsaufgaben angemessene Weisungen?
- Sind in den Weisungen die Kontrollen über deren Einhaltung und Umsetzung ausreichend klar geregelt?
- Gibt es ein Aufsichtskonzept mit einem geschlossenen Regelkreis oder sind Lücken im Kontrollsystem vorhanden?
- Wie werden die Kontrollen in der Praxis gelebt, insbesondere in Fällen mit delegierten Kontrollaufgaben?

Das Ziel der Prüfung liegt darin, gegebenenfalls Handlungsbedarf aufzuzeigen, damit die Sicherheit der einheitlichen Umsetzung von Weisungen erhöht werden kann.

[1] Im vorliegenden Bericht hat Aufsicht des Weisungsamtes folgende spezifische Bedeutung: Pflicht zur Überwachung der Einhaltung einer Weisung.

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Peter Küpfer, Revisionsleiter, und Cornelia Simmen, IT-Prüfungsexpertin durchgeführt. Die EFK hat vom ISB eine Liste aller Verordnungen und Weisungen verlangt.

Die Prüfung der EFK richtet sich nach den wesentlichen Querschnittsaufgaben des ISB. Sie basiert primär auf den Bestimmungen der Bundesinformatikverordnung (BinfV), der IKT-Strategie des Bundes und der Weisungen

- des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB),
- des Bundesrates für das Strategische Controlling im Bereich Informatik und Telekommunikation (IKT),
- des Bundesrates zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes.
- des Eidgenössischen Finanzdepartements (EFD) zur Umsetzung der Bundesinformatikverordnung (WUBinfV),

Die EFK hat die massgeblichen Weisungen durchgesehen und auf ihre Relevanz für diese Prüfung untersucht. Fokussiert wurde auf die Bereiche IKT-Sicherheit, strategisches IKT-Controlling, IKT-Portfoliomanagement und auf ausgewählte Standards.

Die im Titel enthaltene Bezeichnung „Weisung“ wird in diesem Bericht in einer nicht formell rechtlichen Sicht, sondern für jede Art von Vorschrift oder Anleitung verwendet. Weisungen in diesem Sinne umfassen somit auch Richtlinien und Vorgaben aller Art wie z. B. die vom ISB erlassenen Standards oder IKT-Grundschutzmassnahmen.

1.4 Unterlagen und Auskunftserteilung

Die Verantwortlichen und Mitarbeitenden des ISB haben der EFK die notwendigen Auskünfte rasch und kompetent erteilt. Die verlangten Unterlagen standen uneingeschränkt zur Verfügung.

Die Prüfung wurde im Oktober 2015 durchgeführt.

2 Durch dezentrale Verantwortlichkeiten besteht erhöhter Aufsichtsbedarf

Mit Inkrafttreten der überarbeiteten BinfV per 1. Januar 2012 sind die Steuerung und Führung des Einsatzes von IKT in der Bundesverwaltung verstärkt worden. Das ISB als bisherige Strategieinstanz nimmt nun Steuerungsaufgaben wahr. Die vormals weisungsbefugten Gremien Informatikrat des Bundes (IRB) und Ausschuss Informatiksicherheit (A-IS) sind nur noch Konsultativorgane des ISB. Bei den durch den BR beschlossenen und durch das ISB geführten Standarddiensten herrscht je nach Marktmodell Bezugszwang und übt das ISB die LB-Rolle zentral aus. Nach wie vor sind die Leistungserbringer (LE) und Leistungsbezüger (LB) für die Umsetzung der IKT-Vorgaben in ihrem Aufgabengebiet verantwortlich. Durch diese dezentrale Aufbauorganisation der Bundesverwaltung werden die Art und der Umfang von Aufsichtstätigkeiten wesentlich beeinflusst.

3 Die primäre Aufsichts- und Kontrollfunktion sieht das ISB bei der Linie

Der BR bestimmt die IKT-Strategie des Bundes und legt die IKT-Standarddienste sowie deren Marktmodelle fest. Er definiert, wo IKT-Vorgaben nötig sind oder angepasst werden müssen und überwacht die Umsetzung der IKT-Strategie anhand des strategischen IKT-Controllings. Das Eidgenössische Finanzdepartement (EFD) erarbeitet die IKT-Strategie des Bundes und erlässt im Rahmen seiner Aufgaben Verwaltungsverordnungen.

Das ISB hat im Rahmen seiner vielfältigen Aufgaben unterschiedliche Positionen. Bei den Standarddiensten ist es in der Führungsrolle und damit für die Umsetzung von Vorgaben verantwortlich. Die BinfV verpflichtet das ISB zudem, Ausnahmen von den von ihm erlassenen Vorgaben zu prüfen und allenfalls zu genehmigen. Bei der IKT-Sicherheit, beim IKT-Controlling und allen anderen Bereichen sieht sich das ISB dagegen in der Rolle einer Vorgaben- und Unterstützungsinstanz. Die Aufsichtspflicht obliege den Departementen, Aufsichtskompetenzen liessen sich aus den vorhandenen Weisungen für das ISB nicht ableiten. Forderungen nach solchen Aufgaben würden zudem die vorhandenen Ressourcen sprengen. Unterstützt würde die Durchsetzung der Vorgaben insbesondere durch deren sachliche Begründung, unter Beachtung der organisationsrechtlichen Bestimmungen. Dies bedeutet allerdings nicht, dass das ISB gar keine Aufsichtsfunktionen wahrnimmt.

