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

Prüfung des Risiko- und Pendenzenmanagements

Bundesamt für Informatik und Telekommunikation

EFK-21311 | inkl. Stellungnahmen | 23. Mai 2022 | FinDel D4/2022

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	609.21311
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 des Risiko- und Pendenzenmanagements
Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Das Bundesamt für Informatik und Telekommunikation (BIT) als grösster Informatik-Leistungserbinger der Bundesverwaltung (BVerw) steht aktuell in einer grossen Transformation. Es richtet damit seine Prozesse und Organisation auf eine flexiblere und agile Arbeitsorganisation aus und passt sich dem veränderten Umfeld an. Die Modernisierung wird durch den Direktor mit der Transformationsinitiative Midar[1] gesteuert. Mit der Transformation kommt dem Risikomanagement (RM) eine besondere Bedeutung zu.

Die Eidgenössische Finanzkontrolle (EFK) prüfte beim BIT das RM und die Bewirtschaftung der Risiken und Pendenzen, die sich aus der Übertragung von Aufgaben oder bei Funktions- und Rollenwechseln durch die Transformationsinitiative Midar ergeben. Die Prüfung zeigte, dass das BIT die Risiken der Transformation aktiv bewirtschaftet. Zudem befindet sich das RM BIT als Folge der Transformation im Umbau. Die eingeschlagene Stossrichtung ist zielführend und plausibel.

Schliesslich prüfte die EFK auch die offenen Empfehlungen aus dem früheren Auftrag «Prüfung der Plattform Digitalisierung»[2]. Zurzeit sind zwei dieser Empfehlungen noch offen.

Risikobewirtschaftung Midar aufgegleist

Das bestehende Risikomanagement BIT führt die operativen Risiken. Es weist im formellen wie auch in der aktiven Bewirtschaftung Schwächen auf. Eine konsolidierte und konsequente Überwachung sämtlicher BIT-Risiken fehlt. Die separate Risikoberichterstattung Midar erfolgt ebenso direkt an die Geschäftsleitung BIT und gibt einen guten Eindruck zu den Transformationsrisiken. Das eigens etablierte RM Midar wird künftig ins RM BIT einfliessen.

Pendenzen im Zuge der Transformationsinitiative Midar, die aus Aufgaben-, Rollen- oder Funktionswechseln entstehen, werden personenadressiert aktiv bewirtschaftet. Das gewählte Vorgehen ist zielführend und plausibel. Die Transformation hat direkte Auswirkungen auf das Business Continuity Management sowie das IT Service Continuity Management. Hier wurden offene Pendenzen zur Aktualisierung festgestellt. Die EFK erwartet, dass diese Grundlagen aktualisiert und auf Wirksamkeit getestet werden.

Die Risikomanagement Organisation des BIT wird angepasst

Risiken sollen neu auf verschiedenen Ebenen erfasst, bewirtschaftet und verdichtet zuhanden der Geschäftsleitung BIT rapportiert werden. Die Periodizität der Berichterstattung wird auch auf die neue agile Welt angepasst. Die EFK begrüsst den eingeschlagenen Weg. Sie empfiehlt, den Umbau des RM BIT zu terminieren und im Nachgang eine gesonderte Untersuchung der Wirksamkeit des neu etablierten Systems durchzuführen.

---

1 «Midar» bedeutet in der Schweizer Landessprache Rätoromanisch «verändern»; siehe auch Anhang 3, Glossar.

2 Der Prüfbericht 18532 ist auf der Website der EFK verfügbar.

Audit de la gestion des risques et des questions en suspens

Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

L'Office fédéral de l'informatique et de la télécommunication (OFIT) – en tant que plus grand fournisseur de prestations informatiques de l'administration fédérale – est actuellement en pleine transformation. Il oriente ainsi ses processus et son organisation vers plus de flexibilité et d'agilité et s'adapte à un environnement en mutation. Son directeur pilote cette modernisation grâce à l'initiative de transformation Midar[1]. Avec cette transformation, un accent particulier est mis sur la gestion des risques.

Le Contrôle fédéral des finances (CDF) a examiné la gestion des risques de l'OFIT ainsi que la gestion des risques et des questions en suspens résultant du transfert de tâches ou des changements de fonctions et de rôles dans le cadre de l'initiative de transformation Midar. L'audit a montré que l'OFIT gère activement les risques de transformation. En outre, la gestion des risques de l'OFIT est en cours de restructuration suite à la transformation. L'orientation choisie est pertinente et plausible.

Enfin, le CDF a vérifié si les recommandations émises lors de son précédent mandat « Audit de la plateforme de numérisation »[2] avaient été mises en œuvre. Actuellement, deux d'entre elles sont encore en suspens.

La gestion des risques Midar est en cours

La gestion des risques existante de l'OFIT porte sur les risques opérationnels. Elle présente des faiblesses du point de vue formel et actif. Il manque une surveillance consolidée et conséquente de l'ensemble des risques auxquels l'OFIT est confronté. Le compte rendu séparé sur les risques liés à Midar est aussi transmis directement à la direction de l'office. Il donne une bonne idée des risques découlant de la transformation en cours. À l'avenir, la gestion des risques spécifique à Midar sera intégrée dans la gestion des risques de l'OFIT.

Les questions en suspens en relation avec l'initiative de transformation Midar qui résultent des changements de tâches, de rôles ou de fonctions sont gérées de manière active et personnalisée. La procédure retenue est pertinente et plausible. La transformation a des conséquences directes sur la gestion de la continuité des activités *(business continuity management)* et sur la gestion de la continuité des services informatiques *(IT service continuity management)*. Des travaux de mise à jour en suspens ont été identifiés. Le CDF attend que ces bases soient actualisées et que leur efficacité soit testée.

L'organisation de gestion des risques de l'OFIT est adaptée

Les risques doivent désormais être saisis et gérés à différents niveaux et faire l'objet de comptes rendus condensés à l'attention de la direction de l'OFIT. La périodicité des

[1] « Midar » signifie « changer » en romanche, une des langues nationales, cf. annexe 3, Glossaire.

[2] Le rapport d'audit PA 18532 est disponible sur le site Internet du CDF.

comptes rendus sera aussi adaptée au nouveau monde agile. Le CDF salue la voie empruntée. Il recommande de fixer une date pour la transformation de la gestion des risques de l'OFIT et de réaliser par la suite une étude séparée sur l'efficacité du nouveau système mis en place.

Texte original en allemand

Verifica della gestione dei rischi e delle pendenze
Ufficio federale dell'informatica e della telecomunicazione

L'essenziale in breve

L'Ufficio federale dell'informatica e della telecomunicazione (UFIT), il principale fornitore di prestazioni TIC dell'Amministrazione federale, si trova in una fase di grande trasformazione. Nel concreto sta orientando i suoi processi e la sua struttura verso un'organizzazione del lavoro agile e più flessibile, adeguandosi quindi al contesto in costante evoluzione. Il direttore dell'UFCL gestisce questa modernizzazione nel quadro del progetto di trasformazione Midar[1]. Con la trasformazione, la gestione dei rischi assume un'importanza particolare.

