



# Informations- und Kommunikationstechnologie des Bundes

Synthesebericht zu den Prüfungen der Eidgenössischen Finanzkontrolle

---

EFK-25790

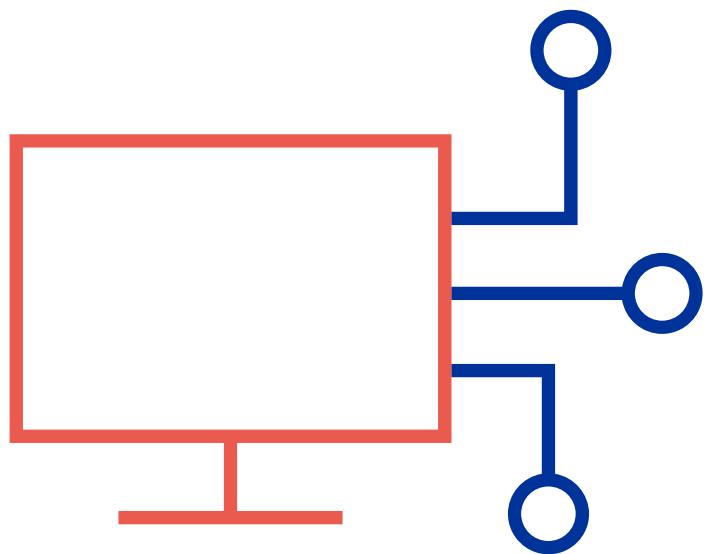
---

VERSION INKL. STELLUNGNAHMEN

---

23.05.2025

---



# DOKUMENTINFORMATION

---

---

**BESTELLADRESSE**

ADRESSE DE COMMANDE  
INDIRIZZO DI ORDINAZIONE  
ORDERING ADDRESS

Eidgenössische Finanzkontrolle (EFK)  
Monbijoustrasse 45  
3003 Bern  
Schweiz

---

**BESTELLNUMMER**

NUMÉRO DE COMMANDE  
NUMERO DI ORDINAZIONE  
ORDERING NUMBER

104.25790

---

**ZUSÄTZLICHE INFORMATIONEN**

COMPLÉMENT D'INFORMATIONS  
INFORMAZIONI COMPLEMENTARI  
ADDITIONAL INFORMATION

[www.efk.admin.ch](http://www.efk.admin.ch)  
info@efk.admin.ch  
+ 41 58 463 11 11

---

**ABDRUCK**

REPRODUCTION  
RIPRODUZIONE  
REPRINT

Gestattet (mit Quellenvermerk)  
Autorisée (merci de mentionner la source)  
Autorizzata (indicare la fonte)  
Authorized (please mention source)

---

**PRIORITÄTEN DER EMPFEHLUNGEN**

Die Eidgenössische Finanzkontrolle priorisiert ihre Empfehlungen auf der Grundlage definierter Risiken: 1 = hoch, 2 = mittel, 3 = gering. Als Risiken gelten beispielsweise unrentable Projekte, Verstösse gegen die Legalität oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Damit werden die Auswirkungen und die Wahrscheinlichkeit des Eintretens beurteilt. Diese Beurteilung richtet sich nach dem konkreten Prüfungsgegenstand (relativ) und nicht nach der Relevanz für die Bundesverwaltung als Ganzes (absolut).

# INHALTSVERZEICHNIS

---

<b>Das Wesentliche in Kürze.....</b>	<b>5</b>
<b>L'essentiel en bref .....</b>	<b>8</b>
<b>L'essenziale in breve.....</b>	<b>11</b>
<b>Key facts .....</b>	<b>14</b>
<b>1      Auftrag und Vorgehen .....</b>	<b>18</b>
1.1    Ausgangslage .....	18
1.2    Zielsetzung des Berichtes.....	18
1.3    Umfang und Grundsätze des Syntheseberichts.....	19
1.4    Schlussbesprechung.....	19
<b>2      Der Orientierungsplan.....</b>	<b>20</b>
<b>3      Externes Umfeld .....</b>	<b>21</b>
3.1    Gesetze .....	21
3.2    Markt .....	22
3.3    Lieferanten.....	23
3.4    Partner.....	23
<b>4      Organisationssteuerung.....</b>	<b>25</b>
4.1    Strategie / IKT-Strategie.....	25
4.2    Governance.....	25
4.3    Richtlinien und Compliance .....	28
4.4    Sicherheitsvorgaben.....	29
<b>5      Prozesse.....</b>	<b>30</b>
5.1    Managementprozesse.....	30
5.2    Hauptprozesse .....	31
5.3    Supportprozesse Beschaffung, Finanzen, Personal, Immobilien und Subventionen.....	32
5.4    Supportprozess IKT-Betrieb .....	34
<b>6      Daten und Informationsmanagement.....</b>	<b>37</b>
6.1    Datenflüsse und Datenqualität.....	37
6.2    Datenschutz und Zugriffskontrollen .....	37
6.3    Datenarchitektur und Taxonomie.....	38
6.4    Stammdaten .....	39
<b>7      Anwendungen und Dienste.....</b>	<b>41</b>
7.1    Fachanwendungen und Schnittstellen .....	41
7.2    Benutzerschnittstellen .....	42
7.3    Clouddienste.....	42

<b>8</b>	<b>Technologie und Infrastruktur .....</b>	<b>44</b>
8.1	Netzwerke.....	44
8.2	Rechenzentren .....	45
8.3	Server und Endgeräte .....	46
8.4	Backups / Sicherheitstechnologien .....	46
8.5	Speicherlösungen und Virtualisierung.....	47
	Anhang 1 – Liste der berücksichtigten Berichte.....	48

# Informations- und Kommunikationstechnologie des Bundes

Synthesebericht zu den Prüfungen der Eidgenössischen Finanzkontrolle

---

## DAS WESENTLICHE IN KÜRZE

In vielen Prüfungen der Eidgenössischen Finanzkontrolle (EFK) spielt die Informations- und Kommunikationstechnologie (IKT) des Bundes eine zentrale Rolle. Angesichts der Vielfalt an Themen und der dezentralen Struktur der Bundesverwaltung fällt es jedoch schwer, den Überblick zu behalten und die Ergebnisse gesamthaft einzuordnen. Dieser Synthesebericht soll hierbei helfen.

Berichte der EFK sind in der Regel kein Transportmittel für gute Neuigkeiten. Das liegt am Vorgehen, wie die EFK die Themen auswählt. Sie freut sich, wenn es im geprüften Bereich keine grossen Beanstandungen gibt. Wenn sich dies häuft, ist es allerdings kein gutes Zeugnis für das risikoorientierte Vorgehen der EFK: Geprüft wird dort, wo sie relevante Risiken sieht – für den sinnvollen Einsatz von Steuergeldern, für die Reputation der Verwaltung oder für das Vertrauen in staatliche Institutionen. Auch wenn sich der Synthesebericht auf über 80 Einzelprüfungen schwerpunktmässig aus den Jahren von 2021 bis 2024 stützt, sind die Ergebnisse nicht zwangsläufig repräsentativ für die gesamte Bundesverwaltung. Die IKT des Bundes ist zu vielschichtig und zu dezentral für ein pauschales Urteil. Doch die Probleme häufen sich an zu vielen Stellen, um von Einzelfällen zu sprechen. Auch wenn der Wille zu Verbesserungen spürbar ist, stehen weiterhin substanziale Arbeiten bevor.

## Es fehlt die Einheit in der Vielfalt der Dezentralisierung

Viele Themen mit IKT-Bezug müssen dezentral geregelt sein – etwa dort, wo eine enge Nähe zum Kerngeschäft und den Kunden entscheidend ist. Aber es gibt auch Bereiche, in denen Dezentralisierung kontraproduktiv ist. Standardisierung, gemeinsame Schnittstellen oder Sicherheitsvorgaben verlieren an Wirkung, wenn jeder seinen eigenen Weg geht. Auch wenn das Bewusstsein für diese Problematik in der Bundesverwaltung vielerorts vorhanden ist, trägt es in der Praxis wenig Früchte. Zu selten gelingt innerhalb der Bundesverwaltung oder im Zusammenspiel mit externen Partnern eine konsequente, zielführende Abstimmung der IKT. Bei sicherheitskritischen Vorfällen fehlt der Eskalationspfad, um eine sofortige Beseitigung der Sicherheitslücken durchsetzen zu können. Auch in der Zusammenarbeit mit den Kantonen dominiert, oft gesetzlich untermauert, beidseitig das Prinzip der Eigenständigkeit.

## Die Bundesverwaltung zeigt guten Willen, bleibt aber oft in ihren ineffizienten Strukturen gefangen

Innerhalb des Bundes fehlt es in vielen Bereichen strukturell an klaren Steuerungsmechanismen. Die Steuerung der Digitalisierung und IKT in der Bundesverwaltung ist zu komplex, wenig effizient und geprägt von unklaren Zuständigkeiten und begrenzter Durchsetzungskraft. Dem Bundesamt für Statistik stehen für die sehr wichtigen Tätigkeiten im Bereich der schweizweiten Harmonisierung und Verwendung von Verwaltungsdaten nur begrenzte Mittel und Einflussmöglichkeiten zur Verfügung. Der Delegierte für Digitale Transformation und IKT-Lenkung wirkt innerhalb seines engen Handlungsspielraums in der Bundesverwaltung so gut er kann, doch eine wirklich effektive, bundesweite Steuerung über Inhalte und Finanzen fehlt. Die Umsetzung einer gemeinsamen Verwaltung und Verwendung von Stammdaten für Geschäftspartner kommen nur langsam vorwärts, nicht zuletzt wegen fehlender Durchsetzungskompetenzen und bundesinterner Widerstände.

## **Wirtschaftlicher Umgang mit IKT-Mitteln: Anspruch und Realität klaffen auseinander**

Auch unabhängig von Föderalismus und departementalen Autonomieprinzip zeigt sich, dass der wirtschaftliche Umgang mit IKT-Mitteln in der Bundesverwaltung häufig hinter den Ansprüchen zurückbleibt. So werden teilweise bundesweite Tools eingeführt, ohne dass die tatsächlichen Bedürfnisse erhoben oder der erwartete Nutzen nachvollziehbar dargelegt wird. Ambitionierte Einsparversprechen, die zur Begründung neuer Projekte dienen, verlieren im Laufe der Umsetzung teilweise an Gültigkeit, werden selten kritisch hinterfragt oder nach Projektende auf Zielerreichung überprüft. Die Betriebskosten von IKT-Systemen bleiben vielfach ausserhalb des Blickfelds; eine transparente, vorausschauende und kritische Auseinandersetzung mit ihnen findet zu selten statt. Zudem führen nationale Zusatzanforderungen im Sinne eines «Swiss Finish» zu Mehrkosten, die nicht ausreichend offengelegt oder begründet wurden. Teure neue Rechenzentren werden nur langsam besiedelt und ihre Überkapazitäten kaum bewirtschaftet.

### **IKT-Führung ohne ausreichende Instrumente**

Der wirtschaftliche Umgang mit Ressourcen im IKT-Umfeld bleibt wiederholt unzureichend, und damit rückt zwangsläufig die Rolle der Führung in den Fokus. Es überrascht wenig, dass die EFK wiederholt feststellen muss, dass zentrale Steuerungsinstrumente wie Portfoliomanagement oder Beschaffungscontrolling entweder ganz fehlen oder nur in eingeschränkter Form vorhanden bzw. im Einsatz sind. Bemerkenswerter als das Fehlen dieser Instrumente ist die Tatsache, dass sie in vielen Fällen nicht vermisst werden. Dabei geht es nicht um zentrale Detailkontrolle oder digitale Planwirtschaft. Es geht um Überblick, Transparenz, Prioritätensetzung und fundierte Entscheidungen – kurz: Es geht um eine aktive Steuerung.

### **Verwaltungsmodernisierung stockt bei den Stammdaten und Automatisierung**

Bei digitalen Transformationen gewinnen die Daten enorm an Relevanz. Sie sind die Grundlage für eine durchgängige Verwaltungsmodernisierung, insbesondere im Sinne des Once-Only-Prinzips. Beim Aufbau einer abgestimmten Stammdatenverwaltung mit zentralen Elementen startet der Bund mit den Geschäftspartnerdaten. Die Umsetzung ist mühsam, und der angedachte Anwendungsbereich wurde eingeschränkt. Außerdem ist seit 2022 die Frage der EFK nach der Hoheit, Kontrolle und Verwendung der Datenbestände nicht abschliessend beantwortet. In diesem Thema ist aktuell in der Bundesverwaltung vieles in Bewegung.

Dass das Potenzial der Digitalisierung nicht ausgeschöpft wird, hat die EFK in ihren Prüfungen zur Digitalen Transformation wiederholt zum Ausdruck gebracht. Doch auch ausserhalb dieser grossen Vorhaben halten sich ineffiziente und fehleranfällige Papierwege sowie manuelle Prozesskontrollen hartnäckiger als wünschenswert. Bei neuen Anwendungen stehen wie zu erwarten die funktionalen Anforderungen zur Aufgabenerfüllung im Vordergrund, an die Möglichkeiten von Maschine-zu-Maschine-Schnittstellen wird noch zu wenig gedacht.

### **IKT-Sicherheit mit System, aber mit systemischen Schwächen**

Der Bund betreibt zahlreiche IKT-Lösungen, die erhöhte Sicherheitsanforderungen erfüllen müssen. Eine Verletzung der Informationssicherheit oder gar ein Ausfall dieser Infrastrukturen hätte weitreichende Folgen für die Bundesverwaltung, externe Partner bzw. die Bevölkerung. Dazu gehören unter anderem das Bundesnetzwerk, sicherheitskritische Anwendungen und deren Zugriffsportale sowie Plattformen für den gesicherten Datenaustausch. Diese Systeme wurden durch die EFK geprüft. Es besteht zwar punktueller Verbesserungsbedarf, insgesamt kann die EFK aber ein gutes Urteil über die Sicherheit im laufenden Betrieb abgeben. Kommt es zu sicherheitsrelevanten Vorfällen, zeigen sich jedoch Schwächen: unzureichend getestete Wiederherstellungsverfahren, langsame Reaktions- und Meldegeschwindigkeit sowie fehlende Eskalationsmöglichkeiten, wenn sich notwendige Massnahmen verzögern.

Weniger positiv sieht es beim Schutz kritischer Infrastrukturen aus. Diese stellen die Versorgungssicherheit in der Schweiz sicher. Sie müssen gut vor Cyberattacken geschützt werden. Das sind sie nur bedingt. Es fehlen teilweise verbindliche Sicherheitsvorgaben für die Betreiber, und die Zuständigkeiten sind zersplittert.

## **Empfehlungen aus den EFK-Berichten werden akzeptiert und umgesetzt**

Sieht die EFK in ihren Prüfungen Handlungsbedarf, gibt sie Empfehlungen ab. Wenn die betroffenen Einheiten mit diesen einverstanden sind, melden sie der EFK, bis wann sie eine Empfehlung umsetzen werden. Diese Terminierung durch die Geprüften ist wichtig, um den Aufwand in die Amtsprioritäten und-aufgaben einplanen zu können. Die Akzeptanz der Empfehlungen ist sehr hoch, die geprüften Bereiche sehen die Risiken und wollen diese adressieren. Bei der Umsetzung bleiben die Einheiten zwar teilweise hinter ihren eigenen Ansprüchen zurück, insgesamt ist die Bereitschaft zur Verbesserung vorhanden. Das stimmt zuversichtlich, wenn es um die Qualität der IKT in der Bundesverwaltung geht. In diesem Zusammenhang ist auch die Politik immer wieder gefordert, um beispielsweise über gesetzliche Rahmenbedingungen oder mit klaren Erwartungen Verbesserungen zu unterstützen bzw. zu beschleunigen.

Die aufgezeigten Muster und Lücken in diesem Synthesebericht basieren auf dem Stand der jeweiligen Einzelberichte. Wie stark sich die jeweilige Situation mittlerweile verbessert hat, wird die EFK in vielen Fällen im Rahmen von Nachprüfungen feststellen und darüber berichten. Solange jedoch die starke Dezentralisierung im Bereich der IKT mit seinen grundsätzlichen strukturellen Eigenheiten bestehen bleibt, ist auch weiterhin mit ihren nachteiligen Auswirkungen zu rechnen. In dieses Thema scheint aktuell zumindest innerhalb der Bundesverwaltung Bewegung zu kommen; das Paradigma «individuell statt gemeinsam» scheint in Frage gestellt zu werden.

## AUDIT

# Technologies de l'information et de la communication de la Confédération

Rapport de synthèse des audits du Contrôle fédéral des finances

## L'ESSENTIEL EN BREF

Les technologies de l'information et de la communication (TIC) de la Confédération constituent un élément important dans de nombreux audits du Contrôle fédéral des finances (CDF). Compte tenu des nombreux thèmes traités et de la structure décentralisée de l'administration fédérale, il est toutefois difficile de conserver une vue d'ensemble et de classer les résultats dans leur globalité. Le présent rapport de synthèse a pour but d'apporter une aide à cet égard.

Les rapports du CDF ne sont généralement pas destinés à annoncer de bonnes nouvelles. Cela est dû à la méthode de sélection des thèmes par le CDF. Lorsqu'il n'y a pas de critique particulière à formuler dans le domaine examiné, le CDF s'en félicite. Cependant, si ce cas de figure se présentait trop souvent, on serait en droit de s'interroger sur l'efficacité de l'approche du CDF, axée sur les risques : le CDF effectue des audits dans des domaines qui comportent, selon son appréciation, des risques importants en termes d'utilisation judicieuse de l'argent des contribuables, de réputation de l'administration ou de confiance dans les institutions de l'État. Même si le rapport de synthèse se fonde sur plus de 80 audits individuels portant principalement sur les années 2021 à 2024, les résultats ne sont pas nécessairement représentatifs de l'ensemble de l'administration fédérale. Les TIC de la Confédération sont trop complexes et décentralisées pour en faire une appréciation globale, les problèmes sont néanmoins trop fréquents et répandus pour que l'on puisse parler de cas isolés. Même si la volonté d'apporter des améliorations est perceptible, il reste encore beaucoup de travail à faire.

## La diversité découlant de la décentralisation pêche par un manque d'unité

De nombreuses questions liées aux TIC doivent être réglées de manière décentralisée, en particulier lorsqu'il est important d'assurer un lien étroit avec l'activité principale et la proximité avec le client. Toutefois, il existe des domaines où une décentralisation est contre-productive. La standardisation, les interfaces communes et les prescriptions en matière de sécurité perdent de leur efficacité lorsque chacun suit sa propre voie. Même si de nombreuses unités de l'administration fédérale ont pris conscience de cette problématique, cela ne se manifeste guère dans la pratique. L'administration fédérale, le cas échéant en collaboration avec des partenaires externes, ne parvient que trop rarement à coordonner les TIC de manière systématique et ciblée. En cas d'incidents critiques en termes de sécurité, la procédure d'escalade hiérarchique, qui permettrait de remédier immédiatement aux failles de sécurité, fait défaut. De même, la collaboration avec les cantons reste de part et d'autre soumise au principe d'autonomie, souvent ancré dans la loi.

## L'administration fédérale fait preuve de bonne volonté, mais reste souvent entravée par des structures inefficaces

La Confédération souffre d'un manque structurel de mécanismes de pilotage clairement définis dans de nombreux domaines. Les modalités du pilotage de la numérisation et des TIC de la Confédération sont trop complexes, peu efficaces et marquées par une répartition peu claire des compétences et une capacité d'action limitée. L'Office fédéral des statistiques ne dispose que de moyens restreints et d'une influence limitée pour mener à bien des tâches essentielles à l'harmonisation et à l'utilisation des données de l'administration à l'échelle nationale. Le délégué à la transformation numérique et à la gouvernance de l'informatique agit du mieux qu'il peut dans le cadre de ses compétences limitées au sein de la Confédération, mais il n'existe pas, à l'échelle nationale, de pilotage véritablement efficace assuré par le biais des contenus et des finances. La mise

en œuvre d'une gestion et d'une utilisation commune des données de base destinées aux partenaires de l'administration ne progresse que lentement, notamment en raison des compétences insuffisantes en matière d'application et des résistances internes au sein de l'administration fédérale.

## Gestion économique des moyens financiers consacrés aux TIC : un fossé entre exigences et réalité

Même en faisant abstraction des principes du fédéralisme et de l'autonomie des départements, force est de constater que la gestion économique des ressources vouées aux TIC par l'administration fédérale reste souvent en deçà des exigences. Ainsi, certains outils sont mis en place à l'échelle de la Confédération sans que les besoins effectifs aient été évalués ou les bénéfices attendus clairement exposés. Les promesses ambitieuses d'économies utilisées pour justifier de nouveaux projets perdent parfois de leur pertinence durant la phase de mise en œuvre, font rarement l'objet d'un examen critique et la réalisation des objectifs visés n'est guère évaluée une fois un projet achevé. Les coûts d'exploitation des systèmes informatiques ne sont pas suffisamment pris en considération ; ils font trop rarement l'objet d'une analyse transparente, prospective et critique. En outre, des exigences supplémentaires au niveau national au sens d'un « *swiss finish* » engendrent des surcroûts de coûts dont la mise en évidence et la justification restent insuffisantes. La mise en service de nouveaux centres de calcul onéreux ne progresse que lentement et leurs capacités pourtant excédentaires ne sont guère exploitées.

## Les instruments utilisés pour assurer le pilotage des TIC sont insuffisants

La gestion économique des ressources dans le domaine des TIC reste encore insuffisante, ce qui met inévitablement en lumière le rôle du pilotage. Il n'est guère étonnant que le CDF constate de manière répétée que des instruments de pilotage tels que la gestion de portefeuille ou le controlling des achats font totalement défaut ou que leur disponibilité ou leur utilisation sont limitées. Plus surprenant encore est le fait que l'absence de ces instruments ne soit que rarement signalée. L'objectif n'est ni d'instaurer un contrôle centralisé approfondi, ni d'imposer une économie numérique planifiée, mais plutôt d'assurer une vue d'ensemble, de garantir la transparence, de fixer des priorités et de prendre des décisions fondées ; en bref, il s'agit de mettre en place un pilotage actif des TIC.