4 Organisation

4.1 Querschnittsaufgaben des Informatiksteuerungsorgans

Gemäss BinfV sind dem ISB folgende wesentlichen Aufgaben zugeteilt:

- IKT-Geschäfte des BR vorbereiten,
- Vollziehen von Aufträgen des BR aus den vorbereiteten IKT-Geschäften,
- dem EFD aufgrund der Anforderungen von Departementen und der Bundeskanzlei (BK) Standarddienste mit Marktmodellen vorschlagen,
- Führen der vom BR beschlossenen Standarddienste,
- Festlegen von IKT-Vorgaben im Rahmen der vom BR bestimmten IKT-Strategie,
- Führen der Melde- und Analysestelle Informationssicherung (MELANI) in Zusammenarbeit mit dem Nachrichtendienst des Bundes.

Zu diesem Zweck nimmt das ISB folgende Funktionen wahr:

- Es klärt als Sachverständigenorgan im Auftrag der Departemente oder der BK vermutete oder erfolgte Sicherheitsvorfälle ab,
- es entscheidet über Abweichungen zu den von ihm erlassenen Vorgaben,
- es stellt den Informatiksicherheitsbeauftragten des Bundes und leitet damit den A-IS,
- es leitet IKT-Programme,
- es ist verantwortlich für die finanzielle Führung der IKT auf Stufe Bund sowie für die Instrumente zur Unterstützung der Steuerung und Führung der IKT, insbesondere für das IKT-Controlling und -Portfoliomanagement.

4.2 Für die zugewiesenen Aufgaben bestehen angemessene Weisungen

Für die wesentlichen Querschnittsaufgaben existieren gesetzliche Bestimmungen, Rechts- und, wo nötig, Verwaltungsverordnungen. Die in Ziffer 1.3 gelisteten Weisungen sind in Gesetzen und Rechtsverordnungen abgestützt. Die EFK hat keine Lücken festgestellt.

Im Gegenzug hat die EFK auch keine Hinweise darauf gefunden, dass inflationär Weisungen erstellt worden wären. Die, die vorgelegt wurden, haben ihre Berechtigung.

4.3 Die Aufsicht und Kontrolle ist ungenügend geregelt, Durchsetzungsinstrumente fehlen mehrheitlich

Die Verantwortlichkeiten bezüglich der weisungsgemässen Umsetzung von Vorgaben finden sich in den Artikeln 8, 10, 21 und 23 der BinfV. Grundsätzlich sind die Verwaltungseinheiten (VE) in der Pflicht, für die Umsetzung von Vorgaben zu sorgen. Damit verbundene Kontrollaufgaben oder Aufsichtspflichten sind nirgends klar festgelegt.

Für die Standarddienste ist die Kontrollfunktion nach Ansicht der EFK durch die Führungsrolle an das ISB übertragen. Dies beinhaltet die bei den Standarddiensten vorgegebenen Standards und betrifft auch die Sicherheitsvorgaben. Dasselbe gilt für die Bereiche IKT-Controlling und -Portfoliomanagement auf Stufe Bund, für welche das ISB gemäss BinfV, Art. 17 Bst. d, verantwortlich ist.

Daneben hat das ISB nach dem Wortlaut verschiedener Weisungen oft eher eine Unterstützungs- als eine Aufsichtsfunktion. Es definiert, nimmt entgegen, bereitet vor, klärt ab, setzt ein und koordiniert. Einzelne Verantwortlichkeiten sind bei verschiedenen Aufgaben genau umschrieben. In vielen Fällen ist eine aktive Rolle des ISB hinsichtlich Aufsicht oder Entscheiden vorgesehen. Es erlässt IKT-Weisungen, vollzieht, entscheidet, legt fest und führt. In den Rechtsgrundlagen fehlen aber klare Durchsetzungsinstrumente. Hier sieht die EFK einen grundlegenden Mangel. Daher stellt sich nicht in erster Linie die Frage, ob das ISB Aufsichtsverantwortung hat, sondern in welchem Umfang und mit welchen pragmatischen Massnahmen diese Überwachung der Einhaltung von Weisungen durchgeführt und inwieweit sie delegiert werden können.

5 Bestehen Regelungen zur Kontrolle der Umsetzung von Weisungen?

5.1 Aufsicht

Weder beim EFD noch beim ISB liegen Aufsichtskonzepte vor, die auf einer Risikoanalyse basieren. Das EFD kann als einziges Departement im Rahmen seiner Aufgaben (Einsatz Sonderstab Informationssicherheit, Erarbeitung und Umsetzung IKT-Strategie) IKT-Verwaltungsverordnungen erlassen. Berichte und Anträge des ISB fliessen immer über das EFD an den BR.