Il Controllo federale delle finanze (CDF) ha verificato la gestione dei rischi dell'UFIT, come pure la gestione dei rischi e delle pendenze risultanti dal trasferimento di compiti o dal cambiamento di funzioni e ruoli nel quadro del progetto Midar. Dalla verifica è emerso che l'UFIT gestisce attivamente i rischi legati alla trasformazione. Inoltre, in seguito alla trasformazione, la gestione dei rischi dell'UFIT viene rinnovata. L'orientamento strategico intrapreso è plausibile ed efficace.

Infine, il CDF ha anche verificato l'attuazione di due raccomandazioni formulate nel precedente mandato «Verifica della piattaforma per la digitalizzazione»[2]. Al momento le due raccomandazioni sono ancora in sospeso.

Avviata la gestione dei rischi Midar

L'esistente gestione dei rischi dell'UFIT si concentra sui rischi operativi. In questo ambito sono state ravvisate lacune sia sotto il profilo formale che operativo. Manca una sorveglianza consolidata e sistematica di tutti i rischi dell'UFIT. I rapporti sui rischi Midar sono redatti separatamente e presentati alla direzione dell'UFIT. Essi forniscono un'idea esaustiva sui rischi legati alla trasformazione. In futuro, la gestione dei rischi Midar istituita appositamente sarà integrata nella gestione dei rischi dell'UFIT.

Le pendenze risultanti dal trasferimento di compiti o dal cambiamento di funzioni e ruoli nel quadro del progetto Midar sono gestite in modo attivo e direttamente con gli interessati. La procedura scelta è plausibile ed efficace. La trasformazione si ripercuote in modo diretto sulla gestione della continuità operativa (Business Continuity Management) e sull'IT Service Continuity Management. In tale ambito sono state accertate pendenze negli aggiornamenti. Il CDF auspica che queste basi vengano aggiornate e che ne sia testata l'efficacia.

L'organizzazione della gestione dei rischi dell'UFIT sarà adeguata

D'ora in poi i rischi dovranno essere rilevati, gestiti e consolidati a differenti livelli e quindi trasmessi alla direzione dell'UFIT. Anche la periodicità nella redazione dei rapporti sarà ade-

[1] In romancio, una delle lingue nazionali della Svizzera, «midar» significa cambiare; cfr. anche l'allegato 3 (glossario).
[2] Il rapporto di verifica PA 18532 è disponibile sul sito Internet del CDF.

guata al nuovo contesto agile. Secondo il CDF, la direzione intrapresa è quella giusta. Raccomanda comunque di fissare una scadenza per il rinnovo della gestione dei rischi dell'UFIT e, una volta terminato, di effettuare un'analisi dell'efficacia specifica del nuovo sistema.

Testo originale in tedesco

Audit of risk and pending item management
Federal Office of Information Technology, Systems and Telecommunication

Key facts

The Federal Office of Information Technology, Systems and Telecommunication (FOITT), the largest IT service provider of the Federal Administration, is currently undergoing a major transformation. It is aligning its processes and organisation with a more flexible and agile work organisation and adapting to the changed environment. The modernisation is being steered by the director with the Midar[1] transformation initiative. The transformation attaches particular importance to risk management.

The Swiss Federal Audit Office (SFAO) audited the FOITT's risk management (RM) and the management of risks and pending items arising from the transfer of tasks and changes in functions and roles due to the Midar transformation initiative. The audit showed that the FOITT actively manages the risks associated with the transformation. In addition, the FOITT RM is undergoing restructuring as a result of the transformation; the direction taken is purposeful and plausible.

Finally, the SFAO also examined the open recommendations from the earlier mandate "Audit of the digitalisation platform DIP"[2]. Currently, two of these recommendations have not yet been implemented.

Midar risk management is up and running

The existing FOITT risk management system handles operational risks. It has weaknesses in terms of both formal and active management. There is no consolidated and consistent monitoring of all FOITT risks; the separate Midar risk reporting is also addressed directly to the FOITT Executive Board. This gives a good impression of the transformation risks. The specially created Midar RM will be incorporated into the FOITT RM in the future.

Pending items that arise in the course of the Midar transformation initiative as a result of changes in tasks, roles and functions are actively managed on a person-by-person basis. The approach chosen is target-oriented and reasonable. The transformation has a direct impact on business continuity management and IT service continuity management; pending items that involve updates to these were identified. The SFAO expects these principles to be updated and tested for effectiveness.

FOITT's risk management organisation to be adapted

Risks are now to be recorded at various levels, managed and reported in condensed form to the FOITT Executive Board. The reporting frequency will also be adapted to the new agile world. The SFAO welcomes the path taken and recommends that the restructuring of the FOITT RM be terminated and the effectiveness of the newly established system be reviewed separately at a later date.

Original text in German

1 "Midar" means "change" in Romansch, one of Switzerland's national languages; see also Appendix 3, glossary

2 The audit report mandate 18532 is available on the SFAO website.

Generelle Stellungnahme des Bundesamtes für Informatik und Telekommunikation

Das BIT empfand die Zusammenarbeit mit den Prüfexperten in den Interviews als sehr angenehm. Einzelne Empfehlungen der Findings aus der Ergebnisbesprechung sind bei SI-SUR (Bereich Sicherheit & Risikomanagement) bereits in der Umsetzung. Zur Umsetzung der noch offenen Empfehlungen der einzelnen Findings werden entsprechende Stories im JIRA erfasst. Die Umsetzung wird quartalsweise der GL BIT rapportiert.

Das BIT dankt der EFK für die gegebenen Hinweise, die uns helfen, das Risikomanagement und das Pendenzenmanagement zu verbessern.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Bundesamt für Informatik und Telekommunikation (BIT) ist der grösste Informatik-Leistungserbringer (IKT-LE) der Bundesverwaltung (BVerw). Rund 1200 Mitarbeitende des BIT betreuen über alle IT-Sparten die BVerw, vom ersten Kundenkontakt bis zum fertigen Informatik-Produkt. Es verantwortet den Betrieb von Rechenzentren, entwickelt und integriert massgeschneiderte informatikgestützte Fachanwendungen, bewirtschaftet die standardisierten Arbeitsplatzsysteme und betreibt die Datennetze und Telekommunikations-Infrastrukturen der BVerw. Das BIT gliedert sich neben den Querschnittsbereichen (Human Resources, Direktionsstab und Transformation) in fünf Hauptbereiche Business Solutions (BS), Plattform Services (PS), Domestic Services (DO), Strategy & Innovation (SI) und Management Services (MS).

Mit der Transformationsinitiative Midar[3] begegnet das BIT den internen organisatorischen Herausforderungen, welche sich aus dem stark ändernden Umfeld ergeben. Midar dient der Steuerung der Transformation in eine agile Organisation. Künftig will das BIT mit dem Scaled Agile Framework (SAFe, siehe Glossar) mit agilen Teams und Arbeitsmethoden flexibel auf Kundenbedürfnisse reagieren können. Im Kontext dieser Transformation von Organisation, Prozessen, Arbeitsmethoden gewinnt das Risikomanagement an Bedeutung. Das BIT muss im Zuge der Transformation beispielsweise sicherstellen, dass bestehende oder neue Aufgaben z. B. bei Rollen- oder Funktionswechseln mit der Transformation konsequent übergeben resp. zugewiesen werden.