## La modernisation de l'administration piétine en ce qui concerne les données de base et l'automatisation

Les données jouent un rôle primordial dans le cadre des projets de transformation numérique. Elles constituent en effet les éléments de base d'une modernisation complète de l'administration, en particulier dans la perspective de l'application du principe « *once only* ». Dans le cadre de la mise en place d'une gestion coordonnée des données de base avec des éléments centraux, la Confédération commence par traiter les données des organismes partenaires. La mise en œuvre est laborieuse et le domaine d'application initialement prévu a été restreint. En outre, depuis 2022, le CDF n'a pas reçu de réponse exhaustive aux questions posées concernant la souveraineté, le contrôle et l'utilisation des bases de données. Or ces différents points connaissent une évolution à l'administration fédérale.

Le CDF a indiqué à plusieurs reprises dans ses audits sur la transformation numérique que le potentiel de numérisation n'était pas pleinement exploité. Or même en faisant abstraction des grands projets en cours, on constate une persistance regrettable des procédures administratives, inefficaces et sources d'erreurs, et des contrôles de processus assurés manuellement. En ce qui concerne les nouvelles applications, les exigences fonctionnelles applicables à l'exécution des tâches sont, comme on peut s'y attendre, d'une importance centrale, mais les possibilités d'interfaces de machine à machine sont trop rarement prises en compte.

## La sécurité des TCI est systématiquement assurée, mais présente des lacunes systémiques

La Confédération exploite de nombreuses solutions informatiques qui doivent satisfaire à des exigences de sécurité accrues. Une atteinte à la sécurité de l'information, voire une défaillance des infrastructures, aurait de graves conséquences pour l'administration fédérale, ses partenaires externes et peut-être même pour la

population. Ces infrastructures comprennent notamment le réseau de la Confédération, des applications d'importance critique en termes de sécurité et leurs portails d'accès ainsi que des plateformes d'échange sécurisé de données. Ces systèmes ont été examinés par le CDF. Bien que des améliorations ponctuelles soient nécessaires, le CDF estime que la sécurité de ces systèmes est globalement assurée dans le cadre de leur exploitation. Des faiblesses sont toutefois constatées en cas d'incident en matière de sécurité : en effet, les procédures de restauration ne sont pas suffisamment vérifiées, les délais de réaction et de notification sont trop longs et les procédures d'escalade hiérarchiques prévues ne sont pas suffisantes lorsque les mesures nécessaires tardent à être prises.

Le bilan concernant la protection des infrastructures d'importance critique est moins positif. Celles-ci assurent la sécurité d'approvisionnement de la Suisse et doivent donc faire l'objet d'une protection adéquate contre les cyberattaques. Or ça n'est que partiellement le cas. Les directives de sécurité applicables aux exploitants ne sont pas toujours contraignantes et les compétences sont fragmentées.

## **Les recommandations émises par le CDF dans ses rapports sont acceptées et mises en œuvre**

Si le CDF constate dans ses audits que des mesures sont requises, il émet des recommandations. Si les unités concernées les acceptent, elles indiquent au CDF dans quel délai elles pensent les mettre en œuvre. Il est important pour les unités auditées d'avoir la possibilité de définir elles-mêmes le calendrier, car elles peuvent ainsi tenir compte des travaux requis à cet effet dans la fixation de leurs priorités et la planification de leurs tâches. Les unités auditées reconnaissant les risques encourus et entendant s'en protéger, elles reçoivent très favorablement les recommandations reçues. Même si elles restent parfois en deçà de leurs propres exigences dans le cadre de la mise en œuvre des recommandations, les unités auditées sont dans l'ensemble ouvertes aux améliorations. Ce constat réjouissant permet d'établir des prévisions optimistes quant à la qualité des TIC dans l'administration fédérale. À cet égard, les responsables politiques aussi sont régulièrement invités à soutenir ou à accélérer les améliorations, par exemple en définissant un cadre légal ou en formulant des attentes claires.

Les tendances et les lacunes mises en lumière dans le présent rapport de synthèse se basent sur les résultats reflétant la situation au moment de l'exécution des différents audits. Dans un certain nombre de cas, le CDF indiquera, dans le cadre d'audits ultérieurs, si et dans quelle mesure les améliorations recommandées ont entre-temps été mises en œuvre et consignera ses constatations dans ses rapports. Le domaine des TIC est fortement marqué, dans ses particularités structurelles, par la décentralisation poussée de l'administration fédérale ; il faut donc s'attendre à ce que les inconvénients qui en découlent continuent de se manifester. La situation semble toutefois évoluer du moins au sein de l'administration fédérale, et le principe du « chacun pour soi » paraît désormais remis en question.

## VERIFICA

# Tecnologie dell'informazione e della comunicazione della Confederazione

Rapporto di sintesi sulle verifiche del Controllo federale delle finanze

---

## L'ESSENZIALE IN BREVE

In molte verifiche eseguite dal Controllo federale delle finanze (CDF), le tecnologie dell'informazione e della comunicazione (TIC) della Confederazione rivestono un ruolo centrale. Tuttavia, data la varietà dei temi e la struttura decentralizzata dell'Amministrazione federale, è difficile mantenere una visione d'insieme e classificare i risultati nel loro complesso. Il presente rapporto di sintesi intende fornire un aiuto in tal senso.

I rapporti del CDF generalmente non comunicano buone notizie. Ciò è dovuto al modo in cui il CDF seleziona i temi. Il CDF è soddisfatto quando non rileva irregolarità di particolare rilievo nell'ambito sottoposto a verifica. Tuttavia, se questo accade spesso, non è un buon segno per l'approccio orientato ai rischi del CDF: le verifiche vengono eseguite laddove il CDF individua rischi rilevanti che intaccano l'impiego appropriato del denaro dei contribuenti, la reputazione dell'Amministrazione o la fiducia nelle istituzioni statali. Nonostante il rapporto di sintesi si basi su oltre 80 verifiche eseguite principalmente tra il 2021 e il 2024, i risultati non sono necessariamente rappresentativi dell'intera Amministrazione federale. Le TIC della Confederazione sono troppo eterogenee e decentralizzate per poter esprimere un giudizio globale. Tuttavia, i problemi aumentano in troppi settori per poter parlare di casi isolati. Sebbene si avverta la volontà di migliorare, resta ancora molto lavoro da fare.

### Mancanza di unità nella diversità della decentralizzazione

Molti temi legati alle TIC devono essere regolamentati a livello decentralizzato, ad esempio dove è fondamentale una stretta vicinanza all'attività principale e ai clienti. Ma vi sono anche settori in cui la decentralizzazione è controproducente. La standardizzazione, le interfacce comuni o le direttive in materia di sicurezza perdono efficacia se ogni unità segue il proprio sistema. Sebbene la consapevolezza di questo problema sia presente in molti ambiti dell'Amministrazione federale, nella pratica produce scarsi risultati. Troppo raramente si riescono ad armonizzare le TIC in modo coerente ed efficace all'interno dell'Amministrazione federale o in collaborazione con partner esterni. In caso di incidenti critici per la sicurezza, manca un percorso di escalation che consenta di risolvere immediatamente le falle di sicurezza. Anche nella collaborazione con i Cantoni prevale da ambedue le parti il principio dell'autonomia, spesso corroborato a livello legislativo.

### L'Amministrazione federale dimostra buona volontà, ma spesso rimane prigioniera delle sue strutture inefficienti

All'interno della Confederazione, in molti settori mancano chiari meccanismi di gestione dal punto di vista strutturale. La gestione della digitalizzazione e delle TIC nell'Amministrazione federale è troppo complessa, poco efficiente e caratterizzata da responsabilità poco chiare e da un'autorevolezza limitata. L'Ufficio federale di statistica dispone di mezzi e possibilità di influenza limitati per svolgere le importanti attività nel campo dell'armonizzazione e dell'utilizzo dei dati amministrativi in tutta la Svizzera. Il delegato alla trasformazione digitale e alla governance delle TIC opera al meglio delle sue possibilità nell'ambito del suo ristretto margine di manovra all'interno dell'Amministrazione federale, ma manca una gestione realmente efficace dei contenuti e delle finanze a livello federale. L'attuazione di una gestione comune e l'utilizzo dei dati di base per i partner commerciali procedono lentamente, anche a causa della mancanza di competenze esecutive e di resistenze interne alla Confederazione.

## Gestione economica dei mezzi TIC: divario tra aspettative e realtà

Anche a prescindere dal federalismo e dal principio di autonomia dei dipartimenti emerge che la gestione economica dei mezzi TIC nell'Amministrazione federale è spesso inferiore alle aspettative. In alcuni casi vengono introdotti strumenti a livello federale senza aver rilevato le necessità effettive o illustrato in modo comprensibile i benefici attesi. Le ambiziose promesse di risparmio che servono a giustificare nuovi progetti perdono in parte validità nel corso della loro attuazione. Raramente vengono esaminate con senso critico o viene verificato il raggiungimento degli obiettivi al termine del progetto. I costi di esercizio dei sistemi TIC spesso non vengono presi in considerazione; troppo raramente vengono esaminati in modo trasparente, lungimirante e critico. Inoltre, le esigenze nazionali aggiuntive nel senso di uno «swiss finish» comportano costi supplementari che non sono stati sufficientemente resi noti o motivati. I nuovi e costosi centri di calcolo vengono occupati solo lentamente e le loro sovrapacità non vengono quasi mai sfruttate.

## Direzione TIC senza strumenti adeguati

La gestione economica delle risorse nel settore delle TIC continua a essere insufficiente, ponendo inevitabilmente al centro dell'attenzione il ruolo della direzione. Non sorprende che il CDF abbia constatato a più riprese che gli strumenti centrali di gestione come la gestione del portafoglio o il controllo gestionale degli acquisti sono del tutto assenti o disponibili e utilizzati solo in misura limitata. Più sorprendente dell'assenza di questi strumenti è il fatto che in molti casi non se ne avverte la mancanza. Non si tratta di un controllo centralizzato dettagliato o di un'economia digitale centralizzata, ma di visione d'insieme, trasparenza, definizione delle priorità e decisioni fondate. In breve, di una gestione attiva.

## Modernizzazione dell'amministrazione in fase di stallo per quanto riguarda i dati di base e l'automazione

Con la trasformazione digitale i dati stanno acquisendo un'enorme rilevanza. Costituiscono la base per una modernizzazione continua dell'amministrazione, in particolare nell'ottica del principio «once only». Per creare una gestione armonizzata dei dati di base con gli elementi centrali, la Confederazione inizia dai dati dei partner commerciali. L'attuazione è complessa e il campo di applicazione previsto è stato limitato. Inoltre, dal 2022 non è stata ancora fornita una risposta esaustiva alla domanda del CDF su sovranità, controllo e utilizzo delle raccolte di dati. In questo ambito sono attualmente in corso molti cambiamenti all'interno dell'Amministrazione federale.

Nelle sue verifiche relative alla trasformazione digitale, il CDF ha ripetutamente sottolineato che il potenziale della digitalizzazione non viene sfruttato appieno. Tuttavia, anche al di fuori di questi grandi progetti, le procedure cartacee inefficienti e soggette a errori nonché i controlli manuali dei processi sono più persistenti di quanto sarebbe auspicabile. Come prevedibile, nelle nuove applicazioni l'attenzione è focalizzata sui requisiti funzionali necessari all'adempimento dei compiti, mentre le possibilità offerte dalle interfacce che consentono la comunicazione da macchina a macchina sono ancora troppo poco considerate.

## Sicurezza TIC sistematica, ma con punti deboli sistematici

La Confederazione gestisce numerose soluzioni TIC che devono soddisfare requisiti di sicurezza elevati. Una violazione della sicurezza delle informazioni o addirittura un guasto di queste infrastrutture avrebbe conseguenze di vasta portata per l'Amministrazione federale, i partner esterni e la popolazione. Tra le soluzioni TIC figurano la rete della Confederazione, le applicazioni critiche sotto il profilo della sicurezza e i relativi portali di accesso nonché le piattaforme per lo scambio sicuro dei dati. Questi sistemi sono stati verificati dal CDF. Nonostante vi sia un margine di miglioramento in alcuni punti, nel complesso il CDF può esprimere un giudizio positivo sulla loro sicurezza durante l'esercizio. Tuttavia, in caso di incidenti relativi alla sicurezza emergono alcune debolezze: procedure di ripristino insufficientemente testate, lentezza nella reazione e nella segnalazione nonché mancanza di possibilità di escalation in caso di ritardi nell'attuazione di misure necessarie.

La situazione è meno positiva per quanto riguarda la protezione delle infrastrutture critiche che garantiscono la sicurezza dell'approvvigionamento in Svizzera. Queste infrastrutture devono essere ben protette dai

ciberattacchi, ma lo sono solo in misura limitata. In alcuni casi mancano disposizioni di sicurezza vincolanti per i gestori e le responsabilità sono frammentate.

### **Le raccomandazioni contenute nei rapporti del CDF vengono accettate e attuate**

Se nel corso delle sue verifiche il CDF ritiene che sia necessario intervenire, formula delle raccomandazioni. Se le unità interessate condividono l'opinione del CDF, gli comunicano entro quanto intendono attuarle. La fissazione di una scadenza da parte delle unità sottoposte a verifica è importante per poter pianificare il lavoro in base alle priorità e ai compiti dell'ufficio. L'accettazione delle raccomandazioni è molto frequente; i settori verificati riconoscono i rischi e intendono affrontarli. Nella fase di attuazione non sempre le unità rispettano i propri impegni, ma nel complesso sono disposte a migliorare. Ciò è motivo di ottimismo per quanto riguarda la qualità delle TIC nell'Amministrazione federale. In questo contesto, anche la politica è chiamata ripetutamente a sostenere o accelerare i miglioramenti, ad esempio definendo condizioni quadro giuridiche o aspettative chiare.

Gli schemi e le lacune evidenziati nel presente rapporto di sintesi si basano sullo stato dei singoli rapporti. In molti casi il CDF determinerà l'entità dei miglioramenti ottenuti nelle situazioni specifiche e ne farà rapporto nel quadro di verifiche successive. Tuttavia, finché persistrà il forte decentramento nel settore delle TIC con le sue peculiarità strutturali fondamentali, si prevedono ulteriori ripercussioni negative. Attualmente sembra esserci un certo movimento riguardo a questo tema, almeno all'interno dell'Amministrazione federale; il paradigma basato sull'azione individuale anziché coordinata sembra essere messo in discussione.

# Federal Information and Communication Technology

Summary report on the audits carried out by the Swiss Federal Audit Office

---

## KEY FACTS

Federal information and communication technology (ICT) plays a central role in many audits carried out by the Swiss Federal Audit Office (SFAO). However, it is not easy to keep track of the results and maintain a holistic and orderly overview due to the variety of topics covered and the decentralised structure of the Federal Administration. This summary report is intended to help with this.

Reports by the SFAO do not tend to be bearers of good news. This is due to the approach taken by the SFAO for selecting the topics. It is a good result for the SFAO if there are no major issues raised about the area being audited. However, if this is a common occurrence, this is also not a good sign for the SFAO's risk-based approach. Audits are carried out wherever relevant risks are identified that could endanger the effective use of taxpayers' money, the reputation of the Administration, or trust in the state institutions. Even though the summary report is primarily based on over 80 individual audits from 2021 to 2024, this does not necessarily mean the results are representative of the entire Federal Administration. The federal ICT is too complex and decentralised to allow a sweeping judgement. Yet the problems arise too frequently in too many places to be considered individual cases. Although the desire for improvement is palpable, substantial work still lies ahead.

### There is a lack of unity in the diversity created by decentralisation

Many topics related to ICT cannot be centrally managed, for example wherever close proximity to the core business and customers is crucial. But there are also areas in which decentralisation is counterproductive. Standardisation, common interfaces or safety regulations would lose effect if everyone was following their own route. Even though there is awareness of this issue in many parts of the Federal Administration, this achieves little in practice. All too often consistent, effective coordination of ICT cannot be achieved between internal departments within the Federal Administration or when working with external partners. In the case of safety-critical incidents, the escalation path is not sufficient to enable security vulnerabilities to be fixed immediately. When working with the cantons, the principle of autonomy is also a dominant factor to both parties, and is often underpinned by statute.

### The Federal Administration has good intentions, but often remains trapped inside its inefficient structures

Structurally, there is a lack of clear governance mechanisms in many areas of the federal government. Governance of digitalisation and ICT in the Federal Administration is overly complex, inefficient, and full of vague responsibilities and limited enforcement power. The Federal Statistical Office is only provided with limited resources and opportunities to influence for the purposes of carrying out very important tasks in national harmonisation and the use of government data. The Federal Council Delegate for Digital Transformation and ICT Steering does the best he can within his narrow scope of action in the Federal Administration, but truly effective, national governance over content and finances is lacking. There is slow progress on implementing the shared management and use of master data for business partners, not least because of insufficient enforcement powers and opposition within federal units.

## **Economic use of ICT resources: where demand and reality diverge**

It is also clear, irrespective of federalism and the principle of departmental autonomy, that the economic use of ICT resources in the Federal Administration often falls short of requirements. As such, tools are sometimes introduced nationwide without the actual requirements being assessed or the expected benefit being clearly explained. Ambitious promises of savings, which serve to justify new projects, lose some of their validity during implementation, and are rarely critically scrutinised or tested at the end of the project against achievement of objectives. In many cases, IT system operating costs remain outside the field of vision; a transparent, forward-looking and critical analysis of them does not take place often enough. Additional quality requirements, to produce what is known as a "Swiss finish", also lead to increased costs which were not sufficiently disclosed or justified. Expensive new data centres are slow to fill up and their excess capacity is barely put to good use.

## **ICT leadership without adequate tools**

The economic use of resources in the ICT environment repeatedly remains inadequate, and this inevitably brings the role of leadership into focus. It is hardly surprising that the SFAO repeatedly finds that central control mechanisms, such as portfolio management or procurement monitoring, are either completely missing or are only available/used to a limited extent. More striking than the lack of these instruments is the fact that in many cases their absence goes unnoticed. This is not a question of centralised detail control or the digital planned economy. It is about having an overview, transparency, setting priorities and making well-informed decisions – in short, it is about active management.

## **Modernisation of administration comes to a standstill at master data and automation**

Data becomes hugely relevant in digital transformations. It is the basis for comprehensive modernisation of administration, especially within the sense of the once-only principle. When setting up a coordinated master data management system with centralised elements, the Confederation starts with the business partner data. The implementation is arduous and the intended area of application has been reduced. In addition to this, since 2022 the SFAO's question on sovereignty, control and use of stored data has not had a definitive answer. Currently, there is a lot happening on this topic in the Federal Administration.

In its audits on digital transformation, the SFAO has repeatedly pointed out that the potential of digitalisation is not being fully exploited. However, even outside these major projects, inefficient and error-prone paper-based workflows and manual process controls are proving more tenacious than is desirable. For new applications, the functional requirements for fulfilling the task take priority, as is to be expected; there is still too little thought being given to the possibilities of machine-to-machine interfaces.

## **Systematic ICT security, but with systemic weaknesses**

The Confederation operates numerous ICT solutions which have to fulfil increased security requirements. A breach of the data security or even the failure of these infrastructures would have far-reaching consequences for the Federal Administration, external partners or the population. This includes the federal network, safety-critical applications and their access portals, as well as platforms for the secure exchange of data. These systems were audited by the SFAO. Although there is a need for certain improvements, the SFAO's assessment of security in routine operations is favourable overall. However, if there are security incidents, weaknesses do come to light: insufficiently tested recovery procedures, slow responses and reporting, and lack of escalation options if necessary measures are delayed.

The picture for the protection of critical infrastructures is less positive. These ensure the security of supply in Switzerland. They need to be well protected from cyber attacks, but this is only partially the case. In some areas, binding safety requirements are lacking, and responsibilities are fragmented.

## Recommendations in the SFAO reports are accepted and implemented

Where the SFAO sees a need for action in its audits, it makes recommendations. If the units affected agree with these, they advise the SFAO how long they will need to implement the recommendation. This scheduling by the audited units is important, in order for the work to be included in the planning of administrative priorities and tasks. Acceptance of the recommendations is very high; the audited areas see the risks and want to address them. Although the units fall short of their own standards in some areas of implementation, there is a general willingness to improve. This is encouraging when considering the quality of the ICT in the Federal Administration. In this regard, politicians are also repeatedly called upon to support or accelerate improvements, for example by establishing a legal framework or setting clear expectations.

The examples and gaps identified in this summary report are based on the status of the respective individual reports. In many cases, the SFAO will identify and report on the degree to which the respective situation has since improved as part of a follow-up audit. However, as long as ICT remains strongly decentralised, with its fundamental structural peculiarities, the adverse effects of this are also expected to continue. Currently, there seems to be movement on this topic, at least within the Federal Administration; the "individuality over collectivity" paradigm appears to be in question.

## ⌚ GENERELLE STELLUNGNAHME DES DIGITALISIERUNGSRAT BUND

---

Der Digitalisierungsrat Bund begrüßt die Erstellung eines Syntheseberichts über die IKT-Prüfungen aus den Jahren 2021 bis 2024. Der Synthesebericht liefert einen Überblick und unterstützt die Entscheidungsträger in der Bundesverwaltung dabei, Muster und Auffälligkeiten zu erkennen. In der Bundesverwaltung laufen aktuell Diskussionen über mögliche Anpassungen der IKT-Steuerung (Governance). Die Erkenntnisse der EFK liefern dazu wertvolle Hinweise. Der Synthesebericht stützt sich auf eine Vielzahl unterschiedlicher Berichte, die teilweise bis zu vier Jahre alt sind. Dem Digitalisierungsrat ist es wichtig, dass für eine umfassende Bewertung die Originalberichte beigezogen werden und der aktuelle Stand der jeweiligen Vorhaben berücksichtigt wird. So haben die Verwaltungseinheiten beispielsweise zu Clouddiensten, KI, Datenmanagement, Systemausfällen von Fachapplikationen oder Sicherheit und Betrieb der Netzwerke seit den Prüfungen zahlreiche (auch über die Empfehlungen der EFK hinausgehende) Massnahmen umgesetzt.