Das ISB stellt Arbeitsinstrumente und Grundlagen für eine konforme Umsetzung der Vorschriften zur Verfügung. Der Grad der Aufsicht bzw. der systematischen Kontrollen hängt stark vom Aufgabengebiet ab. Die zu beaufsichtigenden Bereiche sind auch sehr unterschiedlich. Schon aus diesem Grund wären nachvollziehbare risikobasierte Überlegungen hilfreich.

5.1.1 IKT-Strategie und strategisches IKT-Controlling: Die bestehende Aufsicht muss verbessert werden

Für das strategische IKT-Controlling auf Stufe Bund gibt es ein Konzept, welches als Aufsichtskonzept angesehen werden kann. Aus diesem geht hervor, dass der halbjährliche Bericht an den BR den Umsetzungsstand der IKT-Strategie aufzeigen soll. Die EFK hat in einer vorgängigen Revision festgestellt[2], dass diese Berichte zu wenig aussagekräftig sind. Es kann nicht wirklich nachvollzogen werden, wo der Bund mit der Umsetzung der IKT-Strategie steht. Die dahingehende Empfehlung der EFK zur qualitativen Verbesserung des strategischen IKT-Controllings war vom ISB positiv aufgenommen worden.

Das strategische IKT-Controlling basiert grundsätzlich auf Selbstdeklarationen der Departemente. Beim Masterplan führt das ISB ergänzend Interviews durch, hauptsächlich bei den LE. Dies sind Plausibilisierungen, welche aber nicht systematisch stattfinden. Das ISB vertritt hier die Haltung, dass es in Interessenkonflikte kommt, da auf Stufe Projekte eine enge Zusammenarbeit mit der involvierten VE existiert.

Dieser Argumentation kann sich die EFK nicht verschliessen. Es besteht ein Konfliktpotenzial, weil das ISB einerseits für das strategische IKT-Controlling verantwortlich und andererseits im operativen Geschäft tätig ist. Mit dieser Konstellation würde das ISB mindestens in Teilbereichen seine eigene Arbeit kontrollieren. Dennoch müssen die Berichte an den BR zur Umsetzung der IKT-Strategie einen möglichst korrekten Stand wiedergeben. Entsprechend müssten die von den Departementen gelieferten Daten verifizierbar sein. Diese Verantwortlichkeit trägt das ISB aufgrund der BinfV und des Konzeptes zum strategischen IKT-Controlling. Sie lässt sich nach Ansicht der EFK nicht an die Departemente delegieren.

Empfehlung 1 (Priorität 1):

Die EFK empfiehlt dem ISB, Massnahmen zu definieren, um eine ausreichende Verlässlichkeit der Informationen im strategischen Controlling aus den Departementen bestätigen zu können.

Stellungnahme des ISB:

Das ISB wird das strategische IKT-Controlling an die Stossrichtungen und Planungsunterlagen der neuen IKT-Strategie des Bundes 2016-2019 anpassen. Zu diesem Zweck wird es dem Bundesrat ein entsprechendes Konzept und gegebenenfalls einen überarbeiteten Entwurf der Weisungen des Bundesrates zum strategischen IKT-Controlling unterbreiten. Im Rahmen dieser Arbeiten wird das ISB prüfen, mit welchen Massnahmen die Verlässlichkeit der von den Departementen und der BK erhaltenen Informationen effizient und effektiv erhöht werden kann. Nach der Genehmigung des neuen Konzepts zum strategischen IKT-Controlling auf Stufe Bund durch den Bundesrat werden die beschlossenen Massnahmen im Rahmen der verfügbaren Personalressourcen umgesetzt.

[2] Auswirkungen der revidierten Bundesinformatikverordnung und Wirksamkeit des Informatiksteuerungsorgans - Informatiksteuerungsorgan Bund (PA 14248) im Juli 2015 publiziert – Empfehlung 7: Verbesserung des Reportings zum Umsetzungsstand der IKT-Strategie.

5.1.2 IKT-Portfoliomanagement auf Stufe Bund: Kontrollen sind geregelt und werden auch ausgeführt

Mit dem Cockpit IKT steht seit rund einem Jahr ein Werkzeug zur Verfügung, das die VE zwingend nutzen müssen. Alle geplanten und laufenden mittleren IKT-Projekte, -Grossprojekte und –Schlüsselprojekte sind spätestens ab Beginn der Phase Initialisierung zu erfassen. Auch geplante und laufende Anwendungen müssen einfliessen, ausgenommen sind Kleinanwendungen. Die Erfassung dieser Daten obliegt den jeweils für die IKT-Projekte/-Anwendungen verantwortlichen LB.

