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

Prüfung der Steuerung der IKT

Bundesamt für Polizei

EFK-21203 | inkl. Stellungnahmen | 7. Juli 2022 | FinDel D5/2022

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	403.21203
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Prüfung der Steuerung der IKT
Bundesamt für Polizei

Das Wesentliche in Kürze

Das Bundesamt für Polizei (fedpol) ist die führende Polizeibehörde der Schweiz. Es ist die Ansprechstelle für die Polizeikorps des In- und Auslandes und erfüllt kriminal-, sicherheits-, verwaltungs- und unterstützende Aufgaben. Der Direktionsbereich Ressourcenmanagement und Strategie erbringt in Zusammenarbeit mit der dezentralen Informatik und dem Informatik Service Center des Eidgenössischen Justiz und Polizeidepartements (ISC-EJPD) die für die Geschäftstätigkeit wesentlichen IT-Leistungen.

Das Ziel der Prüfung ist zu beurteilen, ob die Steuerung der Informatikbelange von fedpol angemessen und zielführend funktioniert. Die Prüfung der IT-Governance zeigt ein positives Bild, auch wenn sich viele Grundlagen erst in der Umsetzung befinden. Das Fundament für eine wirksame Steuerung der IKT ist gelegt. Verbesserungsbedarf besteht in den Bereichen der Steuerung interner langfristiger Vorhaben als strategische Projekte und bei der vollständigen Durchführung von Sicherheitsprüfungen. Die in der Prüfung «Führung und Betrieb der Informatik» von 2015 ausgesprochenen Empfehlungen sind inzwischen weitgehend umgesetzt.

Strategien schaffen die Grundlagen für die Digitale Transformation

Um Geschäftsabläufe zu optimieren und den sich wandelnden Anforderungen unterschiedlicher Anspruchsgruppen gerecht zu werden, definiert die Strategie des EJPD übergreifende Stossrichtungen und Zielsetzungen zur Digitalen Transformation. Sie integriert die geschäftlichen Anforderungen, bundesweite Initiativen und legt die strategische Ausrichtung der Informatik fest.

fedpols IKT-Strategie basiert darauf. Der Fokus richtet sich auf die Optimierung der IKT-Governance, die Nutzung von Synergien und die Etablierung von Planungsdisziplinen für die zukunftsorientierte und sichere Weiterentwicklung von Anwendungslandschaften und Dienstleistungen.

Der IT-Leistungserbringer ISC-EJPD fokussiert auf Kundenorientierung und die Einführung von agilen Methoden für die Entwicklung und den Betrieb der Informationssysteme. Ziel ist eine flexible und sichere Technologiearchitektur als Voraussetzung für die Digitale Transformation im Departement.

Unternehmensarchitektur- und Portfoliomanagement werden als Mittel der Steuerung genutzt

Das EJPD führt ein Projekt zum Aufbau des Unternehmensarchitekturmanagements an dem fedpol mitarbeitet. Ziel ist, dank transparenter und vernetzter Informationen bessere Entscheidungen zu treffen. Als Planungs- und Steuerungsinstrument soll dieses ein optimales Zusammenspiel zwischen Geschäft und Informatik sicherstellen.

fedpol hat seine Informationssystemarchitektur erfasst und nutzt diese bereits, um Potenziale und Herausforderungen von Vorhaben im Projekt Portfoliomanagement zu evaluieren. Laufende Projekte und Programme sind thematisch gruppiert und werden auf Stufe

Departement regelmässig in den Portfolio-Besprechungen hinsichtlich Zielerreichung, Abhängigkeiten und Priorisierung analysiert.

Die IT-Dienstleistungserbringung wird gesteuert

Das ISC-EJPD ist der Leistungserbringer für individuelle sicherheitskritische Fachanwendungen. fedpol wählt aus dem Dienstleistungskatalog anforderungsgerecht die für den Betrieb und die Entwicklung benötigten Service Levels aus. Deren Einhaltung wird quartalsweise ausgewertet. Die Auswertungen weisen eine hohe Verfügbarkeit aus. In regelmässigen Abständen bewertet fedpol die Leistungen. Dies wird von den Leistungserbringern zur Optimierung genutzt. Das ISC-EJPD verwaltet das Inventar der für den Fachanwendungsbetrieb benötigten Hard- und Software. Im IT Asset Management wird in Zusammenarbeit mit fedpol der Lebenszyklus der IT Assets zur optimalen Wertausschöpfung geplant und koordiniert. Ein Projekt zum Ausbau ermöglicht in Zukunft weiterführende Betrachtungen im Sinne der Geschäftskontinuität und der Informationssicherheit.

Die Bedeutung von Informationen und Daten als Elemente der Steuerung ist erkannt

fedpol führt ein Projekt zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Dabei steht der Schutzbedarf von Informationen und Daten im Zentrum, konkret: Für welche Aktivitäten und Massnahmen soll welcher angemessene Schutz gewährleistet sein? Optimierte Prozesse sollen für eine Verbesserung der Steuerung und Überwachung der Informationssicherheit sorgen. Im Projekt implementiert fedpol ebenfalls ein IT-Risikomanagement, das mit dem ISMS integriert ist und in das gesamthafte Risikomanagement auf Ebene Amt fliesst. Zur Minimierung von Risiken empfiehlt die EFK, die Vorgaben zur Durchführung von Sicherheitsprüfungen so anzupassen, dass alle Anwendungen regelmässig einer Sicherheitsprüfung unterzogen werden.

Daten sind für die Geschäftstätigkeit von fedpol von höchster Bedeutung. Die Rechtsgrundlagen und Regelwerke definieren im Detail die Regeln zu deren Bearbeitung. fedpol will mit einem Projekt eine amtsweite Data Governance implementieren, die Transparenz zur Datennutzung schafft und alle Phasen des Datenlebenszyklus einheitlich unterstützt. Neue datengetriebene Sichten sollen der Geschäftsentwicklung dienen und Veränderungen vereinfachen.

Mehrheitlich umgesetzte Empfehlungen aus der Prüfung 15386

fedpol hat die wichtigsten Prozesse in der Prozessmanagement-Anwendung Signavio modelliert. Zur Sicherstellung der Geschäftskontinuität besteht eine Auswirkungsanalyse, zudem sind diverse Prozesse zur Widerherstellung des Betriebs erfolgreich getestet worden. Das Risikomanagement befindet sich noch im Aufbau und muss im Zielzustand einerseits sicherstellen, dass aus operativen Risiken resultierende Massnahmen wirksam überwacht werden, andererseits das IT-Risikomanagement integrieren. Für Letzteres führt fedpol zum Prüfungszeitpunkt für einen Teil der Anwendungen die Kontrolle zur Validierung der Benutzerberechtigungen ein.

Audit du pilotage de la TIC
Office fédéral de la police

L'essentiel en bref

L'Office fédéral de la police (fedpol) est la principale autorité policière de Suisse. Il est l'interlocuteur des corps de police suisses et étrangers et accomplit des tâches de police judiciaire, de sécurité, administrative et de soutien. Le domaine de direction Gestion des ressources et stratégie fournit, en collaboration avec le service informatique décentralisé et le Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP), les prestations informatiques essentielles à l'activité de fedpol.

L'audit vise à évaluer si le pilotage des besoins informatiques de fedpol fonctionne de manière adéquate et ciblée. Les résultats de l'audit de la gouvernance informatique sont positifs, même si de nombreuses bases ne sont encore qu'en cours de mise en œuvre. Les fondements pour un pilotage efficace de la TIC sont posés. Des améliorations sont nécessaires dans le domaine du pilotage des projets internes à long terme en tant que projets stratégiques et dans la réalisation complète d'audits de sécurité. Entre-temps, les recommandations formulées dans l'audit « Gestion et exploitation de l'informatique » de 2015 sont largement mises en œuvre.

Les stratégies jettent les bases de la transformation numérique

La stratégie du DFJP définit des orientations et des objectifs généraux en matière de transformation numérique pour optimiser le déroulement des activités et de répondre à l'évolution des exigences des différents groupes d'intérêt. Elle intègre les processus opérationnels, les initiatives à l'échelle fédérale et définit l'orientation informatique stratégique.

La stratégie TIC du DFJP est basée sur ce principe. L'accent est mis sur l'optimisation de la gouvernance TIC, l'exploitation de synergies et l'établissement de contraintes de planification pour le développement futur et sûr des applications et des services.

Le fournisseur de prestations informatiques CSI-DFJP se concentre sur les besoins des clients et l'introduction de méthodes agiles pour développer et exploiter les systèmes d'information. L'objectif est une architecture technologique flexible et sûre, condition préalable à la transformation numérique du département.

La gestion de l'architecture d'entreprise et du portefeuille est utilisée comme outil de pilotage

Le DFJP mène un projet pour mettre en place une gestion d'architecture d'entreprise, auquel fedpol collabore. L'objectif est de prendre de meilleures décisions grâce à des informations transparentes et interconnectées. En tant qu'outil de planification et de pilotage, elle vise à assurer une interaction optimale entre activités et informatique.

fedpol a établi une architecture de système d'information qu'elle utilise déjà pour évaluer les potentiels et défis des projets dans le cadre de la gestion du portefeuille. Les projets et programmes en cours sont regroupés par thème et analysés régulièrement au niveau du département, lors de réunions consacrées au portefeuille, en ce qui concerne la réalisation des objectifs, les dépendances et la priorisation.

La fourniture des prestations informatiques est pilotée

Le CSI-DFJP fournit les prestations pour les applications spécialisées individuelles critiques en termes de sécurité. fedpol choisit dans le catalogue de prestations les niveaux de service nécessaires à l'exploitation et au développement. Des évaluations trimestrielles portant sur le respect de ces niveaux font état d'une disponibilité élevée. fedpol évalue les prestations à intervalles réguliers. Les prestataires optimisent leurs services sur cette base. Le CSI-DFJP gère l'inventaire du matériel et des logiciels nécessaires à l'exploitation des applications spécialisées. Dans le cadre de la gestion des actifs informatiques, le cycle de vie de ces derniers est planifié et coordonné en collaboration avec fedpol afin d'en optimiser l'utilité. Un projet d'extension permettra à l'avenir d'approfondir la réflexion sur la continuité des activités et la sécurité de l'information.

L'importance des informations et des données comme éléments de pilotage est reconnue

fedpol dirige un projet pour mettre en place un système de management de la sécurité de l'information (SMSI). Le besoin de protection des informations et des données est au centre de ces préoccupations. En clair, quel niveau de protection doit être garanti pour quelles activités et mesures ? Des processus optimisés doivent permettre d'améliorer le pilotage et la surveillance de la sécurité de l'information. Dans le cadre du projet, fedpol met également en œuvre une gestion des risques informatiques intégrée au SMSI et qui s'inscrit dans la gestion globale des risques au niveau de l'office. Afin de réduire les risques au minimum, le CDF recommande d'adapter les directives relatives aux audits de sécurité de manière à que toutes les applications soient régulièrement soumises à un contrôle de sécurité.

Les données revêtent une importance capitale pour les activités de fedpol. Les bases légales et les règlements définissent en détail les modalités de leur traitement. fedpol entend mettre en œuvre un projet de gouvernance des données à l'échelle de l'office qui crée de la transparence dans l'utilisation des données et soutient de manière uniforme toutes les phases du cycle de vie des données. De nouvelles approches axées sur les données doivent permettre de développer l'activité et de simplifier les changements.

Les recommandations de l'audit 15386 sont majoritairement mises en œuvre

fedpol a modélisé les principaux processus dans l'application de gestion des processus Signavio. Une analyse d'impact est réalisée pour assurer la continuité des activités, et divers processus permettant de rétablir le service ont été testés avec succès. La gestion des risques est encore en cours d'élaboration. À terme, elle doit d'une part garantir la surveillance efficace des mesures résultant des risques opérationnels et d'autre part intégrer la gestion des risques informatiques. Pour ce dernier point, fedpol met en place, au moment de l'audit, le contrôle de validation des droits d'accès pour une partie des applications.

Texte original en allemand

Verifica concernente la gestione delle TIC
Ufficio federale di polizia

L'essenziale in breve

L'Ufficio federale di polizia (fedpol) è la principale autorità di polizia della Svizzera. È il centro di contatto delle autorità di polizia nazionali ed estere e svolge compiti di polizia giudiziaria e di sicurezza, nonché compiti amministrativi e ausiliari di polizia. L'ambito direzionale Gestione delle risorse e strategia fornisce, in collaborazione con il settore decentralizzato Informatica e il Centro servizi informatici del Dipartimento federale di giustizia e polizia (CSI-DFGP), le prestazioni informatiche essenziali per l'attività operativa.

La verifica mira a valutare se la gestione delle questioni informatiche operata da fedpol funzioni in modo adeguato e mirato. Dalla verifica della governance IT emerge un quadro positivo, anche se molte basi sono ancora in fase di attuazione. Le fondamenta per una gestione efficace delle TIC sono state gettate. Vi è margine di miglioramento negli ambiti della gestione interna di progetti a lungo termine come progetti strategici e nello svolgimento completo di verifiche sulla sicurezza. Nel frattempo, la maggior parte delle raccomandazioni formulate nella «Verifica della gestione e dell'esercizio dell'informatica» del 2015 sono state attuate.

Le strategie messe in atto creano le basi per la trasformazione digitale

Per ottimizzare i processi aziendali e adeguarsi alle mutate esigenze dei diversi gruppi d'interesse, la strategia del DFGP definisce indirizzi strategici e obiettivi trasversali nell'ambito della trasformazione digitale. Essa integra le esigenze aziendali, le iniziative federali e stabilisce l'orientamento strategico dell'informatica.