Mit der vorliegenden Prüfung beurteilt die Eidgenössische Finanzkontrolle (EFK) deshalb das Risikomanagement inklusive der Bewirtschaftung der Risiken des BIT sowie die Handhabung der Aufgabenübertragung im Zuge der Transformation. Zudem soll die Umsetzung der noch offenen Empfehlungen aus der Prüfung 18532 «Prüfung der Plattform Digitalisierung DIP»[4] überprüft werden.

1.2 Prüfungsziel und -fragen

Die EFK beurteilte auf Basis von Interviews und Dokumentenanalysen, ob mit dem Pendenzenmanagement eine effiziente Bewirtschaftung der Risiken sichergestellt ist, anhand folgender Prüffragen:

- Berücksichtigt, steuert und überwacht das BIT seine Risiken im Rahmen des Risikomanagements?
- Fliessen Risiken aus der Transformation angemessen in das Risikomanagement ein?
- Werden die Risiken aus der Transformation angemessen und ausreichend bewirtschaftet?
- Follow-up PA EFK 18532 «Prüfung der Plattform Digitalisierung DIP»

[3] «Midar» bedeutet in der Schweizer Landessprache Rätoromanisch «verändern»; siehe auch Anhang 3, Glossar

[4] «Plattform Digitalisierung - Generalsekretariat des Eidgenössischen Finanzdepartements» (PA 18532), abrufbar auf der Webseite der EFK

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roger Brodmann (Revisionsleiter) und Nicolas Marty vom 15. November 2021 bis 24. Dezember 2021 durchgeführt. Sie erfolgte unter der Federführung von Oliver Sifrig. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK vom Bundesamt für Informatik BIT umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 29. April 2022 statt. Teilgenommen seitens BIT haben der Leiter der Hauptabteilung Strategy and Innovation, der Leiter a. i. der Hauptabteilung Platform Services, der Leiter der Transformation Midar, der Chief Security Officer und die für Compliance sowie für das BCM zuständigen Personen.

Seitens EFK waren der zuständige Mandatsleiter, der zuständige Federführende, der Revisionsleiter und ein Mitglied des Revisionsteams vertreten.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung der Amtsleitung bzw. dem Generalsekretariat GS-EFD obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Informationen zum Prüfgebiet

Transformationsinitiative Midar

Die Transformationsinitiative Midar (nachfolgend kurz Midar) ist das zentrale Führungs- und Steuerungsinstrument, um das BIT in eine agile Organisation zu überführen. Im September 2020 wurde mit dem Start von Midar eine neue Geschäftsleitungsstruktur (siehe Organigramm, Anhang 4) etabliert.

Midar wird durch den Direktor des BIT gemeinsam mit der Geschäftsleitung verantwortet. Die Vorbereitung der Transformation erfolgte bis Mitte 2021 hauptsächlich dezentral in den Hauptabteilungen. Auf den 1. Juli 2021 startete das BIT in die neue Organisation, der designierte Leiter der Transformation nahm seine Arbeit auf. Sein Fokus liegt auf den Querschnittsaufgaben und den übergeordneten strategischen Veränderungen. Er rapportiert direkt dem Direktor des BIT.

Aktuell geht das BIT davon aus, dass die angestossene Transformation Midar rund vier bis fünf Jahre aktiv geführt wird.

Risikomanagement

In der nachfolgenden Berichterstattung werden die folgenden Begriffe verwendet:

- «RM BIT alt»; beschreibt die bisherige RM-Organisation (vor Start Midar)
- «RM Midar»; beschreibt das RM Midar welches eigenständige Regeln definierte basierend auf «RM-BIT alt» (für die Phase des Vorhabens Midar und parallel zu RM-BIT alt)
- «RM BIT neu»; konzeptionell auf die agile Arbeitsweise angepasste RM-Organisation (für Phase nach Midar)

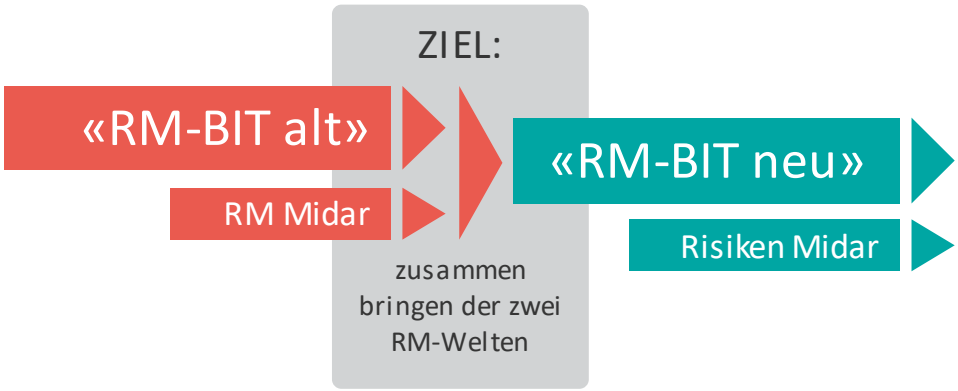

Abbildung 1: Darstellung "Zusammenbringen der zwei RM-Welten" (Darstellung: EFK)

Die Lenkung der Integralen Sicherheit des BIT erfolgt durch den Chief Security Officer (CSO). Er verantwortet die vier Themenbereiche Risikomanagement (RM), Sicherheit (Security), Business Continuity Management (BCM) und Compliance. Seit Herbst 2021 wurde ein Risikocoach BIT eingesetzt, um die Fachbereiche in Risikobelangen zu beraten. Die Berichterstattung des CSO an die GL BIT erfolgt quartalsweise.

Die Einführung des SAFe-Modells im BIT führt zu einer stärkeren Dezentralisierung der RM-Aufgaben (siehe auch Kapitel 3.3.) und der Etablierung der neuen Rolle des Risikochampions in der agilen Arbeitsorganisation.

Für die Transformationsinitiative Midar ist ein separates RM etabliert. Es wird durch die Business Owner (BO) Transformation bewirtschaftet. Die Berichterstattung an die GL BIT erfolgt monatlich durch den Leiter der Transformation Midar.

3 Die Risiko-Organisation im Wandel

3.1 Das Risikomanagement «RM BIT alt» ist zum Teil nicht nachgeführt

Das BIT führt sein Risikomanagement im Governance, Risk- und Compliance-Tool (GRC-Tool). Ergänzend nützt das BIT weitere Tools, z. B. das IKT-Cockpit für die Projektrisiken und rapportiert im «R2C» die Top-Risiken zuhanden des RM-Bund.

Die Risiken werden in Kategorien (bspw. Recht, Compliance) und Themenbereichen (bspw. Risikomanagement, BCM) geordnet. Die Risiken werden durch die dezentralen Einheiten direkt im GRC-Tool erfasst und einem Risikoeigner zugeordnet. Die Abbildung der Risiken konnte nachvollzogen werden. Jedoch war bei den Risiken ausserhalb der Informatiksicherheit teilweise nicht ersichtlich, ob Massahmen ergriffen worden sind oder es fehlte der dokumentierte Umsetzungsstand. Zum Teil waren die Risiken noch Risikoeignern zugeordnet, welche nicht mehr im BIT arbeiten. Ein konsolidiertes Risiko-Monitoring über die im GRC gepflegten Risikolandschaft fehlt. Einzig die Risiken zur Informatiksicherheit (als Teil der gesamten Risikolandschaft BIT) werden aktiv durch die Arbeitsgruppe Informatiksicherheit (AGIS) überwacht.