In den Weisungen des BR zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes sind nebst den Verantwortlichkeiten auch Kontrollen festgelegt. Diese Weisung wurde per 1. Juli 2015 in Kraft gesetzt. Bei deren Ausarbeitung hat die Haltung der FinDel bezüglich Kontrollverantwortung des ISB Wirkung gezeigt. So sollen die Departemente, die BK und das ISB die Einhaltung der Vorgaben zum IKT-Portfolio auf Basis von periodischen Plausibilitätsprüfungen überwachen. Das ISB nimmt diese Aufgabe zunehmend wahr anhand der IKT-Budgets. Damit kann recht zuverlässig die Vollständigkeit des IKT-Portfolios überprüft werden. Stellt das ISB Diskrepanzen fest, so kann es von den Departementen und der BK eine Ergänzung oder Präzisierung der Portfolio-Daten innert nützlicher Frist verlangen. Dem BR wird im Rahmen des strategischen IKT-Controllings über den Umsetzungsstand beim IKT-Portfolio und auch bezüglich IKT-Schlüsselprojekte rapportiert. Zudem prüft die EFK die vom BR definierten IKT-Schlüsselprojekte.

Nach Beurteilung der EFK ist in der Praxis eine Aufsicht vorhanden, auch wenn diese nicht in Form eines Aufsichtskonzeptes geregelt ist. Die Kontrollen im Bereich des IKT-Portfolios erscheinen angemessen und zielorientiert. Der Einsatz des Cockpits IKT als Steuerungsinstrument wird dagegen als ungenügend beurteilt. Dieser Punkt ist ebenfalls im Bericht einer früheren Prüfung[3] weiter ausgeführt.

5.1.3 IKT-Sicherheit: Prozesse und Verantwortlichkeiten sind seit Langem festgelegt, Kontrollen werden nicht systematisch durchgeführt

Die IKT-Sicherheit ist historisch über viele Jahre gewachsen und daher in der Bundesverwaltung gut verankert. Der Prozess und die Verantwortlichkeiten sind in der WIsB geregelt. Zahlreiche über lange Zeit verbesserte Hilfsmittel stehen zur Verfügung. Sowohl die Departemente wie auch die VE müssen Informatiksicherheitsbeauftragte (ISBD und ISBO) bestimmen. Diese koordinieren die IKT-Sicherheitsaspekte und erarbeiten die notwendigen Grundlagen für die Umsetzung der Sicherheitsvorgaben in ihrem Einflussbereich. Die ISBD sind Mitglieder des A-IS, welcher als Konsultativgremium das ISB unterstützt bzw. ebenso neue Sicherheitsthemen einbringt.

Die LB haben zusammen mit dem ISBO die Sicherheitsanforderungen festzulegen. Der IKT-Grundschutz ist zwingend sowohl von den LE wie auch von den LB umzusetzen. Über eine Schutzbedarfsanalyse (Schuban) muss für Projekte und Anwendungen ermittelt werden, wie hoch die Anforderungen an die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit sind. Seit Kurzem müs-

[3] Auswirkungen der revidierten Bundesinformatikverordnung und Wirksamkeit des Informatiksteuerungsorgans - Informatiksteuerungsorgan Bund (PA 14248) im Juli 2015 publiziert – Empfehlung 7: Verbesserung des Reportings zum Umsetzungsstand der IKT-Strategie.

sen weitere Fragen zu Risiken im Bereich der nachrichtendienstlichen Ausspähung beantwortet werden. Zeigt die Schuban einen erhöhten Schutzbedarf auf, so muss ein Informationssicherheits- und Datenschutzkonzept (ISDS) erstellt werden. Die darin ausgewiesenen Massnahmen zur Reduktion der festgestellten Risiken müssen nachfolgend durch LB und LE umgesetzt werden.

Nicht geregelt ist im gesamten IKT-Sicherheitsprozess, wer die Umsetzung der zahlreichen Vorgaben kontrolliert. Das ISB rapportiert dem BR jährlich über den Stand der IKT-Sicherheit. Die Aussagen dazu basieren auf Berichten der ISBD bzw. den vorgelagerten Reports der ISBO. In der Regel hinterfragt das ISB die erhaltenen Informationen nicht. Bei konkreten Hinweisen wird nochmals bei den Departementen nachgehakt. Konkrete Nachweise werden nicht angefordert, z. B. dass für alle IKT-Schutzobjekte eine Schuban und wo nötig die unterzeichneten ISDS-Konzepte vorliegen. Damit erfährt der BR nur von IKT-Sicherheitsmängeln, die von der Linie an das ISB gemeldet wurden.

Die EFK führt regelmässig Prüfungen in unterschiedlichen Bereichen der IKT-Sicherheit durch. Dass dabei immer wieder auf nicht umgesetzte Vorgaben hingewiesen werden muss, zeigt, dass der existierende Regelkreis eine ungenügende Wirkung hat. Das ISB erhält Kenntnis von den durch die EFK abgegebenen Empfehlungen. Mit dem neuen Cockpit IKT besteht nun ein Instrument, das für Vollständigkeitskontrollen oder für Stichproben durch das ISB verwendet werden kann. Es drängt sich auf, dass das ISB hier eine stärkere Rolle einnehmen muss.