Ciò forma la base della strategia TIC di fedpol. L'accento è posto sull'ottimizzazione della governance delle TIC, lo sfruttamento delle sinergie e l'affermazione di discipline sulla pianificazione per uno sviluppo di ambienti applicativi e prestazioni di servizi sicuro e orientato al futuro.

Il fornitore di servizi informatici CSI-DFGP si concentra sull'orientamento alla clientela e sull'introduzione di metodi agili per lo sviluppo e l'esercizio dei sistemi d'informazione. Lo scopo è avere un'architettura delle tecnologie sicura e flessibile come prerequisito per la trasformazione digitale nel Dipartimento.

Gestione dell'architettura aziendale e del portafoglio come strumento di controllo

Il DFGP sta conducendo un progetto sull'espansione della gestione dell'architettura aziendale a cui fedpol partecipa, finalizzato a ottenere decisioni migliori grazie a informazioni più trasparenti e interconnesse. Quale strumento di pianificazione e di controllo, ciò dovrebbe garantire un'interazione ottimale l'attività aziendale e l'informatica.

fedpol ha definito la propria architettura del sistema d'informazione e la sta già utilizzando per valutare il potenziale e le sfide poste da progetti nell'ambito della gestione del portafoglio. I progetti e i programmi in corso sono raggruppati per argomento e vengono analizzati

regolarmente a livello di Dipartimento in colloqui riguardanti il portafoglio circa il raggiungimento degli obiettivi, le dipendenze e la priorizzazione.

Controllo della fornitura delle prestazioni informatiche

Il CSI-DFGP è il fornitore di prestazioni per le applicazioni tecniche «safety critical» individuali. Dal catalogo delle prestazioni, fedpol seleziona in maniera conforme alle esigenze i livelli di servizio necessari per l'esercizio e lo sviluppo. Il loro rispetto viene valutato su base trimestrale. Le valutazioni mostrano un elevato livello di disponibilità. fedpol valuta le prestazioni a intervalli regolari. Tali valutazioni sono utilizzate dai fornitori di prestazioni per ottimizzare la loro offerta. Il CSI-DFGP gestisce l'inventario dell'hardware e del software necessari per il funzionamento delle applicazioni tecniche. L'Asset Management del settore informatico collabora con fedpol per pianificare e coordinare il ciclo di vita degli asset informatici al fine di sfruttarli in maniera ottimale. Un progetto sullo sviluppo di questo ambito permetterà in futuro ulteriori osservazioni incentrate sulla continuità operativa e la sicurezza delle informazioni.

Riconosciuta l'importanza delle informazioni e dei dati come elementi della gestione

fedpol sta conducendo un progetto per l'istituzione di un sistema di gestione della sicurezza delle informazioni (ISMS) che pone l'accento sulla necessità di proteggere informazioni e dati rispondendo alla seguente domanda concreta: qual è il livello adeguato di protezione che dovrebbe essere garantito per le diversei attività e misure? L'ottimizzazione dei processi dovrebbe assicurare un miglioramento della gestione e del monitoraggio della sicurezza delle informazioni. Nell'ambito di questo progetto, fedpol implementa pure una gestione dei rischi informatici integrata con l'ISMS e che confluisce nella gestione complessiva dei rischi a livello di Ufficio. Per ridurre al minimo i rischi, il Controllo federale delle finanze raccomanda di adeguare le prescrizioni per svolgere le verifiche sulla sicurezza in modo che tutte le applicazioni vengano regolarmente sottoposte a una siffatta verifica.

I dati rivestono la massima importanza per l'attività operativa di fedpol. Le basi giuridiche e il quadro normativo definiscono nel dettaglio le regole per il loro trattamento. Tramite un progetto, fedpol intende implementare una governance dei dati a livello di Ufficio, al fine di creare trasparenza sull'utilizzo dei dati e fornire un sostegno uniforme per tutte le fasi del ciclo di vita dei dati. I nuovi esami fondati sui dati dovrebbero servire a sviluppare l'attività e semplificare i cambiamenti.

Attuata la maggior parte delle raccomandazioni formulate nella verifica 15386

fedpol ha modellato i processi più importanti in Signavio, un'applicazione per la gestione dei processi. Un'analisi dell'impatto garantisce la continuità operativa, inoltre sono stati testati con successo diversi processi per ripristinare l'esercizio. La gestione dei rischi è ancora in fase di sviluppo. L'obiettivo è, da un lato, garantire che le misure risultanti dai rischi operativi vengano monitorate in maniera efficace e, dall'altro, integrare la gestione dei rischi informatici. Per quanto riguarda il secondo obiettivo, al momento della verifica fedpol stava introducendo il controllo per convalidare le autorizzazioni degli utenti per una parte delle applicazioni.

Testo originale in tedesco

ICT steering audit
Federal Office of Police

Key facts

The Federal Office of Police (fedpol) is Switzerland's supreme police authority. It is the point of contact for the police forces in Switzerland and abroad, and performs tasks in the areas of crime, security, administration and support. The Resource Management and Strategy Directorate, together with the decentralised IT units and the Federal Department of Justice and Police's IT Service Centre (ISC-FDJP), provides key IT services for operational areas.

The aim of the audit is to assess whether the steering of fedpol's IT needs is appropriate and target-oriented. The audit of IT governance yielded a positive picture, although many principles are still in the process of being implemented. The foundation for effective ICT steering has been laid. There is room for improvement in the steering of longer-term internal plans as strategic projects and in the full implementation of security checks. Most of the recommendations made in the 2015 audit report "Operation and maintenance of IT systems" have now been implemented.

Strategies lay the foundations for digital transformation

In order to optimise business processes and meet the changing requirements of different stakeholders, the FDJP's strategy defines the overarching direction and targets for the digital transformation. It integrates the business requirements and federal initiatives, and sets the strategic direction for IT.

It forms the basis for fedpol's ICT strategy. The focus is on optimising ICT governance, exploiting synergies and establishing planning disciplines for the forward-looking and secure further development of application landscapes and services.

The IT service provider ISC-FDJP focuses on customer orientation and the introduction of agile methods for the development and operation of information systems. The goal is a flexible and secure technology architecture as a prerequisite for digital transformation in the department.

Enterprise architecture and portfolio management are used as steering instruments

The FDJP is conducting a project to expand enterprise architecture management, and fedpol is involved in this. The aim is to achieve better decision-making through more transparent and networked information. This planning and steering instrument is intended to ensure an optimum interplay between business operations and IT.

fedpol has defined its information systems architecture and is already using it to evaluate the potential of, and challenges posed by, aspects of the portfolio management project. Ongoing projects and programmes are grouped together thematically and the portfolio discussions include a regular assessment regarding the achievement of goals, dependencies and prioritisation.

IT service provision is steered

The ISC-FDJP is the service provider for individual security-critical specialist applications. fedpol selects the service levels from the service catalogue on the basis of its operational and development needs. Compliance is assessed on a quarterly basis. Evaluations show a high level of availability. fedpol evaluates the services at regular intervals, and the service providers use these evaluations for optimisation purposes. The ISC-FDJP manages the inventory of the hardware and software needed for operating the specialist applications. IT Asset Management works together with fedpol to plan and coordinate the life cycle of the IT assets with a view to achieving optimum value added. An expansion project will allow a wider-ranging view in future, with a focus on business continuity and information security.

The importance of information and data as steering elements is well known

fedpol is conducting a project to set up an information security management system (ISMS). It is centred around the protection requirements for information and data. Specifically, what is the appropriate level of protection that should be guaranteed for which activities and measures? Optimised processes should ensure improved steering and monitoring of information security. In this project, fedpol is also implementing IT risk management which is integrated with the ISMS and flows into the overall risk management at office level. To minimise risk, the SFAO recommends that the specifications for performing security checks be adjusted so that all applications are regularly subjected to a security check.

Data is extremely important for fedpol's business operations. The legal foundations and regulations define the rules on data processing in detail. A fedpol project aims to implement office-wide data governance which creates transparency on data usage and provides consistent support for all phases of the data life cycle. New data-driven views should promote business development and simplify changes.

Most recommendations from audit 15386 have been implemented

fedpol modelled the most important processes in the Signavio process management application. An impact analysis ensures business continuity; in addition, various processes for restoring operations were successfully tested. Risk management is still being developed. The finished product must, firstly, ensure that measures in response to operational risks are effectively monitored and, secondly, incorporate the management of IT risks. As regards the latter, at the time of the audit fedpol had introduced validation checks on user permissions for some applications.

Original text in German

Generelle Stellungnahme der Geprüften

Stellungnahme des fedpol

fedpol bedankt sich bei der EFK für die sorgfältige Durchführung der Prüfung, die kollaborative und bereichernde Zusammenarbeit sowie für den fundierten Bericht, welcher die Wichtigkeit der IKT-Steuerung aufgezeigt und die damit verbundenen Herausforderungen ausgewogen darlegt. fedpol nimmt die zahlreichen positiven Feststellungen zur IKT-Strategie, der steuernden Wirkung der IKT-Organisation sowie der Bestätigung des eingeschlagenen Weges dankend entgegen. Da die IKT-Steuerung bei fedpol anhand einer sehr hohen Messlatte durch das COBIT-Framework bewertet wurde, ermutigen die positiven Bewertungen und zielgerichteten Empfehlungen, die Anstrengungen der letzten Jahre fortzusetzen.

Stellungnahme des ISC-EJPD

Das ISC-EJPD bedankt sich bei der Eidgenössischen Finanzkontrolle für die konstruktive Durchführung der Prüfung.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Bundesamt für Polizei (fedpol) ist Teil des Eidgenössischen Justiz und Polizeidepartements (EJPD). Es ist auf Bundesebene die Ansprechstelle für die Polizeikorps des In- und Auslandes und erfüllt kriminal-, sicherheits-, verwaltungs- und unterstützende Aufgaben. Die Bundeskriminalpolizei verantwortet die kriminalpolizeilichen Aufgaben. Der Bundessicherheitsdienst erfüllt die sicherheitspolizeilichen Aufgaben des Schutzes von Personen und Gebäuden. Die Polizeiunterstützung wird namentlich mit den polizeilichen Informationssystemen geleistet, die von fedpol zugunsten der Strafverfolgungsorgane der Kantone und des Bundes betrieben werden. Der Direktionsbereich Internationale Polizeikooperation ist zuständig für die nationale Plattform in Sachen Information, Koordination und Analyse für kantonale und internationale Partner.

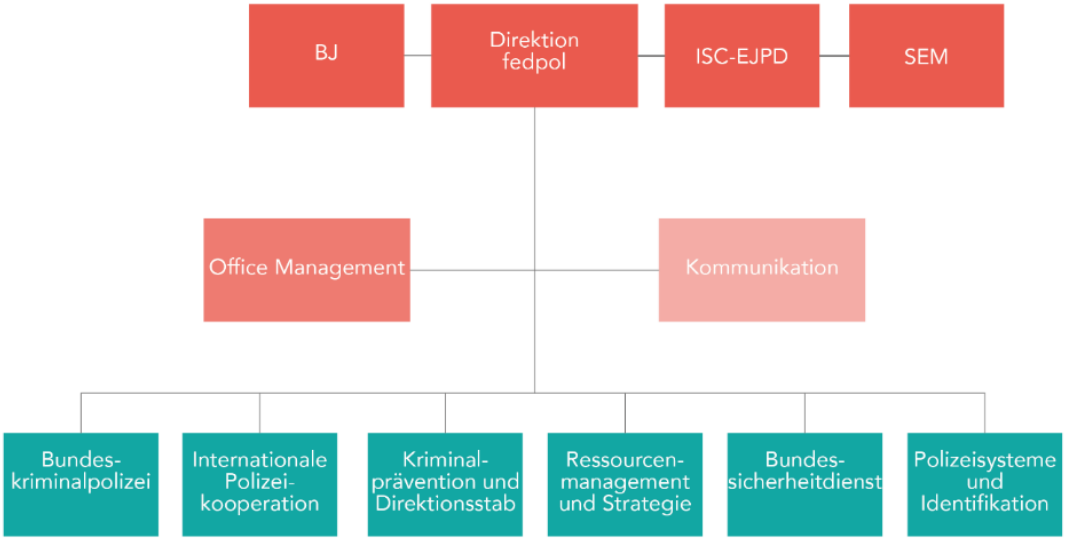

Abbildung 1: Organigramm von fedpol (Quelle: fedpol)

Viele IKT-Aufgaben sind dezentral in den Direktionsbereichen integriert. Der Direktionsbereich Ressourcen Management und Strategie (RMS) steuert die IKT-Aktivitäten übergreifend. So stellt RMS die IKT-Sicherheit, -Wirtschaftlichkeit und -Architektur sicher. Das Bundesamt für Informatik und Telekommunikation (BIT) und das Informatik Service Center (ISC-EJPD) sind die wichtigsten IKT-Leistungserbringer und betreiben 58 Fachanwendungen für fedpol. Die Bundeskriminalpolizei betreibt mit Ausnahmebewilligung sieben Anwendungen. fedpol stellt seine IKT-Anwendungen einem erweiterten Nutzungskreis zur Verfügung: darunter anderen Mitarbeiterinnen und Mitarbeitern des EJPD sowie kantonalen und internationalen Polizeiorganisationen. Zusätzlich entwickelt und betreibt fedpol nationale Informationssysteme und stellt diese den Sicherheits- und Migrationsbehörden von Bund und Kantonen zur Verfügung.