Der Synthesebericht adressiert auch grundlegende Themen, insbesondere die Rahmenbedingungen der Digitalisierung. An seiner Sitzung vom 30. April 2025 hat der Bundesrat Massnahmen im Eigenbereich zum Entlastungspaket 2027 beschlossen. Ein Teil davon betrifft Verbesserungen im IKT-Bereich. Außerdem hat die Generalsekretärenkonferenz (GSK) in einer Sondersitzung am 9. Dezember 2024 eine erste Diskussion zur Governance der Digitalisierung geführt. Die Departemente äusserten sich in der GSK grundsätzlich positiv gegenüber dem bestehenden Lenkungsmodell und zur Art, wie es innerhalb der Rahmenbedingungen umgesetzt wird. Die Departemente sehen aber ein Optimierungspotenzial bei den Rahmenbedingungen und möchten insbesondere, dass der Bund bei der Digitalisierung mehr gemeinsam macht und dass der Bereich DTI der Bundeskanzlei eine stärkere Rolle dabei spielen soll. Der Bereich DTI hat Vorschläge gemacht, wie dies umgesetzt werden könnte. Die GSK hat den Bereich DTI beauftragt, dem Bundesrat bis Ende 2025 einen Antrag mit den nötigen rechtlichen, organisatorischen und finanziellen Anpassungen zu unterbreiten, um Anpassungen an der Governance der Digitalisierung vorzunehmen.

# 1 AUFTRAG UND VORGEHEN

---

## 1.1 Ausgangslage

Die Informations- und Kommunikationstechnologie (IKT) ist ein wesentlicher Bestandteil der Schweizer Bundesverwaltung. Gemäss Beschaffungszahlen aus 2023 wurde dafür beim Bund für rund 1,5 Milliarden Franken beschafft. Die fünf IKT-Leistungserbringer der Bundesverwaltung<sup>1</sup> verrechneten im gleichen Jahr IKT-Leistungen im Umfang von rund 800 Millionen Franken an ihre internen Kunden, wobei diese sowohl intern erbrachte als auch extern bezogenen Leistungen beinhalten.

Die Personalausgaben des Bundes betragen über 6 Milliarden Franken jährlich. Der weitaus grösste Teil dieser Ausgaben entfällt auf den Lohn. Die Bundesverwaltung beschäftigt bei den internen Leistungserbringern rund 3500 Personen, das ist fast jede zehnte Stelle in der Bundesverwaltung. Gesamtzahlen, wie viele Anwendungen und IKT-Projekte derzeit in der Bundesverwaltung laufen, gibt es keine, da beispielsweise Kleinanwendungen und -projekte nicht erfasst werden müssen.

Auch ohne diese Zahlen ist offensichtlich, dass die Abhängigkeit von einer IKT, die den Geschäftsbetrieb der Bundesverwaltung ermöglicht, hoch ist – Tendenz weiter steigend. Kein Wunder also, dass die EFK mit ihrem risikobasierten Vorgehen kontinuierlich eine Vielzahl an Prüfungen durchführt, die die IKT des Bundes betreffen. IKT ist ein weites Feld mit vielen verschiedenen Aspekten. Es ist daher nicht einfach, die zahlreichen EFK-Prüfberichte richtig einzuordnen oder den Überblick zu behalten. Aus diesem Grund hat sich die EFK entschieden, diesen Synthesebericht zu erstellen.

## 1.2 Zielsetzung des Berichtes

Mit diesem Bericht sollen drei Ziele erreicht werden:

- **Muster und Auffälligkeiten aus einer Reihe einzelner Prüfungen aufzeigen:** Es liegen genügend Berichte zum Thema IKT des Bundes mit aussagekräftigen Ergebnissen vor. So viele, dass die Themen «Digitale Transformation» und «IKT-Schlüsselprojekte» bereits – bzw. demnächst – in separaten Berichten behandelt werden<sup>2</sup>.
- **Orientierung und Transparenz schaffen:** Die Vielzahl an IKT-Themen erschwert es, EFK-Einzelberichte einzuordnen. Dieser Bericht gibt einen strukturierten Rahmen und ein Gesamtbild.
- **Verstanden werden:** Der Synthesebericht verzichtet soweit möglich auf technische Fachsprache. Er soll für breite Leserkreise klar verständlich sein.

Details zu den angeführten Beispielen finden sich in den Einzelberichten, die im Anhang 1 gelistet sind. Sofern nicht anders angegeben, sind die referenzierten Berichte publiziert und unter der angegebenen Nummer auf [efk.admin.ch](http://efk.admin.ch) abrufbar. Der Synthesebericht spiegelt den Wissensstand zum jeweiligen Prüfungszeitpunkt wider, es erfolgten im Rahmen dieses Syntheseberichtes keine zusätzlichen Prüfungshandlungen zur Aktualisierung des Standes.

---

<sup>1</sup> Bundesamt für Informatik und Telekommunikation (BIT), Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD), Kommando Cyber (Kdo Cy), Information Service Center des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung (ISCeCo), Informatik des Eidgenössischen Departements für auswärtige Angelegenheiten (IT EDA)

<sup>2</sup> 22742 Digitale Transformation: Synthesebericht vergangener Prüfungen. Aktualisierung des Syntheseberichtes zu den Schlüsselprojekten vorgesehen für 2026

### 1.3 Umfang und Grundsätze des Syntheseberichts

Die vorliegende Synthese wurde vom 5. bis 29. März 2025 von Brigitte Christ erstellt. Punktuell kamen KI-Tools zum Einsatz. Diese Ergebnisse wurden vor der Verwendung von der Autorin gründlich geprüft und angepasst.

- Die Synthese stützt sich auf wesentliche Erkenntnisse aus EFK-Berichten seit 2021. Ältere Inhalte werden berücksichtigt, sofern sie kontextrelevant bzw. bezüglich der übergeordneten Erkenntnisse weiterhin gültig sind.
- IKT-Aspekte spielen in nahezu allen EFK-Prüfungen eine Rolle, in unterschiedlichem Ausmass. Der Bericht erhebt daher keinen Anspruch auf Vollständigkeit, sondern fokussiert auf Einzelberichte mit besonderer Relevanz für ein Thema.
- Die EFK hat 2023 einen Bericht zur digitalen Transformation veröffentlicht. Eine neue Ausgabe des Syntheseberichts zu den Schlüsselpunkten ist für 2026 geplant. Deshalb werden diese Themenblöcke im vorliegenden Bericht nicht im Detail behandelt. Einzelne Prüfungen werden jedoch erwähnt, wenn sie für die hier behandelten Themen direkt relevant sind.
- Prüfungen zur IKT-Sicherheit sind berücksichtigt, soweit sie Muster erkennen lassen.
- Der Umfang der für diesen Bericht berücksichtigten Prüfungen beschränkt sich auf die zentrale Bundesverwaltung. Im Bereich der schutzkritischen Infrastrukturen wurden Feststellungen, die die Betreiber betreffen, ebenfalls berücksichtigt.

### 1.4 Schlussbesprechung

Die mehr als 80 Einzelberichte wurden im Rahmen der jeweiligen Berichterstattung mit den verantwortlichen Stellen besprochen. Eine zusätzliche Besprechung dieses Syntheseberichtes bringt daher keine wesentlichen neuen Erkenntnisse. Allerdings hat die EFK den Digitalisierungsrat Bund, der sich aus Vertreterinnen und Vertretern der Departemente und dem Delegierten für Transformation und IKT-Lenkung zusammensetzt, zu einer allgemeinen Stellungnahme eingeladen.

EIDGENÖSSISCHE FINANZKONTROLLE

## 2 DER ORIENTIERUNGSPLAN

Es gibt viele Modelle, um die IKT einer Organisation in einem Gesamtbild darzustellen. Die EFK hat ein vereinfachtes Modell entwickelt, das sich an gängigen Architekturkonzepten orientiert, aber schlanker gehalten ist. Es soll strukturiert (vom Umfeld bis zur Technologie), verständlich für Nicht-IKT-Experten und praxisnah anwendbar sein. Zu Beginn eines jeden Hauptkapitels findet sich eine kurze Definition der zu gehörigen Komponenten.

Die sechs Ebenen der IKT-Umgebung (zur direkten Navigation Begriffe anklicken):



### 3 EXTERNES UMFELD



#### Das, worauf die Organisation reagieren muss

Das externe Umfeld umfasst die Faktoren ausserhalb der Verwaltung, die sie beeinflussen und auf die sie reagieren muss, um ihre Aufgaben erfolgreich zu erfüllen. Dazu gehören

- Gesetze: Gesetzliche Vorgaben und politische Rahmenbedingungen, die der Arbeit der Verwaltung zugrunde liegen.
- Markt: Entwicklungen und Innovationen, die die Verwaltung beeinflussen, wie z. B. Künstliche Intelligenz, Cloud Computing, technologische Trends, Konkurrenz und Fachkräfte auf dem Arbeitsmarkt, gesellschaftliche Entwicklungen oder Veränderungen in den Erwartungen der Bevölkerung.
- Lieferanten: Unternehmen, die der Verwaltung IKT-Produkte und-Dienstleistungen bereitstellen bzw. erbringen.
- Partner: Öffentlichen oder privaten Akteuren, mit denen die Bundesverwaltung zur Aufgabenerfüllung zusammenarbeitet, z. B. Kantone und Gemeinden, andere Länder, Hochschulen und Forschungseinrichtungen.

#### 3.1 Gesetze



#### Politischer Ruf nach digitaler Verwaltungslandschaft der Schweiz trifft auf föderale Zurückhaltung

Viele Aufgaben kann der Bund nicht alleine erfüllen, sondern nur im Verbund mit Partnern wie den Kantonen. Auch in diesem Kontext widmet sich die EFK in ihren Prüfungen immer wieder IKT-Fragen, z. B. im Zusammenhang mit den gesamtschweizerischen Registern. Nach den Erkenntnissen aus diversen Einzelprüfungen zog die EFK 2022 Bilanz: Die Schweiz hat in vielen Bereichen Schwierigkeiten, die kantonal erfassten Daten auf gesamtschweizerischer Ebene zu konsolidieren. Dies verhindert neben anderen Punkten die Umsetzung des Once-Only-Prinzips. Diese besorgniserregende Situation beeinträchtigt vor allem die Arbeit der Nutzerinnen und Nutzer der Register, wie z. B. die kantonalen Verwaltungen, die Bundesverwaltung oder die Strafverfolgungsbehörden. Die Gründe sind vielfältig: Die Verwaltungen auf Kantons- oder Gemeindeebene sind in der Regel mit der Datenerhebung und -erfassung betraut und verwenden unterschiedliche Softwareprogramme; gemeinsame Datenmodelle fehlen, sind unvollständig oder unverbindlich; die Daten sind unterschiedlich definiert oder von schlechter Qualität. 2011 zeigte ein Rechtsgutachten des Bundesamts für Justiz, dass die Verabschiedung einer verfassungsmässigen Rechtsgrundlage ein vernünftiger Weg sei, um die Situation im IT-Bereich zu ändern. Mögliche Lösungsansätze werden diskutiert, aber bisher stellt sich noch niemand dieser Aufgabe.

Ein weiteres Beispiel für Hürden in der schweizerischen Verwaltungsdigitalisierung zeigt sich im Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG), das 2023 verabschiedet wurde. Ziel des Gesetzes ist es, die elektronische Abwicklung von Geschäftsprozessen des Bundes zu fördern, um ein Digital First-Prinzip umzusetzen. Dies betrifft die Interaktion zwischen den Behörden auf allen Staatsebenen sowie mit Unternehmen und Bevölkerung. Artikel 12 und 13 des Gesetzes verdeutlichen jedoch den engen Handlungsspielraum des Bundes: Sie kann verbindliche Standards nur innerhalb der Bundesverwaltung durchsetzen und somit nicht sicherstellen, dass ausserhalb der Bundesverwaltung unterschiedliche Systeme, Technologien und Organisationen problemlos miteinander arbeiten können. Es gibt keine gesetzliche Verpflichtung für Kantone, Gemeinden und private Partner, z. B. elektronische Schnittstellen für den Datenaustausch zu nutzen. Das erschwert die Digitalisierung und das reibungslose Zusammenspiel der verschiedenen Verwaltungsebenen.

Die Politik ist aktiv: Diverse Vorstösse<sup>3</sup> drängen den Bund, gesetzliche Grundlagen zu erarbeiten, um die Steine auf dem Weg zu einer effizienten und schlagkräftigen digitalen Verwaltungslandschaft in der Schweiz aus dem Weg zu räumen. Ob deren Inkraftsetzung realistisch ist, wird sich am Willen der Beteiligten inkl. der politischen Entscheidungsträger zeigen und ist in der föderalen Schweiz ungewiss.

### **Ungleichgewicht von Aufgaben, Kompetenzen und Verantwortlichkeiten stören Zielerreichung**

Für viele Aufgaben, die der Bund mit Partnern (Kantone, Gesundheitseinrichtungen, paritätische Kommissionen etc.) erfüllt, werden IKT-Infrastrukturen eingesetzt, die unter der Federführung des Bundes geschaffen bzw. erneuert werden müssen. Um diese IKT-Infrastrukturen zielführend erstellen zu können, muss definiert sein, wer für welche Aufgaben zuständig ist, wer wofür zahlt, welche Befugnisse bestehen und wer letztlich die Verantwortung trägt. Wenn diese drei Elemente nicht im Einklang sind, wird es schwierig, die angestrebten Ziele zu erreichen. Die EFK findet dazu in ihren Prüfungen immer wieder Beispiele, z. B. im Gesundheitswesen (Elektronisches Patientendossier, Dgisanté) oder der Registerführung (Handelsregister). Der Bund trägt oft die Verantwortung für die Erstellung bzw. Erneuerung der IKT-Infrastruktur, kann aber die beteiligten Partner nicht zur Mitwirkung verpflichten. Wenn die EFK in ihren Prüfungen auf die negativen Folgen dieses Ungleichgewichts hinweist, stösst sie zum Teil auf ein stilles Hinnnehmen seitens der Ämter, die sich auf die rechtlichen Vorgaben berufen, ohne diese zur Änderung anregen zu wollen.

## **3.2 Markt**



### **Dem Mangel an IKT-Fachkräften begegnet man auf Bundesstufe zu wenig koordiniert**

Personen mit den «richtigen» Fähigkeiten am richtigen Ort zur richtigen Zeit zu haben, ist gerade im IKT-Bereich aufgrund der teilweise kurzlebigen Anforderungsprofile anspruchsvoll. Mit steigender Tendenz gibt es in der Bundesverwaltung etwa 3500 IT-Stellen. 2023 konnten rund 600 offene IT-Stellen nur mit Mühe besetzt werden. Die anstehende Pensionierungswelle kann das Problem noch verschärfen. Fehlt es an internen Experten, muss man auf externe ausweichen. Somit steigt die Abhängigkeit von Beratern und anderen IKT-Dienstleistern. Ausserdem treibt es die Kosten in die Höhe; Externe sind in der Regel teurer als internes Personal.

Im Kampf gegen den Fachkräftemangel stellt die EFK dem dezentralen Organisationsmodell im Personalwesen des Bundes keine guten Noten aus: Die Prüfung aus 2023 zeigt, dass die Bundesverwaltung eine starke Dachmarke hat und gute Arbeitsbedingungen bietet. Die meisten der fünf IKT-Leistungserbringer sind hingegen kaum bekannt bzw. weniger auf dem Arbeitsmarkt präsent als beispielsweise die staatsnahen Betriebe. Es fehlt an Informationen, welche Einheiten bzw. welche Profile besonders vom Fachkräftemangel betroffen sind. Die Bundesverwaltung kann also einzelne Zielgruppen nicht gezielt angehen. Bundesweite Ansätze fehlen, sowohl auf strategischer als auch auf operativer Ebene. Immerhin – die IKT-Leistungserbringer bilden mehr Lernende aus als andere Verwaltungseinheiten, und gute 59 % davon bleiben anschliessend dort. Die Rekrutierungsprobleme bei anspruchsvollen IKT-Stellen für Berufserfahrene lassen sich hingegen damit lösen.

---

<sup>3</sup> 24.4045 Die Verfassung braucht einen Digitalisierungsartikel // 23.3050 Verbindliche Standards für die digitale Verwaltungslandschaft der Schweiz // 22.3890 Rahmengesetz für die Sekundärnutzung von Daten // 24.312 Digitale Transformation schweizweit mit gebündelten Kräften angehen

### 3.3 Lieferanten



«Den Bund» als Beschaffer gibt es nicht, obwohl er einer der grössten Einkäufer des Landes ist und eine entsprechende Marktmacht und Verantwortung hätte. Neben den zentralisierten Beschaffungsstellen werden durch Delegationen zahlreiche Ämter selbst zu Einkäufern. Das Ergebnis: Ein Anbieter kann für verschiedene Ämter tätig sein, ohne dass diese voneinander wissen. Angesichts eines jährlichen milliardenschweren Beschaffungsvolumens überrascht es zudem nicht, dass Lieferanten nicht immer nur gute Qualität liefern. Kommt es zu Problemen, muss der Anbieter nur die Beziehung zu seinem jeweiligen Auftraggeber pflegen. Er muss nicht befürchten, dass seine Leistungen bei anderen Ämtern enger überwacht oder er von neuen Aufträgen ausgeschlossen wird.

Bereits 2017 hat die EFK dem Bundesamt für Bauten und Logistik empfohlen, die Voraussetzungen zu schaffen, um wichtige Lieferanten des Bundes wirksam zu überwachen und zu steuern. Die Hoffnung ruhte auf dem revidierten Bundesgesetz über das öffentliche Beschaffungswesen (BöB) von Juni 2019. Mit den Artikeln 44 und 45 BöB erhielt der Bund darin die Möglichkeit, Lieferanten vom Verfahren auszuschliessen, Zuschläge zu widerrufen oder Sanktionen zu verhängen. Die Finanzdelegation der eidg. Räte betonte in ihrem Tätigkeitsbericht 2021, dass diese Massnahmen greifen sollen, wenn ein Lieferant frühere öffentliche Aufträge mangelhaft erfüllt hat oder in anderer Weise erkennen liess, dass er kein verlässlicher und vertrauenswürdiger Vertragspartner ist.

Voraussetzung für einen solchen Entscheid wäre aber die Transparenz darüber, bei wem ein Lieferant welche Leistung innerhalb des Bundes erbringt, sowie ein funktionierender Austausch zwischen den Ämtern. Die Prüfung der EFK im Jahr 2023 brachte eine herbe Enttäuschung: Noch immer fehlen die gesetzlichen Grundlagen, um die Rolle des Bundes als Beschaffer zu stärken und schwache Lieferanten gezielter zu bewirtschaften. Das BöB erfüllt diesbezüglich die hohen Erwartungen nicht, es braucht ein Umdenken: Weg vom Ausschluss hin zum Lieferantenmanagement mit einer kontinuierlichen Bewertung. Dieses befindet sich zwar bei einzelnen Bundesämtern im Aufbau, aber es besteht kein einheitliches Vorgehen zwischen den Beschaffungsstellen. So werden die Ämter also auch weiterhin auf Medienbeiträge oder Prüfberichte der EFK angewiesen sein, die von Problemen in der Zusammenarbeit der Verwaltung mit Lieferanten berichten.

Immerhin: Der Katalog der Gründe für den Ausschluss eines Lieferanten von Bundesaufträgen wurde im Beschaffungsgesetz per 1. April 2025 um ein wichtiges Element erweitert. Kann ein Lieferant eine Sicherheitslücke bei Hard- oder Software nicht innerhalb einer gegebenen Frist beheben, kann der Vertrag mit ihm beendet werden.

### 3.4 Partner



#### **Register: Zähe Konsolidierung der IKT-Infrastrukturen**

Aus Effizienz- und Qualitätsgründen sind vereinheitlichte IKT-Infrastrukturen inkl. Anwendungen vorteilhaft. Der Weg dorthin ist lang, wie anhand von zwei Beispielen veranschaulicht werden kann: Seit mehr als 15 Jahren versucht das Bundesamt für Justiz (BJ), das Handelsregister weiterzuentwickeln. Der Reformbedarf ist erkannt, wie die EFK 2024 feststellt. Dennoch erwies sich auch der letzte Anlauf zur Vereinheitlichung der IKT-Infrastruktur als nicht zielführend. Die Einbindung der Anspruchsgruppen war unzureichend, und ein gemeinsamer Dialog mit ihnen auf strategischer oder operativer Ebene fand nicht ausreichend statt. Das bestehende Weisungsrecht des Bundes, um die Einheitlichkeit der Daten herzustellen, wird kaum genutzt. Eine EFK-Empfehlung aus 2018 bleibt damit auch weiterhin offen. Neu ist die Umsetzung auf Mitte 2026 zugesagt. Ein anderes Beispiel aus 2022 findet sich im Grundbuchwesen. Seit 2001 hat der Bund wichtige konzeptionelle Grundlagen für die Standardisierung und den elektronischen Austausch von Grundbuchdaten geschaffen. Der Versuch des BJ, gemeinsam mit einer Begleitgruppe eine Vision bzw. Strategie zur Digitalisierung des Grundbuchs zu entwickeln, scheiterte 2017 bzw. 2018 am

Widerstand der Kantone. Inzwischen haben sich verschiedene Stakeholder abgestimmt und könnten wertvollen Input für eine gemeinsame Vision und Strategie des Grundbuchwesens liefern. Die EFK empfahl dem BJ, zusammen mit dem Beauftragten für die Digitale Verwaltung Schweiz ein gemeinsames Vorgehen und konkrete Massnahmen für die Digitalisierung des Grundbuchwesens zu erarbeiten. Dies soll bis Ende 2026 erfolgen.

