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

Prüfung des Service Continuity Managements

Direktion für Ressourcen

EFK-20060 | inkl. Stellungnahmen | 30. Juni 2020 | FinDel D5/2020

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	1.20060.202.00442
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
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

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

Inhaltsverzeichnis

Prüfung des Service Continuity Managements
Direktion für Ressourcen

Das Wesentliche in Kürze

Die Direktion für Ressourcen (DR) ist verantwortlich für die Sicherstellung und Steuerung der Ressourcen im Eidgenössischen Departement für auswärtige Angelegenheiten (EDA). Die erforderlichen Dienstleistungen werden für das Departement und die Schweizerischen Vertretungen im Ausland erbracht, u. a. auch von der Informatikabteilung IT EDA, welche über rund 100 Mitarbeitende verfügt. Die Kosten der IT EDA belaufen sich seit Jahren konstant auf etwa 50 Millionen Franken pro Jahr. 2019 waren es 49 Millionen, davon 37 Millionen für den Betrieb und 12 Millionen für Projekte. Betrieben werden rund 70 Fachanwendungen für ca. 5050 Benutzer, davon 1850 im Inland und 3200 im Ausland an 165 Standorten.

Die Prüfung sollte aufzeigen, ob die IT EDA über alle Störungssituationen hinweg sicherstellt, dass sie die Kerngeschäfte gemäss den vertraglichen Vereinbarungen mit ihren Kunden gewährleisten kann. Die IT EDA erhält gute Noten von ihren Leistungsbezügern. Gemessen an relevanten Standards ist sie jedoch noch nicht auf dem zu erwartenden Reifegrad eines IT Service Continuity Managements (IT SCM).

Die IT EDA erfüllt ihren Auftrag zur Zufriedenheit der Nutzer

Die IT EDA hat in der Vergangenheit immer wieder gezeigt, dass sie über die Fähigkeit zur fristgerechten Bewältigung von Störungen verfügt. Aufgrund der zentralisierten Ressourcen und der starken Integration mit den Bezügern der Leistung sind die Kommunikationswege kurz und direkt. Im EDA wird viel Wert auf Kommunikation und Zusammenarbeit gelegt. Die wiederkehrenden Zufriedenheitsumfragen bei den Leistungsbezügern zeigen, dass die Arbeit der IT EDA geschätzt und als gut bewertet wird.

Wichtige Elemente eines IT SCM sind vorhanden, es bestehen jedoch Lücken

Die IT EDA ist auf grundlegende Vorarbeiten auf Geschäftsseite im Bereich des Business Continuity Managements (BCM) angewiesen. Dafür besteht seit Mitte 2017 eine Richtlinie des EDA als Vorgabe. Diese wurde noch nicht so umgesetzt, dass die IT EDA alle erforderlichen Voraussetzungen in der nötigen Präzision vorfindet. Daher empfiehlt die EFK dem Generalsekretariat des EDA eine Präzisierung des Auftrags zum Aufbau des BCM.

Operativ wesentliche Elemente des IT SCM sind vorhanden. Es fehlen aber wichtige Komponenten. So liegt beispielsweise keine Übersicht der effektiven und möglichen Störungsszenarien mit einer systematischen Auswirkungsanalyse vor (Business Impact Analysis). Zudem gibt es keine zusammenhängende Dokumentation, welche die vorhandenen und noch zu realisierenden Elemente des IT SCM aufzeigt. Für ein entsprechendes Projekt wurden lediglich erste Initialisierungsarbeiten durchgeführt.

Die EFK empfiehlt der DR / IT EDA einen zielgerichteten und pragmatischen Ausbau des IT SCM auf der Basis der mit vorgesetzten Stellen und Kunden zu vereinbarenden Anforderungen und Eckwerte.

Audit du Service Continuity Management
Direction des ressources

L'essentiel en bref

La Direction des ressources (DR) assure la disponibilité et le pilotage des ressources au Département fédéral des affaires étrangères (DFAE). Les services nécessaires sont fournis au département et aux représentations suisses à l'étranger, notamment par la division Informatique du DFAE (IT DFAE), qui compte une centaine de collaborateurs. Les coûts de la division IT DFAE sont constants depuis des années et se montent à quelque 50 millions de francs par an. En 2019, le montant s'élevait à 49 millions, dont 37 millions pour l'exploitation et 12 millions pour des projets. La gestion porte sur environ 70 applications spécialisées pour environ 5050 utilisateurs, dont 1850 en Suisse et 3200 à l'étranger sur 165 sites.

L'audit devait permettre de déterminer si, dans toutes les situations de panne, la division IT DFAE est en mesure d'assurer les activités de base conformément aux dispositions contractuelles conclues avec ses clients. La division IT DFAE obtient de bonnes notes de la part des bénéficiaires de ses prestations. Par rapport aux normes applicables, elle n'a toutefois pas encore atteint le niveau de maturité attendu d'une gestion de la continuité des services informatiques (IT Service Continuity Management – IT SCM).