1.2 Prüfungsziel und -fragen

Mit dieser Prüfung beurteilt die EFK, ob die Steuerung der Informatikbelange angemessen und zielführend funktioniert.

Die der Prüfung zugrunde gelegten Fragen lauten:

1. Ist die Steuerung der Informatik zweckmässig und konsistent definiert sowie angemessen als Führungsaufgabe verankert?
2. Wird die Führung der Informatikbelange auf allen Funktionsstufen entsprechend den Vorgaben und zielführend wahrgenommen?
3. Werden IT- und Informationssicherheitsrisiken identifiziert und angemessen gehandhabt?
4. Wurden die Empfehlungen der Prüfung 15386 umgesetzt?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Stefano Iafigliola und Warren Paulus in der Zeit vom 1. Februar bis 11. März 2022 durchgeführt. Bernhard Hamberger nahm die Federführung wahr. Die Prüfung orientierte sich an der Vorgabe P000 - Informatikprozesse in der Bundesverwaltung sowie am Rahmenwerk COBIT[1] 2019 der ISACA[2]. Die Prüfhandlungen erfolgten bei fedpol und dem ISC-EJPD. Der vorliegende Bericht gibt den Stand per Mitte März 2022 wieder.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 16. Mai 2022 statt. Teilgenommen haben

seitens fedpol: Stv. Direktorin, Chief Information Officer, Unternehmensarchitekt, Informationssicherheitsbeauftragter, Abteilungschef Finanzen Beschaffung und Controlling und

seitens ISC-EJPD: Chief Technology Officer.

Die EFK war vertreten durch den Federführenden und das Revisionsteam.

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

EIDGENÖSSISCHE FINANZKONTROLLE

[1] Das COBIT (Control Objectives for Information and Related Technology) Framework liegt aktuell in der Version 2019 vor und ist ein international anerkanntes Referenzmodell, das dem Anwender bei der besseren Verwaltung von Informationen und Technologien hilft.

[2] ISACA ist ein unabhängiger, globaler Berufsverband für IT-Revisoren, Wirtschaftsprüfer sowie Experten der Informationssicherheit und IT-Governance.

2 Die IKT-Steuerung bei fedpol

2.1 Ein angemessenes IT Management Framework

Das Eidgenössische Justiz- und Polizeidepartement (EJPD) hat die IT-Governance geregelt. Die bundesweite Organisation, die führenden Gremien und die geltenden Vorgaben sind spezifiziert und das Zusammenspiel zwischen den Organisationseinheiten detailliert ausgeführt. Die Aufbauorganisation der IKT-Steuerung und Führung innerhalb des Departements ist mittels Prozessbeschreibungen und der Zuordnung von Aufgaben, Rollen und Lieferobjekten formell geregelt.

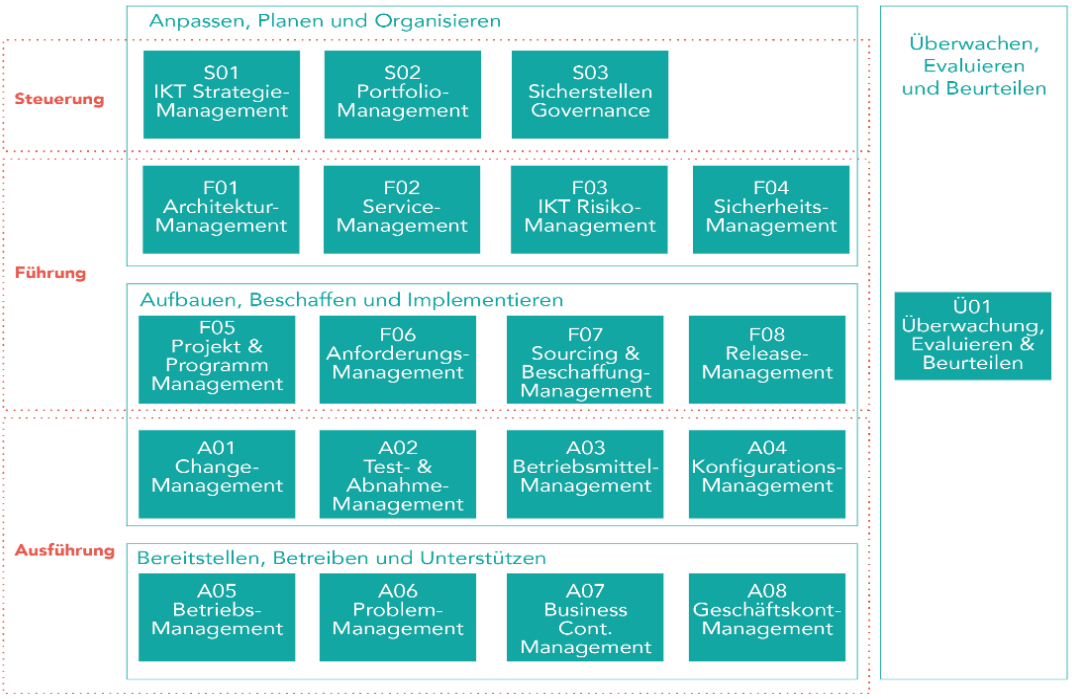

Abbildung 2 : IT Management Framework (Quelle: fedpol)

Das EJPD IKT-Prozesshandbuch führt als Regelwerk die Grundlagen der IKT-Governance aus. Es beschreibt im Detail die Prozesse, die Rollen sowie die Aufgaben und dient als Handlungsgrundlage für alle am Prozess beteiligten Mitarbeiter. Zusätzlich sind für die einzelnen Prozesse Prinzipien und Abgrenzungen definiert. Die Prinzipien geben wertvolle Kontextinformationen und helfen bei der Umsetzung der Vorgaben. Die EFK fokussiert bei dieser Prüfung auf die IKT-Prozesse aus der Prozessgruppe «Anpassen, Planen und Organisieren».

Die kontinuierliche Optimierung der IT-Governance unterstützt die Umsetzung der Unternehmensziele

fedpol hat seinerseits in der IKT-Strategie das Handlungsfeld «IKT Organisation und Steuerung optimieren» definiert. Die Umsetzung der IKT-Strategie hat zum Ziel eine etablierte und wirksame Governance zur organisationsweiten Steuerung der IKT zu ermöglichen. Mit Hilfe der Governance soll sichergestellt werden, dass die IKT die Unternehmensziele und Unternehmensstrategie optimal unterstützt. Wichtige Bestandteile der anvisierten IKT-Governance sind Prozessstrukturen, Organisationsvorgaben und Führungsstrukturen für

die dezentrale IKT Organisation. Eine erste Version der IKT Governance fedpol liegt zum Zeitpunkt der Prüfung vor, welche unter Einbezug der zentralen Stakeholder erarbeitet wurde.

Die Gremien STAR und FIT sind für die Steuerung essentiell

2018 hat fedpol für die Steuerung die Gremien STAR (Steuerungsboard) und FIT (Fachgremium Informatik) erneuert. Das Steuerungsboard ist das Vorgremium der Geschäftsleitung. Es berät die Direktion bei der strategischen Steuerung und Führung und bearbeitet die Themen Strategie, Projektportfolio, IKT, Finanzen und Kommunikation. Des Weiteren hat es zum Ziel, bestehende Meinungsverschiedenheiten aus der Geschäftstätigkeit oder aus anderen Fachgremien zu diskutieren und wirkungsvoll zu bereinigen.

Das FIT befasst sich ganzheitlich mit der Informatik und fungiert als Mittel für die operative Führung und Steuerung auf Basis der strategischen Vorgaben. Es informiert und berät sämtliche Rollenträger der IKT hinsichtlich der Themen Architektur, Informationssicherheit, Datenschutz, IKT-Controlling und bearbeitet die Koordination der Vorhaben und die Ausschöpfung von allfälligen Synergien.

Anwendungen unterstützen die Umsetzung der Governance

fedpol nutzt verschiedene Anwendungen zur Unterstützung der Geschäftstätigkeit. Die Prozessmanagement Anwendung Innovator soll bald die Anwendung Signavio ersetzen. Mit Innovator können Informationen zu den Geschäftsprozessen übergreifend und durchgängig in einem einzigen Werkzeug dargestellt werden. Es eignet sich für die Modellierung von Prozessen, Daten, sowie Architekturen und integriert verschiedene fachspezifische Modellierungssprachen. Die vollständige und durchgängige Abbildung der Geschäftstätigkeit ist grundlegend, um mit verschiedenen Analysewerkzeugen bspw. Geschäftsprozesse zu optimieren.

Für das Risiko Management ist im 2021 ein Projekt zur Aktualisierung der Lösung GRC Toolbox umgesetzt worden. Die GRC Toolbox ist eine zentrale und integrierte Softwarelösung für «Governance, Risk and Compliance» (GRC). Von der Identifikation, Analyse und Bewertung der Risiken bis zur Überwachung der Kontrollen und Massnahmen bietet die Lösung ein geeignetes Mittel um das Risiko Management effektiv und effizient zu unterstützen.

Beurteilung

Das «IT Management Framework» von fedpol ist angemessen. Die grundlegenden Elemente der Aufbau- und Ablauforganisation, die involvierten Rollen und die Ziele sind im Detail definiert. fedpol bewertet regelmässig die Wirksamkeit und definiert Massnahmen zur Verbesserung. So sind kürzlich die Gremien für die Abstimmung STAR und FIT optimiert worden, so dass Querschnittsthemen wie bspw. das Portfolio Management, die Architektur und Informationssicherheit besser gesteuert werden können.

fedpol hat geeignete Anwendungen im Einsatz um die Geschäftstätigkeit genau abzubilden und allfällige Optimierungen vorzunehmen. Für eine effiziente und gezielte Aktualisierung von Prozessen ist die zentralisierte Verwaltung im Prozessmanagement Tool Innovator gewinnbringend. Des Weiteren ist die Nutzung der Anwendung GRC Toolbox für die Überwachung und Steuerung von Massnahmen zielführend.

2.2 Die Strategie zur Digitalen Transformation vereint das Geschäft und die IKT

Die zunehmende Vernetzung der Geschäftsabläufe, die rasch steigenden Anforderungen der Bevölkerung sowie der Wirtschaft und das damit verbundene hohe Tempo der Digitalen Transformation haben das Bedürfnis generiert eine Digitalisierungsstrategie zu erstellen, welche Stossrichtungen und Zielsetzungen auf Stufe EJPD vereint. Die Strategie integriert die Vorhaben auf Bundesebene, die Geschäftsstrategien der Verwaltungseinheiten und Stossrichtungen der IKT auf Stufe Departement und des Direktionsbereichs Ressourcenmanagement und Strategie von fedpol. Das EJPD steuert die Digitale Transformation im Rahmen der Supportprozesse. fedpol fokussiert auf deren Umsetzung und das Vorantreiben der Digitalisierung seiner Kernprozesse. Beide Bereiche sollen die Digitale Transformation des Departements befähigen.

Die Strategie ist anhand einer zentralen Vision formuliert. Diese definiert ein langfristiges Zielbild und reicht damit weiter als die vierjährigen Umsetzungszyklen der IKT-Strategien. Fünf übergeordnete Ziele leiten sich von der Vision ab und bilden die Grundpfeiler der Digitalen Transformation. Des Weiteren sind in den Stossrichtungen die verschiedenen Intentionen thematisch gruppiert, sodass der Transformationsplan mit einer Roadmap und mit definierten Meilensteinen umgesetzt werden kann. In der Roadmap werden über den Zeitraum von 10–12 Jahren anhand eines Reifegradmodells die anvisierten Zielzustände beschrieben. Das EJPD wendet für die Umsetzung der Strategie ein agiles Vorgehen an.

Vision

«Das EJPD versteht die Digitale Transformation als Mittel zur effizienteren und qualitativ besseren Aufgabenerfüllung. Die Digitale Transformation soll kein Selbstzweck sein, sondern dazu führen, dass das EJPD seine Geschäftsprozesse innerhalb des Departements, mit seinen Partnern, Wirtschaft und Bürgerinnen und Bürgern durchgehend digital und auf einem hohen Sicherheitsniveau abwickelt».