Strategische Risiken (z. B. die Breite des Leistungsportfolios des BIT, beschränkt vorgehaltene Technologie-Stacks, Sicherstellung der Stabilität im ESTV-Portfolio des BIT bzw. der DIP) werden isoliert durch die GL BIT behandelt. Diese werden derzeit nicht über die RM-Prozesse aktiv geführt. Es findet also keine Spiegelung dieser relativ neuen Themen in der Risikomanagement Organisation BIT statt.

Mit Blick auf das RM-Bund diskutiert die GL BIT die Top-Risiken zwei Mal pro Jahr. Gestützt auf den GL-Beschluss erfolgt dann die Risikomeldung an das Generalsekretariats EFD und die Abbildung im bundesweiten RM-Tool R2C. Im Mai 2021 wurde ein besonderes Augenmerk auf die Massnahmen gelegt, die neu von fortlaufend auf terminiert gestellt wurden. Im September 2021 hat die GL BIT entschieden, im Frühjahr 2022 einen separaten Workshop zur generellen Risikosituation des BIT durchzuführen.

Angestossen durch die Transformation Midar und die Einführung der agilen Arbeitsmethoden ist das BIT daran, das Risikomanagement «RM BIT alt» zu überarbeiten. Inskünftig soll es durch das «RM BIT neu» abgelöst werden. Der konzeptionelle Überbau zum «RM BIT neu» befindet sich erst in der Erarbeitung (siehe Kapitel 3.3).

Beurteilung

Die durch die AGIS ausgeführte Überwachung ist plausibel und zweckmässig. Sie deckt jedoch nur einen Teil der Risikolandschaft ab. Eine vergleichbare Überwachung für andere Risikogebiete fehlt. Das Risikomanagement «RM BIT alt» hat Schwächen in der Risikobewirtschaftung hinsichtlich der Aktualität, der Adressierung der Risikoeigner und der Hinterlegung von Massnahmen. Das Fehlen von strategischen Risiken schwächt die Aussagekraft zusätzlich. Mit zunehmendem Transformationsfortschritt sollten deshalb auch die strategischen Risiken künftig entlang der RM-Prozesse bearbeitet werden. Die EFK geht davon aus, dass das BIT diese Aspekte im Rahmen seiner Weiterentwicklung des RM-BIT neu aufnimmt und verzichtet deshalb auf eine Empfehlung.

3.2 Dringlicher Handlungsbedarf beim BCM

Die Risiken aus Midar werden separat geführt

Zur Steuerung von Midar ist in Absprache mit den Verantwortlichen im Bereich RM BIT neben den ordentlichen RM-Prozessen bewusst ein zweiter RM-Pfad etabliert worden. Damit verfolgt das BIT das Ziel, die Risiken aus Sicht der Transformation separat zu identifizieren und im Rahmen der Steuerung der Transformation zu bewirtschaften und mit Massnahmen zu unterlegen.

Für Midar wurden dazu RM-Grundlagen definiert. Diese Grundlagen werden innerhalb der Transformation angewendet. Methodische Inkonsistenzen bestehen gegenüber dem «RM BIT alt» in der Verwendung einer veränderten Risikomatrix. Zudem sind für RM Midar keine Aktualisierungsintervalle und keine klaren Methoden für die Risikoidentifikation definiert.

Die formalisierte Identifikation und Beurteilung der Transformationsrisiken wurde mit dem Stellenantritt des Transformationsleiters ab Juli 2021 verstärkt. In einem ersten Schritt wurde auf die Erhebung der Risiken fokussiert. Die Abstimmung der Risiken erfolgt durch die BO Transformation und über die CoP Midar. Dabei werden sowohl zentrale, also hauptabteilungsübergreifende Risiken, wie auch lokale Risiken durch RM Midar berücksichtigt. Letztere werden in den Risikoregistern der Hauptabteilungen und nicht im Risikoregister RM Midar geführt. Davon ausgenommen sind operative Risiken innerhalb den Hauptabteilungen. Diese werden weiterhin über das «RM BIT alt» geführt.

Im Rahmen der Erstellung des monatlichen Reportings durch die CoP Midar bzw. die BO Transformation werden auch die Risiken durchgesprochen und aktualisiert. Dies stellt die laufende Aktualisierung sicher. Hierfür sind die BO Transformation in laufendem Kontakt mit den jeweiligen Risikoeignern aber auch mit ihrem Vorgesetzten (Mitglied GL BIT). Zum Prüfzeitpunkt waren die Midar-Risiken noch nicht konsequent terminiert. Eine tiefergehende Aktualisierung der in RM Midar geführten Risiken und dazugehörigen Inhalte (z. B. Terminierung der Massnahmen) war jedoch für Januar 2022 geplant. Anschliessend soll ein vierteljährliches Reporting durch Risikochampions über die Risikosituation in ihren Zuständigkeitsbereichen etabliert werden.

Beurteilung

Die Identifikation der Midar-Risiken und Eingabe ins RM Midar ist plausibel und konnte nachvollzogen werden. Das Risikoregister RM Midar und die monatlichen GL-Midar-Statusreporting vermitteln insgesamt ein gutes Bild hinsichtlich der Bewirtschaftung der Transformationsrisiken. Die Terminierung der Massnahmen muss noch verbessert werden und ist durch den Leiter der Transformation sicher zu stellen.

Pendenzen aus der Transformation werden aktiv bewirtschaftet

Durch die Transformation entstehen, bei Zuständigkeitswechseln von Personen oder Organisationsbereichen sowie neuen oder wechselnden Aufgaben, Pendenzen. Per Definition des BIT entspricht jede Pendenz einem «Rucksack» welcher aktiv zu übergeben ist.

Pendenzen werden innerhalb der Hauptabteilungen geführt. Die Führung der «Rucksacklisten» erfolgt durch die BO Transformation, welche die hauptabteilungsübergreifende Abstimmung über das Transformationsgremium CoP Midar sicherstellen. Die Übergabe von

Rucksäcken bedingt Vorarbeiten. Insbesondere wird vor der Übergabe von Pendenzen abgeklärt, ob die Arbeit noch notwendig ist oder ob eine einfachere Lösung möglich wäre sowie an wen konkret übergeben wird. Dort wo Pendenzen noch nicht abgeschlossen oder übergeben worden sind, trägt die Organisation /Abteilung und damit die ursprünglich zuständige Person die Verantwortung. Teilweise müssen Doppelrollen in der «alten und neuen Welt» erfüllt werden. Die Übergaben der Pendenzen erfordern einen hohen Abstimmungsbedarf auf allen Ebenen und führt oft zu Anpassungen der internen Mitarbeitenden-Netzwerke.

Es ist vorgehsehen und terminiert, die letzten kritischen, noch offenen und nicht terminierten Rucksäcke mit Unterstützung der BO Transformation per Ende des ersten Quartals 2022 anzugehen.

Beurteilung

Das Konzept der Pendenzenbewirtschaftung und insbesondere Übergabe in die neue Organisation respektive neuen Verantwortlichkeiten mittels «Rucksäcke» ist etabliert und plausibel. Die Terminierung der Pendenzen und die Übersicht über noch offene Pendenzen ist durch den Leiter der Transformation sicher zu stellen.