### **Nationale IKT-Lösungen: Nicht zwingend, sondern strategisch zu bewerten**

Ob die Schweiz nationale IKT-Lösungen und Standards braucht oder will, ist eine berechtigte Frage – insbesondere im Hinblick auf Effizienz, Interoperabilität und die Anbindung an internationale Systeme. Ein Beispiel ist das Armeeprojekt Integriertes Planungs- und Lageverfolgungs-Informationssystem (IPLIS), das mit 250 Millionen Franken budgetiert ist und auf internationale Standards statt teuren «Helvetisierungen» setzt, was aus finanzieller Perspektive zu begrüssen ist. Die EFK hält in ihrem Bericht 2023 fest, dass die Frage des anzuwendenden Standards über das Einzelprojekt hinausgeht und einen Grundsatzentscheid auf Armeeebene erfordert. Beispiele wie das Schweizer Emissionshandelssystem oder das Produktergister Chemikalien führen zu der Frage, ob der Schweizer Markt jeweils gross genug ist, um nationale Lösungen zu rechtfertigen. Dabei handelt es sich um keine IKT-Frage, sondern es geht um die Positionierung der Schweiz in einem Thema. Solche Entscheidungen haben jedoch Auswirkungen auf IKT-Lösungen und-Kosten, die daher frühzeitig und strategisch mitgedacht werden sollten.

## 4 ORGANISATIONSSTEUERUNG



### Das *Warum* und *Wie*

Diese Ebene stellt sicher, dass die Organisation klare Ziele verfolgt und nach sinnvollen Regeln gesteuert wird. Sie definiert die Ausrichtung und sorgt dafür, dass diese effizient, transparent und regelkonform verfolgt wird. Zugehörige Komponenten sind:

- Strategie / IKT-Strategie: Legen fest, wie sich die Organisation weiterentwickeln soll und welche Rolle die IKT dabei spielt.
- Governance: Bestimmt Entscheidungsstrukturen und Verantwortlichkeiten für eine effektive Steuerung.
- Richtlinien und Compliance: Schaffen klare Vorgaben, um einheitliche und effiziente Abläufe zu gewährleisten und stellt sicher, dass diese eingehalten werden.
- Sicherheitsvorgaben: Definieren Massnahmen zum Schutz von Daten, Systemen und Informationen vor Bedrohungen.

### 4.1 Strategie / IKT-Strategie



Die Frage der (IKT-)Strategietauglichkeit bzw. das Zusammenspiel von IKT- und Geschäftsstrategie im Zusammenhang mit Prüfungen von Programmen und Projekten ist wichtig und wird in den Berichten der EFK zur Digitalen Transformation bzw. zu den Schlüsselprojekten des Bundes dargestellt.

### 4.2 Governance



#### Delegierter für die Digitale Transformation und IKT-Lenkung – gute Leistung innerhalb eines begrenzten Handlungsspielraums

Am 3. April 2020 beschloss der Bundesrat die Ausgestaltung der überdepartementalen IKT-Lenkung in der Bundesverwaltung<sup>4</sup>. Er wählte diejenige Variante, die eine starke Rolle der Generalsekretärenkonferenz (GSK) vorsieht. Damit wurden Defizite des vormaligen Systems, namentlich fehlende Entscheidungsdurchsetzung, schwerfällige Entscheidungsprozesse sowie unklare Verantwortlichkeiten nur im Ansatz angegangen.

Eine zentrale Rolle spielt der Delegierte für die Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei. Er unterstützt und koordiniert die digitale Transformation der Bundesverwaltung. Er ist befugt, Weisungen zu den Standards und zur Unternehmensarchitektur zu erlassen. Zudem stellt er der Verwaltung sogenannte Standarddienste (z. B. Webauftritt, Telefonie, Mail) zentral zur Verfügung. Ausserhalb der Standarddienste hat er kaum Möglichkeiten zur Steuerung über Finanzmittel. Das Setup für die Steuerung der digitalen Transformation setzt auf ein sog. Lenkungsmodell. Wie die EFK in ihrer Prüfung aus 2023 feststellt, ist der Abstimmungsbedarf vielfältig und geht über das Lenkungsmodell hinaus: GSK, Digitalisierungsrat, Ämter bzw. Departemente, Bundesamt für Cybersicherheit, Staatsekretariat für Sicherheitspolitik, Digitale Verwaltung Schweiz, Informatikbetreiberkonferenz, Steuerungsausschuss

<sup>4</sup> Bundesratsbeschluss vom 3.4.2020 betreffend «Zukünftige Ausgestaltung der überdepartementalen IKT-Lenkung in der Bundesverwaltung».

Supportprozesse, Ausschuss Informatiksicherheit und der Bundesratsausschuss Digitalisierung und IKT sind einige der Stakeholder. Es ist oft nicht klar, welches Gremium für welche Fragen zu kontaktieren ist.

Die Departemente haben eine sehr starke Position gegenüber dem DTI. Die Ämter und Departemente können, um ihre Gestaltungshoheit auch im Zusammenhang mit IKT-Vorhaben zu erhalten, direkt an ihren Generalsekretär oder Bundesrat gelangen, um ihren Anliegen Gehör zu verschaffen. Sie verfügen ausserdem autonom über den grössten Anteil der Finanzen für die IKT. Die Durchsetzungskraft des DTI ist systemisch begrenzt und für die Zielsetzung einer bundesweiten Steuerung mit dem Ziel von Effizienzsteigerungen nicht zielführend. Dennoch, es gelingt dem DTI, sich in dieser Situation recht gut zurechtzufinden.

### **Datengovernance und Stammdatenverwaltung à la Bundesverwaltung**

Der Bund bewirtschaftet eines seiner zentralen Vermögenswerte nicht gut genug: seine Daten. Die Lücken beispielsweise bei der Umsetzung des Once-Only-Prinzips oder redundante Datenhaltungen sind stark von der gewollt schwachen übergreifenden Steuerung – auch im Zusammenspiel mit den föderalen Ebenen – geprägt. Dass hier Handlungsbedarf besteht, hat man mit der Schaffung des Data Board Bund (DBB) in 2024 anerkannt. Dieses Fachgremium soll den departementsübergreifenden Abgleich für Datengovernance,-management und-operabilität sicherstellen. Ausserdem soll dieses Gremium der datenzentrierten Zusammenarbeit und Weiterentwicklung in rechtlichen, organisatorischen, semantischen und technischen Belangen dienen. Betrachtet man die Vielzahl an Aufgaben und Mitgliedern<sup>5</sup>, erkennt man die Komplexität bei der Lösung von bundesweiten Problemen. Daneben gibt es ausserdem die Stammdatenverwaltung Bund<sup>6</sup>, die über sieben strategische und Steuerungsrollen den Ausbau der gemeinsamen Stammdatenverwaltung unterstützen möchte. Die EFK kommt zum Ergebnis, dass bisher die gewählten Governancemodele zwar komplex, aber nicht unbedingt wirksam sind.

### **Fehlende Datengovernance gefährdet Steuerung und Datennutzung nach Programmende von SUPERB**

Mit dem Programm SUPERB sollen die Supportprozesse Beschaffung, Finanzen, Personal und Immobilien nicht nur auf eine neue technische Plattform gebracht, sondern bundesweit standardisiert und optimiert, sowie mit zentralen Stammdaten unterlegt werden. Bereits 2022 hat die EFK bei ihrer Prüfung eines Teilbereiches, den Immobilien, empfohlen, eine Datengovernance als strategischen Grundstein u. a. für die Datenmodellierung nicht nur für die Immobilien, sondern über alle Supportprozesse hinweg zu klären. Sonst bleibt unklar, wer die Autorität und Kontrolle über Datenbestände hat und wie diese Datenbestände verwendet werden dürfen. Das System umfasst die Personen, Prozesse und Technologien, die erforderlich sind, um die Daten sowie deren Wege zu schützen und effizient zu verwalten. Die Datengovernance soll bis 2025 parallel zu den Prozessen entwickelt werden. Dem Vorgehen, die Governance nicht vorgelagert zu klären, steht die EFK kritisch gegenüber. Die Empfehlung, die als besonders wichtig eingestuft ist, hätte 2022 umgesetzt werden sollen. Neues Zieldatum ist Mitte 2025.

### **Teure IKT-Tools allein lösen keine Probleme**

Die Relevanz von durchdachten Geschäftsprozessen, die sich abgestimmt zusammenfügen und von Anwendungen zielführend unterstützt werden, ist in der Bundesverwaltung unbestritten und wird auch von der EFK in ihren Prüfungen immer wieder hervorgehoben. Vor diesem Hintergrund ist die Initiative zu begrüßen, verbindliche Vorgaben im Bereich Prozess- und Architekturmodellierung zu erlassen. Bereits seit 2019 gilt eine bundesweite Weisung, welche Werkzeuge für die Modellierung, Darstellung und Publikation der Unternehmensarchitektur und der Prozesse verwendet werden müssen.

Vier Jahre später war es Zeit für die EFK, den Nutzen dieser Vorgaben zu prüfen. Die Prüfung konzentrierte sich auf die Anwendung im EFD, doch viele der Erkenntnisse sind auch auf Bundesebene relevant. Im EFK-Bericht aus 2023 wird aufgezeigt, dass grundlegende Fragen zu Verantwortlichkeiten, Ressourcenausstattung und Governance der eingesetzten Werkzeuge offen waren. Die Applikationen mit externen Kosten von max. 20,3 Millionen Franken bis Ende 2031 wurden ursprünglich eng mit Blick auf ein Amt beschafft;

---

<sup>5</sup> Bundeskanzlei: Data Board Bund (DBB)

<sup>6</sup> Bundeskanzlei: Stammdatenverwaltung

die Bedürfnisse der Anwender und Auswirkungen auf die Geschäftsbereiche der breiteren Bundesverwaltung wurden unzureichend abgeklärt und unterschätzt. Die Migration bzw. Einführung im EFD erfolgte mit erheblichem Aufwand, obwohl grundlegende Fragen offenblieben und es an konkreten, messbaren Nutzenzielen bis zum Prüfungszeitpunkt fehlte.

Dieses Beispiel illustriert, dass sich das Ziel einer stimmigen Unternehmensarchitektur nicht mit der Einführung eines Tools erreichen lässt. Es ist ein teures Experiment mit hohem Frustrationspotenzial. Übrigens: Trotz hohem Energieeinsatz hatte das EFD auch bei der Prüfung 2023 noch keine Unternehmensarchitektur, und das Potenzial der Standardisierung in den Prozess- und Architekturmodellierungswerkzeugen war zum Prüfungszeitpunkt unausgeschöpft.

### **Erfreuliche Fortschritte bei IKT-Architektur und IKT-Governance im EJPD**

2022 und 2023 konnte die EFK feststellen, dass das Eidgenössische Justiz- und Polizeidepartement (EJPD) ein Unternehmensarchitekturmanagement aufbaut. Das EJPD arbeitete aktiv an der Umsetzung seiner Vision und seines Zielbilds in diesem Bereich. Dazu wurden Hilfsmittel erarbeitet, die konsequent genutzt und weiterentwickelt werden müssen. Auch auf Ebene einzelner Ämter des EJPD schreitet die Erarbeitung der Grundlagen voran, wenngleich sie Zeit braucht. Die Aktivitäten werden mit jenen auf Departements-ebene abgestimmt. Die EFK begrüßt diese Tätigkeiten und betont, dass klare Vorgaben, koordinierende Mechanismen und eine zentrale Steuerung eine einheitliche Ausrichtung sicherstellen müssen. Diese Steuerungsinstrumente befinden sich aktuell im Aufbau und entwickeln sich weiter. Die EFK bewertet die bisherigen Fortschritte in diesem Bereich als erfreulich.

Zur IKT-Governance beim EJPD konnte die EFK Positives feststellen. 2022 bestätigte sie, dass das EJPD ein solides IT-Management-Framework etabliert hat. Das bedeutet, dass intern Gremien, Vorgaben und Verantwortlichkeiten definiert sind und das Zusammenspiel zwischen den Organisationseinheiten geregelt wird. Bei fedpol wird dieser Ansatz noch weiter ausgebaut: Hier wurden spezifische, amtsinterne Gremien für Steuerungs- und Expertenfragen implementiert. Im Vergleich zu anderen Departementen ist der Reifegrad in diesem Bereich gut.

### **Die IKT-Governance im VBS ist im Umbruch und am Entstehen**

In bisherigen Berichten hat die EFK wiederholt die fehlende Steuerung der IKT im VBS bemängelt, die sich in grossen Rückständen bei Projekten, mangelhafter Ressourcensteuerung, finanziellen Überraschungen, schwacher Planung oder Problemen in konkreten Projekten manifestierte. Das VBS erkannte die Notwendigkeit, auf Departementsstufe zu reagieren und ein strukturiertes Portfoliomanagement zu etablieren. 2023 publizierte die EFK ihren Bericht über die IKT-Governance beim VBS. Zu diesem Zeitpunkt war im Departement viel im Fluss und zahlreiche Aktivitäten am Laufen, um den Reifegrad der IKT-Governance zu erhöhen. Die EFK begrüßt den Willen zu durchgreifenden Massnahmen auf Stufe Departement. Sie konnte Hinweise auf viele Themen geben, die noch bearbeitet werden müssen. Dazu gehören beispielsweise ein einheitliches Verständnis wesentlicher Begriffe, Kriterien für die Abgrenzung ziviler von militärischer IKT, oder Zielvorgaben für die operative Umsetzung der IKT-Governance. Eine abschliessende Beurteilung war angesichts der fehlenden Arbeitsergebnisse jedoch nicht möglich. Zahlreiche Arbeiten sind noch bis mindestens 2027 notwendig.

### **IKT-Entflechtung im VBS: Systeme mit erhöhten Sicherheitsanforderungen sind abzugrenzen**

Wie wichtig eine konsequente Überlegung ist, wie man seine IKT-Umgebung zusammenfügt oder eben voneinander abgrenzt, hat die EFK in einer Prüfung 2022 festgehalten. Im Fokus stand die Entflechtung der Informations- und Kommunikationstechnik des VBS, bei der IT-Systeme mit speziellen Sicherheitsanforderungen von anderen Systemen getrennt werden sollten. Die Prüfung zeigte, dass es an übergeordneten Architekturen fehlt, um diese Trennung vertikal über alle Architekturebenen hinweg konsequent umzusetzen. Von Ebene Geschäftsprozess bis auf Netzwerkebene und Endgerät war offen, wie die angestrebte Trennung mit welchen Konsequenzen umgesetzt werden soll: Braucht ein Mitarbeiter beispielsweise zwei getrennte PC, einen für die zivilen Bereich und einen für die Arbeiten mit speziellen Sicherheitsanforderungen? Dieser konzeptionelle «Schnitt bis auf den Boden» war noch nicht erfolgt. Die EFK

vergab eine Empfehlung der höchsten Wichtigkeitsstufe und wird in 2025 nachprüfen, ob sie, wie vom VBS gemeldet, ausreichend umgesetzt ist.

## 4.3 Richtlinien und Compliance



### **Leitfaden hilft bei Ausgestaltung von Rechtsgrundlagen für Digitalisierungsvorhaben zu wenig**

Mit der Digitalisierung und flexibleren Nutzung von Daten sollen Effizienz und Wirksamkeit in der Bundesverwaltung steigen. Bei diesen Vorhaben stoßen die Ämter immer wieder an gesetzliche Grenzen. Digitalisierungsvorhaben mit ihrem agilen Vorgehen wollen schnell nutzbare Ergebnisse liefern. Gesetze anzupassen, braucht Zeit. Es passt also nicht zusammen. Es gibt keine bundesweiten Vorgaben, wie Rechtsgrundlagen für agil geführte Digitalisierungsprojekte ausgestaltet werden sollten. Daher hat die EFK schon 2021 dem Bundesamt für Justiz empfohlen, den Leitfaden für die Gesetzgebungsprojekte zu überarbeiten. Ziel sollte sein, Gesetze datenschutzkonform und technologienutral zu gestalten, und nur so viel wie notwendig bzw. so wenig wie möglich auf Gesetzesstufe zu regeln. Das Bundesamt für Justiz hat gemeldet, dass diese Empfehlung der höchsten Wichtigkeitsstufe per Ende 2023 umgesetzt wurde, 1 ½ Jahre später als ursprünglich vorgesehen. Das Bundesamt für Justiz hat in der Zwischenzeit den neuen Fachbereich Rechtsetzung in Digitalisierungsfragen implementiert. Ob damit die notwendige Wirkung entfacht wird, wird die EFK noch beurteilen.

### **Sinnfrage von Vorgaben steht nicht oben auf der Prioritätenliste**

Mit der Einführung von Microsoft 365 in der Bundesverwaltung wird unter anderem eine sog. Labelingpflicht für Office-Dokumente eingeführt, unabhängig von ihrem Speicherort (z. B. in Geschäftsverwaltungssystemen oder Dateiablagen). Dies führt zu einem Mehraufwand für die Mitarbeitenden, wie die EFK in einer Kurzanalyse 2025 festgestellt hat. Das Labeling soll vor allem festlegen, ob ein Dokument in der Public Cloud gespeichert werden darf. Da die meisten Dokumente aber in internen Systemen abgelegt sind und eine Speicherung in der Public Cloud von Microsoft daher nicht vorgesehen ist, wäre das Labeling für viele Dokumente bei ihrer Bearbeitung gar nicht nötig. Außerdem wird für das Labeling eine neue Klassifizierung eingeführt, die nicht identisch ist mit dem Informationssicherheitsgesetz bzw. der zugehörigen Verordnung, da es auch die Anforderungen des Datenschutzgesetzes abbilden soll. Trotz dieser Mängel entschieden die Verantwortlichen, den Roll-out in der Bundesverwaltung bis Oktober 2025 fortzusetzen und das Labeling erst nach Vorliegen der Bearbeitungsvorschriften zum Informationsschutzgesetz zu überarbeiten. 40 000 Mitarbeitende, die also ihre Arbeit mit neuen Labels starten und dann allenfalls umlernen müssen.

### **Neue Vorgaben, ohne sich um die Folgekosten zu kümmern**

Nicht alles, was isoliert betrachtet sinnvoll erscheint, ist auch verhältnismässig. Ein Beispiel dafür findet sich in der Verordnung zur Umsetzung des Datenschutzgesetzes, wo aufgrund eines «Swiss Finish» substantielle IKT-Mehrkosten entstehen. Die neue extensive Protokollierungspflicht in der Datenschutzverordnung Artikel 4 kostet nach bundesinternen Schätzungen einmalig rund 165 Millionen Franken, anschliessend jährlich 32 Millionen Franken – Kosten, welche in einem spürbaren Umfang vermieden werden können. Seit 2022 warnt die EFK immer wieder vor diesem Mehraufwand, der sich finanzpolitisch nicht rechtfertigen lässt. Die Hartnäckigkeit der EFK zeigt Früchte; es zeichnet sich eine Anpassung dieser Bundesratsverordnung ab, die sich hoffentlich positiv auf die Kosten auswirken wird. Aber Vorsicht: Gespert wird nicht. Es können bestenfalls Zusatzkosten vermieden werden.

### **Ein Dschungel an Vorgaben**

Bei einer Prüfung 2023 stellt die EFK fest, dass auf Stufe Bund für die Bereiche Digitalisierung und IKT eine Sammlung von rund 200 Weisungen mit unterschiedlicher Detaillierungstiefe und Zielsetzung besteht. Das Weisungswesen muss vereinfacht werden, möglichst mit dem Ziel, die Dichte der Vorgaben zu reduzieren.

## Es geht auch ohne Bundesvorgaben, zumindest eine Zeitlang

Der Einsatz von Künstlicher Intelligenz (KI) in der Verwaltung nimmt zu, beispielsweise durch Chatbots. Während die IKT-Leistungserbringer an zentralen Lösungen arbeiten, setzen Ämter bereits eigene Projekte um. Die EFK hat 21 Chatbots in der Bundesverwaltung identifiziert – meist einfache, kostengünstige Web-Anwendungen, während komplexere, sicherheitskritische Lösungen noch in Entwicklung sind. Die Umsetzungskosten liegen je nach Vorhaben zwischen 9000 Franken und 3 Millionen Franken. Die EFK hat geprüft, ob innerhalb der Bundesverwaltung Synergien erkannt und genutzt werden. Das Ergebnis: Es erfolgt auf informelle und experimentelle Art. Das Kompetenznetzwerk für künstliche Intelligenz (CNAI) wird vom Bundesamt für Statistik betrieben und soll Behörden, Forschende und Organisationen bei der effizienten und ethischen Nutzung von KI unterstützen. Es kann seinen Auftrag aber bisher nicht vollständig erfüllen. Daher verfolgen Ämter einen eigenständigen Ansatz. Die gewonnenen Erkenntnisse aus diesem pragmatischen Ansatz sollten nun konsolidiert werden, um unter anderem rasch Hilfsmittel zu rechtlichen Grundlagen, Datenschutz und Infrastruktur bereitzustellen. So kann eine effiziente Ressourcennutzung sichergestellt und Wildwuchs vermieden werden, bis eine übergeordnete Steuerung etabliert ist. Diese Hilfsmittel sind entscheidend für den erfolgreichen KI-Einsatz in der Bundesverwaltung und sollen bis Ende 2025 entwickelt werden.