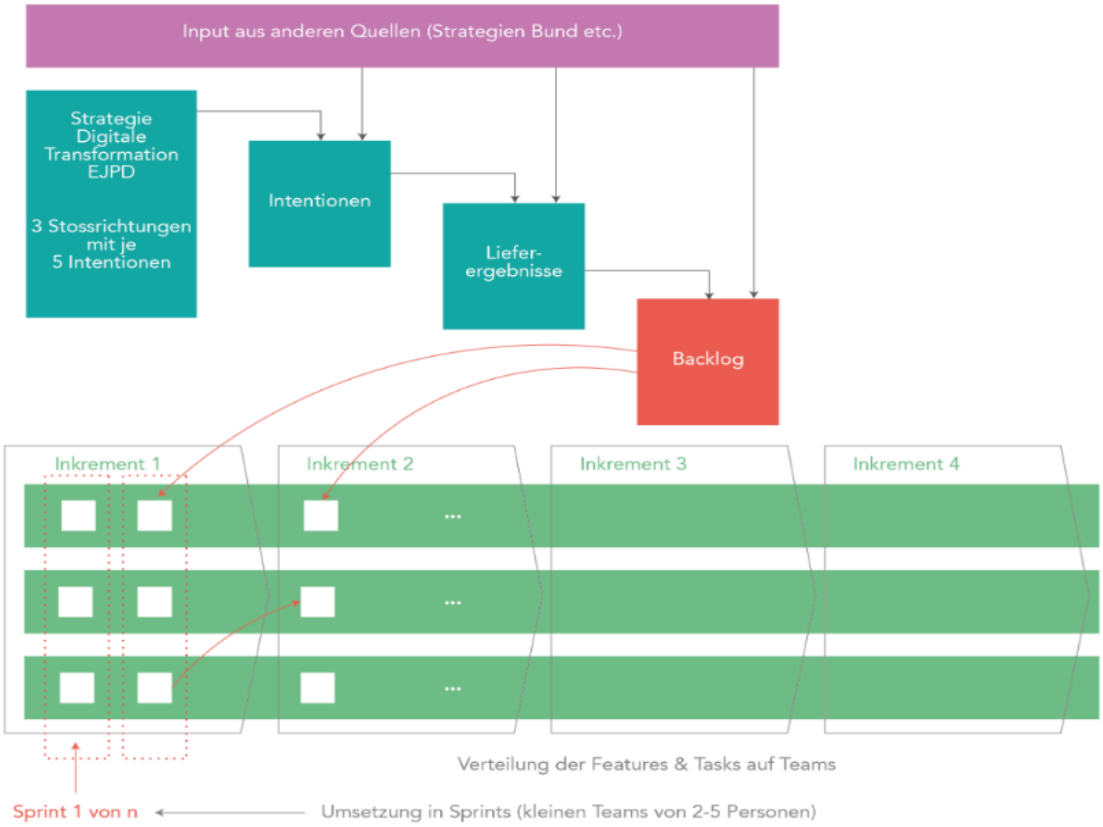

Abbildung 3: Strategieentwicklung (Quelle: EJPD)

Die Direktionsbereiche von fedpol erstellen neue Geschäftsstrategien

Um die Strategie zur Digitalen Transformation zu unterstützen und um den Fokus auf die Digitalisierung der Kernprozesse zu setzen, erstellen die fedpol Direktionsbereiche in einem vierjährigen Zyklus eigene Teilstrategien. Die Unternehmensstrategie fedpol bildet die Grundlage und enthält eine Vision, eine Mission sowie direktionsbereichsübergreifende Ziele. Mit dieser Grundlage erarbeiten die Direktionsbereiche die Teilstrategien mit Mission und Zielen. Die Wichtigkeit der IKT ist in einer der vier Missionen «Wir entwickeln und betreiben nationale Informationssysteme und Kompetenzzentren» strategisch verankert. Die verschiedenen Teilbereichsstrategien sind teilweise in Überarbeitung. Diese sollen sich in den Kontext der bestehenden Digitalisierungsstrategie eingliedern. Zur Förderung der fedpol Kultur sind Werte definiert, welche die Mitarbeitenden bei der täglichen Arbeit als Leitbild begleiten.

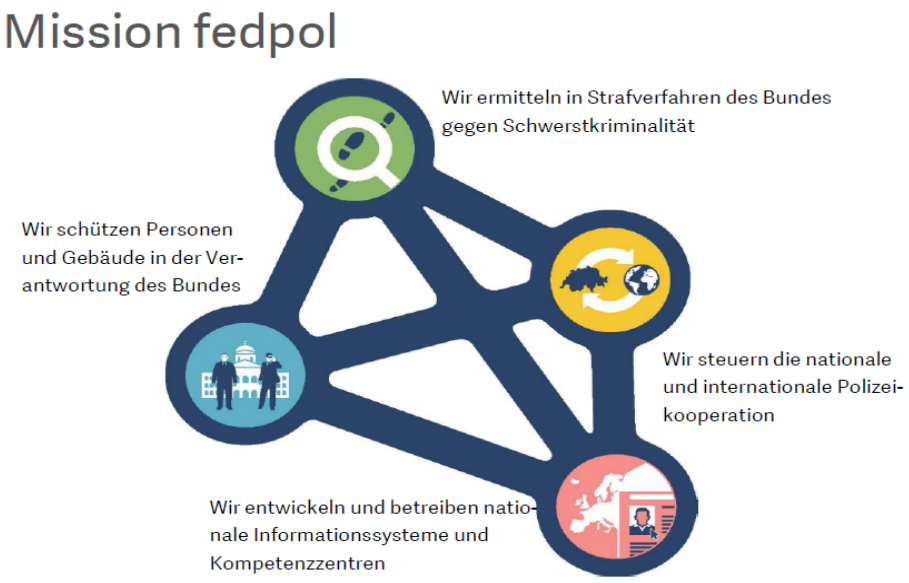

Abbildung 4: Geschäftsstrategie (Quelle: fedpol)

Die IKT-Strategie von fedpol stärkt Planungs- und Steuerungsinstrumente

fedpol hat für die Erstellung der IKT-Strategie vorab das Umfeld, den Nutzen und die Ziele definiert. Das Strategie Team hat in einem ersten Schritt die Interessensvertreter befragt und für die strategischen Bereiche die Maturität bewertet. Damit sind die Anforderungen aufgenommen worden und eine GAP Analyse ist entstanden. Das Team hat aus der Analyse einen Massnahmenkatalog abgeleitet, welcher mit dem Masterplan 2021–2025 umgesetzt werden soll.

Die IKT-Strategie 2021–2025 dient vor allem der zielorientierten Ausrichtung der Bereichsübergreifenden Planungs- und Steuerungsinstrumente. Die IKT-Strategie hat eine Vision und basiert auf den fedpol Werten. Sie gibt Grundsätze vor für den IKT-Einsatz zur Erfüllung der Mission fedpol und benennt Handlungsfelder mit Zielen und Massnahmen. Daraus resultierende Umsetzungsvorhaben sind die Basis für die Digitalisierung der Prozesse von fedpol.

Vision IKT fedpol

Sicher, geschäfts- und zukunftsorientiert – «fit for mission»

«Unsere IKT-Services erlauben fedpol und Kooperationspartnern schnell und effizient auf wechselnde Lagen der öffentlichen Sicherheit zu reagieren und so effiziente Polizeiarbeit zu leisten. Wir liefern unseren Kunden und Partnern sichere und gesetzeskonforme IKT-

Services als Basis für überzeugende Resultate in Prävention, Kooperation und Verfolgung. Mit innovativen Lösungen ermöglichen wir Fortschritt und Zukunftsfähigkeit und sind im polizeilichen Umfeld der Schweiz der technologische Vorreiter».

Um das Handeln nach den Grundsätzen auszurichten, definiert die IKT-Strategie prioritäre Handlungsfelder mit klaren Zielen:

1. *IKT-Organisation und -Steuerung optimieren*
2. *Informationssicherheit durch Prozesse stärken*
3. *Applikationslandschaft durch strategische Werkzeuge weiterentwickeln*
4. *Businessanforderungen ins Zentrum stellen*
5. *Organisationsweit standardisierte IKT-Prozesse etablieren.*

Die wichtigen Vorhaben zur Etablierung einer Unternehmensarchitekturfunktion und eines Informationssicherheits-Management Systems (ISMS) werden zum Prüfungszeitpunkt durch Projekte umgesetzt.

Die Geschäftsstrategie des ISC-EJPD fokussiert auf Kundenorientierung

Als Informatik-Leistungserbringer im sicherheitskritischen Umfeld ist das ISC-EJPD vielfältigen Anforderungen ausgesetzt. Um die erforderliche Kundenorientierung sicherzustellen, will das ISC-EJPD flexibel auf Anforderungen reagieren und gleichzeitig Stabilität im sicherheitskritischen Umfeld bieten können. Dies bedinge neue Organisations- und Zusammenarbeitsformen und agile Projektorganisationen.

Als Ausgangspunkt für die Strategieentwicklung hat das ISC-EJPD eine Situations- und Umfeldanalyse durchgeführt. Die Geschäftsstrategie ISC-EJPD setzt sich aus mehreren Elementen zusammen: Der Vision, die durch die strategischen Grundsätze konkretisiert wird, den strategischen Stossrichtungen und den dazugehörenden strategischen Zielen. Die Umsetzung der Strategie wird durch die Definition von Jahreszielen mit entsprechenden Messkriterien periodisch überprüft. Bei Bedarf werden entsprechende Anpassungen vorgenommen.

Vision ISC-EJPD

«Das ISC-EJPD ist die erste Wahl als Gesamtlösungsanbieter für individuelle Fachanwendungen mit erhöhten Anforderungen in den Aufgabenbereichen des EJPD. Mit schnellem Agieren, Lernen und Umsetzen von Kundenanforderungen stellen wir den Kundennutzen ins Zentrum».

Beurteilung

Die angewendeten Methoden zur Entwicklung der Strategien sind angemessen. Die Digitalisierungsstrategie auf Stufe Departement und die Geschäftsstrategien von fedpol enthalten die wesentlichen Elemente und definieren Ziele. Die Strukturierung und Granularität ermöglichen die Verwirklichung und eine periodische Validierung des Umsetzungsstands. Die IKT-Strategie von fedpol ist an den übergeordneten Elementen ausgerichtet und angemessen um Planungs- und Steuerungsinstrumente zu stärken.

2.3 Das Unternehmensarchitekturmanagement befindet sich im Aufbau

Das EJPD führt aktuell ein Projekt zum Aufbau des Unternehmensarchitekturmanagements (UAM). Die Umsetzung ist eine wichtige Voraussetzung zur Unterstützung der Massnahme «Planungsdisziplinen etablieren» im Sinne des «Once-Only-Prinzips» der IKT-Strategie des Bundes. Das EJPD definiert das Zielbild, das Geschäftsorganisationskonzept und eine entsprechende Roadmap, welche in Zusammenarbeit mit den Ämtern (darunter auch fedpol) den übergreifenden Aufbau koordiniert. Durch die Unternehmensarchitektur soll eine gemeinsame und integrierte Sicht auf das Geschäft und die IKT geschaffen werden. Neue Architektursichten sollen die Darstellung von komplexen Zusammenhängen und folglich die Bereitstellung fundierter Entscheidungsgrundlagen für die Definition und Priorisierung von Vorhaben ermöglichen. Künftig will das EJPD Synergiepotenziale vereinfacht erkennen und die IKT optimal an die Geschäftsanforderungen ausrichten können. Die folgende Abbildung zeigt die Einbettung des UAM in der Organisation:

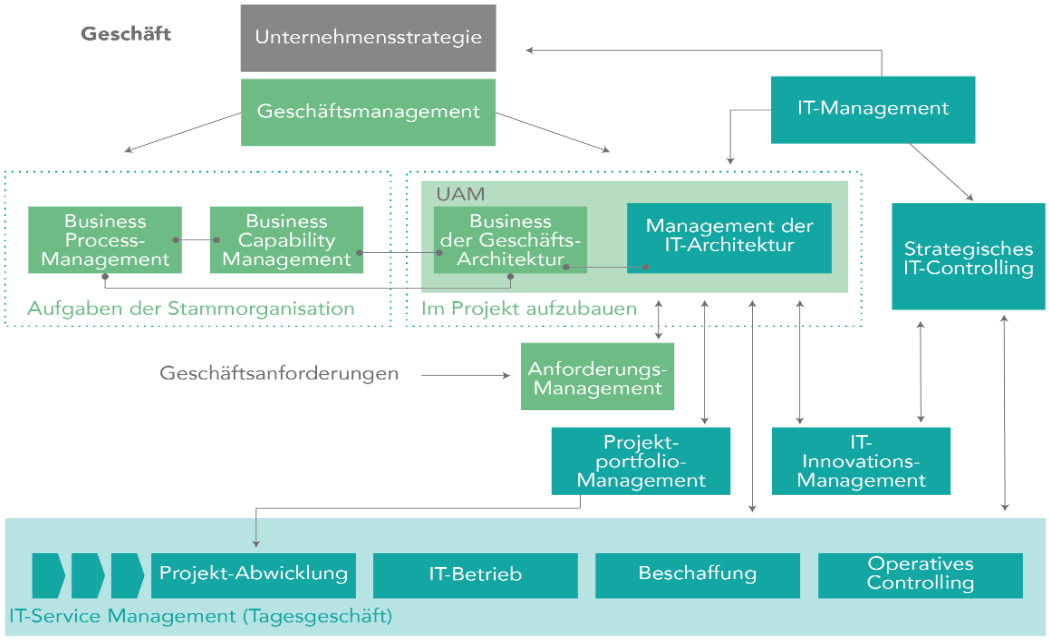

Abbildung 5: Unternehmensarchitektur Konzept (Quelle: EJPD)

Die Informationssystemarchitektur von fedpol ist erfasst

fedpol führt für den Aufbau der Unternehmensarchitektur in Abstimmung mit den übergreifenden Vorgaben und Vorhaben das Projekt «IKT Asset Management». Ziel ist es, eine vollständige Landschaft der Informationssysteme von fedpol zu erstellen. Dadurch entsteht eine gesamtheitliche Sicht über alle Informationssysteme, deren Schnittstellen und übertragenen Daten. fedpol nutzt die neuen Artefakte um grundlegende Informationen über die Informationssysteme sichtbar zu machen. Die Anwendungsverantwortlichen und Projektleiter nutzen diese Informationen um die Umsetzbarkeit von Vorhaben und Projekten zu bewerten und um Aspekte der Informationssicherheit zu beurteilen. Die Konzepte zur Informationssystemmodellierung und das Betriebshandbuch bestehen schon und spezifizieren im Detail die Elemente um die Erstellung und Pflege der Informationssystemarchitektur zu ermöglichen.