La division IT DFAE remplit son mandat à la satisfaction des utilisateurs

La division IT DFAE a régulièrement montré par le passé qu'elle a la capacité de maîtriser les pannes dans des délais raisonnables. Grâce aux ressources centralisées et à la forte intégration avec les bénéficiaires de prestations, les canaux de communication sont rapides et directes. Au sein du DFAE, la communication et la collaboration revêtent une grande importance. Les enquêtes de satisfaction réalisées régulièrement auprès des bénéficiaires de prestations montrent que le travail de la division IT DFAE est apprécié et bien noté.

Les éléments importants d'un IT SCM sont là, mais des lacunes subsistent

La division IT DFAE dépend des travaux préparatoires de base effectués du côté opérationnel en matière de gestion de la continuité des activités (Business Continuity Management – BCM). Depuis mi-2017, le DFAE a mis en place une directive à cet effet. Celle-ci n'a pas encore été mise en œuvre de manière à ce que la division IT DFAE puisse identifier toutes les conditions préalables nécessaires avec la précision requise. Dès lors, le CDF recommande au secrétariat général du DFAE de préciser le mandat lié à l'établissement du BCM.

Les éléments opérationnels essentiels du IT SCM sont présents. Il manque toutefois des composantes importantes. Ainsi, par exemple, il n'existe aucune vue d'ensemble des scénarios de panne effectifs et possibles avec une analyse d'impact systématique (Business Impact Analysis). En outre, il manque une documentation cohérente qui présente les éléments existants du IT SCM et ceux qu'il reste à réaliser. Seuls des travaux d'initialisation préliminaires ont été menés pour un projet correspondant.

Le CDF recommande à la DR / IT EDA de développer le IT SCM de manière ciblée et pragmatique sur la base d'exigences et de valeurs de référence à convenir avec les instances supérieures et les clients.

Texte original en allemand

Verifica del Service Continuity Management
Direzione delle risorse

L'essenziale in breve

La Direzione delle risorse (DR) è responsabile della garanzia e della gestione delle risorse nel Dipartimento federale degli affari esteri (DFAE). Le prestazioni di servizio necessarie al Dipartimento e alle rappresentanze svizzere all'estero vengono fornite soprattutto attraverso la divisione Informatica DFAE, che dispone di circa 100 collaboratori. Da anni i costi della divisione sono rimasti costanti e ammontano a circa 50 milioni di franchi all'anno; nel 2019 erano pari a 49 milioni, 37 dei quali per l'esercizio e 12 per progetti. Vengono gestite circa 70 applicazioni specifiche per approssimativamente 5050 utenti, 1850 dei quali in Svizzera e 3200 all'estero, distribuiti in 165 sedi.

La verifica era finalizzata a indicare se, in caso di guasti, la divisione Informatica DFAE fosse in grado di assicurare le attività principali conformemente agli accordi contrattuali conclusi con i propri clienti. La divisione ha ricevuto un giudizio positivo dai beneficiari delle sue prestazioni. Tuttavia, in base agli standard rilevanti non ha ancora raggiunto il grado di maturità atteso da un IT Service Continuity Management (ITSCM).

La divisione Informatica DFAE svolge il proprio mandato con soddisfazione degli utenti

In passato, la divisione si è sempre dimostrata capace di affrontare i guasti in tempo utile. Grazie alla centralizzazione delle risorse e alla forte integrazione con i beneficiari della prestazione, i canali di comunicazione sono brevi e diretti. Nel DFAE si attribuisce una grande importanza alla comunicazione e alla collaborazione. I sondaggi ricorrenti sulla soddisfazione svolti presso i beneficiari delle prestazioni mostrano che il lavoro della divisione Informatica DFAE viene apprezzato e valutato positivamente.

Gli elementi importanti di un ITSCM sono presenti, ma con lacune

La divisione Informatica DFAE necessita di lavori preliminari di base sul versante operativo, per quanto riguarda la gestione della continuità delle attività (Business Continuity Management – BCM). Il DFAE dispone da metà 2017 di una direttiva in materia. Tuttavia essa non è ancora stata attuata in modo da permettere alla divisione di trovarvi tutti i requisiti necessari con la dovuta precisione. Pertanto, il CDF raccomanda alla Segreteria generale del DFAE di esplicitare il mandato finalizzato alla creazione della BCM.