Empfehlung 2 (Priorität 1):

Die EFK empfiehlt dem ISB, den Regelkreis im IKT Sicherheitsbereich so zu stärken, dass künftig überprüfbare Aussagen zur Einhaltung der Vorgaben gemacht werden können und eine Roadmap für die Beseitigung allfälliger Sicherheitslücken besteht.

Stellungnahme des ISB:

Um künftig noch überprüfbarere Aussagen zur Einhaltung der Sicherheitsvorgaben zu machen, werden im Rahmen des IKT-Sicherheitsreportings weitergehende Angaben zu den Anwendungen und Systemen mit erhöhtem Schutzbedarf verlangt. Es ist darin z.B. auszuweisen, ob die entsprechenden Schutzbedarfsanalysen (Schuban) und Informationssicherheits- und Datenschutzkonzepte (ISDS-Konzepte) vorliegen sowie aktuell und genehmigt sind (Ziffer 3.2 WIsB). Bei festgestellten Lücken sind durch die Departemente Massnahmen zum Schutz der sensiblen Daten und Informationen festzulegen sowie deren Umsetzung in einer Roadmap festzuhalten und zu dokumentieren.

5.1.4 Informatikstandards: Bei der Beschaffung wird kontrolliert, Ausnahmen müssen genehmigt werden

Es bestehen rund hundert verschiedene Standards, davon gut dreissig im Bereich eCH[4]. Letztere sind von der Prüfung ausgeschlossen worden. Die restlichen siebzig betreffen Produkte, Prozesse, Teilstrategien, Methoden und anderes. Die Standards haben empfehlenden oder zwingenden Charakter. Die EFK hat nur die zwingenden Standards einer näheren Prüfung unterzogen, die bundesweite Relevanz haben. Dabei handelt es sich mehrheitlich um Produktstandards, d. h. Hard- und Software. Solche sind direkt mit Beschaffungen verbunden.

Das BBL ist für alle Standardprodukte die zentrale Beschaffungsstelle (z. B. gesamte Microsoft-Palette). Mit der jährlichen Beschaffungsstatistik übt das BBL eine direkte und zunehmend wirksame Kontrolltätigkeit aus. Daneben sind die LE verpflichtet, vom LB geforderte Abweichungen von Standards dem ISB zu melden bzw. solche abzulehnen. Die LB können in begründeten Fällen beim ISB eine befristete oder unbefristete Ausnahmebewilligung beantragen, um einen zwingenden Standard nicht einsetzen zu müssen. Das ISB hat die Kompetenz, Ausnahmen zu erteilen oder auch zu verweigern. Es führt und bewirtschaftet eine Liste der erteilten Ausnahmebewilligungen. Das ISB geht davon aus, dass diese Liste mindestens seit 2014 vollständig ist. Wenn sich LE oder LB nicht an die Meldepflicht halten und auch die Kontrollen des BBL nicht greifen, so ist das ISB machtlos.

Die EFK hat den Eindruck erhalten, dass bei den Produktestandards mehrheitlich wirkungsvolle Kontrollen stattfinden. Das ISB scheint aufgrund seiner Tätigkeiten gut Bescheid zu wissen, was auf der operativen Ebene abläuft.

5.2 Regelkreis

Im Sinne eines systemorientierten Ansatzes stellt sich die Frage, ob in den geprüften Prozessen Regelkreise vorhanden sind. Ein Regelkreis soll die Steuerung und Kontrolle von Aufgaben erlauben, die bundesweite Vorgaben zu den Prozessen im IKT-Bereich beinhalten. Die nachfolgenden Ausführungen beurteilen nur den konzeptionellen Aufbau. Die Durchführung, insbesondere auch von Kontrollen, wird hier nicht mit beurteilt.

5.2.1 IKT-Strategie und -Controlling: Ein Regelkreis ist definiert

Mit dem halbjährlichen strategischen IKT-Controllingbericht wird dem BR der Stand der Umsetzung der IKT-Strategie dargelegt. Der dazugehörende Masterplan legt die weiteren Schritte und Termine fest. Die zugrunde liegenden Daten werden durch die Departemente in Selbstdeklaration geliefert. Durch den aufgesetzten Prozess ist ein Regelkreis definiert. Wie in Ziffer 5.1.1 ausgeführt, wird er aber qualitativ nicht ausreichend ausgeführt.

---

[4] eCH ist ein Verein, bzw. eine Plattform zur Förderung von eGovernment in der Schweiz.

5.2.2 IKT-Portfolio Bund: Ein Regelkreis ist festgelegt

Die Departemente müssen die geforderten Daten in der gemäss Pflichtfeldern gewünschten Qualität im zentralen Cockpit IKT regelmässig nachtragen. Das ISB ist für die finanzielle Führung der IKT sowie für das IKT-Portfolio Bund verantwortlich. Die dazu notwendigen Instrumente sind vorhanden. Ein Regelkreis ist festgelegt.