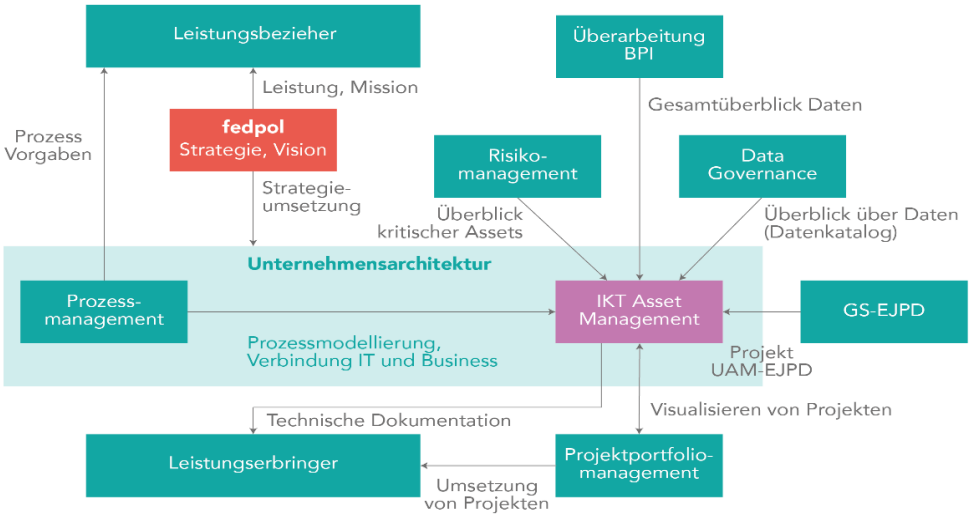

Abbildung 6: Unternehmensarchitektur Konzept (Quelle: fedpol)

Die Revision des BPI eröffnet neue Chancen

Die Direktorin fedpol hat den Auftrag erteilt das Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) zu revidieren und ein technologie- und anwendungsneutrales Gesetz zu schaffen.

Das BPI regelt die Nutzung von Informationssystemen, die historisch unabhängig sind und mittels Schnittstellen interagieren. Dies ist nicht mit den Geschäftsanforderungen und der daraus resultierenden zukünftigen Informationssystem- und Datenarchitektur von fedpol kompatibel. Es besteht das Bedürfnis, Daten aus verschiedenen Anwendungen zu aggregieren und auf verschiedene Datenquellen zuzugreifen. Das BPI entspricht deshalb datenschutzrechtlich nicht mehr den Ansprüchen bezüglich Transparenz und ist zudem nicht technologieneutral formuliert. Dadurch besteht aufgrund der laufenden Weiterentwicklungen der IKT-Landschaft ein ständiger Revisionsbedarf der Gesetzgebung. Aufgrund der Dauer dieser Verfahren besteht das Risiko, dass die IKT-Landschaft nicht mit dem geltenden Recht konform ist.

Beurteilung

Die Vorgehensweise zum Aufbau des Unternehmensarchitektur Managements im Departement und bei fedpol ist sinnvoll. Um die Funktion Unternehmensarchitektur im Zielzustand vollumfänglich als Steuerungsinstrument zu nutzen, ist es von grosser Bedeutung, dass die Ebene Unternehmensarchitektur erfasst und die Technologiearchitektur integriert wird. Dies ermöglicht die organisationsübergreifende, geschäftsgetriebene und abgestimmte Entwicklung von Soll- und Transitionsarchitekturen. Ein etabliertes UAM ist Voraussetzung, um Ressourcen effizienter zu steuern und die Digitale Transformation zu ermöglichen.

Des Weiteren begrüsst die EFK die geplante Revision des BPI, sodass in Zukunft Veränderungen der IKT-Landschaft nicht mehr zwingend einen Revisionsbedarf des BPI zur Folge haben. Zum Revisionszeitpunkt bestehende Einschränkungen bei der Ausschöpfung des UAM können voraussichtlich gelöst werden.

2.4 Portfoliomanagement mit Bezug zu strategischen Zielen

fedpol beurteilt alle Projekte und Programme hinsichtlich ihres Strategiebeitrags. Bei der Erstellung der Projektaufträge muss das Projektteam den Bezug zu geltenden Strategien erläutern und bewerten. Auf Stufe Projektportfoliomanagement ermittelt das Steuerungsboard STAR auf Grund von drei vordefinierten Kriterien strategisch relevante Projekte und Programme. Diese Projekte und Programme werden im Falle von Ressourcenengpässen priorisiert.

Der Projekt-Review-Prozess ermöglicht eine vielseitige Beurteilung

fedpol nutzt für die Freigabe von Vorhaben und Projekten einen zweistufigen Prozess. Die Vorhabenskizze beschreibt die Ausgangslage und die Ziele des Vorhabens. Nach der Prüfung und Freigabe durch den Informatikcontrollingbeauftragten, das Projektportfoliomanagement und das Fachgremium Informatik und Projekte (FIT) erstellt das Projektteam einen detaillierten Projektinitialisierungsauftrag gefolgt von einem Projektauftrag. Die Projektfreigabe erfolgt nachdem verschiedene Fachexperten und die FIT-Mitglieder das Projekt erneut beurteilt haben, sodass verschiedene Aspekte wie bspw. Informationssicherheit, Integration, Qualität- und Risikomanagement berücksichtigt werden.

Regelmässige Portfolio Besprechungen für eine projekt- und organisationsübergreifende Abstimmung

fedpol und das ISC-EJPD haben Projekte in «Städte» und «Quartiere» gruppiert, um diese im Rahmen der monatlichen Portfolio Besprechungen zu diskutieren. Für die einzelnen Städte existiert eine aggregierte Sicht zu den Dimensionen Ressourcen, Meilensteine und Risiken. Ein Ampelsystem unterstützt die Verantwortlichen bei der Identifikation von Differenzen zwischen der Planung und dem Ist und der darauffolgenden Definition von Massnahmen. Die Rück- und Ausblicke werden genutzt um allgemeine Pendenzen und Massnahmen wirksam mit Zuordnung der Verantwortlichkeiten zu verfolgen.

Vierteljährlich findet das «Big Room Planning Meeting» statt. An diesem Anlass findet eine projektübergreifende Abstimmung in Bezug zu Risiken, Abhängigkeiten und Meilensteinen statt. Die verschiedenen Interessensvertreter diskutieren anhand des aktuellen Erreichungsgrads allfällige Anpassungen in der Ressourcenallokation.

Übergeordnet führt das EJPD jährlich eine Portfolio-Besprechung zur übergreifenden Erfassung des aktuellen Stands der Projekte und zur departementalen Prioriserung durch.

Eine Richtlinie zur Unterstützung bei der Abwicklung von Projekten und Programmen

Bei der Projekt- und Programmabwicklung sind eine Vielzahl von Vorgaben zu berücksichtigen, welche teilweise unzureichend dokumentiert und methodisch nicht in die Projektmanagementmethode HERMES integriert sind. Das EJPD hat festgestellt, dass es für Projektauftraggeber und Projektleiter eine Herausforderung ist, sich einen Überblick über alle relevanten Vorgaben zu verschaffen bzw. alle laufenden Veränderungen im Auge zu behalten. Zur Unterstützung hat das EJPD eine Richtlinie definiert. Diese regelt im Rahmen der anwendbaren Vorgaben die Abwicklung von IKT-Projekten und IKT-Programmen, berücksichtigt ebenfalls die Verwendung von agilen Methoden und fördert Synergien und Skaleneffekte.

Das IKT-Cockpit unterstützt die finanzielle Führung

Die Abteilung Finanzen, Beschaffung und Controlling gibt für die IKT-Aufwendungen gesamthaft jährlich ein Budget vor. Diese bewilligten Mittel bilden die Grundlage für die finanzielle Führung. Die IKT-Kosten gliedern sich in zwei Hauptkategorien. Eine Kategorie umfasst interne Aufwendungen für Hardware, Software, Lizenzen, Entwicklungs- und Beratungsdienstleistungen welche bei fedpol selbst anfallen. Der wesentliche Teil der IKT-Kosten fällt in die zweite Kategorie. Sie umfasst alle IKT-Dienstleistungen, welche im Rahmen von Leistungsvereinbarungen bspw. vom ISC-EJPD und dem BIT erbracht werden. Die Anwendung IKT-Cockpit unterstützt die finanzielle Führung und die Berichterstattung. fedpol führt zur Überwachung der Kosten ein Controlling auf monatlicher Basis durch und kann gegebenenfalls Massnahmen ergreifen. Die Berücksichtigung des Nutzens und die Priorisierung der Ressourcen erfolgt innerhalb des Projektportfoliomanagements.

Ein Planungs- und Visualisierungstool soll die Führungsunterstützung vereinfachen

fedpol führt im Rahmen eines laufenden Projekts ein Planungs- und Visualisierungstool ein, welches unter anderem für das Projektportfoliomanagement genutzt werden kann. Die notwendigen Kennzahlen werden aktuell situativ in Form von Berichts- und Planungsprodukten zur Verfügung gestellt. Die Menge an Daten und Informationen wächst jedoch stetig und das manuelle Aufbereiten und Zusammenstellen der Geschäftsdaten erfordert einen grossen Zeitaufwand und ist fehleranfällig. Die neue Lösung soll die Entscheidungsfindung anhand von korrekten Daten auf strategischer und operativer Ebene durch zielgruppengerechte Berichte und Analysen verbessern.

Beurteilung

Die Aktivitäten des Portfoliomanagements sind angemessen. fedpol hat Methoden zur Evaluation der durchzuführenden Projekte und Programme und geeignete Mittel zur Überwachung von Ressourcen, Risiken, Erreichungsgrad und Abhängigkeiten. Die EFK begrüsst das Projekt zur Einführung eines Planungs- und Visualisierungstool für eine optimierte Führungsunterstützung.

fedpol klassifiziert Projekte anhand von drei Kriterien als politisch-strategisch bedeutsam. Diese Kriterien leiten sich hauptsächlich von exogenen Faktoren ab. Projekte mit dem Ziel interne Strukturen langfristig optimal auf die Organisation auszurichten, haben wenig Gewicht.

Empfehlung 1 (Priorität 2)

Die EFK empfiehlt fedpol eine Anpassung der Projektportfoliobewertung, so dass Vorhaben mit interner und langfristiger Perspektive auch als «strategische Projekte» berücksichtigt werden.

Die Empfehlung ist akzeptiert.

Stellungnahme des fedpol

fedpol ist mit der Empfehlung einverstanden, die Projektportfoliobewertung zu überarbeiten, um internen Projekten mehr Gewicht zu geben.

2.5 Angemessenes Servicemanagment und hohe Verfügbarkeit

fedpol bezieht die Dienstleistungen für die Bereitstellung der Büroautomation und Clients vom BIT und dem Eidgenössischen Department für auswärtige Angelegenheiten. Das ISC-EJPD ist für fedpol der Leistungserbringer für individuelle Fachanwendungen mit erhöhten Anforderungen an die Sicherheit. Es betreibt spezifische und sicherheitskritische Fachanwendungen in den Bereichen "Polizei, Justiz und Migration". Diese Fachanwendungen erleichtern die Zusammenarbeit zwischen den Behörden auf nationaler, kantonaler und kommunaler Ebene sowie den Informationsaustausch zwischen der Schweiz und ausländischen Behörden.

IKT-Betrieb mit hoher Verfügbarkeit im Jahr 2021

fedpol hat für die Nutzung von IKT-Leistungen Dienstleistungsvereinbarungen abgeschlossen. Diese basieren auf dem Dienstleistungskatalog des ISC-EJPD und umfassen den Betrieb und Support der Fachanwendungen. Für die Verfügbarkeit können anforderungsgerecht verschiedene Service Levels vereinbart werden. Für diese sind die entsprechenden Parameter definiert, wie beispielsweise die maximale Zeit, die nach Störungen bis zum Übergang in den Normalbetrieb verstreichen darf oder der nach Störungen maximal tolerierbare Datenverlust. Zusätzlich kann auf Wunsch die Datenspeicherung zur Gewährleistung von Georedundanz ausgelagert werden.

fedpol verwendet nach Bedarf für zusätzliche Leistungen Projekt- und Dienstleistungsvereinbarungen. Mit diesen können zusätzlich auftragsspezifisch Arbeitspakete, Lieferobjekte, Termine und Rahmenbedingungen geregelt werden.

Das ISC-EJPD stellt quartalsweise Berichte zur Verfügung. Diese bestätigen eine hohe Verfügbarkeit der Anwendungen und informieren die Leistungsbezüger über allfällige Ausfälle. Serviceverletzungen sind transparent und allfällige Massnahmen können gemeinsam erarbeitet werden. Jährlich aktualisiert das ISC-EJPD anhand eines Kalkulationsblattes die verrechnungsrelevanten Grunddaten für das Folgejahr. Diese werden anschliessend mit fedpol neu verhandelt.

Kundenumfragen zur Verbesserung der Dienstleistungen

Das BIT und das ISC-EJPD machen regelmässig Umfragen um die Dienstleistungserbringung zu messen und zu verbessern. Die Kriterien umfassen quantitative Elemente wie Verarbeitungszeiten und Verfügbarkeit sowie auch qualitative Elemente wie bspw. Freundlichkeit und Betreuung.

Beurteilung

Das verwendete Rahmenwerk und die Aktivitäten des Service Managements zwischen dem Leistungsnehmer fedpol und den Leistungserbringern ISC-EJPD und BIT sind angemessen.