## 4.4 Sicherheitsvorgaben



### Schwache Governance und unverbindliche Vorgaben beim Schutz kritischer Infrastrukturen vor Cyberangriffen

Der Schutz der kritischen Infrastrukturen (SKI) hat zum Ziel, die Verfügbarkeit von wichtigen Gütern und Dienstleistungen in der Schweiz zu gewährleisten. Ausfälle wie z. B. durch Cyberattacken sollen verhindert werden bzw. Vorfälle sollen sich möglichst wenig auf Bevölkerung und Wirtschaft auswirken, der Normalbetrieb soll so schnell wie möglich wiederhergestellt werden. SKI ist eine Gemeinschaftsaufgabe von Bund, Kantonen und Betreibern von kritischen Infrastrukturen. 2021 bemängelte die EFK, dass auf Bundesebene keine eindeutigen Verantwortlichkeiten für die jeweiligen Teilsektoren festgelegt sind und die zahlreichen Akteure eine Abstimmung erschweren. Die Zuständigkeiten für die Teilsektoren sind oftmals auf mehrere Bundesstellen verteilt.

2024 erstellte die EFK einen Synthesebericht, der die Ergebnisse von neun Einzelprüfungen zusammenführt. Das ernüchternde Ergebnis: Es muss mehr unternommen werden, um die Cybersicherheit von Informationen und Systemen zu gewährleisten. Es mangelt an effektiven Kontroll- und Steuerungsstrukturen sowie klar definierten Rollen und Verantwortlichkeiten. Die Vorgaben zum Thema Cybersicherheit sind häufig nur Empfehlungen, wie etwa der Minimalstandard zur Verbesserung der IKT-Resilienz des Bundesamtes für wirtschaftliche Landesversorgung. Diese Standards sind für Betreiber kritischer Infrastrukturen nicht verbindlich. Die Aufsicht kann meistens lediglich zur Verbesserung der Schutzmassnahmen anregen, aber oft nicht deren Umsetzung einfordern. Dies ist alarmierend, da es hier um die Sicherstellung der Versorgung der Schweiz geht – ein Bereich, in dem Versäumnisse gravierende Folgen haben können.

### Ungelöste Fragen: Wie sicher soll die Bundesverwaltung sein und was darf das kosten

Die Überwachung von Netzwerken und IKT-Systemen ist wichtig, um die Sicherheit und den reibungslosen Betrieb der Bundes-IKT zu gewährleisten. Die EFK hat im 2023 bei den fünf IKT-Leistungserbringern des Bundes überprüft, wie gut die Erkennung und Reaktion auf eingetretene Ereignisse funktionieren. Die Ergebnisse zeigen deutliche Unterschiede, und die EFK gab Empfehlungen ab, wo und wie die Sicherheit erhöht werden kann. Wie hoch das Sicherheitsniveau jedoch sein soll und wieviel Ressourcen dafür eingesetzt werden sollen, ist in der Bundesverwaltung nicht abschliessend festgelegt. Die EFK kann diese Lücke nicht füllen und sieht hier das Bundesamt für Cybersicherheit (bis Mitte 2025) bzw. das Staatssekretariat für Sicherheitspolitik gefordert. Sie sind verantwortlich, in Zusammenarbeit mit den Departementen ein kostenoptimiertes ausreichendes Sicherheitsniveau zu definieren und darauf hinzuarbeiten.

## 5 PROZESSE



### Das *Was* und *Wie* der täglichen Arbeit

Die Ebene Prozesse beschreibt alle Abläufe, die notwendig sind, damit die Verwaltung ihre Aufgaben erfüllen kann – von der direkten Leistungserbringung bis hin zu unterstützenden und steuernden Tätigkeiten. Sie gliedern sich in folgende Bereiche:

- Managementprozesse steuern und koordinieren die Verwaltung. Sie umfassen beispielsweise die Planung und Steuerung von Ressourcen, Qualitätssicherung oder die Entwicklung neuer Vorgaben.
- Hauptprozesse sind die zentralen Verwaltungsaufgaben, die direkt der Bevölkerung oder den Unternehmen dienen – etwa die Bearbeitung eines Antrags oder die Ausstellung eines Dokuments.
- Supportprozesse unterstützen die Hauptprozesse, damit die Verwaltung reibungslos arbeiten kann. Dazu gehören z. B. Finanz- und Ressourcenmanagement (inkl. IKT), Personalmanagement, Beschaffung, Immobilienbewirtschaftung oder Subventionen. Aus Lesbarkeitsgründen wurden die IKT-Supportprozesse in ein separates Kapitel genommen.
- Supportprozess IKT-Betrieb: Dazu gehören Systemwartung und-administration, Support und Helpdesk, Überwachung der Systeme und Netzwerke sowie das Sicherheitsmanagement.

### 5.1 Managementprozesse



#### Fehlende Gesamtsicht und Steuerungsdefizite im Portfoliomanagement auf Stufe Bund

Die Übersicht über die Digitalisierungsvorhaben reicht laut einer Prüfung der EFK aus dem Jahr 2022 nicht aus, um eine bundesweite Steuerung zu ermöglichen – sofern sie überhaupt angestrebt würde. Anfang 2022 waren in der zivilen Bundesverwaltung vier auf SAP basierende Portfoliomanagementanwendungen im Betrieb, daneben rund 30 unterschiedliche Anwendungen ausserhalb von SAP. Mit der Ablösung der alten SAP R/3 Umgebung durch SAP S/4HANA im Rahmen des Programms SUPERB hätte die Chance bestanden, ein bundesweit nutzbares Werkzeug für eine übergreifende Steuerung der Projekte (IKT-Cockpit, Immobilien, Organisationsprojekte und weitere) bereitzustellen. Sie wurde zum Prüfungszeitpunkt nicht ergriffen, unter anderem, weil die Nachteile einer Konsolidierung in 2022 höher gewichtet wurden als die Vorteile und weil die Bundeskanzlei keine rechtliche Kompetenz hatte, Vorgaben und Instrumente für einheitliche Führungsinformationen im Bereich des Portfoliomanagements durchzusetzen. Die EFK hatte daher empfohlen, letzteres zu ändern. Die entsprechende Empfehlung der EFK soll bis Ende 2025 umgesetzt sein. Sollte dies nicht gelingen, besteht das Risiko unverändert, dass Systemablösungen nicht gezielt erfolgen und mehrere Anwendungen für gleichartige Zielsetzungen entwickelt werden.

#### Portfoliomanagement auf Departements- und Amtsstufe mit ähnlichen Defiziten

Die EFK stellt immer wieder fest, dass es an einer Gesamtsicht der IKT-Projekte und Anwendungen zur effektiven Ressourcensteuerung fehlt. In ihren Berichten kann man dann die konkreten Auswirkungen auf die Stamm- und Projektorganisationen nachlesen, wie folgende Beispiele zeigen:

Der Dienst zur Überwachung des Post- und Fernmeldeverkehrs in der Schweiz ist dem Eidgenössischen Justiz- und Polizeidepartement zugeordnet. Er sorgt unter anderem dafür, dass Überwachungsmassnahmen zum Schutz der Privatsphäre der Bevölkerung rechtskonform durchgeführt werden. In ihrer Prüfung 2024 stellte die EFK fest, dass ein systematisches Portfoliomanagement sowie eine Ressourcen- und Budgetplanung noch fehlen. Zum Zeitpunkt der Prüfung waren unterschiedliche Technologien und Werkzeuge im Einsatz. Der Nutzen von Standardisierungen wird auch vom Dienst zur Überwachung des Post- und Fernmeldeverkehrs selbst gesehen. Auch eine Prüfung im Staatssekretariat für Migration 2024 zeigt, dass es noch keine Gesamtübersicht der Anwendungen und Projekte gibt, die eine effektive Steuerung

ermöglichen würde. Das Bundesamt für Justiz hat bisher erfolglos versucht, ein Portfoliomanagement zu etablieren. Das führte beispielsweise im Projekt zur Erneuerung des Personenstandsregisters Infostar dazu, dass man erst spät erfuhr, dass das Projekt E-ID eine Schnittstelle zu Infostar benötigt, um die Identitäten von Personen überprüfen zu können.

Das Projektportfoliomanagement im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) ist auch 2024 noch im Aufbau und nicht ausreichend entwickelt. Das bedeutet, dass die fehlende Übersicht über die Vorhaben und ihre gegenseitigen Abhängigkeiten innerhalb der Programme und Projekte kompensiert werden muss, wie die EFK in ihrem Jahresbericht 2023 nach einer Vielzahl an Einzelprüfungen schreibt. Diese Feststellung wurde auch 2024 bei weiteren Prüfungen im VBS bestätigt. Die gegenseitigen Abhängigkeiten der Topprojekte im Departement werden zwar mittlerweile in einer Matrix dargestellt, die halbjährlich aktualisiert und Teil des Controllingberichts des VBS ist. Die EFK prüfte 2024 das Schlüsselprojekt SDVN plus des Bundesamts für Bevölkerungsschutz und stellte fest, dass die Übersicht der Abhängigkeiten unvollständig ist und keine fundierte Analyse zugrunde liegt. Eine übergeordnete departementale Steuerung wird frühestens 2027 möglich sein.

Auch beim Bundesamt für Statistik bemängelte die EFK 2024 bei der Prüfung des Schlüsselprojektes Nationale Datenbewirtschaftung das fehlende Portfoliomanagement, was angesichts der Vielzahl und Relevanz der Projekte, in Kombination mit wenig klar definierten Arbeitspaketen ohne Aufwandsschätzung und der sehr engen Ressourcensituation als kritisch zu bewerten ist. Im Bundesamt für Zoll und Grenz sicherheit kann die Strategie zur Bereinigung des Betriebsimmobilienportfolios per 2024 nicht umgesetzt werden, da Daten für die Priorisierung fehlen bzw. unzuverlässig sind. Da die finanziellen Mittel noch nicht genehmigt sind, hat das Amt noch die Gelegenheit zu Verbesserungen.

### Defizite bei der strategischen Steuerung der IKT-Beschaffungen der Bundesverwaltung

Je nach Auftragsvolumen (sog. WTO-Schwellenwerte) müssen **öffentliche Aufträge international ausgeschrieben** werden. Im Jahr 2023 hat die Bundesverwaltung gemäss Reporting Set Beschaffungscontrolling<sup>7</sup> Leistungen im Wert von 6,39 Milliarden Franken über diesem Schwellenwert beschafft; der Anteil, der auf IKT entfällt, ist nicht publiziert. Der Bundesrat beschloss 2020 die Umsetzungsstrategie zur Totalrevision des öffentlichen Beschaffungsrechts für die Strategieperiode 2021–2030. Ziel ist unter anderem, die bundeseigenen Beschaffungen strategisch über sechs Stossrichtungen zu steuern und das Beschaffungscontrolling zu reformieren.

Veränderungen wie die Ablösung von SAP R/3 durch die Nachfolgelösung SAP S/4HANA bieten hier Chancen. Neben Effizienzgewinnen erhofft man sich vor allem Informationen für die strategische Steuerung und Führungsunterstützung bei Beschaffungen. Welche Daten für diese Steuerung benötigt werden (z. B. zu Innovation, Qualität, Nachhaltigkeit), war bei der EFK-Prüfung 2021 unbekannt. Ebenso war offen, ob und wie zentrale Prozessteile für zivile und militärische Beschaffungen gleichermaßen gelten sollten.

## 5.2 Hauptprozesse



Der Synthesebericht der EFK zu den Vorhaben der Digitalen Transformation aus 2023 gibt einen profunden Einblick in die typischen Stolperfällen und Erfolgsfaktoren bei der Entwicklung nutzerorientierter, medienbruchfreier Abläufe vom Anfang bis zum Ende eines Geschäftsprozesses.

### Stiefkind automatisierte Kontrollen

In diversen EFK-Berichten findet sich ein wiederkehrendes Thema, den geringen Appetit auf Automatisierung zur Vermeidung und Bekämpfung von Fehlern oder Betrug. Hierzu einige Beispiele: Bei der Erwerbsersatzordnung werden nach 600 000 Anträgen jährlich Entschädigungen in Höhe von fast 700 Millionen Franken bezahlt. Mit der geplanten Digitalisierung plant das Bundesamt für Sozialversicherungen

<sup>7</sup> Reporting Set Beschaffungscontrolling Bundesverwaltung 2023

Einsparungen von rund 6 Millionen Franken pro Jahr für Unternehmen und Ausgleichskassen. 2024 stellte die EFK fest, dass es kein Konzept gibt für ein effizientes automatisiertes Kontrollsysteem zur Vermeidung von Fehlern oder Betrug. Die Potenziale der Digitalisierung werden damit nicht ausgeschöpft.

Im Bereich der Arbeitslosenversicherung gab es durchaus Pläne für automatisierte Missbrauchskontrollen. Aufgrund von Verzögerungen bei der Ablösung des alten Auszahlungssystems für Arbeitslosengelder (ASAL) wurden diese jedoch vorerst auf Eis gelegt, sollen aber zu einem späteren Zeitpunkt implementiert werden. Auch wenn kompensierende Kontrollen vorgesehen sind: Ohne automatisierte Kontrolle bleibt vorerst die Wahrscheinlichkeit hoch, dass ungerechtfertigt bezogene Gelder noch eine Weile unentdeckt bleiben.

Das Bundesamt für Zoll und Grenzsicherheit (BAZG) arbeitet an einer Anwendung, um die Verfahren des Warenverkehrs an der Grenze zu vereinfachen und zu beschleunigen. Mit der Einfuhr nimmt das Amt im Schnitt jährlich rund 13 Milliarden Franken Mehrwertsteuer ein. Die Kontrollen über dieses Massengeschäft werden zwar überarbeitet, allerdings nicht früh genug, um automatisierte Kontrollen rechtzeitig identifizieren und implementieren zu können.

Auch im Projekt eSubventionen im Eidgenössischen Departement des Inneren werden Möglichkeiten wie z. B. automatisierte Vollständigkeitsprüfungen der eingehenden Gesuche nicht genutzt.

### **Digitalisierungsstau hält Papierprozesse am Leben**

Eine langsame Digitalisierung und das Fehlen durchgängiger elektronischer Unterstützung führen dazu, dass zentrale Bereiche der Sozialversicherung weiterhin auf ineffiziente und fehleranfällige papierbasierte Verfahren setzen. Im Bereich der Invalidenversicherung werden jährlich rund 1,6 Millionen Leistungsrechnungen bearbeitet – 2017 rund 70 Prozent davon auf Papier. Damals stellte die EFK fest, dass den IV-Stellen keine Werkzeuge zur automatisierten Verarbeitung zur Verfügung stehen und bestehenden Möglichkeiten bei der zuständigen Bundesbehörde nicht genutzt werden. Fortschritte werden erzielt, die Umsetzung der entsprechenden Empfehlung verzögert sich allerdings seit Jahren; neuer Termin ist Ende 2025.

Auch in der Arbeitslosenversicherung bleiben papierbasierte Verfahren dominierend. Trotz vorhandener Onlinedienste (e-Services) für Kurzarbeitsentschädigungen nutzen nur rund 20 Prozent der Unternehmen diese Möglichkeit. Die Entwicklung weiterer e-Services für weitere Leistungen wie Arbeitslosen-, Insolvenz- und Schlechtwetterentschädigung wurde zurückgestellt. Seit Jahren wird ein neues System zur Auszahlung der Arbeitslosengelder entwickelt. Nach Intervention der EFK 2021 sollen beide Vorhaben – e-Services und Auszahlungssystem – wo möglich koordiniert bis Ende 2025 eingeführt werden.

Im Bereich der Erwerbsersatzordnung sollen trotz digitalisiertem Prozess Zahlungsbestätigung per Brief verschickt werden. Allein die Portokosten belaufen sich auf eine halbe Million Franken pro Jahr.

In der Eidgenössischen Steuerverwaltung (ESTV) ist bei der Digitalisierung seiner Hauptprozesse weit fortgeschritten. Allerdings ist der Digitalisierungsgrad bei der Erhebung der Verrechnungssteuer (Bruttoeinnahmen 38,1 Mrd. Franken) ernüchternd. Die EFK hat 2018, 2021 und 2024 auf Digitalisierungsmöglichkeiten in diesem Bereich hingewiesen. Wichtige Erhebungsdeklarationen können von den Steuerpflichtigen weiterhin nicht digital bei der ESTV eingereicht werden.

## **5.3 Supportprozesse Beschaffung, Finanzen, Personal, Immobilien und Subventionen**



### **Beschaffung: Keine Standardisierung und kein nachgewiesener Nutzen der dualen Lösungen**

Die Beschaffungsstrategie 2020 gibt vor, die Prozesse zu digitalisieren, zu standardisieren und benutzerfreundlicher zu gestalten. Der Bund setzt dabei auf zwei Anwendungen: SAP, das bundesweit verbindlich ist, aber erst ab der Vertragsunterzeichnung genutzt wird, und Acta Nova, das den vorangehenden Beschaffungsprozess abdeckt und teilweise optional ist.

Bei ihrer Prüfung 2024 stellt die EFK fest, dass der Nachweis für einen messbaren Nutzen der Acta Nova Anwendung fehlt. Zudem wird die angestrebte Standardisierung der Beschaffungsprozesse in der Bundesverwaltung verfehlt. Die Schnittstellen zwischen den beiden Systemen für einen durchgängigen, medienbruchfreien Prozess vom Bedarf bis zum Vertragsende sind nicht definiert. Die EFK fordert, dass die Notwendigkeit und der Nutzen der dualen Lösung nachgewiesen werden muss.

Die bisherige Vertragsmanagementlösung in SAP kann nicht wie geplant per Ende 2025 ausser Betrieb gesetzt werden. Sie wird bis voraussichtlich Ende 2027 weiter betrieben. In der Folge werden zwei SAP-Systeme parallel geführt. Dies führt zu zusätzlichen Betriebskosten von schätzungsweise einer Million Franken pro Jahr. Eine Ursache dafür liegt auch in den Diskussionen, vom Standard zugunsten amtsspezifischer Bedürfnisse abzuweichen. Die EFK spricht sich ausdrücklich dagegen aus; genau diese individuellen Ausprägungen wollte man in der Verwaltung mit der Einführung von SAP S/4HANA bereinigen.

### **Sichere Logistiklösung für Armee frühestens 2030 mit millionenschweren Folgekosten**

Es liegt nahe, dass zivile und militärische Bereiche der Bundesverwaltung wo möglich dieselben Systeme nutzen wollen. Diese gemeinsame Nutzung stösst an ihre Grenzen, sobald es um konkrete Einsatzfälle für das Militär geht. In einsatzkritischen Situationen besteht die Verteidigung auf eine autonom funktionierende Logistik, also auch wenn die zivilen Systeme ausfallen. Laut einer Botschaft aus 2018 sind daher zwei separate SAP-Systemlandschaften erforderlich, da die Armee im Ernstfall auf ein besonders abgesichertes, autonom funktionierendes System angewiesen sei. Der Architekturentscheid dazu war 2019 bei der ersten Prüfung der EFK nicht getroffen. Zwei Prüfungen später 2024 steht der Entscheid für eine auftarke Lösung noch immer aus, und der Plan einer Lösung mit SAP wird aus technischen Gründen nicht weiterverfolgt. Das VBS schätzt, dass eine einsatzkritische Logistiklösung frühestens 2030 bereitstehen wird. Die Kosten werden im hohen zweistelligen Millionenbereich geschätzt. Die Information an den Bundesrat und das Parlament ist im Rahmen der Botschaft zum Rüstungskredit 2027 geplant.

Bei den Immobilien scheint das Ziel der Nutzung von gemeinsamen Funktionalitäten realistischer zu sein: Im Bericht aus 2022 kommt die EFK zum Ergebnis, dass zumindest auf konzeptioneller Ebene an der Standardisierung und Nutzung gemeinsamer Prozesse z. B. für das Flächenmanagement, das Erhaltungsmanagement und die Kollaborationsplattform, gut gearbeitet wird. Über die Umsetzung kann die EFK noch kein Urteil abgeben.

### **SUPERB: Zugesagte Einsparungen von mehr als 400 Millionen Franken sind ungewiss**

Die Ablösung von SAP R/3 mit SAP S/4HANA beschäftigt die Bundesverwaltung und die EFK schon seit Jahren. Die externen Kosten des Programms SUPERB (ziviler Bereich) für die Jahre 2020-2027 werden auf rund 420 Millionen Franken und die Gesamtkosten des Programms ERP Systeme V/ar (VBS) auf rund 360 Millionen Franken geschätzt<sup>8</sup>. 2020 hat der Bundesrat dem Parlament in Aussicht gestellt, mit den beiden Ablösevorhaben im zivilen und militärischen Bereich langfristige Einsparungen in der Höhe von mehr als 400 Millionen Franken zu erzielen. Der EFK-Bericht aus 2024 zeigt, dass die angekündigten Einsparpotenziale von den Departementen und Verwaltungseinheiten noch nicht bestätigt sind. Bereits eingeführte Prozesse führen teilweise zu erheblichem Mehraufwand. Es bestehen daher Zweifel, ob die gewünschten Einsparungen als kausale Folge des Systemwechsels tatsächlich erreicht werden können. Zudem wird erwartet, dass die Betriebskosten laut Schätzungen des IKT-Leistungserbringers stark ansteigen. Die geplanten Einsparungen könnten also durch diese höheren Kosten aufgezehrt werden. Sehr positiv hervorzuheben ist jedoch, dass der Technologiewechsel im zivilen Bereich erfolgreich abgeschlossen wurde. Ausserdem beaufsichtigen die Finanzkommissionen der Eidg. Räte die Entwicklung der Einsparungen sehr eng.