5.2.3 IKT-Sicherheit: Ein Regelkreis ist seit Langem etabliert

Die ISBD und ISBO verfügen über Prozesse und Hilfsmittel, um in ihrem Umfeld für die Umsetzung von Vorgaben sorgen zu können. Die Departemente und die BK müssen dem ISB regelmässig über die Umsetzung von Sicherheitsmassnahmen berichten. Der BR wird jährlich über diesen Umsetzungsstand orientiert. Dieser Regelkreis ist seit 2004 etabliert. Wie vorgängig ausgeführt, wird er aber qualitativ nicht ausreichend umgesetzt.

5.2.4 Informatikstandards: Ein Regelkreis ist nur bei Produktbeschaffungen ersichtlich

Jeder Standard regelt ein Teilgebiet und beinhaltet verbindliche oder empfehlende Vorgaben. Nur bei verbindlichen Standards ist ein Regelkreis gefordert. Ein solcher liegt vor, wenn der Standard über Produktbeschaffungen läuft oder die Standarddienste betrifft.

6 Welche Aufsicht ist sinnvoll?

Im Vergleich mit den anderen Querschnittsämtern nimmt das ISB einen Sonderstatus ein. Es verfügt durch die BinfV über weitgehende Kompetenzen hinsichtlich Steuerung der IKT. Für die mit Artikel 17 Bst. c der BinfV übertragenen Führungsaufgaben bei den Standarddiensten herrscht bezüglich Aufsichts-, Kontroll- und Durchsetzungspflicht Einigkeit zwischen der EFK und dem ISB. Dagegen bestehen unterschiedliche Auffassungen bei den übrigen Aufgaben, die das ISB wahrnimmt. Systematische Kontrollen im Sinne von Aufsicht hat die EFK hier nicht feststellen können, höchstens Ansätze dazu. Es geht hier nicht darum, wer im Recht ist. Vielmehr soll offengelegt werden, dass eine widersprüchliche oder zumindest nicht eindeutige Situation besteht. Diese fusst möglicherweise auf einem Systemfehler, der korrigiert werden müsste.

Die Departemente sind gemäss BinfV in allen IKT-Bereichen verpflichtet, für die Umsetzung von Vorgaben zu sorgen. Verschiedenste Gremien sorgen für den Informationsaustausch zwischen den Departementen und dem ISB, sowohl auf strategischer wie auf operativer Ebene. Die aufgesetzten Prozesse und die vom ISB zur Verfügung gestellten Werkzeuge stellen zunehmend sicher, dass sich die VE an die Vorgaben halten bzw. eine konkrete Aussage zur Erfüllung der Vorgaben abgeben müssen. Die Departemente wiederum müssen dem ISB den Umsetzungsstand in den wichtigsten IKT-Bereichen regelmässig und systematisch melden. Mit dem Cockpit IKT ist seit 2014 ein zentrales und griffiges Instrument vorhanden. Einerseits kann die Vollständigkeit der deklarierten Anwendungen und Projekte anhand des Budgets plausibilisiert werden. Andererseits gibt es Pflichtfelder, die weitere Kontrolltätigkeiten ermöglichen würden.

Grundsätzlich sollte die Kontrolle der Umsetzung von zentral erlassenen Weisungen auch departementsübergreifend organisiert sein. Es liegt somit in der Verantwortung des ISB, die Einhaltung der wesentlichen Vorgaben zu kontrollieren, überprüfen zu lassen oder durch systemische, prozessintegrierte Massnahmen abzusichern. Welches die wesentlichen Bereiche sind, ist durch eine Risikoanalyse zu ermitteln. Dabei gilt es, nicht nur die finanziellen und wirtschaftlichen Aspekte, sondern auch das Reputationsrisiko zu berücksichtigen.

Grundsätzliche Voraussetzung ist die Klärung der Verantwortung und die Stärkung der Durchsetzungsinstrumente. Das abweichende Rechtsverständnis zeigt, dass die Rechtsgrundlagen bzw. der konkrete Auftrag in dieser Hinsicht nicht klar genug sind. Zur Durchsetzung ist ein Eskalationsverfahren denkbar, welches sich an vorgesetzte Instanzen richtet.

Empfehlung 3 (Priorität 1):

Die EFK empfiehlt dem ISB, eine Anpassung der Bundesinformatikverordnung (BinfV) zu erwirken. Die generelle Aufsichtspflicht und die Aufsichtskompetenz des ISB müssen unmissverständlich hervorgehen. Durchsetzungsinstrumente sind in die BinfV aufzunehmen bzw. zu präzisieren. Das ISB soll im Rahmen seiner Querschnittsaufgaben über die Amts- und Departementsgrenzen hinweg intervenieren und eskalieren können.