Es existieren passende Vereinbarungsformen zur formellen Regelung der Beziehungen. Die Vereinbarungen umfassen sinnvolle Messgrössen. Diese werden in angemessenen Zeitabständen erhoben und rapportiert. Die EFK begrüsst die Tatsache, dass der Leistungserbringer Kundenumfragen zur Bewertung und Verbesserung der Dienstleistungen durchführt. fedpol nutzt dieses Instrument aktiv.

2.6 Systematisches IKT Asset Management

Das ISC-EJPD führt das Life-Cycle Management der Fachanwendungen von fedpol. Es ist verantwortlich für die Erhebung der Assets in Bezug auf Wert, Kosten und Planung. In Zusammenarbeit mit den Ämtern generiert der Life Cycle Manager einen Quartalsbericht und eine Jahresplanung.

In einem ersten Interview validiert der Life-Cycle Manager die Zuordnung der Verantwortung und stellt die Vollständigkeit und Genauigkeit des IKT Asset Liste sicher. Der Life-Cycle Verantwortliche informiert die Projektverantwortlichen von fedpol über den Status und die erarbeitete Life Cycle-Lösungsvariante. Mit Hilfe der Empfehlungen beauftragt und priorisiert fedpol im Portfolio Management seine Projekte. Das Life-Cycle Board des ISC-EJPD verifiziert das Planungsfeedback seitens fedpol und kommuniziert die finale Jahresplanung im ISC-EJPD. Ein Quartalsbericht bildet die Grundlage für die Finalisierung der Jahresplanung und der Budgetempfehlung für die nächsten fünf Jahre.

Die Bundeskriminalpolizei plant jährlich den Life-Cycle für die selbst betriebenen Anwendungen basierend auf einer Bedarfserhebung.

Das Projekt «IKT Asset Management» eröffnet neue Beurteilungsperspektiven

fedpol führt im Rahmen des Aufbaus der Unternehmensarchitektur das Projekt «IKT Asset Management». Das Ziel ist es, einen gesamtheitlichen Überblick über alle Informationssysteme und deren Schnittstellen zu generieren. In der IKT-Landschaft sollen sich strukturiert Informationen verwalten lassen, welche für unterschiedliche Interessensvertreter wie bspw. Anwendungsverantwortliche und Projektleiter nützlich sind. Für die Informationssicherheit soll eine Grundlage entstehen, um neue Perspektiven zu gewinnen und Bewertungen vorzunehmen. Zusammenhänge zwischen den Informationssystemen und den Organisationen, welche die Informationssysteme nutzen sollen transparent werden. Die Kritikalität von Anwendungen wird bekannt, sodass bessere Einschätzungen zum Erhalt der Geschäftskontinuität möglich werden. Die Erstellung von Sicherheitskonzepten und die Ableitung von Risikoanalysen und Anforderungen zur Verbesserung der Informationssicherheit und des Datenschutzes sollen vereinfacht werden.

«Pooling» optimiert die Verwendung von Lizenzen

Das ISC-EJPD benötigt für den Betrieb der Infrastruktur Lizenzen vor allem für Server Produkte von Microsoft und Linux. Die Bundesverwaltung hat 2020 den Vertrag mit Microsoft erneuert. Dieser ist aus finanzieller Sicht grundlegend für die Lizenzierung aller Microsoft Produkte. Das ISC-EJPD prüft mit Hilfe des Tools Virtual Center jährlich manuell das Mengengerüst. Es meldet sowohl den Mehrbedarf wie auch allfällige Lizenzrückgaben. Dieses wird an das Bundesamt für Bauten und Logistik (BBL) übermittelt, welches mit Unterstützung von SoftwareOne die Mengen validiert. Das BBL konsolidiert die Meldungen und kann überzählige Lizenzen zwischen den Ämtern optimal umverteilen.

Beurteilung

Das ISC-EJPD hat ein geeignetes Vorgehen um IKT Assets zu identifizieren, zu erfassen und aktuell zu halten. Die Verantwortlichkeiten sind bekannt. Es existiert ein angemessener Prozess um den Lebenszyklus der IKT Assets unter Berücksichtigung von unterschiedlichen Interessensvertretern zu koordinieren und eine abgestimmte Planung vorzunehmen. Durch

den Prozess können die Ämter die geschäftlichen Anforderungen und die optimale Wertausschöpfung der IKT Assets berücksichtigen.

Für die selbst betriebenen Anwendungen existiert ein bedarfsgetriebener Life-Cycle Prozess bei der BKP.

Die Durchführung des Projekts «IT Asset Management» eröffnet sinnvolle Beurteilungsperspektiven in den Domänen Informationssicherheit, Business Continuity Management und Risiko Management.

Das Lizenzen Management für Microsoft Server Produkte ist angemessen. Mit Virtual Center existiert ein Register für die Verwaltung der Lizenzen und ein Vorgehen zur Validierung der Verwendung. Der Partner SoftwareOne analysiert als zentrale Anlaufstelle im Auftrag des BBL den Bedarf und kann amtsübergreifende Optimierungen identifizieren und umsetzen.

2.7 Die Bedeutung von Informationen und Daten als Elemente der Steuerung ist erkannt

Für Anwendungen mit erhöhtem Schutzbedarf führt fedpol ein Bearbeitungsreglement. Die verwendeten Daten sind entsprechend den Informationssicherheits- und Datenschutzanforderungen klassifiziert. Die Zugriffsberechtigungen, Rollen und die autorisierten Zugriffstellen sind im Detail aufgeführt und den autorisierten Organisationen und Stellen zugeordnet. Die Benutzerverwaltungsprozesse sind definiert und regeln die Vergabe, Mutation und Löschung für die verschiedenen Systemumgebungen in Abhängigkeit der Organisation. Die Bearbeitungsreglemente definieren für die Geschäftsfunktionalitäten durch wen und in welcher Art Daten bearbeitet werden können. In Bezug auf die Archivierung bestehen Konzepte, welche die archivwürdigen Daten spezifizieren und das Vorgehen im Detail beschreiben.

Eine «Data Governance» entsteht

Aufgrund der historisch organisationsgetriebenen Informationssystemarchitektur von fedpol existieren für vergleichbare Anwendungsfälle verschiedene Lösungen und Daten. Dies hat zu Redundanzen geführt, welche eine einheitliche Führung der Datenbearbeitung erschweren. Diesbezügliche Schwierigkeiten sind bereits in der Prüfung «19394 Audit de l'efficacité de la lutte contre la cybercriminalité» identifiziert worden. fedpol hat für die Bewertung des Ist Zustands eine Analyse der «Data Governance» durchgeführt.

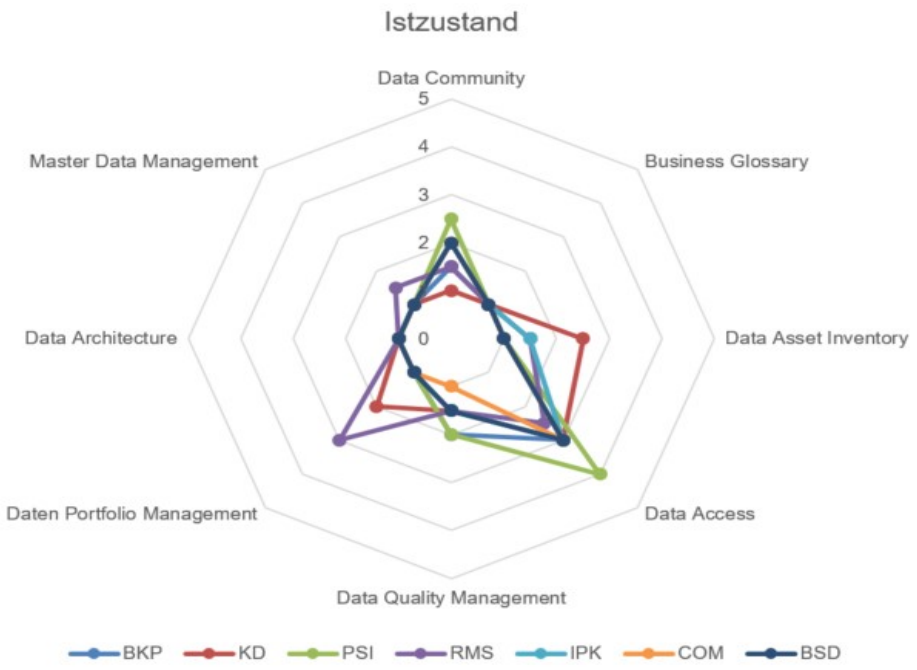

Abbildung 7: Datamanagement Maturität (Quelle: fedpol)

Resultierend aus der Analyse der Stärken, Schwächen und Ursachen hat fedpol folgende Handlungsfelder identifiziert:

1. *Amtsweite Data Governance etablieren.*
2. *Schlüsselfunktionen für die Datenbewirtschaftung etablieren.*
3. *Kommunikation, Sensibilisierung und Schulung durchführen.*

Mit der Durchführung des Projekts «DataGov» will fedpol eine amtsübergreifende Data Governance umsetzen. Dies beinhaltet die Definition von Regeln und Prozessen, welche die Entscheidungsfindung rund um Daten optimal unterstützen soll. Damit sollen verschiedene Potenziale ausgeschöpft werden können. Einerseits besteht dann Transparenz zum aktuellen Datenstand und dem Datenbearbeitungszweck. Dadurch soll die Identifikation und die Auflösung von Redundanzen erleichtert werden. Andererseits kann das Geschäft zielgerichtet weiterentwickelt werden, indem die gleichen Daten nur durch eine Lösung bearbeitet werden oder indem man durch die Verknüpfung von Daten neue Informationen generiert. Die Massnahmen zur Einhaltung bestehender Anforderungen hinsichtlich Datenschutz, Datenqualität, Datensicherheit und Kontrolle sollen kohärent und effizient umgesetzt werden können. Programme und Projekte sollen aus einer neuen Perspektive beurteilt werden und Anpassungen der Rechtssetzung vereinfacht umgesetzt werden können. Das Vorhaben befindet sich in der Projektinitialisierungsphase und die Zeitachse ist noch in Arbeit.

Beurteilung

Die EFK begrüsst die Bestrebungen zur Etablierung einer Data Governance, da hier spezifischer Handlungsbedarf besteht. Die Umsetzung generiert neue Perspektiven, welche grundlegend sind für die optimale Weiterentwicklung der datengetriebenen Aufgaben des fedpol und die Stärkung von Domänen wie Architektur, Projektmanagement und Informationssicherheit.

2.8 Die Sicherheitsdokumentation wird effizient erstellt

Das ISC-EJPD ist der wichtigste IKT-Leistungserbringer von fedpol. Weiter laufen Bestrebungen, die noch von fedpol selbst betriebenen Anwendungen an das ISC-EJPD zu übergeben. Die EFK fokussiert daher bei den betrieblichen Sicherheitsthemen auf das ISC-EJPD. Das EJPD hat eine IKT-Sicherheitsrichtlinie definiert. Diese führt die Anforderungen aus dem IKT-Grundschutz aus und dient als Handlungsanweisung für die vereinfachte Anwendung der übergeordneten Vorgaben. Das EJPD definiert für Projekte, welche beim ISC-EJPD durchgeführt werden, ein optimiertes Vorgehensmodell zur Erstellung der Sicherheitsdokumentation. Es existiert ein für alle Schutzobjekte geltendes unterschriebenes IKT-Grundschutz Dokument. Das EJPD stellt für EJPD Fachanwendungen mit Schutzniveau zwei eine standardisierte Risikoanalyse zur Verfügung. Gemäss dieser Analyse existieren keine Risiken, für welche bei einzelnen Fachanwendungen mit Standard Architektur weitergehende Sicherheitsanforderungen und Massnahmen notwendig sind. Die Schutzbedarfsanalyse und die schutzobjektspezifischen Teile des IKT-Grundschutzes sind integrale Bestandteile des Informations- und Datenschutzkonzepts (ISDS) und werden nicht in eigenständigen Dokumenten gepflegt. Für aus Projekten resultierende neue Anwendungen, welche nicht dem Standard entsprechen, müssen eigene Risikoanalysen durchgeführt sowie entsprechende Massnahmen zur Risikominimierung definiert und umgesetzt werden.

2.9 Die Vorgaben zur Durchführung von Sicherheitsprüfungen müssen angepasst werden

Gemäss IKT-Grundschutz in der Bundesverwaltung müssen alle Anwendungen und IKT-Systeme während der Entwicklung, vor der Inbetriebnahme und im laufenden Betrieb periodisch auf Schwachstellen überprüft werden. Das ISC-EJPD hat hierfür auf der Ebene Anwendung das Vorgehen der Schwachstellenprüfungen beschrieben. Möglich sind statische und dynamische Prüfungen in Abhängigkeit der eingesetzten Technologie und dem Entwicklungsstand. Für verschiedene Anwendungen sind seit der Inbetriebnahme keine Sicherheitsprüfungen durchgeführt worden.

Beurteilung

Das GS-EJPD verfügt über ein optimiertes Vorgehensmodell zur Erstellung der Sicherheitsdokumentation. Somit bestehen für alle Fachanwendungen mit Schutzniveau zwei nur ein IKT-Grundschutz Dokument und nur ein ISDS Konzept. Die EFK hat festgestellt, dass die Sicherheitsdokumentation für Anwendungen ausserhalb der Standard Architektur teilweise nicht aktuell ist. Sie verzichtet jedoch auf eine Empfehlung, da durch die Operationalisierung des ISMS (vgl. 2.10) diese Schwächen adressiert werden.