Die Transformation sollte zur Erneuerung von BCM bzw. ITSCM führen

Die Transformation führt auch zu Veränderungen und Pendenzen im Bereich Business Continuity Management (BCM) sowie IT Service Continuity Management (ITSCM).

BCM-Risiken werden durch Midar bewusst ausgeklammert, da BCM den operativen Risiken zugeordnet wird und damit in der Stammorganisation verbleibt und weiterhin durch das RM BIT abgedeckt wird. Während der Transformation verbleiben die BCM-Verantwortlichkeiten bis zur abgeschlossenen Übergabe der neuen Zuständigkeiten, z. B. über einen Rucksack, unverändert.

Dennoch hat die Transformation eine Auswirkung auf das BCM. Es bestehen insbesondere offene Aufgaben im Bereich der Überarbeitung von BCM-Grundlagendokumenten wie bspw. die Wiederanlaufpläne (WAP). Die Aktualität der BCM-Dokumentation ist daher nicht gegeben. Dies zeigt sich beispielhaft an verschiedenen Dokumenten (BCM-Strategie, BCM-Szenarien, BCM-Krisenhandbuch, BCM-Krisenorganisation, Kommunikationsmatrix oder dem BCM-Handbuch) wo die letzte Überarbeitung bzw. Genehmigung teilweise mehrere Jahre zurückliegt.

Zudem zeigt auch der WAP-Masterplan verschiedene Pendenzen wie laufende Abklärungen oder noch nicht erfasste Stellvertretungen und untergeordnete WAP-Pläne, die neu bearbeitet werden müssen. Mittelfristig ist gemäss Auskunft der BCM-Verantwortlichen auch die Überarbeitung der Business Impact Analysis (BIA) notwendig.

Die BCM-Verantwortlichen des BIT sind sich der Pendenzen zur Überarbeitung der BCM-Dokumentation bewusst. Teilweise wurde mit der Überarbeitung der Dokumente begonnen. Die neuen BCM-Policies wurden durch die GL BIT bereits 20. September 2021 abgenommen.

Die letzte umfassende BCM-Übung fand im Jahr 2016 statt. Im Jahr 2020 wurde die Coronavirus-Pandemie als Krisenfall im BIT ausgerufen und die BCM-Prozesse direkt angewendet. So erfolgte ein minimaler Test unter realen Bedingungen. Der Direktor BIT entschied aufgrund der Transformation Midar, eine nächste Übung für das Jahr 2023 vorzusehen.

Im Bereich der ITSCM-Tests fanden seit Transformationsbeginn keine Tests mehr statt. Der Bereich ITSCM wird derzeit transformiert und die Durchführung von Tests war nach Entscheid BIT aufgrund der ohnehin bereits stark beanspruchten Ressourcen sowie aufgrund der anstehenden Rollenveränderungen nicht zielführend. Eine weitere Herausforderung im Bereich ITSCM ist, dass die Supportprozesse (Major-)Incidents und Task Force in einer neuen Hauptabteilung geführt werden und von dort aus die anderen Hauptabteilungen instruiert und befähigt werden müssen.

Beurteilung

Die BCM-Grundlagen sind laufend aktuell zu halten und regelmässig zu überprüfen. Die bisherig angewendeten Überarbeitungszyklen sind deshalb kritisch zu bewerten. Die regelmässige Überprüfung der BCM- und ITSCM-Dokumentation in einem auf die agile Arbeitsweise abgestimmten Turnus ist anzustreben. Die BCM- und ITSCM-Prozesse und -Grundlagen müssen zudem regelmässig und umfassend auf ihre Wirksamkeit getestet werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem Bundesamt für Informatik und Telekommunikation BIT, die BCM- und ITSCM-Grundlagen rasch zu überarbeiten, zu implementieren und im Nachgang gesondert zu testen.

Die Empfehlung ist akzeptiert.

Stellungnahme Bundesamt für Informatik und Telekommunikation BIT

BIT CSO: Die Überarbeitung der BCM-Dokumente wurde bereits initialisiert. Dabei liegt der Fokus auf dem Relaunch des ITSCM. Die BIA wird überarbeitet, wenn sich zur Erreichung der Handlungsfähigkeit des BIT grundlegende organisatorische und/oder technische Änderungen manifestieren. Die Prioritäten werden auf die Erarbeitung des Big Picture BCM/ITSCM, die Aktualisierung der Krisenlogistik sowie die Prozessoptimierung gelegt. Der Stand der Umsetzung wird quartalsweise der GL BIT rapportiert. Im Rahmen des ITSCM ist im zweiten Quartal 2022 ein Test des Wiederanlaufplans (WAP) im RZ Frauenfeld geplant. Die nächste grosse BCM-Übung ist in Absprache mit dem Direktor BIT im Jahr 2023 geplant.

3.3 Das Risikomanagement wird an neue Rahmenbedingungen angepasst

Mit Midar erfolgt auch ein Umbau des RM-BIT alt. Der Umbau auf «RM-BIT neu» wurde im August 2021 mit der RM-Policy durch die Geschäftsleitung BIT beauftragt und soll bis 30. April 2022 abgeschlossen werden. Künftig sollen die Risiken auf verschiedenen Ebenen erfasst und über mehrere Stufen bis in die GL BIT verdichtet werden:

Abbildung 2: Eskalationsstufen in den ARTs (Quelle und Darstellung: BIT; IT-Richtlinie ARTs Erfassung Risiken und Impediments)

Mit dem Umbau des RM BIT alt wird auch die Periodizität der neuen agilen Welt angepasst. Dabei muss laufend - spätestens mit dem PI-Planning - die Risikoidentifikation, die Risikoanalyse, die Risikobewertung und die Beurteilung/Bewältigung erfolgen. Das Reporting erfolgt auf mehreren Ebenen (bei Team-Sitzungen, beim Austausch zwischen Business Owner und Hauptabteilungsleiter, dem Hauptabteilungsleiter und dem Risikocoach). In einem 1/4-jährlichem Bericht legt der Risikochampion Rechenschaft über die Risikosituation in seinem Zuständigkeitsbereich an den Risikocoach ab.

Die Herausforderung im Umbau ist die Tatsache, dass die Vorgaben für das Risikomanagement des BIT aus verschiedenen Quellen mit unterschiedlichen Anforderungen stammen. Es gilt, künftig die Vorgaben aus RM Bund mit den Top-Risiken (R2C), diejenigen des IKT-Cockpit in SAP-PPM für Projekte und Programme, sowie die BO-Risiken die im GRC-Tool geführt und die ART-Risiken welche in Jira werden, zu konsolidieren.

Während aufseiten RM Midar das Risikoreporting klar strukturiert und auch gegenüber der GL sehr transparent und für einen unabhängigen Dritten nachvollziehbar erscheint, wirkt die Risikoberichterstattung aufseiten «RM BIT alt» eher schwerfällig.

Bis zur vollzogenen Harmonisierung erhält die Geschäftsleitung BIT kein konsolidiertes Gesamtrisikobild

Im Jahr 2021 hat die GL BIT über zwei Kanäle Informationen zur Risikolage des BIT erhalten. Zum einen über die quartalsweise erstellten «BIT-Sicherheitsberichte». Diese umfassen Informationen zu risikomanagementnahen Bereichen. Sie stellen jedoch nicht das Risikomanagement selbst dar. Zum anderen erfolgt die Information der GL BIT zu den Risiken aus der Transformation im Rahmen des monatlichen Statusberichts Midar.