---

<sup>8</sup> Bundesamt für Bauten und Logistik: Programm «SUPERB»

## Subventionen: Der «organische» Ansatz bremst die Wirksamkeit einer zentralen Lösung

Knapp 60 % des Bundeshaushalts, d. h. rund 50 Mia. Franken jährlich, werden als Subventionen ausgezahlt. Trotz der zentralen Bedeutung des Subventionsprozesses verwenden die subventionsgebenden Verwaltungseinheiten eigene Anwendungen zur Bearbeitung der Subventionsgesuche. Eine dieser Anwendungen im Eidgenössischen Departement des Innern (EDI) muss bis Ende März 2025 ersetzt werden. Dies bietet eine Chance, eine Lösung für die gesamte Bundesverwaltung zu entwickeln. Der Bundesrat hat dem EDI daher den Auftrag erteilt, bis Ende 2025 ein Konzept für die Ausrollung der Lösung eSubventionen vorzulegen. Die EFK hat dieses Projekt 2024 geprüft. Der Ansatz erscheint zunächst vielversprechend: Statt eines grossen, bundesweiten Projekts wird eine kleinere, optimierte Anwendungsentwicklung angestrebt. Ob mit der Ausrollung auch eine verbindliche Nutzung für alle subventionsgebenden Verwaltungseinheiten einhergehen wird, war zum Prüfungszeitpunkt offen. Um das Effizienzsteigerungspotenzial bei der Vergabe von Subventionen vollständig zu nutzen, müssten die bereits mitwirkenden Verwaltungseinheiten ihre Prozesse und Daten jetzt schon anpassen. Ein verbindlicher Auftrag dazu fehlt. Zudem gibt es Widerstand gegen Automatisierungen: Es gäbe Möglichkeiten zur Verbesserung, etwa durch die automatisierte Vollständigkeitsprüfung der eingehenden Gesuche. Bekannte Schwächen der Subventionsvergabe werden nicht angegangen, wie z. B. die vertiefte Prüfung der Eigenleistungen der Subventionsempfänger oder das Vermeiden von Mitnahmeeffekten. Auch Elemente der vorgeschriebenen periodischen Subventionsüberprüfung, wie etwa eine Risikoanalyse über die Subventionsempfänger, werden nicht berücksichtigt. Die Entwicklung und Einführung eines späteren Bundestools überschreiten organisatorisch und finanziell die Fähigkeiten des Departments, was es auch in seiner Stellungnahme im EFK-Bericht zum Ausdruck bringt. Zudem ist ein wirtschaftlicher Nutzen dieser einheitlichen Lösung wünschenswert, aber noch nicht nachgewiesen.

## 5.4 Supportprozess IKT-Betrieb



### IKT-Betriebskosten als unscharfer Fleck auf der Kostenlandkarte

Den erhofften Einsparungen, die normalerweise mit der Digitalisierung von Geschäftsprozessen einhergehen, stehen häufig steigende Kosten für Weiterentwicklungen und Betrieb gegenüber. In ihren Prüfungen hat die EFK wiederholt festgestellt, dass Betriebskosten unterschätzt, nicht erhoben oder ausgewiesen wurden, oder dass die erwarteten Kostensenkungen nicht erreicht werden. Dies war Anlass für die EFK, 2024 in einer Prüfung den Auswirkungen von Digitalisierungsvorhaben auf die IKT-Betriebskosten nachzugehen. Sie konzentrierte sich dabei auf neun konkrete Fallbeispiele bei den Bundesämtern für Sozialversicherung, Gesundheit und Strassen sowie der Eidgenössischen Steuerverwaltung.

Die steigenden IKT-Betriebskosten hängen meist mit Anpassungen der technischen Infrastruktur und dem zunehmenden Datenvolumen zusammen. Weitere Kostentreiber sind Legacy-Systeme, also veraltete Systeme, die noch genutzt werden. Im ersten Quartal 2025 soll ein Lösungsvorschlag für die Ablösungen und einen verbindlichen Migrationsplan vorliegen. Teurer wird es auch, wenn alte und neue Systeme parallel längere Zeit weiterbetrieben werden müssen, z. B. wenn es zu Verzögerungen bei der Einführung der neuen Systeme kommt.

Dass Weiterentwicklungen von IKT-Systemen und neue Digitalisierungsprojekte erhebliche Auswirkungen auf diese Kosten haben, berücksichtigen die Ämter und Departemente oft nicht ausreichend. Es fehlt an Transparenz bei der Planung. Häufig werden die voraussichtlichen Betriebskosten nicht abgeschätzt, und es gibt keine bundesweiten Vorgaben, wie diese Schätzungen erfolgen sollen. Wenn Botschaften verfasst werden, müssten detaillierte Angaben zu den Mehr- oder Minderkosten für den Bund gemacht werden. Die EFK stellt fest, dass diese Angaben häufig fehlen, was dem Parlament wichtige Informationen zur Beurteilung neuer Digitalisierungsprojekte vorenthält.

2024 nimmt die EFK beim Staatsekretariat für Migration zur Kenntnis, dass die Gesamtkosten für das Projekt zur Ablösung von ZEMIS (zentrales Migrationsinformationssystem der Schweiz) von den geplanten 65,9 Millionen Franken in 2022 auf mittlerweile 193 Millionen geschätzt werden. Ausserdem hat der Bundesrat das Kostensenkungsziel angepasst. Einsparungen von 15 bis 20 Prozent seien nicht mehr realistisch.

Betriebskosten wirken sich auch ausserhalb des Bundes aus: Für die ZEMIS-Nutzung werden Gebühren erhoben. Da diese generell auf dem Kostendeckungsprinzip basieren, wird es also vermutlich nicht günstiger für die Kunden.

Eine weitere Ursache ist der fehlende Fokus auf die IKT-Kosten über den gesamten Lebenszyklus bei Beschaffungen: Ohne entsprechende Forderung bereits in der Ausschreibung haben die Lieferanten kaum Anreiz, in ihren Angeboten die gesamten Lebenszykluskosten offenzulegen oder klar zwischen Investitions- und Betriebskosten zu unterscheiden. In der Regel werden nur die Investitionskosten offeriert und verhandelt. Fallen die Verhandlungsergebnisse aus Sicht des Lieferanten zu tief aus, kann er diese später kompensieren – etwa durch höhere laufende Lizenzkosten.

### **Anwendungen sind fertig, die Organisation ist es nicht**

Der Dienst zur Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF) des EJPD ist für die technische Unterstützung der Strafverfolgungsbehörden bei der Durchführung von Fernmeldeüberwachungsmaßnahmen zuständig. Um die Anwendung selbst zu betreiben und weiterzuentwickeln, muss sich der Dienst ÜPF neu aufstellen, wofür er 2022 eine Reorganisation lancierte und 12 zusätzliche Stellen besetzte. 2023 stellt die EFK fest, dass die Reorganisation nur schleppend voranschreitet. Da die Teams, die die Anwendungsweiterentwicklung übernehmen sollen, noch nicht gebildet waren, mussten auslaufende Verträge mit einigen externen Mitarbeitenden bis Mitte bzw. Ende 2024 verlängert werden.

Ein weiteres Beispiel findet sich im Bundesamt für Zoll und Grenzsicherheit, das seine Teilnetze im Grenzgürtel der Schweiz auf Polycom umstellt. Polycom ist das sichere Kommunikationsnetz in der Schweiz, das von Blaulichtorganisationen wie Polizei, Feuerwehr und Rettungsdiensten genutzt wird. Bei ihrer Prüfung stellt die EFK 2023 fest, dass das Projekt bei hohem Tempo solide geführt wird, und die geplante Erneuerung der Infrastruktur in greifbarer Nähe ist. Die Schattenseite ist, dass der hohe Migrationsdruck Arbeiten zugunsten der Betriebsübergabe in den Hintergrund drängte. Wichtige Grundlagen, um die Sicherheit und den späteren Betrieb zu gewährleisten, sind in Rückstand geraten und noch zu wenig ausgereift. Dies ist riskant, da die neue Technologie bereits im Einsatz ist und ein kritisches Funksystem unterstützt, das auch in Notfällen funktionieren muss.

### **Sicherheitsrisiken als Auswirkungen agiler Entwicklungsmethoden**

Im klassischen Softwareentwicklungsmodell erfolgen Releases in grossen, seltenen Abständen. Im agilen Umfeld hingegen werden Releases in kurzen Zyklen geplant, so dass neue Funktionen schrittweise und schnell ausgeliefert werden können. Dies hat jedoch Auswirkungen auf die Testvorgehen: Während im klassischen Modell umfangreiche Testphasen am Ende einer (Weiter-)Entwicklung vorgesehen sind, erfordert die agile Entwicklung kontinuierliches Testen unter Zeitdruck. Die Tests müssen automatisiert, schnell und zuverlässig sein, was hohe Anforderungen an Testabdeckung, Testdaten, Infrastruktur und Teamkoordination stellt. Ob das beim Bundesamt für Informatik und Technologie funktioniert, hat die EFK 2024 geprüft. Sie stellte fest, dass die automatisierten Tests die Einhaltung des IKT-Grundschutzes abdecken; anwendungsspezifische Tests müssen – wenn überhaupt vorgesehen – noch immer über manuelle Schritte durchgeführt werden. Außerdem können obligatorische Testschritte von den Entwicklern deaktiviert werden. Konsequenz: Anwendungen können mit unvollständigen Tests produktiv gesetzt werden. Die EFK Empfehlung hat das Amt mittlerweile als umgesetzt gemeldet.

### **IKT-Sicherheit leidet unter isolierten Strukturen**

Laut der EFK-Prüfung 2024 sind die fünf IKT-Leistungserbringer der Bundesverwaltung für die System- und Netzwerküberwachung gut aufgestellt. Sie setzen rund um die Uhr Überwachungswerzeuge ein, die bei Bedarf Alarm auslösen. Notfallteams übernehmen erste Massnahmen. Allerdings steht keine permanente Analysekapazität zur Verfügung, um Angriffe bzw. Anomalien sofort auszuwerten. Bisher kann dies nur der militärische Bereich zeitweise mit Milizpersonal sicherstellen. Angesichts der weltweiten Vernetzung der Bundesverwaltung, wie zum Beispiel im Eidgenössisches Departement für auswärtige Angelegenheiten, wäre eine solche Überwachung jedoch auch im zivilen Bereich wichtig. Die IKT-Leistungserbringer geben an, dass sie dies wegen Personalmangel nicht allein leisten könnten. Die EFK empfiehlt daher,

Ressourcen in eine zentrale Überwachung zu bündeln oder enger zusammenzuarbeiten, um eine ständige Sicherheitsüberwachung zu ermöglichen.

#### **Unbeliebt und aufwändig, aber notwendig: End-to-end Wiederherstellungstest**

Der Zweck von Wiederherstellungstests ist es sicherzustellen, dass die Verwaltung nach einem Ausfall tatsächlich weiterarbeiten kann – nicht nur auf technischer, sondern auch auf operativer Ebene. Wie die EFK bei zehn Prüfungen von teilweise sehr wichtiger Systemen und Anwendungen feststellen muss, sind technische Wiederherstellungstests meist vorgesehen und finden statt, aber entweder zu selten oder ohne die betroffenen Geschäftsprozesse zu berücksichtigen. Ein End-to-End-Test betrachtet den gesamten Wiederherstellungsprozess und stellt sicher, dass nicht nur einzelne Netzwerke, Systeme oder Anwendungen, sondern die gesamte betroffene Organisation handlungsfähig bleibt. Dazu gehört die Einbindung der relevanten Abteilungen, die Überprüfung von Datenintegrität, Abhängigkeiten und Zugriffsrechten sowie die Sicherstellung, dass zeitkritische Prozesse gesetzliche und vertragliche Vorgaben erfüllen. Nur durch solche umfassenden Tests lässt sich gewährleisten, dass kritische Teile der Verwaltung nach einem Ausfall rasch wieder uneingeschränkt funktionsfähig sind. Ein gutes Gegenbeispiel findet sich bei den umfassend durchgeführten Notfalltests der Private Cloud Lösung des EJPD.

#### **IKT-Kontrollen bei den finanzrelevanten Systemen beim IKT-Leistungserbringer sind gut**

IT General Controls (ITGC) sind **grundlegende IKT-Kontrollen**, die die **Zuverlässigkeit, Verfügbarkeit und Integrität** von IT-Systemen und Daten sicherstellen, unabhängig von einzelnen Anwendungen. Ohne sie könnten Daten manipuliert, unberechtigt abgerufen oder durch Fehler und ineffiziente Prozesse gefährdet werden. ITGC umfassen insbesondere das Zugriffsrecht- und Änderungsmanagement sowie Kontrollen des IKT-Betriebs. Die EFK prüft jährlich die Jahresrechnung des Bundes, wobei auch die ITGC der finanzrelevanten Anwendungen beim Bundesamt für Informatik und Technologie validiert werden. In jüngster Zeit wurden dabei keine wesentlichen Schwachstellen festgestellt und die EFK konnte ein gutes Zeugnis ausstellen.

## 6 DATEN UND INFORMATIONSMANAGEMENT



### Die richtigen Daten am richtigen Ort

Diese Ebene sorgt dafür, dass alle wichtigen Informationen in der Organisation gut strukturiert, sicher und zuverlässig verfügbar sind. Daten sind die Grundlage für Entscheidungen und Abläufe und müssen daher gut organisiert und geschützt sein. Dazu gehören Elemente wie

- Datenflüsse und -qualität: Wie Daten gesammelt, gespeichert und genutzt werden und ob sie korrekt und aktuell sind.
- Datenschutz und Zugriffskontrollen: Wer auf welche Daten zugreifen darf und wie sensible Informationen geschützt werden.
- Datenarchitektur und Taxonomie: Eine klare Struktur und einheitliche Begriffe (Taxonomie) helfen, Daten effizient auszutauschen und zu nutzen.
- Stammdaten: Wichtige Basisdaten (z. B. Einwohner- oder Unternehmensdaten), die in vielen Prozessen gebraucht werden.

### 6.1 Datenflüsse und Datenqualität



#### Entscheide brauchen Vertrauen, Vertrauen braucht saubere Daten

Schlechte Datenqualität ist eine Tatsache, die die EFK immer wieder in ihren Berichten festhalten muss. Dies trifft häufig dann zu, wenn die Datenpflege dezentral von vielen unterschiedlichen Einheiten erfolgt, keine bzw. nur wenige automatisierte Kontrollen Fehler und unfeasible Eingaben verhindern und die nachgelagerte Qualitätssicherung keine ausreichenden Instrumente hat, um allfällige Korrekturen durchzusetzen. Beispiele finden sich beim Personenregister für ausländische Staatsangehörige ZEMIS, beim Handelsregister, im Grundbuchwesen (vor allem im Bereich der Langzeitsicherung), bei den Objektdaten zu den Betriebsimmobilien des Bundesamtes für Zoll und Grenzsicherheit oder dem bundesinternen Cockpit IKT. Datenpflege ist aufwändig und ein fortlaufender Prozess. Die Alternativen sind allerdings verzögerte oder nicht belastbare Entscheide, die auf falschen oder fehlerhaften Daten basieren und mehr Schaden anrichten können, als die Datenpflege kosten würde.

### 6.2 Datenschutz und Zugriffskontrollen



#### Sicherheitslücken durch fehlende Eskalationswege und verzögerte Massnahmen

Die Überwachung von Netzwerken und IKT-Systemen ist wichtig, um die Sicherheit und den reibungslosen Geschäftsbetrieb zu gewährleisten. Eine Prüfung bei den fünf IKT-Leistungserbringern des Bundes im Jahr 2024 zeigt, dass Sicherheitslücken in Anwendungen von den Leistungserbringern in der Regel schnell erkannt und adressiert werden. Allerdings müssen oft auch die Leistungsbezüger und mögliche externe Lieferanten rasch Massnahmen ergreifen. Beispielsweise können Anpassungen an Komponenten erforderlich sein, die von externen Firmen im Auftrag der Leistungsbezüger entwickelt wurden. In solchen Fällen müssen diese die Arbeiten in Auftrag geben. Dies wird teilweise nicht oder nicht rechtzeitig erledigt. Die meisten IKT-Leistungserbringer hatten keine Weisungsbefugnis, um diese Massnahmen durchzusetzen bzw. unzureichend gewartete Systeme einfach abzuschalten. Das führte unweigerlich dazu, dass Sicherheitslücken über längere Zeit bestehen blieben.

## Bei Cybervorfällen sind die Meldewege zu langsam

Die Fachstelle IKT-Sicherheit des Bundes des VBS hat 2022 Vorgaben zur Cybersicherheit innerhalb der Bundesverwaltung erlassen, deren Einhaltung überprüft und die Verwaltungseinheiten bei der Beseitigung von Schwachstellen unterstützt<sup>9</sup>. 2022 fasste die EFK zusammen, wie gut der Bund auf konkrete Cybervorfälle innerhalb der Verwaltung reagiert. Bei einem Vorfall ist ein schneller Informationsfluss von der Quelle zum BACS, sowie rasche Massnahmen und Information zu den relevanten Stellen essenziell.

Wenn es um die sofortige Meldung geht, stimmt das damalige Ergebnis nicht zuversichtlich. In zwei untersuchten Fällen dauerte es einmal 13, einmal 11 Tage von der Entdeckung des Vorfalls bis zur Meldung an das BACS. Das ist eine kleine Ewigkeit, wenn es um Cyberangriffe geht. Auch die Meldung des BACS an das Netzwerk der Informationssicherheitsbeauftragten erfolgte zu spät – sie ist erst nach dem Abschluss des Cybervorfalls vorgesehen. Bei diesen Vorfällen muss die Kommunikation nicht nur mit den Betroffenen transparent und schnell sein, sondern auch mit denen, für die ein Vorfall auch ohne direkte Betroffenheit relevant ist. Erfreulich: Mittlerweile wurden und werden diverse Weisungen überarbeitet, und seit 1. April 2025 gilt eine sofortige Meldepflicht bei Cybervorfällen. Ausserdem konnte die EFK dem BACS gute Noten ausstellen, wenn es um die Prozesse zur inhaltlichen Bewältigung eines Vorfalls geht. Generell hat sich in diesem Bereich in den letzten 12 Monaten viel verändert, nicht nur seit der Schaffung des Staatssekretariats für Sicherheitspolitik SEPOS im VBS.

## 6.3 Datenarchitektur und Taxonomie



### Die Nationale Datenbewirtschaftung: Ein ehrgeiziges Ziel mit stumpfen Instrumenten

Unternehmen und Personen müssen ihre Daten an verschiedene Behörden auf allen föderalen Ebenen übermitteln. Das kann zu problematischen Mehrfacherfassungen und inkonsistenten Daten führen. Daher beauftragte der Bundesrat bereits 2019 und 2020 das Bundesamt für Statistik (BFS), Lösungen zu entwickeln. Ziel des Programms Nationale Datenbewirtschaftung (NaDB) ist es, mit einem Metadatenkatalog Transparenz über vorhandene Daten in der Verwaltung zu schaffen und die Mehrfacherfassung zu vermeiden (sog. Once-Only-Prinzip). Das BFS bietet sozusagen eine «Suchmaschine» an, um vor der Erhebung neuer Daten zu prüfen, ob und in welcher Struktur die benötigten Informationen bereits bei einer anderen Behörde vorliegen. Das bedeutet jedoch nicht, dass die Daten einfach geteilt werden können, aber es bietet einen ersten Anhaltspunkt.

Dieses ehrgeizige Unterfangen, das auch die Rolle des BFS grundlegend verändert, hat ein Preisschild: 23,8 Millionen Franken für 2020 bis 2023. Erstaunlich ist dabei der Anspruch, dass das BFS Aufwand und Ausgaben intern kompensieren muss, trotz des nationalen Nutzen von diesem Vorhaben. Daher überrascht es nicht, dass die EFK bei der Prüfung 2021 eine Finanzierungslücke von etwa 15 Millionen Franken zur Kenntnis nehmen musste.

Bei der Folgeprüfung 2024 konstatiert die EFK schleppende Fortschritte bei der Harmonisierung und Standardisierung der Verwaltungsdaten. Die Verantwortung pro definiertem Themengebiet liegt dafür bei den Dateneigentümern in der Verwaltung. Das BFS kann lediglich koordinieren und hat keinerlei Mittel, die Arbeiten zu forcieren. Ausserdem kann es nur dabei unterstützen, dass die Daten inhaltlich gleich verstanden werden (sog. **semantische Interoperabilität**). Fragen der rechtlichen, organisatorischen und technischen Fähigkeiten, reibungslos Daten auszutauschen und gemeinsam zu nutzen, sind hingegen bei der Bundeskanzlei angesiedelt.

---

<sup>9</sup> Eidg. Finanzverwaltung: Staatsrechnung 2022, Band 1A

## Swisstopo: Fehlende Ausrichtung an der Geoinformationsstrategie

Geodaten sind in der Schweiz unerlässlich für Raumplanung, Umweltschutz, Verkehr, Landwirtschaft, Eigentumsfragen und Forschung. Die Verwaltungseinheiten des Bundes stellen ihre Geodaten auf der Plattform map.geo.admin.ch kostenlos zur Verfügung, die Kantone betreiben die Plattform geodienste.ch. Diese Plattformen sollen gemäss der Strategie Geoinformation vom 2020 inklusive Standards (Metadaten, Geo-Basisdaten) und Verfahren langfristig zu einer Nationalen Geodateninfrastruktur weiterentwickelt werden. Zum Zeitpunkt der EFK Prüfung 2023 bei swisstopo war eine Roadmap dafür in Erarbeitung. Swisstopo arbeitet an einer neuen Produktionsplattform, die von den strategischen Entwicklungen im Geodatenbereich beeinflusst werden wird. Eine Abstimmung der Ziele, die Nutzung allfälliger Synergiepotenziale oder die Vermeidung von Doppelspurigkeiten mit anderen Vorhaben und Strategien fehlte. Bei der Folgeprüfung 2024 konnte die EFK zwar Verbesserungen feststellen, allerdings besteht unverändert deutlicher Handlungsbedarf.