Die Spezifikation des Vorgehens zur Durchführung von Sicherheitsprüfungen ist sinnvoll. Für verschiedene Anwendungen sind seit der Inbetriebnahme jedoch keine Sicherheitsprüfungen durchgeführt worden, weil es keine wesentlichen Programmänderungen gab. Somit besteht die Notwendigkeit zusätzliche Kriterien zur Auslösung von Sicherheitsprüfungen zu definieren.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem ISC-EJPD, die Vorgaben zur Durchführung von Sicherheitsprüfungen so anzupassen, dass alle Anwendungen regelmässig einer Sicherheitsprüfung unterzogen werden.

Die Empfehlung ist akzeptiert.

Stellungnahme des ISC-EJPD

Das ISC-EJPD wird die Empfehlung der EFK operationalisieren, indem künftig die Ämter über die Anwendungsverantwortlichen (AV) im Rahmen des jährlichen Planungszyklus angehalten werden, die entsprechenden Sicherheitsprüfungen ihrer Anwendungen einzuplanen und die Durchführung zu organisieren.

2.10 fedpol setzt ein Projekt zur Einführung eines Informationssicherheitsmanagemensystems um

Projekte lösen die Verfahren zur Erstellung von sicherheitsrelevanter Dokumentation aus. Eine kontinuierliche Erhebung und Einstufung der Informationssicherheitsrisiken findet nur begrenzt statt. Die Informationssicherheitsrisiken sind nicht im Gesamtrisikomanagement und im Gesamtrisikokatalog integriert. Es existiert kein zentrales Register zur Verwaltung von aus den ISDS-Konzepten resultierenden Restrisiken. Diese werden dezentral von den Anwendungsverantwortlichen verwaltet. Ebenso findet eine Neubeurteilung der Restrisiken nur unregelmässig statt.

fedpol führt darum ein strategisches Projekt zum Aufbau eines Informationssicherheits-Management Systems (ISMS) durch. Mit dem Projekt soll die Steuerung, die Überwachung und die Sicherstellung der Informationssicherheit verbessert werden. Das Projekt sollte bis Ende 2022 umgesetzt werden. Hierbei liegt der Fokus auf dem kontinuierlichen Verbesserungsprozess zur Erreichung, Haltung und Optimierung eines angemessenen Schutzniveaus. Für die Umsetzung des ISMS sind detaillierte Sicherheitsziele und Massnahmen definiert. Diese umfassen im Wesentlichen die Zuordnung von Verantwortlichkeiten, die systematische Führung eines Risikokatalogs mit entsprechenden Massnahmen und die nachvollziehbare Zuordnung von Aufgaben und Schutzbedarf zu Informationen. Für die Umsetzung des ISMS sind die involvierten Rollen und deren Aufgaben für folgende Themen im Detail spezifiziert:

1. *Verwaltung der Schutzobjekte*
2. *ISDS-Prozesse*
3. *Verwaltung und Steuerung der Informationssicherheitsrisiken*
4. *Security Incident Management*
5. *Verwaltung von Ausnahmen*
6. *Reporting*
7. *Kontinuierliche Verbesserung.*

Im neuen Konzept stehen Informationen im Mittelpunkt von Sicherheitsbeurteilungen und Massnahmen

Im Zentrum der Betrachtung stehen Informationen, welche als Schutzobjekte definiert sind. Die für die Organisation wertvollen und schützenswerten Informationen werden identifiziert und nach Schutzbedarf klassifiziert. Sie werden zentral in einem Inventar verwaltet. Basierend auf dem Schutzbedarf kann eine abstrahierte Risikobetrachtung vorgenommen werden, welche nicht mehr im Kontext der Fachanwendungen, sondern der behandelten

Informationen stattfindet. Weiterführend wird der Schutzbedarf nicht mehr für ein IKT-Objekt, sondern für das verwendete Informationselement bestimmt. Daran müssen sich in der Folge alle Informationsträger ausrichten.

Das Risikomanagement integriert IKT- und Informationssicherheitsrisiken

Das Projekt «Aufbau ISMS» umfasst ebenfalls das IKT-Risikomanagement. fedpol hat hierzu ein Konzept erstellt. Dieses soll verwendet werden, um die Umsetzung des IKT-Risikomanagements zu erleichtern. Im Wesentlichen beschreibt es das Vorgehen zum Führen des Risiko- und Massnahmenkatalogs der IKT-Risiken. Das IKT-Risikomanagement soll das Management der Informationssicherheitsrisiken umfassen und systematisch Teil des Risikomanagements werden.

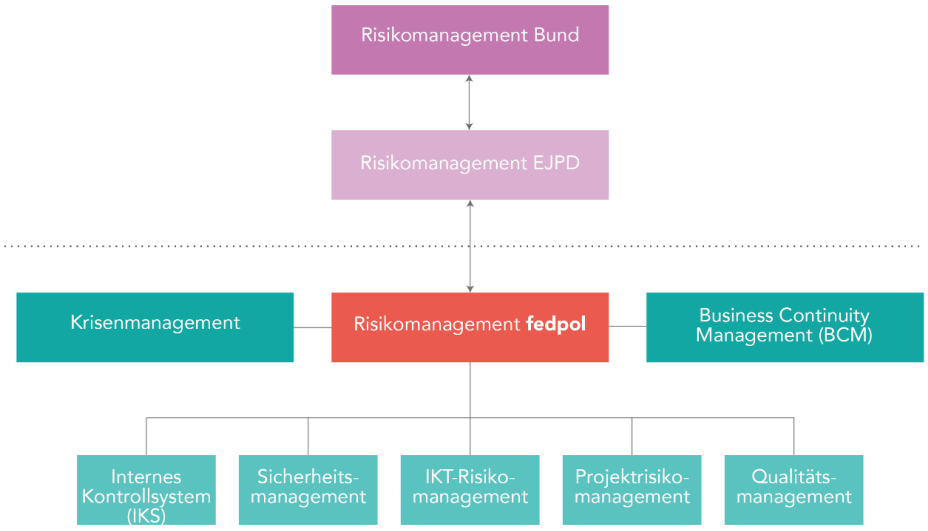

Abbildung 8: Risikomanagement Konzept (Quelle: fedpol)

Das IKT-Risikomanagement soll die Identifikation, Behandlung und Verwaltung aller IKT-Risiken steuern. Die zentrale Bewirtschaftung wird über die Elemente Risikokatalog, Risikobehandlungsplan, Risikoakzeptanzliste und Massnahmenkatalog erfolgen. Operationelle IKT-Risiken sollen ebenfalls verwaltet und als solche im Risikokatalog gekennzeichnet werden. Diese werden ebenfalls einem Informationsschutzobjekt und somit einem Risikoeigner zugeordnet. Für die Unterstützung der Prozesse will fedpol die Anwendung Swiss GRC Toolbox nutzen. Die Verantwortung für die regelmässige Überprüfung und Bewirtschaftung der Risiken sowie die Überprüfung der Massnahmenumsetzung obliegt dem Informatiksicherheitsbeauftragten (ISBO) der Organisation. Dieser trägt die Verantwortung für die Aktualität des IKT-Risikomanagements, des Massnahmenkatalogs sowie der Eingliederung in das Risikomanagement. Für die Validierung der Umsetzbarkeit hat fedpol für die beschriebenen Elemente einen «Proof of Concept» erstellt.

Beurteilung

Die EFK befürwortet die Erarbeitung, Umsetzung und der Plan für die Einführung des ISMS. Hierbei können identifizierte Schwachstellen behoben und verschiedene Optimierungen umgesetzt werden. Aufgrund der Tatsache, dass Informationssicherheitsrisiken sich organisationsunabhängig manifestieren und deren Behandlung die Beteiligung unterschiedlicher Interessensvertreter erfordert, ist die gemäss fedpol geplante Definition und

Umsetzung einer RACI[3]-Matrix basierend auf den definierten Prozessen zur Stärkung der Governance zielführend.

In Bezug auf das IKT-Risikomanagement nimmt die EFK zur Kenntnis, dass dieses operativ im Wesentlichen über die gleichen Verfahren der Informationssicherheit gesteuert und durchgeführt werden soll. Dabei ist darauf zu achten, dass das IKT-Risikomanagement zusätzlich zu Informationssicherheits- und Datenschutz Risiken auch weitere Domänen wie bspw. Auslagerungsverhältnisse, Lizenzen und Management Aktivitäten angemessen berücksichtigt. Hierzu existieren umfassende Rahmenwerke, wie z. B. COBIT 5 for Risk, an denen sich fedpol orientieren kann.

Um die Wirksamkeit der vorgelagerten Aktivitäten Identifikation, Bewertung und Behandlung zu stärken ist die Überwachung der Umsetzung essentiell. Hierfür hat fedpol mit der Anwendung Swiss GRC Toolbox ein geeignetes Werkzeug.

2.11 Die zielgesteuerte Personalentwicklung wird ausgebaut

Die Rekrutierung und Einstellung erfolgt unter Berücksichtigung des Bundespersonalgesetzes dem standardisierten Prozess der Bundesverwaltung.

Nach der Einstellung führt der Vorgesetzte jährlich mindestens ein Zielvereinbarungs-, wie auch ein Mitarbeitergespräch mit den Mitarbeitenden. In der Standortbestimmung beschreibt der Mitarbeiter die Dimensionen Zusammenarbeit, Aufgabenkreis, Arbeitsmittel und die zeitliche Auslastung. Er hat die Möglichkeit Anmerkungen zum Führungsverhalten des Vorgesetzten anzubringen. Der Vorgesetzte erstellt eine umfangreiche Beurteilung inkl. einem Soll/Ist-Vergleich bezüglich Zielerreichung. Die Leistungsziele sind beschrieben und haben Leistungsindikatoren zur Messung. Abschliessend kann der Vorgesetzte für die gezielte Mitarbeiterförderung auch Verhaltens- und Kompetenzziele vereinbaren und diese mittels der Definition von geeigneten Erwartungswerten prüfen.

Abbildung 9: Kompetenzen (Quelle: fedpol)

[3] RACI: Responsible, Accountable, Consulted, Informed

Das Management der Kompetenzen ist im Aufbau

Bei fedpol besteht zum Revisionszeitpunkt keine übergreifende Sicht über die bestehenden und zukünftig benötigten Fähigkeiten. Deshalb will fedpol ein Skillsmanagement lancieren. Damit soll sichergestellt werden, das vorhandenes Wissen und Fähigkeiten erhalten bleiben und neue entstehen. Das Skillmanagement ermöglicht eine langfristige, zielgerichtete Personalentwicklung. Der Bedarf an Know-how-Trägern für bestimmte Themen wie bspw. die Digitalisierung und qualifizierte Fach-, Projektleitungs- und Führungskräfte muss in Abstimmung mit den strategischen Zielen strukturiert aufgebaut werden.

Beurteilung

Die Prozesse zur Rekrutierung und Bewertung der Mitarbeitenden sind angemessen.

Der Aufbau eines langfristigen Kompetenz-Managements ist von grosser Bedeutung. Dieser wird von fedpol beabsichtigt. Aus diesem Grund verzichtet die EFK auf eine Empfehlung. Die grundlegenden Daten bestehen und können für die Mitarbeiterentwicklung und die langfristige Steuerung genutzt werden. Für die Stärkung von direktionsbereichsübergreifenden Disziplinen und der Innovationsfähigkeit, könnte die Nutzung eines «Job Rotation» Konzepts für das Skillsmanagement förderlich sein.

3 Umsetzung der Empfehlungen aus Bericht 15386

Von den zehn Empfehlungen (siehe Anhang 1) aus der Prüfung 15386 «Führung und Betrieb der Informatik» wurden sechs umgesetzt. Diese betreffen die Erfassung der Geschäftsprozesse, den Aufbau des Geschäftskontinuitätsmanagements und die Zentralisierung der IT. Die Empfehlungen 15386.003, 15386.004, 15386.005 und 15386.010 sind noch nicht vollständig erledigt. Die Empfehlungen betreffen die Domänen Risiko Management, Benutzerverwaltung, die Erfassung der IT und Informationssicherheitsprozesse.