Per Ende 2021 war der Wandel des RM BIT erst angestossen. Bis zum Abschluss des gestarteten Umbaus wird das herkömmliche RM BIT alt vorerst unverändert weitergeführt. Das «RM Midar» fokussiert auf die Risiken der Transformation und wird parallel geführt und bewirtschaftet.

Die Dokumente zum Umbau des neue-RM-BIT zeigen im Endzustand eine systematische Kaskadierung mit entsprechenden Eskalationsstufen (inkl. Integration «RM Midar») in das «RM BIT neu». Dabei werden die Transformationsrisiken «RM Midar» vergleichbar zu einem ART innerhalb des RM BIT geführt. Zudem wird der Aufbau des neuen integralen RM BIT die agile Arbeitsmethodik berücksichtigen (explizite Vorgabe das RM laufend zu führen und zu aktualisieren) und zu einer zusätzlichen quartalsweisen Risikoberichterstattung der Risikochampions führen.

Beurteilung

Das gewählte Vorgehen führt dazu, dass bis zum Abschluss des Umbaus und der Neupositionierung des RM BIT, die «alte RM-Welt» (Fokus auf operative Risiken) und das «RM Midar» (Fokus auf transformationsspezifische Risiken) mit ihren jeweiligen Schwächen in getrennten Silos laufen und auch getrennt in die GL BIT rapportieren. Die Schwächen wurden in Kapitel 3.1 und 3.2 beschrieben. Die Art der RM-Berichterstattung aufseiten Midar zeigt in welche Richtung sich auch die RM BIT Berichterstattung entwickeln sollte.

Die Schaffung eines RM BIT das alle Ebenen der Risikolandschaft des BIT abzudecken vermag, ist herausfordernd. Das Ziel muss dennoch ein integrales RM mit nachvollziehbarer Dokumentation der Verdichtung von den operativen Risiken zu einer aggregierten Sicht auf strategischer Stufe sein, welches auch die Verknüpfung mit dem Risikomanagement Bund (R2C) gewährleistet. Es muss zwingend sichergestellt werden, dass künftig sämtliche Risiko-Themen aktiv bewirtschaftet, zentral überwacht und in der GL BIT systematisch thematisiert werden.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem Bundesamt für Informatik und Telekommunikation BIT, den Umbau des Risikomanagements rasch abzuschliessen und eine dauerhaft aktive Risikobewirtschaftung und –überwachung über alle Risikokategorien zu etablieren. Zudem sollte das BIT im Nachgang zum Umbau gesondert eine umfassende Beurteilung des RM auf seine Wirksamkeit durchführen.

Die Empfehlung ist akzeptiert.

Stellungnahme Bundesamt für Informatik und Telekommunikation BIT

BIT CSO: Ein erster Workshop mit der GL BIT hat stattgefunden. Die Vorgabe für die Erfassung und Bearbeitung der Risiken in den Agile Release Trains liegt vor. Das neue Tool des RM Bund ist freigegeben. Die Herausforderung liegt in der Führung der Risiken über alle Risikokategorien, weil es insbesondere bei den Projektrisiken darum geht die Vorgaben des BR und des BIT umzusetzen ohne diese an mehreren Stellen pflegen zu müssen. Das Risikomanagement wird in der GL BIT regelmässig mit dem Ziel, die Umsetzung der definierten Massnahmen zu beurteilen, traktandiert,

Die Umsetzung der Empfehlung wird quartalsweise der GL BIT rapportiert.

4 Follow-up: Integration der DIP in das BIT

Die Plattform Digitalisierung (DIP) ist seit 2019 IKT-Leistungserbringerin für die Eidgenössische Steuerverwaltung (ESTV) und als solche während vier Jahren von Artikel 23 der Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV[5]) ausgenommen. Die DIP als Verwaltungseinheit war zu Beginn dem Generalsekretariat des Eidgenössischen Finanzdepartements (EFD) angegliedert. Der Bundesrat hat am 3. April 2020 entschieden, die DIP bis Ende 2020 in das BIT zu integrieren.

Die Integration der DIP in das BIT erfolgte anfangs 2021 als geschlossene Einheit inklusive der Mitarbeitenden (inkl. FTE) in die Hauptabteilung Strategy & Innovation (SI). Ende Januar 2022 wird die DIP in die Hauptabteilung Business Solutions (BS) verschoben. Die DIP nutzt bereits vereinzelte Prozesse des BIT, bspw. Kunden-, Incident-, Monitoring- und auch Beschaffungsprozesse. Die DIP arbeitet mit fünf Entwicklungsteams für die ESTV und wird vorerst als Agile Release Train (ART) geführt. Mit dem vorliegenden Follow-Up wurde der Umsetzungsstand der Empfehlungen ans DIP im Lichte des Standes dessen Integration in die Betriebsprozesse BIT betrachtet.

Das Portfolio der DIP wird über eine Roadmap und über eine Anwendungsarchitektur gemeinsam mit der ESTV geführt, eine Systemübersicht der Anwendungen existiert (Empfehlung 18532.002) und ein ISDS-Konzept für die Microservices wurde erstellt (Empfehlung 18532.004). Die Nutzerzahlen werden für die wichtigsten Anwendungen erhoben (Empfehlung 18532.001). Die DIP ist jedoch noch nicht beim Thema «Risikomanagement» berücksichtigt worden. Risiken werden auf Ebene der Projekte durch die Product Owner (PO) geführt. Eine abgestimmte Risikoinventur ist noch nicht vorgenommen worden. Die entsprechende Empfehlung 18532.001 ist noch nicht vollständig umgesetzt. Da das Risikomanagement DIP auch vom Umbau des Risikomanagements BIT (siehe Kapitel 3.3) tangiert ist, wird das Thema neu für das ganze BIT in Empfehlung Nr. 2 adressiert.

Mit der Integration in die Hauptabteilung BS will das BIT weitere Synergien identifizieren und realisieren. Das BIT hat erkannt, dass es für die Entwicklung im agilen Umfeld seine Prozesse insgesamt überarbeiten muss. Bis Ende 2022 soll ein Prozess mit dazugehörender Toolchain zur Verfügung stehen. Damit will das BIT für alle Entwicklungen ein einheitliches Vorgehen zur Entwicklung, Integration und Weiterentwicklung von Anwendungen sicherstellen. Die DIP wird dabei vollständig in die Prozesse des BIT integriert, auch bezüglich der Querschnittsthemen (IKS, RM, BCM/ITSCM, ITGC und ISDS) wie sie in den Empfehlungen adressiert waren. Für die BCM/ITSCM Thematik fand eine erste Wissensvermittlung statt, die bestehenden Konzepte und Tools sind den DIP Verantwortlichen vorgestellt worden. Bis zur vollständigen Integration der DIP und der Umsetzung der Toolchain bleiben die beiden Empfehlungen 18532.003 und 18532.005 offen.

Beurteilung

Mit der Integration der DIP in die Hauptabteilung BS wurde ein erster Schritt vollzogen und die Grundlage geschaffen, die DIP vollumfänglich in die Standardprozesse des BIT zu integrieren.