## Digitale Transformation basiert auf Daten, nicht auf Abläufen

Bei der digitalen Transformation gewinnen die Daten an Bedeutung. Daten bestimmen, was möglich ist. Prozesse legen fest, wie das Potenzial genutzt wird. Prozesse müssen sich auf verlässliche, strukturierte Daten abstützen können. Dieses Prinzip ist noch nicht überall berücksichtigt. Beispiel hierfür ist das Zentrale Migrationsformationssystem (ZEMIS), das Personenregister zu ausländischen Staatsangehörigen in der Schweiz, das erneuert werden muss. Mit mehr als zehn Millionen Datensätzen ist es ein Hauptarbeitsinstrument des Staatssekretariats für Migration. In einer Vorstudie ist von diversen Defiziten bei den Daten die Rede, insbesondere Silo-Strukturen, Redundanzen, unnötige Felder sowie mangelnde Datenqualität. Das Datenmodell wurde über die letzten 15 Jahre wiederholt um- und ausgebaut, seine Wartung wird immer schwieriger. Ziel ist es unter anderem, Abfragen künftig bis zu 50 % schneller zu beantworten und dies trotz steigendem Datenvolumen. Dafür wäre eine frühzeitige Bereinigung der Datenstruktur nötig. Diese ist jedoch erst vorgesehen, nachdem die Prozesse definiert wurden – aus Sicht der EFK zu spät.

## 6.4 Stammdaten



### Die gemeinsame Stammdatenverwaltung für Geschäftspartner des Bundes bleibt Wunschdenken

Im Dezember 2018 hat der Bundesrat die Strategie zur Entwicklung der gemeinsamen Stammdatenverwaltung des Bundes verabschiedet. Im Rahmen der Umstellung auf SAP S/4HANA für Beschaffung, Finanzen, Immobilien und Personal sollten die Stammdaten der Unternehmen als «Geschäftspartner» der Bundesverwaltung zentral geführt werden. Eine Prüfung der EFK 2021 zeigte erheblichen Klärungsbedarf, um die gemeinsame Stammdatenverwaltung voranzutreiben.

Mit der Einführung von SAP S/4HANA wird die zentrale Verwaltung der Stammdaten der Geschäftspartner durch das «Master Data Government» zwingend. Diese Umstellung betrifft nicht nur SAP, sondern wirkt sich auch erheblich auf Fachanwendungen und die von ihnen unterstützten Geschäftsprozesse aus. Die Verwaltungseinheiten müssten die Bewirtschaftung der Stammdaten der Geschäftspartner neugestalten, Fachanwendungen und Schnittstellen anpassen sowie Daten bereinigen und migrieren. Diesen Aufwand hat die Verwaltung vorerst vermieden, indem die Idee der zentralen Stammdaten nur für die Supportprozesse und nur auf SAP beschränkt verfolgt wurde. Konkret: Selbst, wenn eine Fachanwendung auf SAP läuft, muss sie momentan nicht die zentralen SAP Stammdaten von Geschäftspartnern verwenden. So ent- bzw. bestehen Parallel-Datenbestände, was wiederum zu Mehrkosten, hohe Komplexität und redundante fehleranfälliger Prozesse führen kann. Zudem fehlen grundlegende Elemente, die eigentlich selbstverständlich sein sollten. So hat die EFK bereits 2020 darauf hingewiesen, dass es für das Master Data Government eine eindeutige Identifikation für natürliche Personen braucht, ähnlich wie die UID für Unternehmen. Bei der EFK-Nachprüfung 2024 fehlt sie noch immer.

Zum Prüfungszeitpunkt standen ein paar Grundsatzentscheide bei den Stammdaten an, andere Aktivitäten wurden im Sinne der EFK-Empfehlungen initiiert. Dennoch war das Ergebnis wenig überraschend,

dass die Bundesverwaltung von einer übergeordneten Stammdatenverwaltung mit zentralen Elementen für Geschäftspartner noch weit entfernt ist.

Das Thema ist in Bewegung: Im November 2024 hat der Bundesrat beschlossen, die Geschäftspartnerstammdaten grundsätzlich nun für alle Geschäftsprozesse – also auch ausserhalb der SAP-Supportprozesse – nutzbar zu machen. Dazu soll die entsprechende Verordnung bis Ende 2025 angepasst werden. Zwei Jahre später soll dann in einem Bericht aufgezeigt werden, wie diese Stammdaten langfristig schweizweit genutzt werden könnten und welche Kosten damit verbunden wären.

### **Kaum Wille, dezentrale Stammdatenbestände aufzuheben**

Bei einer Prüfung bei der Eidgenössischen Steuerverwaltung 2023 stellte die EFK fest, dass das Amt unverändert ein eigenes Partnerverwaltungssystem betreibt, das nicht mit dem bundesweiten Stammdatenmanagement des Programms SUPERB identisch ist. Weder das Programm SUPERB noch die Steuerverwaltung waren zum Prüfungszeitpunkt für eine Zusammenführung ihrer Systeme bereit, so müssten u. a. Stammdaten und Codes vereinheitlicht und Daten bereinigt werden.

Die EFK hat 2024 beim Bundesamt für Justiz geprüft. Infostar, das Personenstandsregister der Schweiz und kritische Fachanwendung für die innere Sicherheit, muss erneuert werden. Es hat fast 1200 Benutzerinnen und Benutzer in 142 Standesämtern. Basis des Registers sind Stammdaten der natürlichen Personen in der Schweiz. Synergiepotenziale in der Datenhaltung, zum Beispiel mit dem Programm Erneuerung Zentrales Migrationsinformationssystem des Staatssekretariats für Migration oder im Rahmen der laufenden Aktivitäten der Stammdatenverwaltung Bund, wurden bisher nicht untersucht. Der Beauftragte für die Digitale Verwaltung Schweiz (DVS) und die Bundeskanzlei evaluieren aufgrund einer EFK-Empfehlung die Machbarkeit einer Architekturvision sowie einer Roadmap für die gemeinsame Bewirtschaftung der Stammdaten natürlicher Personen. Das Bundesamt für Justiz ist trotz seiner zentralen Rolle in diesem Thema nicht daran beteiligt.

### **Wohnadressen natürlicher Personen: Zielbild und Massnahmen fehlen**

Für viele Kontakte der Bevölkerung mit den Behörden wird die Adresse der natürlichen Person benötigt. Ein nationales Register für Wohnsitzadressen ist eine logische Umsetzung des Once-Only-Prinzips. Bereits 2018 hat das Bundesamt für Statistik das Projekt für einen Nationalen Adressdienst (NAD) gestartet. Im föderalen Kontext – die Daten werden in den Gemeinden nach unterschiedlichen kantonalen Vorgehensweisen erhoben und gepflegt – ist dieses Unterfangen ein Abenteuer. 2023, also fünf Jahre nach dem Start, konstatierte die EFK, dass Funktionsweise und Ausrichtung des Gesamtsystem der Stammdaten natürlicher Personen über alle föderalen Ebenen hinweg und über den NAD hinaus noch nicht definiert sind. Auf strategischer Ebene stimmen die Ziele der Bundeskanzlei und des DVS zum Thema Stammdaten natürlicher Personen weitgehend überein. Ein abgestimmtes Zielbild zum Gesamtsystem sowie eine koordinierte Massnahmenplanung bestehen aber nicht. Die spätere Integration des NAD in den übergeordneten Gesamtkontext der Stammdatenverwaltung natürlicher Personen ist somit ungeklärt.

## 7 ANWENDUNGEN UND DIENSTE



### Die Werkzeuge für den Arbeitsalltag

Diese Ebene befasst sich mit den Anwendungen und Diensten, die den Arbeitsalltag der Organisation unterstützen. Sie sorgt dafür, dass die richtigen digitalen Tools vorhanden sind, die effizient miteinander kommunizieren und den Arbeitsprozess erleichtern. Sie umfasst

- Fachanwendungen und Schnittstellen: Spezialisierte Programme, die bestimmte Aufgaben in der Verwaltung abwickeln, sowie Schnittstellen, die den Austausch von Daten zwischen Systemen ermöglichen.
- Benutzerschnittstellen: Die Oberflächen und Programme, die es den Anwenderinnen und Anwendern ermöglichen, mit den Systemen zu interagieren und Informationen einzugeben oder abzurufen.
- Clouddienste: IT-Ressourcen, die über das Internet bereitgestellt werden, entweder in einer öffentlichen oder privaten Umgebung. Sie bieten eine flexible, skalierbare und kosteneffiziente Möglichkeit, Infrastruktur, Anwendungen und Daten zu nutzen, ohne dass eine eigene physische Infrastruktur benötigt wird.

### 7.1 Fachanwendungen und Schnittstellen



#### Kleine Schritte bei den «Maschine zu Maschine Schnittstellen», aber ermutigende Beispiele

Maschine zu Maschine (M2M) Schnittstellen gewinnen an Bedeutung. Es gibt eine Vielzahl von Anwendungsfällen, wie Unternehmen Daten beispielsweise direkt aus einem Buchhaltungs- oder Logistiksystem an eine Behörde übermitteln können und wie Informationen direkt zurückfliessen. Dies ermöglicht unter anderem die automatisierte Abwicklung von Behördengängen. Neu ist das Thema nicht, auch für die Politik nicht, die schon seit 2018 immer wieder M2M Zugänge fordert. Seitens Bundesverwaltung arbeitet man schon seit 2008 an diesem Thema. Wie Prüfungen der EFK 2020 bei den IT-Portalen oder 2022 im Landwirtschaftsbereich zeigen, in den geprüften Fällen mit bescheidenem Erfolg und ohne hohe Priorität. Einfach ist diese Arbeit nicht, bedingt sie doch einheitliche Terminologie und Standards. Auch wenn es insgesamt langsam vorangeht, trifft die EFK auch auf positive Beispiele, die das enorme Effizienzsteigerungspotenzial eines **direkten Datentransfer zwischen Maschinen (Systemen)** aufzeigen:

Beim Portal Agate im Landwirtschaftsbereich verwenden viele der rund 70 Teilnehmersysteme (sowohl öffentlich- als auch privat-rechtlich) den Direktzugriff auf die Tierverkehrsdatenbank. Beim Bundesamt für Zoll und Grenzsicherheit haben die M2M Schnittstellen eine hohe Priorität und werden beispielsweise bei Passar, dem neuen Warenverkehrssystem für die digitale Abwicklung der Zollverfahren zusammen mit der Logistikbranche entwickelt. Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden können Informationen aus ihren eigenen Systemen mit einem Klick im Strafregisterinformationssystem VOSTRA des EJPD speichern, anstatt sie von Hand einzugeben oder separat zu übermitteln. Dies ist ein wichtiger Schritt in Richtung Digitalisierung der Strafjustiz. secure data exchange (sedex) ist eine sichere Plattform des Bundesamtes für Statistik für den sicheren Datenaustausch zwischen Fachapplikationen von Organisationseinheiten der öffentlichen Verwaltung. Heute wird sedex von über 8000 Teilnehmerinnen und Teilnehmern der Bundesverwaltung, aus Kantonen und Gemeinden, sowie von zugelassenen Dritten verwendet. Im Jahr 2022 wurden ca. 28,6 Millionen Meldungen via sedex übermittelt.

## 7.2 Benutzerschnittstellen



### Risiko des Wildwuchses bei Portalen

Die Systemlandschaft an den Online-Portalen der Bundesverwaltung ist historisch gewachsen. Wie die EFK 2021 festhält, braucht es eine Sollarchitektur für die Zukunft, die im Rahmen der Digitalen Verwaltung Schweiz (DVS) erarbeitet werden soll, also die Klärung einer gemeinsamen Linie für Organisation, Technik und Betrieb. Rasche Ergebnisse sind allerdings nicht zu erwarten. Offen ist, wie die Standardisierung erreicht werden soll. Mit dem aktuellen Vorgehen ist nicht klar, wie dem Risiko einer unkontrollierten Vermehrung von Portalen begegnet werden soll. Weitere Portale sind also nicht ausgeschlossen, eine zentrale Steuerung oder Überwachung erfolgt nicht. Die faktische Notwendigkeit zur Zusammenarbeit innerhalb der Verwaltung bahnt sich ihren mühsamen Weg, wie die EFK feststellt: «Erste Schritte zur Harmonisierung zwischen den Portalen sind angelaufen.». Neben der bundesinternen Perspektive darf man die der externen Anwenderinnen und Anwender nicht aus den Augen verlieren, die je nach Anliegen mit unterschiedlichen Portalen arbeiten müssen.

### Sicherheitsrisiken dezentraler Portallösungen

Die konkreten Probleme bei dezentralen Portallösungen lässt sich an einer EFK-Prüfung aus 2023 illustrieren: Über das e-Portal des EFD stellten zum Prüfungszeitpunkt die Eidgenössische Steuerverwaltung und das Bundesamt für Zoll und Grenzsicherheit Bevölkerung, Unternehmen und anderen Behörden Services zur Verfügung, beispielsweise für die Mehrwertsteuerabrechnung oder Verkehrsabgaben. Die EFK bemängelte ein fehlendes Kontinuitätsmanagements bzw. Notfallkonzept. Das kann dazu führen, dass nach einem Ausfall der Betrieb nicht innerhalb einer bestimmten Frist wiederhergestellt werden kann. Das beeinträchtigt die Aufgabenerfüllung und das Ansehen der Verwaltung.

Das Single-Sign-On-Portal ist die zentrale und strategische IKT-Sicherheitsinfrastruktur des EJP. Es regelt den Zugriff auf sicherheitskritische Fachanwendungen. Das Informatik Service Center verwaltet knapp 43 000 Benutzer, die über das Portal auf 124 Applikationen zugreifen. Die Betriebskosten für 2021 betragen rund 2,8 Millionen Franken. Die EFK kommt in ihrer Prüfung 2021 zu einem guten Ergebnis, wenn es um die Stabilität und die Sicherheit im Betrieb geht. Bei den Tests der Wiederherstellungsverfahren besteht hingegen punktueller Handlungsbedarf.

## 7.3 Clouddienste



Im Cloud-Bereich ist innerhalb der Bundesverwaltung aktuell vieles in Bewegung, was sich in den hier zusammengefassten Prüfungsergebnissen nicht abbildet. Die EFK begleitet diesen Prozess auch weiterhin prüferisch und hofft, hier rasche Fortschritte feststellen zu können.

### Lückenhafte Cloud-Modelle und Fragezeichen bei der Speicherung von Personaldaten bei Microsoft

Das Konzept, Software oder Infrastruktur nicht selbst zu betreiben, sondern als Dienst zu nutzen (SaaS bzw. IaaS), ist nicht neu. Auch die Speicherung wenig sensibler Dokumente ausserhalb der eigenen Infrastruktur ist gängige Praxis. Externe Anbieter stellen ihre globalen Infrastrukturen bereit und versprechen durch Skaleneffekte und Elastizität konkurrenzlose Kostenvorteile. Kein Wunder also, dass Cloud-Lösungen eine zentrale Rolle in der digitalen Transformation der Bundesverwaltung spielen. Sie sollen innovative Lösungen schneller, flexibler und kostengünstiger umsetzen helfen. Daher verabschiedete der Bundesrat bereits 2020 eine Strategie, die den Einsatz verschiedener Cloud-Modelle regelt: bundesinterne Private Clouds, externe Public Clouds und Hybrid-Lösungen.

2023 prüfte die EFK die Umsetzung der Cloud-Strategie und stellte fest, dass die Cloud-Modelle sowie ihre Nutzungsbedingungen nicht klar voneinander abgegrenzt waren. Zudem fehlten Kriterien für die Auswahl eines Modells. Der Bundesrat forderte die Bundeskanzlei auf, bis Ende 2024 das Modell zu

präzisieren. Die bisherigen Arbeiten decken nicht die gesamte Strategie ab. Eine detaillierte Untersuchung der Chancen und Risiken der einzelnen Cloud-Modelle fand nicht statt – lediglich die Public Cloud wurde allgemein betrachtet. Damit blieb die Umsetzung einer Empfehlung der EFK aus 2021 hinter den Erwartungen zurück, die auf allgemein verbindliche Vorgaben sowie Hilfsmittel für den Einsatz von Cloud-Technologien abzielte.

Parallel zur Grundlagenentwicklung beginnen erste Bundesämter bereits mit der Cloud-Nutzung, wie das Bundesamt für Meteorologie. Das Amt verlagert seine geschäftskritischen Anwendungen in die Public Cloud, die durch Amazon betrieben wird, um ausfallsichere Leistungen sicherzustellen. Die EFK stellte 2023 fest, dass zum Zeitpunkt der Prüfung keine ausreichende Risikobeurteilung vorlag. Das Amt war dazu auch nur eingeschränkt in der Lage, da seine Sicherheitsspezialisten aus Gründen der Vertraulichkeit der ausgehandelten Verträge keinen Zugang zu relevanten Informationen über die Sicherheitsmassnahmen der Public Cloud erhielten. Entsprechend war es längere Zeit nicht möglich, die verbleibenden Risiken oder den Bedarf an zusätzlichen Schutzmassnahmen zu ermitteln.

In der Nachprüfung 2024 zu Empfehlungen, die die EFK bei vorgängigen Prüfungen der SAP-Migration auf SAP S/4HANA im zivilen und militärischen Bereich abgegeben hat, konnte sich die EFK davon überzeugen, dass auf Stufe Bund Fortschritte erzielt wurden, z. B. mit einer ersten Version des rechtlichen Rahmens und den Cloud-Prinzipien. Dennoch bleiben noch Lücken, vor allem im Bereich der Sicherheitsüberlegungen. Ohne diese kann man Unangenehmes erleben, die das Beispiel der Cloud-Lösung für den Personalbereich aus 2024 zeigt: Ab 1. April 2025 sollten grundlegende Personaldaten in der Public Cloud von Microsoft gespeichert werden. Die Entscheidung und die damit verbundenen Risiken für die Stakeholder, z. B. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, wurden nicht gut kommuniziert bzw. verstanden, so dass einige Ämter erst kurz vor der Umsetzung Bedenken äusserten. Die Situation muss neu beurteilt werden. Die EFK sieht darin eine Chance, mit kritischer Distanz mögliche Optionen und das weitere Vorgehen mit Blick auf Sicherheit und Wirtschaftlichkeit zu prüfen.

### **Die Verwaltung nutzt die Public Cloud von Microsoft, noch ohne gemeinsame Regeln**

2023 stellte die EFK fest, dass bereits mehr als 30 Bereiche in der Bundesverwaltung Microsoft Azure (die Cloud-Computing-Plattform von Microsoft) nutzen. Anders als Organisationen, die ihre Cloud-Nutzung zentral bündeln, arbeitet der Bund mit zahlreichen eigenständigen Zugängen. Für diese sollte es zumindest gemeinsame Regeln geben, und die Bundeskanzlei sollte deren Einhaltung überwachen und Ausnahmen genehmigen. Dass das in der Praxis so gelebt wird, konnte die EFK nicht bestätigen. Zudem fehlten zu diesem Zeitpunkt abgestimmte Vorgaben z. B. in Bezug auf die Sicherheitsanforderungen, die die Cloud-Anbieter erfüllen müssen.

### **Bundeseigene Private Cloud+ beim EJPD mit guten Noten**

Mit der Cloud-Strategie Bund hat der Bundesrat im 2020 ein Cloud-Stufen-Modell beschlossen, welches vier Sicherheitsstufen definiert. Das Informatik Service Center des EJPD betreibt eine Secure Private Cloud, die der höchsten Sicherheitsstufe IV (Bundeseigene Private Cloud+) entspricht. Die IKT-Sicherheit ist zwischen dem Cloud-Anbieter und den Leistungsbezügern aufgeteilt. Das bedeutet, dass beide Seiten Verantwortung übernehmen müssen: Der Anbieter sorgt für eine sichere Infrastruktur, während die Anwender sicherstellen müssen, dass ihre Anwendungen und Daten geschützt sind. Der IKT-Leistungserbringer hat Vorgaben erstellt, die erfüllt sein müssen, damit eine Fachanwendung sicher auf seiner Cloud betrieben werden kann und überprüft deren Einhaltung. Die EFK kommt zum Schluss, dass das EJPD ihre Cloud im Griff hat. Da die Cloud künftig aber auch für Verwaltungseinheiten ausserhalb des EJPD genutzt werden sollen, braucht es eine weitere Detaillierung der Vorgaben sowie weitergehende technische Schutzmassnahmen.

## 8 TECHNOLOGIE UND INFRASTRUKTUR



### Das Fundament für einen reibungslosen Ablauf

Diese Ebene umfasst die technischen Ressourcen und Systeme, die notwendig sind, um alle anderen Bereiche der Organisation zu unterstützen und einen stabilen Betrieb zu gewährleisten. Sie stellt sicher, dass alle Anwendungen, Daten und Prozesse zuverlässig und sicher laufen. Sie umfasst:

- Netzwerke: Die Verbindungen, die es ermöglichen, dass Daten zwischen verschiedenen Systemen und Standorten ausgetauscht werden – sowohl innerhalb der Organisation als auch nach aussen.
- Rechenzentren: Die physischen Einrichtungen, in denen die Server und IKT-Ressourcen untergebracht sind, um einen stabilen Betrieb und eine hohe Verfügbarkeit zu gewährleisten.
- Server und Endgeräte: Die Hardware, die für das Verarbeiten, Speichern und Abrufen von Daten genutzt wird, von den zentralen Servern bis hin zu den Endgeräten der Nutzer (wie Computer, Tablets oder Smartphones).
- Backups: Lösungen zur regelmässigen Sicherung von Daten, um im Falle eines Ausfalls oder Verlusts eine rasche Wiederherstellung zu ermöglichen.
- Sicherheitstechnologien: Schutzmassnahmen, die die IKT-Infrastruktur vor Angriffen, Missbrauch und unbefugtem Zugriff schützen, wie Firewalls, Antivirenssoftware und Verschlüsselung.