Stellungnahme des ISB: Das ISB wird die Frage der generellen Aufsichtspflicht und die Aufsichtskompetenz des ISB mit dem Vorsteher des EFD thematisieren und dann gegebenenfalls Änderungen im Rahmen einer nächsten BinfV-Revision erarbeiten.

6.1 Die Behebung festgestellter Mängel muss überwacht werden

Die EFK will der Risikoanalyse und dem Aufsichtskonzept des ISB nicht vorgreifen. Der Kontrollbedarf muss im Rahmen dieser Grundlagenarbeiten ermittelt werden. Hier wird sich auch zeigen, auf welche Hilfsmittel zurückgegriffen werden kann oder welche Kontrollen delegiert werden können. Für einen wirkungsvollen Regelkreis ist zwingend, dass die Behebung der festgestellten Mängel beaufsichtigt wird. Dabei ist wichtig, dass der Gesamtüberblick über die wesentlichen Feststellungen und Mängel beim Weisungsamt ist, ohne dass Doppelspurigkeiten entstehen. Die Aufsicht über die wichtigen Feststellungen ist dem ISB selbst oder den Departementen zuzuteilen. Die, die durch die Departemente kontrolliert werden, sollten mit einer qualifizierten Rückmeldung abgeschlossen werden. Durch das ISB selbst beaufsichtigte Feststellungen sollten auf die VE als Gesamtes zielen. Korrekturen in einzelnen Prozessen oder einzelnen Ereignissen erachtet die EFK als nicht stufengerecht. Hingegen ist bei wesentlichen Sicherheitsmängeln das Monitoring der Mängelbehebung Pflicht.

Empfehlung 4 (Priorität 1):

Die EFK empfiehlt dem ISB, die Behebung der im Regelkreis festgestellten bzw. gemeldeten wesentlichen Mängel zu beaufsichtigen, ohne damit Doppelspurigkeiten bei der Kontrolle zu verursachen. Das ISB legt fest, welche Mängelbehebungen es selbst kontrolliert und bei welchen es sich die Umsetzung von Empfehlungen beispielsweise durch qualifizierte Rückmeldungen bestätigen lässt.

Stellungnahme des ISB:

Das ISB wird künftig im Rahmen des strategischen IKT-Controllings und des Sicherheitsreportings festlegen, wie und durch wen Mängelbehebungen zu überwachen sind.

Dabei ist ein angemessenes Aufwand-Nutzen-Verhältnis anzustreben und die verfügbaren Personalressourcen sind zu berücksichtigen. Zudem wird das ISB anstreben, dass keine unnötigen Doppelspurigkeiten entstehen.

6.2 Das Aufsichtskonzept ist zu dokumentieren

Die EFK beurteilt ein Aufsichtskonzept als zentral, damit Kontrollbedarf erkannt wird, gezielte Kontrollen möglich sind und Doppelspurigkeiten vermieden werden. Das Aufsichtskonzept basiert auf der Risikoanalyse. Es soll zeigen, welche Bereiche wesentlich sind, wer, was, wie kontrolliert und auf welche Weise die Informationen an die verantwortliche Instanz zurückfliessen.

Wie im Bericht dargelegt, erkennt die EFK in einzelnen Bereichen implizit ein Aufsichtskonzept, es bestehen zudem Aufsichtsinstrumente und Regelkreise sind auch erkennbar. Vereinzelt werden angemessene Kontrollen durchgeführt. Was fehlt, sind eine systematische Dokumentation bzw. die Systematik und die Nachvollziehbarkeit der Massnahmen. Dieser Mangel kann mit der entsprechenden Dokumentation behoben werden. Die EFK setzt hier auf eine pragmatische Umsetzung. Es sollte Klarheit darüber geschaffen werden, welche Instrumente und Massnahmen bereits existieren und was noch ergänzt werden muss. Einleitend müssten die Bereiche nach ihrer Bedeutung bzw. den inhärenten Risiken gegliedert werden. Anschliessend sind für bedeutende Bereiche die vorhandenen Kontroll- und Aufsichtsinstrumente zusammenzustellen. Die Zusammenstellung sollte auch mögliche Lücken aufzeigen. Es müsste ersichtlich sein, wer für welche Kontrollen verantwortlich ist und wie die Feststellungen an das ISB zurückfliessen.

Empfehlung 5 (Priorität 2):

Die EFK empfiehlt dem ISB, ein umfassendes Aufsichtskonzept für die wesentlichen IKT-Bereiche zu dokumentieren. Der Regelkreis der Aufsicht ist dabei abzubilden.

Stellungnahme des ISB:

Sollte die Umsetzung der Empfehlung 15562.003 zur einer BinfV-Revision führen, wird in diesem Rahmen auch ein entsprechendes Konzept erstellt.