[5] Die BinfV ist heute nicht mehr in Kraft und wurde durch die Verordnung über die digitale Transformation und die Informatik (VDTI) abgelöst; siehe auch Anhang 1, rechtliche Grundlagen.

Erst mit der vollständigen Integration der DIP in die Prozesse des BIT werden die Grundlagen geschaffen, um die Forderungen aus den vorgenannten Empfehlungen Nr. 18532.003 und Nr. 18532.005 zu erfüllen. Die Empfehlungen bleiben daher offen. Die Empfehlungen 18532.002 (Architekturthematik) und 18532.004 (ISDS-Konzept zu Mikroservice) sind bereits zu einem früheren Zeitpunkt erledigt worden. Die Zielsetzung der Empfehlung Nr. 18532.001 wird in der neuen Empfehlung Nr. 2 aufgenommen und kann, trotz unvollständiger Umsetzung in Bezug auf das RM, geschlossen werden.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über den eidgenössischen Finanzhaushalt (Finanzhaushaltgesetz, FHG) vom 7. Oktober 2005 (Stand am 1. Januar 2022), SR 611.0
Finanzhaushaltverordnung (FHV) vom 5. April 2006 (Stand am 1. Januar 2022), SR 611.01
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand 1. Januar 2021), SR 614.0
Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung, Verordnung über die digitale Transformation und die Informatik, VDTI, vom 25. November 2020 (Stand am 1. Januar 2022), 172.010.58
Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung, Bundesinformatikverordnung, BinfV, vom 9. Dezember 2011 (Stand am 1. Juli 2020), [SR 172.010.58 – nicht mehr in Kraft]
Regierungs- und Verwaltungsorganisationsverordnung, RVOV, vom 25. November 1998 (Stand am 1. Januar 2022), 172.010.1
Organisationsverordnung für das Eidgenössische Finanzdepartement, OV-EFD, vom 17. Februar 2010 (Stand am 1. Januar 2022), 172.215.1
Geschäftsordnung des Bundesamtes für Informatik und Telekommunikation BIT, GO-BIT, vom 13. Dezember 2021, inkl. Anhänge 1–5 - Anhang 1 GO BIT: Organisatorische Struktur des BIT - Anhang 2 GO BIT: Ziele, Auftrag und Aufgaben des BIT sowie seiner Organisationseinheiten - Anhang 3 GO BIT: Führungsorganisation BIT - Anhang 4 GO BIT: Kompetenzen und Unterschriftenregelung - Anhang 5 GO BIT: Unterschriften- und Kompetenzregelung im Bereich der Ausgaben sowie weiterer spezifischer Prozesse und HR

Anhang 2: Abkürzungen

BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Impact Analyse
BIT	Bundesamt für Informatik
BO	Business Owner
BS	Business Solutions, Hauptabteilung im BIT
BVerw	Bundesverwaltung
DIP	Digitalisierungsplattform
DO	Domestic Services, Hauptabteilung im BIT
DTI	Bereich Digitale Transformation und IKT-Lenkung
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
FHG	Finanzhaushaltgesetz
FHV	Finanzhaushaltverordnung
FKG	Finanzkontrollgesetz
HA	Hauptabteilung
IKT-LB	Informatik Leistungsbezüger
IKT-LE	Informatik Leistungserbringer
ISB	Informatiksteuerungsorgan des Bundes (neu: Bereich Digitale Transformation und IKT-Lenkung DTI)
IT	Informationstechnologie
ITSCM	IT Service Continuity Management
MS	Management Services, Hauptabteilung im BIT

PS	Platform Services, Hauptabteilung im BIT
R2C	Risk2Chance
RM	Risikomanagement
SD	Standarddienste
SI	Strategy & Innovation, Hauptabteilung im BIT
SI-SUR	Abteilung Sicherheit und Risikomanagement des BIT
SUR	Chief Security Officer; Organisationseinheit im BIT

Anhang 3: Glossar

BCM	Das BCM ist Bestandteil eines integrierten Risikomanagementsystems. Das Risikomanagement setzt sich vorausschauend (Pre-Loss) mit den Gefahren für die Aufgabenerfüllung und die Zielerreichung auseinander und stellt sicher, dass Massnahmen ergriffen werden, um das Eintreten der Risiken zu verhindern. Demgegenüber fokussiert das BCM auf den Ereignisfall (Post-Loss). Dabei steht die Minimierung der Auswirkungen eines Ausfalls von kritischen Geschäftsprozessen im Vordergrund («Resilienz», → Widerstandsfähigkeit). Diese Vorbereitung erfolgt in den 4 Dimensionen Lieferanten, Organisation, Informatik und Logistik/Infrastruktur. (Quelle: BCM Begriffsdefinitionen EFD, Version 1.0 vom 30.11.2018)
BCP	Ein Business Continuity Plan basiert auf der Business Impact Analyse und ist ein Katalog von Handlungsanweisungen und Massnahmen, die im Falle des Eintretens eines Risikos Schäden von einem Unternehmen abwenden oder begrenzen sollen. (Quelle: BCM Begriffsdefinitionen EFD, Version 1.0 vom 30.11.2018)
BIA	Eine Business Impact Analyse (BIA) ist im Business Continuity Management eine Methode zur Sammlung und Identifizierung von Prozessen und Funktionen innerhalb einer Organisation, um die den Prozessen zugrundeliegenden Ressourcen zu erfassen. Des Weiteren können durch eine BIA wechselseitige Abhängigkeiten zwischen Prozessen und/oder Unternehmensbereichen aufgezeigt, die Auswirkungen bei Ausfällen von Prozessen, die Kritikalität jedes Prozesses für den Gesamtkonzern und die benötigte Wiederanlaufzeit aufgedeckt werden. (Quelle: BCM Begriffsdefinitionen EFD, Version 1.0 vom 30.11.2018)
Business Owner (BO)	Arbeitsorganisation: Sie/Er trägt die gesamtheitliche Verantwortung für das ihr/ihm zugewiesene (Teil-)Geschäftsfeld.
Business Owner (BO) - Chapters	Sie/Er trägt die übergeordnete Verantwortung für die personelle Führung aller internen und externen Mitarbeitenden der jeweiligen Hauptabteilung.
Business Owner (BO) - Transformation	Sie/Er trägt die gesamtheitliche Verantwortung für die Transformation der ihr/ihm zugewiesenen Hauptabteilung.