### 8.1 Netzwerke



#### Sicherheitskommunikation: Fehlende Einbettung, vernachlässigte Synergien

Das Bundesamt für Bevölkerungsschutz verfolgt mit drei grossen Vorhaben die technologische Erneuerung seiner Kommunikationssysteme und will deren Ausfallrisiko senken. Die EFK stellte 2021 fest, dass diese Systeme unabhängig voneinander entstanden und lose in einem Verbund zusammengefasst sind. Eine strategische Gesamtsicht fehlte – trotz wachsender technischer Koppelung. Auch Synergien über die Amtsgrenzen hinweg wurden nicht geprüft. Ebenso kritisierte die EFK die mangelnde Einbettung in die Netzwerkstrategie des Bundes sowie ausstehende Architektur- und Betriebsentscheide, die durch Uneinigkeiten zwischen dem Bundesamt und der Bundeskanzlei verzögert wurden. Die Prüfung 2024 zeigt positive Fortschritte: Architekturentscheide sind klarer, mögliche Synergien erkannt und Abhängigkeiten besser bekannt. Deren systematische Bewirtschaftung fehlt jedoch weiterhin.

Ein Beispiel, dass Synergien frühzeitig erkennbar wären, zeigt sich in der Armee: Das Führungsnetz Schweiz (rund eine Milliarde Franken Beschaffungsvolumen) und die Telekommunikation der Armee (rund 1,6 Milliarden Franken) verfolgen ähnliche Ziele, ein separates Projekt soll Synergien zwischen beiden Netzen erschliessen. Wie dies konkret geschehen soll, war bei einer Prüfung in 2022 noch offen, aber die Stossrichtung ist zu begrüssen.

#### Vertrauen ist gut, Kontrolle sichert das Gesamtsystem

Das Bundesamt für Informatik und Telekommunikation (BIT) betreibt Datennetze und Telekommunikationsinfrastrukturen für die gesamte zivile Bundesverwaltung. Seine rund 1700 Mitarbeitenden betreuen die IKT-Infrastrukturen für die 38 000 Arbeitsplatzsysteme und zirka 6300 Server. Das Netzwerk des Bundes ist in unterschiedliche Zonen aufgeteilt. Netzwerkzonen sind voneinander getrennte Bereiche, die je nach Schutzbedarf unterschiedliche Sicherheitsregeln haben. Die Vorgaben zu den Zonen sind entscheidend für die Netzwerksicherheit. Ob diese wirklich eingehalten werden, wird vom BIT gemäss einer Prüfung aus 2021 nicht überprüft. Man setzt ausschliesslich auf die Eigenverantwortung der jeweiligen Betreiber, was angesichts der enormen Relevanz des Netzwerkes für die Bundesverwaltung nicht ausreichend ist. Es gibt noch Lücken beim Grundschatz, in der Überwachung und bei Wiederherstellungs- tests, aber insgesamt kann die EFK dem BIT für den sicheren Betrieb gute Noten ausstellen.

## 8.2 Rechenzentren



Überkapazitäten, Verzögerungen und fehlende Planung bei den Rechenzentren

Im Juli 2014 genehmigte der Bundesrat die Konsolidierung der Rechenzentrenlandschaft der Bundesverwaltung in einen Verbund aus vier Rechenzentren. Ziel war es, die Zahl der Rechenzentren deutlich zu reduzieren und den zukünftigen Kapazitätsbedarf der Bundesinformatik kostengünstiger sowie umweltfreundlicher zu decken. 2017 verabschiedete der Bundesrat hierzu das «Betriebsmodell Rechenzentrenverbund Zielbild 2020», das regelt, welche internen IKT-Leistungserbringer künftig welche Infrastrukturdienste im Rechenzentrenverbund bereitstellen, um Synergien zu nutzen. Das Betriebsmodell gibt zudem vor, dass neben den vier Rechenzentren des Verbundes keine weiteren Rechenzentren mehr gebaut, erweitert oder modernisiert werden dürfen.<sup>10</sup>

Die Rechenzentren PRIMUS (zivile Nutzung), CAMPUS (zivile und militärische Nutzung) und FUNDAMENT (militärische Nutzung) sind in Betrieb. Das Projekt Rechenzentrum KASTRO II (militärische Nutzung) soll bis 2033 und damit 10 Jahre später als ursprünglich geplant abgeschlossen werden.

fedpol plante bereits vor Inkrafttreten der IKT-Strategie 2012-2015 zusammen mit dem Bundesamt für Bauten und Logistik einen Rechnerraum im Campus G1 (Guisanplatz), der 2018 fertiggestellt wurde. Die Begründung für diese genehmigte Lösung ausserhalb des Rechenzentrenverbunds waren besondere Anforderungen an Schutzniveau und Verfügbarkeit.

Die EFK prüfte 2021, 2022 und 2024 den Konsolidierungsstand. Im Jahr 2021 meldeten die Departemente der Bundeskanzlei, dass im zivilen Bereich 25 Rechenzentren in Betrieb seien. Angesichts derer geplanter Integration in den Rechenzentrenverbund hätte ein klarer Bedarf an Fläche bestanden. Dennoch lag die Auslastung bei CAMPUS zu diesem Zeitpunkt nur bei 20 % mit dem Ziel, 50 % zu erreichen. Diese Überkapazitäten verursachen zusätzliche Kosten, und ein Plan zur wirtschaftlichen Nutzung fehlt. 2024 musste die EFK daher feststellen: «Das übergeordnete Ziel von vier Rechenzentren für die gesamte Bundesverwaltung, davon zwei zur zivilen Nutzung, scheint nicht mehr konsequent verfolgt zu werden.»

Ausserdem verzögert sich die Besiedelung des neuen zivilen Rechenzentrums CAMPUS mit seinem Gesamtaufwand von 31,1 Millionen Franken, obwohl die Infrastruktur dafür bereit ist. Ein altes Rechenzentrum in Bern konnte fristgerecht zurückgebaut werden. Die Verschiebung der Systeme erfolgte jedoch nicht direkt nach CAMPUS, sondern über einen «Zwischenschritt» in das alte bestehende Rechenzentrum PRIMUS. Dieser Schritt war nötig, da sich herausstellte, dass die geschätzten 1600 Anwendungen einzeln auf Kosten der Ämter für den Betrieb in CAMPUS angepasst werden müssen. Ein Gesamtprojekt, Zeitplan und eine Kostenplanung dafür fehlen. Neben der Tatsache der Überkapazitäten in CAMPUS, entwickelt sich PRIMUS immer mehr zum Klumpenrisiko: Dieser Standort muss in den kommenden Jahren komplett saniert und die Stromversorgung auf den erhöhten Bedarf durch neue Hochleistungsrechner angepasst werden.

### Fehlende Georedundanzen

Ein Problem bei den Rechenzentren ist die fehlende Georedundanz: Erst bei einer vollständigen Nutzung des Rechenzentrums CAMPUS, die Stand 2024 noch ein paar Jahre auf sich warten lassen wird, besteht eine umfassende Georedundanz für die zivilen Bereiche. Im militärischen Bereich ist es gleich: Bis zur geplanten Fertigstellung von KASTRO II im Jahr 2033 gibt es für das militärische Rechenzentrum keine umfassende georedundante Absicherung. Dies stellt ein Risiko dar, falls die Schweiz z. B. in einen bewaffneten Konflikt geraten sollte.

### Offene Zukunft

Der Bundesrat hat der Bundeskanzlei den Auftrag erteilt, bis Mitte 2025 eine überarbeitete Rechenzentrenstrategie vorzulegen. Nach aktuellem Wissensstand der EFK basieren die Konzepte weiterhin auf vier

---

<sup>10</sup> Medienmitteilung "Bundesrat treibt Rechenzentren-Verbund weiter voran" 22.2.2017

Rechenzentren, doch die EFK stellt fest, dass sich die Realität, etwa bei der Anzahl der Rechenzentren und der Besiedlung von CAMPUS, anders entwickelt hat als vorgesehen. Dehnt man z. B. die Nutzung von Public Cloud Lösungen aus, verringert sich der Bedarf an eigenen Rechenzentrumskapazitäten. Die nachteiligen Auswirkungen der Unterbelegung von CAMPUS könnte sich also noch verschärfen. Eine gegenteilige Wirkung könnte hingegen das Streben nach digitaler Souveränität haben. Daher sind eine neue Standortbestimmung und die konsequente Umsetzung der getroffenen Entscheidungen erforderlich. Kurz gesagt: Die zukünftige Strategie für die Rechenzentren der zentralen Bundesverwaltung ist offen.

## 8.3 Server und Endgeräte



### Sichere Entsorgung von Speichermedien verbessern

Der IKT-Grundschutz verlangt, dass bei der Entsorgung von Datenträgern und Speichermedien keine Rückschlüsse auf Inhalte oder gespeicherte Daten möglich sind. Die praktizierte Löschmethode festverbauter Speichermedien (z. B. Flash-Speicher<sup>11</sup>, EEPROM<sup>12</sup>) beim Bundesamt für Informatik und Telekommunikation erfüllten diese Vorgabe aus dem Grundschutz nicht, wie die EFK 2022 festgestellt hatte, was zu Datenabflüssen führen konnte. Speichermedien müssen also bei der Entsorgung einem sicheren Lösch- oder Vernichtungsverfahren unterzogen werden. Mittlerweile hat der IKT-Leistungserbringer entsprechende Massnahmen ergriffen.

## 8.4 Backups / Sicherheitstechnologien



### Schutz vor Verschlüsselungstrojanern hat höchste Priorität

Das Bundesamt für Informatik und Telekommunikation muss **Daten zuverlässig sichern und im Notfall wiederherstellen**. 2022 hat die EFK die Datensicherungen beim IKT-Leistungserbringer BIT geprüft. Das Ergebnis: Die vorhandenen Sicherheitsmaßnahmen entsprechen den Anforderungen, allerdings mit zwei Ausnahmen: Die vertraglich vereinbarten Wiederherstellungszeiten können bei grossen Datenbanken aufgrund ihrer Volumen nicht volumnäßig sichergestellt werden. Ausserdem war noch nicht ausgeschlossen, dass sogenannte Verschlüsselungstrojaner die Backupsysteme infizieren und diese wertlos machen. Eine gefährliche Angriffsfläche, deren Beseitigung der IKT-Leistungserbringer rasch in Angriff genommen hat.

### Gute Fortschritte bei zentraler Anmeldeinfrastruktur des Bundes

Die Bundesverwaltung stellt das e-Government Identity and Access Management zur Verfügung. elAM ist die zentrale Login-Infrastruktur des Bundes mit dem Ziel, dass nicht für jede Applikation ein eigenes Loginverfahren entwickelt werden muss. Dank dieser Zentralisierung sollen Kosten gespart und für alle Applikationen dieselben Zugangsdaten verwendet werden. Es spielt dabei keine Rolle, wie und wo die Zielapplikation betrieben wird, elAM kann Applikationen auf der ganzen Welt bedienen. Täglich nutzen etwa 100 000 Benutzerinnen und Benutzer die elAM-Lösung, um auf über 800 Anwendungen zuzugreifen, wobei täglich rund 250 000 Anmeldungen verarbeitet werden. Die jährlichen Betriebs- und Weiterentwicklungskosten der elAM-Lösung betragen rund 20 Millionen Franken. Nach der letzten Prüfung im Jahr 2018 konnte die EFK in der Prüfung 2024 beachtliche Fortschritte zur Reduktion der Abhängigkeit vom Lieferanten feststellen. Allerdings gibt es Lücken in der Notfallvorsorge: Die Tests zur Wiederherstellung des Betriebs nach einer Störung erfolgen derzeit nicht mit allen Umsystemen.

---

<sup>11</sup> Ein Speicherchip, der Daten auch ohne Strom behält. Er wird in USB-Sticks, SSDs und Speicherkarten verwendet

<sup>12</sup> Ein Speicher, der elektronisch gelöscht und neu beschrieben werden kann. Er enthält wichtige Steuerungsprogramme z. B. in Netzwerkroutern, Druckern oder Zugangskontrollsystmen, und kann bei Bedarf aktualisiert werden.

## **Sicherheitslücken in der Gebäudesteuerung wurden geschlossen, neue entdeckt**

Als Gebäudeautomation oder Domotik wird die Gesamtheit von Überwachungs-, Steuer-, Regel- und Optimierungseinrichtungen in Gebäuden bezeichnet. Bereits im Jahresbericht 2020 hat die EFK von Sicherheitslücken im Bereich der Gebäudesteuerung berichtet. Externe Lieferanten installieren und warten diese Systeme, die in der Regel für einen Langzeitbetrieb von sieben bis zwanzig Jahren angelegt sind. Die damalige Prüfung hat gezeigt, dass es Defizite in den Bereichen der Überwachung und der Schwachstellenanalyse gibt. Erfreulicherweise hat das Bundesamt für Bauten und Logistik gemeldet, die Empfehlungen des EFK-Berichtes umgesetzt zu haben.

Allerdings stellte die EFK in einer Prüfung 2021 fest, dass Änderungen an der Gebäudeautomation in den beiden zivilen Hauptrechenzentren ohne sog. Integrationstests direkt in die Produktivumgebung eingespielt werden und dort zu massiven Fehlern führen können. Das Problem war dem Projektausschuss zwar bekannt, sollte allerdings wegen fehlender Finanz- und Personalressourcen erst in 2023 angegangen werden mit der Aussicht, dass eine Test- und Integrationsumgebung in 2024 zur Verfügung stehen soll. Die EFK wird den Stand in 2025 prüfen.

## **8.5 Speicherlösungen und Virtualisierung**



Aus den EFK-Prüfungen der letzten Jahre lassen sich keine Kernaussagen zu diesem Thema ableiten.

## ANHANG 1 – LISTE DER BERÜCKSICHTIGTEN BERICHTE

---

NR.	TITEL	BERICHTS-NR.
1	Datenanalysen in der Arbeitslosenversicherung	23630
2	Digitale Transformation: Prüfung der Direktzahlungskontrollen in der Landwirtschaft	21325
3	Digitale Transformation: Prüfung der Prozesseffizienz bei der Ablösung von FIS Heer	23151
4	Digitale Transformation: Prüfung der Prozesseffizienz von Core-IT	22524
5	Digitale Transformation: Prüfung des Programmes EO-Digitalisierung	24600
6	Digitale Transformation: Prüfung des Projektes eSubventionen	24632
7	Digitale Transformation: Prüfung des Projektes zur Erneuerung der Handelsregister-Applikationen	24273
8	Digitale Transformation: Synthesebericht vergangener Prüfungen	22742
9	Evaluation der Lenkungswirkung des Emissionshandelssystems	16393
10	Funktionsprüfung Einnahmeprozess Verrechnungs- und Stempelsteuer (nicht publiziert)	24520
11	Jahresbericht der EFK 2020	
12	Jahresbericht der EFK 2023	
13	Kurzanalyse der Auswirkungen des Dokumentenlabelings in Microsoft 365 auf die Anwender	24133
14	Nachprüfung der Umsetzung wesentlicher Empfehlungen: Schlüsselprojekt ASALfutur	24607
15	Projektprüfung Nationaler Adressdienst	23619
16	Prüfung der Auswirkung von Digitalisierungsvorhaben auf die IT-Betriebskosten	24179
17	Prüfung der Behandlung und Kontrolle der Rechnungen für individuelle Leistungen bei der AHV und IV	14490
18	Prüfung der Einsatztauglichkeit der Aufklärungsdrohne	24171
19	Prüfung der Identitäts- und Zugriffsverwaltung Bund IAM Bund	24141
20	Prüfung der IKT-Governance	20436
21	Prüfung der Informatiksicherheit der Sedex-Plattform (nicht publiziert)	22657
22	Prüfung der Oberaufsicht über das Grundbuchwesen	21529
23	Prüfung der Produktivsetzung von Anwendungen in einem agilen Umfeld	23701
24	Prüfung der Schlüsselprojekte Werterhalt Polycom 2030 und Nationales sicheres Datenverbundsystem sowie des Projektes Mobiles breitbandiges Sicherheitskommunikationssystem	21539
25	Prüfung der sicheren Integration von Fachanwendungen im ePortal (nicht publiziert)	23532
26	Prüfung der Sicherheit der Datenbank Infostar	21135
27	Prüfung der Sicherheit der Secure Cloud (nicht publiziert)	24110
28	Prüfung der Sicherheit des Strafregister-Informationssystems VOSTRA (nicht publiziert)	24200
29	Prüfung der Sicherheit und des Betriebs der Anwendung Netbackup	22752
30	Prüfung der Sicherheit und des Betriebs der Informatik (nicht publiziert)	24102
31	Prüfung der Sicherheit und des Betriebs der Netzwerke (nicht publiziert)	20415
32	Prüfung der Sicherheit und des Betriebs des Single Sign-On Portals (nicht publiziert)	21525
33	Prüfung der Sicherheit und Verfügbarkeit im Betrieb Gever	20385
34	Prüfung der Steuerung der IKT	21203

NR.	TITEL	BERICHTS-NR.
35	Prüfung der Synergien beim Einsatz von künstlicher Intelligenz am Beispiel Chatbot-Lösungen	24181
36	Prüfung der Transformation von der IKT-Steuerung zur Steuerung der Digitalisierung Bund	23759
37	Prüfung der Umsetzung der Cloud-Strategie	23766
38	Prüfung der Umsetzung der Objektstrategie für die Betriebsimmobilien	23504
39	Prüfung der Umsetzung Stammdatenstrategie	20526
40	Prüfung der Wirksamkeit der Vorfallbewältigung beim Schutz der Bundes-IKT vor Cyberrisiken	21070
41	Prüfung des Beschaffungswesens	17117
42	Prüfung des Fachkräftemangels im Informatikbereich	23503
43	Prüfung des Nutzens der verbindlichen Vorgaben im Bereich Prozess- und Architekturmödellierung im Eidgenössischen Finanzdepartement	22538
44	Prüfung des Programms Nationale Datenbewirtschaftung	21156
45	Prüfung des Projektes Infostar New Generation	24246
46	Prüfung des Schlüsselprojektes ASALfutur	21304
47	Prüfung des Schlüsselprojektes Cloud Enabling Büroautomation	23740
48	Prüfung des Schlüsselprojektes DaziT	20287
49	Prüfung des Schlüsselprojektes DaziT mit Schwerpunkt Entwicklung und Einführung Warenverkehr – Passar 2.0	24511
50	Prüfung des Schlüsselprojektes Entflechtung IKT-Basisleistungen VBS	22102
51	Prüfung des Schlüsselprojektes Erneuerung Zentrales Migrationsinformationssystem	24253
52	Prüfung des Schlüsselprojektes Erneuerung Zentrales Migrationsinformationssystem mit Schwerpunkt Digitale Transformation	22207
53	Prüfung des Schlüsselprojektes Fernmeldeüberwachung	23261
54	Prüfung des Schlüsselprojektes Führungsnetz Schweiz	22122
55	Prüfung des Schlüsselprojektes Migration RZ CAMPUS BIT 2020	24136
56	Prüfung des Schlüsselprojektes Migration RZ CAMPUS BIT 2020 – Migrationsarbeiten	22739
57	Prüfung des Schlüsselprojektes Nationale Datenbewirtschaftung (NaDB)	24113
58	Prüfung des Schlüsselprojektes Neue Produktionssysteme NEPRO	22157
59	Prüfung des Schlüsselprojektes Neue Produktionssysteme NEPRO	24120
60	Prüfung des Schlüsselprojektes Rechenzentren VBS/Bund 2020	21462
61	Prüfung des Schlüsselprojektes RZPlus – Ausfallsichere Rechenleistung	23623
62	Prüfung des Schlüsselprojektes Schengen/Dublin Weiterentwicklung	23262
63	Prüfung des Schlüsselprojektes Sicheres Datenverbundnetz plus (SDVN+)	24140
64	Prüfung des Schlüsselprojektes SUPERB	21451
65	Prüfung des Schlüsselprojektes SUPERB – Projekt Personal: Umsetzung der Hybrid-Cloud-Strategie	24507
66	Prüfung des Schlüsselprojektes SUPERB – Teilprojekt Beschaffung	21535
67	Prüfung des Schlüsselprojektes SUPERB – Teilprojekt Fachanwendungen	22754
68	Prüfung des Schlüsselprojektes SUPERB – Teilprojekt Immobilien mit Schwerpunkt Gebäudedaten	21313
69	Prüfung des Schlüsselprojektes SUPERB – Teilprojekt PPM	22741

NR.	TITEL	BERICHTS-NR.
70	Prüfung des Schlüsselprojektes SUPERB mit Schwerpunkt Stammdaten	20407
71	Prüfung des Schlüsselprojektes Telekommunikation der Armee	22121
72	Prüfung des Schlüsselprojektes Werterhalt Polycom 2030 mit Schwerpunkt Teilnetz Grenzsiccherheit	23538
73	Prüfung des Schutzes kritischer Infrastrukturen – Governance und integrales Risikomanagement	22116
74	Prüfung von Synergiepotenzialen bei IT-Portalen des Bundes	20386
75	Querschnittsprüfung der Erkennung von Sicherheitsvorfällen (nicht publiziert)	23703
76	Querschnittsprüfung der Massnahmen bei Systemausfällen von Fachapplikationen	22520
77	Querschnittsprüfung der Umsetzung des harmonisierten Beschaffungsprozesses Bund	24158
78	Querschnittsprüfung des Umgangs des Bundes mit problematischen Stoffen	23489
79	Querschnittsprüfung zur Umsetzung der Artikel 44 und 45 des Bundesgesetzes über das öffentliche Beschaffungswesen	23737
80	Schlüsselprojekte Programm ERPSYSVAR und SUPERB – Nachprüfung der Umsetzung wesentlicher Empfehlungen	24182
81	Schutz kritischer Infrastrukturen: Synthesebericht vergangener Prüfungen mit Schwerpunkt Cyberresilienz	23160
82	Standortbestimmung Nutzen-Synergie-Potenzial bei SUPERB	23774
83	Subventionen: Synthesebericht vergangener Prüfungen	22537
84	Synthesebericht vergangener Prüfungen Gesamtschweizerische Register	22245