Anhang 1: Empfehlungen aus Bericht 15386

Referenz	Status Umsetzung Empfehlung	
15386.001	Empfehlung	Die EFK empfiehlt, die Zentralisierungsvarianten wie z. B. in der IT-Forensik oder im Bereich der Bekämpfung der Internetkriminalität hinsichtlich absehbarer Vor- und Nachteile vollständig zu bewerten und zu dokumentieren. Basierend auf diesen Informationen ist die Zentralisierungsabsicht zu bestätigen oder zu widerlegen. Dabei ist darauf zu achten, dass alle relevanten Faktoren wie Strategien, Varianten, Risiken/Massnahmen, Kosten/Nutzen, etc. in die Überlegungen einbezogen werden (vgl. Bst. h Ziff. 2.1.2 fedpol Informatikstrategie 2014-2017). Gegebenenfalls ist rechtzeitig vor der gemäss Bundesratsbeschluss bis 2018 abzuschliessenden Migrationen eine weitere Ausnahmeregelung zu beantragen.
	Priorität	1
	Status	Umgesetzt; die Empfehlung wird geschlossen.
	Kommentar EFK	Eine Ausnahmeregelung besteht. Innerhalb fedpol laufen mehrere Vorhaben und Bestrebungen, welche die Zentralisierung der IKT-Systeme zum Ziel haben.
15386.002	Empfehlung	Die EFK empfiehlt, die Analyse der Abhängigkeiten der kritischen Prozesse von Einzelpersonen bei fedpol periodisch nachzuführen (z. B. alle zwei Jahre) und diesen Sachverhalt zentral zu dokumentieren. Darauf basierend sind Massnahmen vorzusehen, welche für selektierte Prozesse (risikoorientiertes Vorgehen) eine angemessene Stellvertretung sicherstellen.
	Priorität	2
	Status	Umgesetzt; die Empfehlung wird geschlossen.
	Kommentar EFK	Die Business Impact Analyse ist aktualisiert worden.
15386.003	Empfehlung	Die EFK empfiehlt, Fachspezialisten gezielt und umfassend in das Risikomanagement einzubeziehen. Insbesondere sollten Fachspezialisten auch im Risiko-Controlling zum Einsatz kommen. Dadurch wird die Nutzung des vorhandenen Know-hows erhöht. Insbesondere ist die Beurteilung des Restrisikos ein Tätigkeitsfeld, welches ohne Fachspezialisten nur schwer abgedeckt werden kann.
	Priorität	2

	Status	In Arbeit; die Empfehlung wird reaktiviert. fedpol wird gebeten für die definitive Umsetzung im Empfehlungs-controlling eine kurze Nachfrist zu beantragen
	Kommentar der EFK	Die Grundsätze des Risikomanagements Bund sind im «Handbuch zum Risikomanagement Bund» der Eidgenössischen Finanzverwaltung (EFV) definiert. Die fedpol führt entsprechend ein Risiko-Controlling für strategische Risiken aus. Über die Vorgaben der EFV hinausgehend existiert ein Handbuch «integriertes Risiko Management», welches die Risiko Management Prozesse von fedpol definiert. Die Massnahmen zur Gewährleistung einer integrierten und durchgängigen Risiko-Sicht befinden sich in der Umsetzung. Mit der Umsetzung der im Handbuch definierten Prozesse wird die Empfehlung umgesetzt sein.
15386.004	Empfehlung	Die EFK empfiehlt, den Prozess des Risikomanagements gemäss allgemeinen Standards auszubauen und insbesondere eine Phase für das Massnahmen-Controlling vorzusehen. Letzteres soll sinnvollerweise in ein Management-Reporting einfliessen. Hierdurch wird eine effektive Umsetzung der Massnahmen unterstützt.
	Priorität	1
	Status	In Arbeit; die Empfehlung wird reaktiviert. fedpol wird gebeten für die definitive Umsetzung im Empfehlungs-controlling eine kurze Nachfrist zu beantragen.
	Kommentar der EFK	Die Grundsätze des Risikomanagements Bund sind im «Handbuch zum Risikomanagement Bund» der Eidgenössischen Finanzverwaltung (EFV) definiert. fedpol führt entsprechend das Massnahmen-Controlling und Management Reporting für strategische Risiken aus. Über die Vorgaben der EFV hinausgehend existiert ein Handbuch «integriertes Risiko Management», welches die Risiko Management Prozesse von fedpol definiert. Für die vollständige Umsetzung der Empfehlung, muss das im Handbuch «integriertes Risiko Management» definierte Massnahmen Controlling für operative Risiken wirksam sein und nachvollziehbar dokumentiert werden.

15386.005	Empfehlung	Die EFK empfiehlt, für die Anwendungsbereiche bei denen noch keine periodische Kontrolle durchgeführt wird, diese einzuführen. Auf den Systemen eingetragene Benutzer, Rollen und Rechte müssen mit dem tatsächlichen Mitarbeitenden Bestand und deren Aufgaben übereinstimmen. Damit können übrig gebliebene Zuordnungen sicher erkannt und entfernt werden. Zudem ist eine Gesamtübersicht der Rechte zu erstellen und aktuell zu halten, welche pro Mitarbeitende auch die dezentralen und relevanten externen Rechte enthält.
	Priorität	1
	Status	In Arbeit; die Empfehlung wird reaktiviert. fedpol wird gebeten für die definitive Umsetzung im Empfehlungscontrolling eine kurze Nachfrist zu beantragen.
	Kommentar der EFK	Es existiert eine Zugriffsmatrix, welche den Zugriff von Geschäftsrollen zu Anwendungen regelt. Das EJPD hat im 2017 eine Anwendung zur Unterstützung der Benutzerverwaltung eingeführt. Die Kontrolle zur Validierung der Benutzerberechtigungen wird teilweise durchgeführt. Für die vollständige Umsetzung der Empfehlung, muss die Kontrolle zur Validierung der Benutzerberechtigungen für alle Anwendungen durchgeführt werden.
15386.006	Empfehlung	Die EFK empfiehlt, die Vollständigkeit der Anforderungen an die Verfügbarkeit für den Normalbetrieb sowie für Katastrophenszenarien für die kritischen Leistungen von fedpol zu überprüfen. Darauf ausgerichtete Massnahmen sind vorzusehen und regelmässig zu testen. Die Tests sind angemessen zu dokumentieren. Bei den Massnahmen und bei den Tests soll ein risikoorientiertes Vorgehen angewandt werden, d. h. es müssen Prioritäten gesetzt werden. Ziel ist es, die kritischen Leistungen von fedpol auch im Katastrophenfall sicherstellen zu können.
	Priorität	1
	Status	Umgesetzt; die Empfehlung wird geschlossen
	Kommentar der EFK	Die Business Impact Analyse ist aktualisiert worden und die Business Continuity Prozeduren sind getestet worden.

15386.007	Empfehlung	Die EFK empfiehlt, in einem stufenweisen Vorgehen (Top-Down) alle relevanten Prozesse im Prozessmanagement-Tool (z. B. SIGNAVIO) zu erfassen. Zur Sicherstellung einer zeitgerechten Erfassung ist eine Planung zu erstellen. Die Umsetzung ist dem Management zu rapportieren.
	Priorität	2
	Status	Umgesetzt; die Empfehlung wird geschlossen
	Kommentar der EFK	Die Organisationseinheit RMS-UE-RPM erstellt die Prozessdokumentation zentral in Zusammenarbeit mit den Fachspezialisten aus den Direktionsbereichen. Die Prozessmodelle werden stichprobenartig überprüft und aktualisiert.
15386.008	Empfehlung	Die EFK empfiehlt, die IKT-Prozesse auf Stufe Amt sowie die Schnittstellen zu Departments- oder bundesweiten IKT-Prozessen in einem zentralen Prozessmanagement-Tool zu erfassen. Damit soll eine zentrale Verwaltung sowie die Kontrolle innerhalb der Prozesse unterstützt werden.
	Priorität	2
	Status	Umgesetzt; die Empfehlung wird geschlossen
	Kommentar der EFK	Die Organisationseinheit RMS-UE-RPM erstellt die Prozessdokumentation zentral in Zusammenarbeit mit den Fachspezialisten aus den Direktionsbereichen. Die Prozessmodelle werden stichprobenartig überprüft und aktualisiert.
15386.009	Empfehlung	Die EFK empfiehlt, neben dem (finanziellen) IKS auch die wichtigsten übrigen Prozesskontrollen (Schlüsselkontrollen) zentral zu erfassen. Zur Erfassung der Kontrollen und der Referenzieren auf Anwendungen bietet sich z. B. das Prozessmanagement-Tool an.
	Priorität	2
	Status	Umgesetzt; die Empfehlung wird geschlossen
	Kommentar der EFK	Die Organisationseinheit RMS-UE-RPM erstellt die Prozessdokumentation zentral in Zusammenarbeit mit den Fachspezialisten aus den Direktionsbereichen. Die Prozessmodelle werden stichprobenartig überprüft und aktualisiert. Eine Risiko-Kontrollmatrix existiert für die Leistungsgruppen Finanzen, Controlling und Personalwesen. Die IT Schlüsselkontrollen sind im Dokument «Richtlinie für IKT-Schlüsselkontrollen im EJPD» definiert.

15386.010	Empfehlung	Die EFK empfiehlt, die Prozesse für das Risikomanagement und für die Informationssicherheit vollständig zu dokumentieren. Dabei ist insbesondere beim Prozess für die Informationssicherheit darauf zu achten, dass dieser flexibel bleibt, um aktuellen Gefahren, wie z. B. Cyber-Threats oder Data-Leakage-Risiken, zeitnah und angemessen begegnen zu können.
	Priorität	2
	Status	In Arbeit; die Empfehlung wird reaktiviert. fedpol wird gebeten für die definitive Umsetzung im Empfehlungscontrolling eine kurze Nachfrist zu beantragen.
	Kommentar der EFK	Über die Vorgaben der EFV hinausgehend existiert ein Handbuch «integriertes Risiko Management Handbuch», welches die Risiko Management Prozesse der fedpol definiert. Im Rahmen des Projekts «Aufbau ISMS» werden für die Informationssicherheit neue Prozesse und Kontrollen definiert. Die EFK erachtet die Empfehlung als umgesetzt, sobald die neuen Prozesse dokumentiert sind.

Anhang 2: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die polizeilichen Informationssysteme des Bundes vom 13. Juli 2008, SR 361
Bundesgesetz über den Datenschutz vom 24. März 2022, SR 231.1
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020, SR120.73
Bundespersonalgesetz vom 14. Dezember 2012, SR 172.220.1
Schweizerische Strafprozessordnung vom 05. Oktober 2007, SR 812.121
Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung vom 25. November 2020, SR 172.010.58
Verordnung über den Schutz von Informationen des Bundes vom 30. Juni 2010, SR 410.0411
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 24. Februar 2021, SR 120.73
Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 9. Dezember 2011, SR 172.010.58
Verordnung des EJPD über das beratende Organ im Bereich der Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017, SR 780.112
Verordnung über das automatisierte Polizeifahndungssystem vom 26. Oktober 2016, SR 361.0
Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN vom 04. Dezember 2009, SR 120.52
Verordnung über das Informationssystem der Bundeskriminalpolizei vom 17. Dezember 2014, SR 360.02
Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement vom 17. November 1999

Anhang 3: Abkürzungen

BIT	Bundesamt für Informatik und Telekommunikation
BPI	Bundesgesetz über die polizeilichen Informationssysteme
CI	Configuration Item
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössische Justiz und Polizei Departement
FHG	Finanzhaushaltgesetz
FHV	Finanzhaushaltverordnung
FIT	Fachgremium Informatik
FKG	Finanzkontrollgesetz
GRC	Governance Risk and Compliance
ICBO	Informatikcontrollingbeauftragter
IKT	Informations- und Kommunikationstechnologie
ISC	Informatik Service Center
ISMS	Informationssicherheits-Management System
PPM	Projekt-Portfolio Management
RACI	Responsible, Accountable, Consulted, Informed
STAR	Steuerungsboard
UAM	Unternehmens Architektur Management

Priorisierung der Empfehlungen

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

Anhang 4: Glossar

Business Continuity Management	Betriebskontinuitätsmanagement bezeichnet in der Betriebswirtschaftslehre die Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung der Organisation ernsthafte Schäden oder vernichtende Verluste zufügen würden zu schützen bzw. alternative Abläufe zu ermöglichen. Ziel ist somit die Sicherstellung des Fortbestands des Unternehmens im Sinne ökonomischer Nachhaltigkeit im Angesicht von Risiken mit hohem Schadensausmass
Configuration Item	Configuration Items sind im Wesentlichen Hardware- oder Software-Komponenten, die zum einen durch ihre Attribute charakterisiert sind und zum anderen durch ihre Beziehung zu anderen CIs.
Data Management	Datenmanagement ist die Menge aller methodischen, konzeptionellen, organisatorischen und technischen Maßnahmen und Verfahren zur Behandlung der Ressource „Daten“ mit dem Ziel, sie mit ihrem maximalen Nutzungspotenzial in die Geschäftsprozesse einzubringen und im laufenden Betrieb deren optimale Nutzung zu gewährleisten.
Enterprise Architecture	Die Unternehmensarchitektur im Rahmen der Informationstechnik beschreibt das Zusammenspiel von Elementen der Informationstechnologie und der geschäftlichen Tätigkeit im Unternehmen.
HERMES	HERMES ist die Projektmanagement-Methode für Informatik, Dienstleistung, Service und Geschäftsorganisationen und wurde von der schweizerischen Bundesverwaltung entwickelt. Die Methode steht als offener Standard vom Verein eCH allen zur Verfügung.
IT Asset Management	IT Asset Management bezeichnet die strategische Verwaltung von Software- und Hardware-Assets während ihres Lebenszyklus. Ziel ist die Maximierung ihres Geschäftswerts. Zum Asset-Management gehören der Definition nach auch die Inventarisierung und Finanzierung sowie Vertrags-, Lizenz- und Risikomanagement.
IT Governance	IT Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die Informationstechnik die Unternehmensstrategie und Ziele unterstützt
IT Service Management	IT-Service-Management bezeichnet die Gesamtheit von Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen. ITSM beschreibt insofern den Wandel der Informationstechnik zur Kunden- und Serviceorientierung

Information Security Management System	Ein Information Security Management System ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
Portfolio Management	Das Projektportfoliomanagement umfasst die Analyse und übergeordnete Führung eines Projektportfolios anhand der Schlüsseleigenschaften der Projekte.
Pooling	Unter Pooling versteht man die zentrale Bündelung von vorliegenden dezentralen Ressourcen oder eine zentrale Bestandsbildung von Ressourcen dergestalt, dass diese nach der Bündelung ganz oder teilweise für die Nutzung Dritter zur Verfügung stehen.