Community of Practice (CoP)	In einer CoP organisieren sich Mitarbeitende aus allen Hauptabteilungen mit demselben Fachwissen oder den gleichen Interessen. Dies mit dem Ziel, Informationen auszutauschen, Fähigkeiten zu verbessern und Wissen aufzubauen. Eine CoP beschränkt sich nicht auf eine Hauptabteilung, ist aber in derjenigen Hauptabteilung verankert, in welcher das entsprechende Fachwissen verankert ist und gepflegt wird. Beispiel: CoP Midar – vereint die Businessowner Transformation zu einem Steuerungs- und Abgleichgremium der Transformation Midar.
FTE	Full Time Equivalent, zu Deutsch: Vollzeitäquivalent; rechnerische Größe zur Messung von Arbeitszeit.
Head of Chapter	Die/Der Head of Chapter ist die formale Linienführungsperson von den nach Fachthemen gruppierten internen und externen Mitarbeitenden. Die/Der Head of Chapter ist die Führungsperson, die den personellen und kulturellen Aspekten grosses Gewicht beimisst und diese als gelebte Praxis von allen einfordert. Weiter lebt sie/er die Agilität vor und fokussiert auf das Individuum. Sie/Er trägt die gesetzliche Fürsorgepflicht für alle Mitarbeitenden in ihrem/seinem Zuständigkeitsbereich. Weiter sorgt sie/er dafür, dass immer genügend und ausreichend qualifizierte interne und externe Mitarbeitende des zuständigen Fachgebietes zur Verfügung stehen und ausgelastet sind. Sie/Er verantwortet und führt die Kostenstelle und ist für deren Ergebnis und Zielerreichung (quantitativ und qualitativ) verantwortlich. Auch führt sie/er das Thema des Chapters in den Bereichen Fachfähigkeiten, Arbeitsmethoden und Regeln sowie Normen.
ITSCM	IT Service Continuity Management basiert auf den BCM Anforderungen in der Dimension Informatik. Es ist auf die Aufrechterhaltung der kritischen IT Funktionen beim Ereignisfall fokussiert. Verwaltungseinheiten ohne eigenen IT Betrieb leiten ihre ITSCM Anforderung aus ihrem eigenen BCM ab, vereinbaren diese mit ihrem IKT-Leistungserbringer und kontrollieren diese. (Quelle: BCM Begriffsdefinitionen EFD, Version 1.0 vom 30.11.2018)
Midar	«Midar» bedeutet in der Schweizer Landessprache Rätoromanisch «verändern». Es ist der Name und die Darstellung der Transformationsinitiative des BIT. Diese Darstellung spiegelt Beweglichkeit und Dynamik auf eine lockere und fröhliche Art wieder. (Quelle: Intranet GS-EFD; BIT)

R2C	Für das Erfassen und Verwalten der Risiken steht den Ämtern mit «R2C» (Risk to Chance) eine zentrale IT-Anwendung zur Verfügung.
Release Train Engineer (RTE)	Die/Der RTE ist für das reibungslose Zusammenspiel aller Komponenten und Rollen im Tribe bzw. Agile Release Trains (ART) verantwortlich. Sie/Er leitet die Zeremonien auf Stufe Programm und unterstützt die Rollen auf Stufe Team. Sie/Er ist methodisch Coach für die Rollen auf der Programmebene, unterstützt die PM und PO bei der Erarbeitung der Backlogs und stellt sicher, dass Features und Stories eine hohe Qualität haben. Sie/Er optimiert die Abläufe und die im Team eingesetzten Werkzeuge. Des Weiteren bearbeitet bzw. beseitigt sie/er aktiv Impediments auf Stufe Programm des ART.
Risiko	Unter Risiko werden Ereignisse und Entwicklungen verstanden, die mit einer gewissen Wahrscheinlichkeit eintreten und wesentliche finanzielle und nichtfinanzielle Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der Bundesverwaltung haben. (Quelle: BCM Begriffsdefinitionen EFD, Version 1.0 vom 30.11.2018)

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: Organigramm BIT

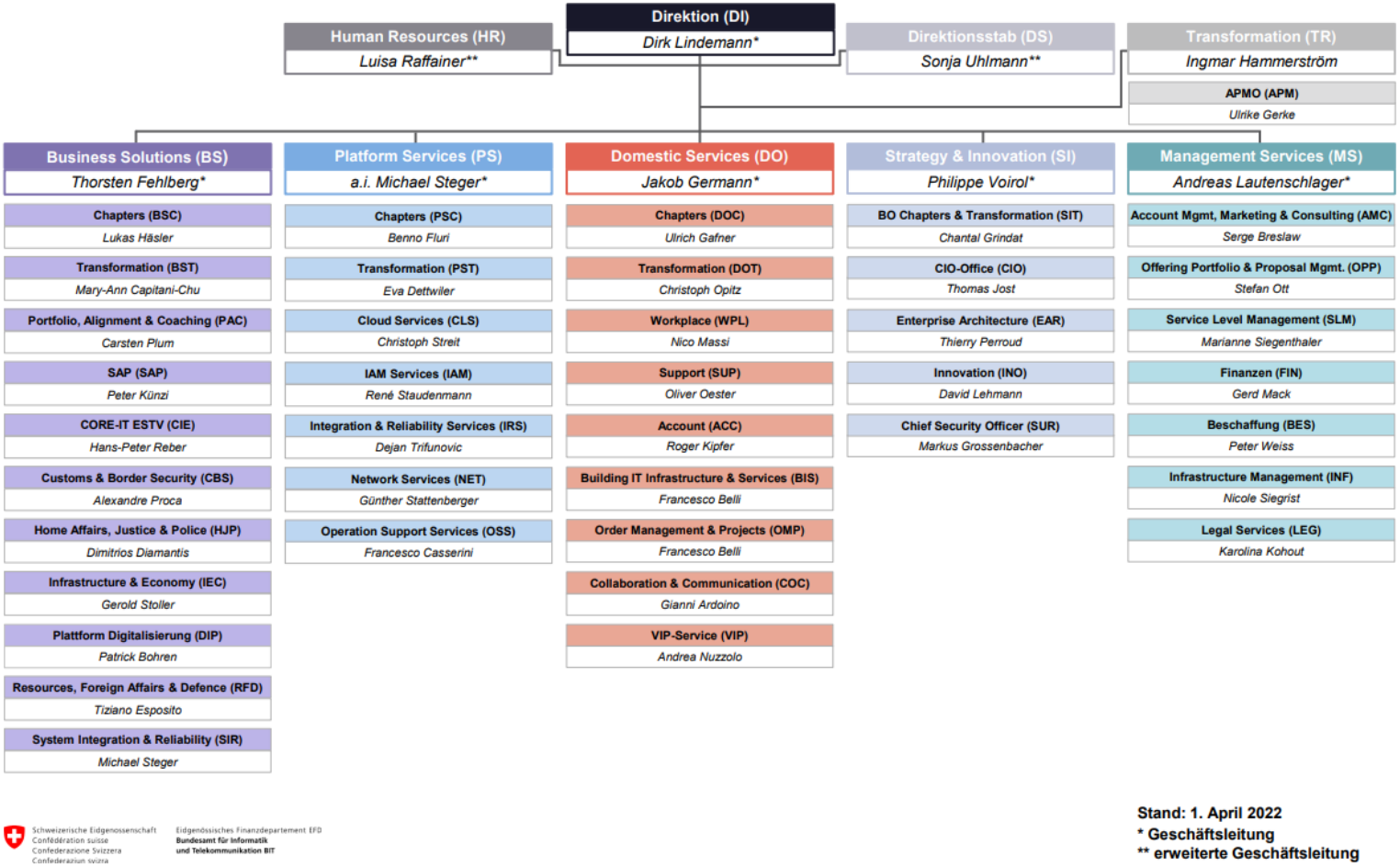

Abbildung 3: Organigramm Bundesamt für Informatik BIT, Stand 1. April 2022[6]

[6] Siehe auch: https://www.bit.admin.ch/bit/de/home/das-bit/organisation.html