7 Schlussbesprechung

Die Schlussbesprechung fand am 9. März 2016 statt. Teilgenommen haben Fischer Peter, Delegierter für die Informatiksteuerung des Bundes, Brigmann Thorsten, Leiter IKT-Finanzen und -Controlling, Frauenknecht Marcel, Leiter IKT-Sicherheit, Roth Herbert, Leiter IKT-Planung und -Steuerung, Schuppisser Ka, Verantwortliche Stab ISB. Seitens EFK haben Christ Brigitte, Stellvertretende Direktorin, Wagner Hans-Rudolf, Fachbereichsleiter, Simmern Cornelia, IT-Prüfungsexpertin und Küpfer Peter, Revisionsexperte, teilgenommen.

Sie ergab Übereinstimmung hinsichtlich den im Bericht aufgeführten Feststellungen und Empfehlungen.

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

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Rechtsgrundlagen

Finanzhaushaltgesetz (FHG, *SR 611.0*)

Finanzhaushaltverordnung (FHV, *SR 611.01*)

Finanzkontrollgesetz (FKG, *SR 614.0*)

Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV, *SR 172.010.58*)

Weisungen des EFD zur Umsetzung der Bundesinformatikverordnung (WUBinfV)

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

Weisungen des Bundesrates für das Strategische Controlling im Bereich Informatik und Telekommunikation (IKT)

Weisungen des Bundesrates zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes

IKT-Strategie des Bundes 2012 - 2015

Standards der Bundesverwaltung gemäss Publikation des ISB

Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen

Abkürzungen

A-IS	Ausschuss Informatiksicherheit
BBL	Bundesamt für Bauten und Logistik
BinfV	Bundesinformatikverordnung
BR	Bundesrat
BVerw	Bundesverwaltung
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
EPA	Eidgenössisches Personalamt
FinDel	Finanzdelegation der Eidgenössischen Räte
FKG	Finanzkontrollgesetz
IKT	Informations- und Kommunikationstechnik
IRB	Informatikrat des Bundes
ISB	Informatiksteuerungsorgan Bund
ISBD	Informatiksicherheitsbeauftragte Departement
ISBO	Informatiksicherheitsbeauftragte Organisationseinheit
ISDS	Informationssicherheits- und Datenschutzkonzept
LB	Leistungsbezüger
LE	Leistungserbringer
Schuban	Schutzbedarfsanalyse
VE	Verwaltungseinheit
WIsB	Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung
WUBinfV	Weisungen des EFD zur Umsetzung der Bundesinformatikverordnung

Glossar

Aufsicht	Mit der Aufsicht stellen der Bundesrat, die Departemente und die Bundeskanzlei die Erfüllung der verfassungsmässigen und gesetzlichen Aufgaben sicher. (Regierungs- und Verwaltungsorganisationsverordnung SR 172.010.58) Generell: Überwachung der Verwaltung durch eine übergeordnete Behörde bzw. Überwachung einer nachgeordneten Behörde. Im vorliegenden Bericht hat Aufsicht folgende spezifische Bedeutung: Pflicht zur Überwachung der Einhaltung einer Weisung.
Controlling	Teilfunktion der Unternehmensführung als ausgeübte Steuerungsfunktion sowie als Führungs- und Informationssystem gesehen. Das Controlling umfasst die Beschaffung, Aufbereitung, Prüfung und Interpretation von Informationen zur Steuerung und Führung. (Quellen: Institut für Management-Innovation, Prof. Dr. Waldemar Pelz und Bundesinformatikverordnung SR 172.010.58)
Kontrolle	Eine Sache oder Person daraufhin untersuchen, ob diese bestimmte Kriterien oder Anforderungen erfüllt. Kontrollen erfolgen innerhalb der Prozessorganisation sowie in der dem Prozess übergeordneten verantwortlichen Linie. (Quellen: Duden „Deutsch Grundschule“ und Weisungen des Bundesrates für IKT-Schlüsselprojekte)
Regelkreis	In diesem Bericht umfasst dieser Begriff folgende Wechselwirkung: Erlass einer Weisung, Kontrolle der Umsetzung, Aufsicht über die Mängelbehebung, allfälliger Follow-up oder Anpassung der Weisung.
Revision	Vom Tagesgeschäft unabhängige, objektive Prüfungsaktivität in einer Organisation. Bei Prüfungen gilt der Grundsatz der Prozessunabhängigkeit. Die Prüfenden sind an den Prozessen nicht operativ beteiligt. Die Prüfergebnisse weisen Soll-Ist-Differenzen aus, die für die Kontrollen verwendet werden können. (Quellen: Institut für Management-Innovation, Prof. Dr. Waldemar Pelz und Weisungen des Bundesrates für IKT-Schlüsselprojekte)
Verantwortung	Die mit einer bestimmten Aufgabe, einer bestimmten Stellung verbundene Verpflichtung, dass das jeweils Notwendige und Richtige getan wird und möglichst kein Schaden entsteht. Verpflichtung für etwas Geschehenes einzustehen. (Quelle: Duden „Deutsch Grundschule“)

Priorisierung der Empfehlungen

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