Dal punto di vista operativo, gli elementi fondamentali dell'ITSCM sono presenti. Mancano però componenti importanti. Ad esempio non esiste una panoramica degli scenari di guasto effettivi e possibili corredata da un'analisi di impatto sistematica (Business Impact Analysis – BIA). Manca anche la relativa documentazione che mostri gli elementi esistenti dell'ITSCM e quelli ancora da realizzare. Per il pertinente progetto sono stati effettuati soltanto dei lavori di avvio preliminari.

Il CDF raccomanda alla DR / Informatica DFAE di sviluppare in modo mirato e pragmatico l'ITSCM sulla base dei requisiti e dei parametri da convenire con le istanze superiori e con i clienti.

Testo originale in tedesco

Audit of service continuity management
Directorate for Resources

Key facts

The Directorate for Resources (DR) is responsible for ensuring the availability and management of resources within the Federal Department of Foreign Affairs (FDFA). It provides the services required by the department and Switzerland's network of representations abroad, including the FDFA IT section, which has around 100 employees. FDFA IT's costs have remained constant for years, at approximately CHF 50 million per year. In 2019 they stood at CHF 49 million, of which CHF 37 million were operating costs and CHF 12 million were for projects. It operates about 70 specialist applications for around 5,050 users, of which 1,850 are in Switzerland and 3,200 abroad across 165 locations.

The purpose of the audit was to determine whether FDFA IT ensures that it can guarantee core business operations in accordance with the contractual agreements with its clients in the event of any type of disruption. FDFA IT received good ratings from its service recipients. However, when measured against relevant standards, it is not yet at the expected level of maturity for IT service continuity management (IT SCM).

FDFA IT performs its function to the satisfaction of users

FDFA IT has repeatedly demonstrated in the past that it has the capacity to deal with disruptions in a timely manner. Communication channels are short and direct due to centralised resources and strong integration with the service recipients. The FDFA places great emphasis on communication and collaboration. The regular satisfaction surveys conducted among service recipients show that FDFA IT's work is appreciated and rated as good.

Important elements of IT SCM in place, gaps exist

FDFA IT is dependent on fundamental preparatory work in the area of business continuity management (BCM). Since mid-2017, the FDFA has had guidelines in place for this purpose. These have not yet been implemented in such a way that FDFA IT is able to identify all necessary prerequisites with the necessary precision. The SFAO therefore recommends that the General Secretariat of the FDFA define the mandate for setting up BCM in more precise detail.

Key operational elements of IT SCM are in place, although important components are missing. For example, there is no overview of effective and possible disruption scenarios which includes a systematic business impact analysis. In addition, there is no coherent documentation showing the existing IT SCM elements and those still to be implemented. Only the preliminary work for a project to this effect has been carried out.

The SFAO recommends that the DR/FDFA IT carry out a targeted and pragmatic expansion of the IT SCM on the basis of requirements and benchmarks to be agreed with upstream offices and clients.

Original text in German

Generelle Stellungnahme der Direktion für Ressourcen

Le SG et la DR remercient le CDF pour l'audit qui nous apporte des éléments précieux dans l'amélioration de notre BCM ainsi que de notre IT-SCM. Lors de la crise de la COVID-19, le DFAE a bénéficié des travaux qu'il avait effectués dans le cadre de la réalisation de son BCM. Ce dernier a été mis en place au sein des directions dès 2018. Bien qu'il ne corresponde pas entièrement à la directive du 28.06.2017, il est pragmatique et a démontré sa valeur. Les mesures prévues ont été rapidement mises en œuvre et étaient adaptées aux particularités de cette crise. La continuité des activités (BCM) a bien fonctionné et il n'y a eu aucune lacune importante.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Informatik EDA (IT EDA) erbringt in den Bereichen Informations- und Kommunikationstechnologie Leistungen für das Eidgenössische Departement für auswärtige Angelegenheiten (EDA). Sie umfasst 100 Mitarbeitende und ist gegenüber den 5050 Nutzern als umfassender Dienstleister positioniert. Nebst der Unterstützung der Verwaltungstätigkeit in der Schweiz («Zentrale») ist sie auch für die IT-Infrastruktur und Vernetzung in den rund 165 Vertretungen weltweit verantwortlich. Einheiten wie das Schweizerische Korps für Humanitäre Hilfe (SKH) benötigen zudem mobile Einsatzmittel. Die IT EDA betreibt etwa 70 Fachanwendungen, 300 physische Server (wovon 250 im Ausland), gut 6000 Notebooks, 1400 Smartphones und 1320 Multifunktionsgeräte / Drucker.

Die Leistungserbringung ist teilweise abhängig von weiteren Dienstleistern, beispielsweise dem Bundesamt für Informatik und Telekommunikation (BIT) für Netzwerkdienste.

Finanziell beläuft sich das Portfolio der IT EDA auf 49 Millionen Franken pro Jahr. 37 Millionen werden für den Betrieb aufgewendet (Service Operation), 12 Millionen für Vorhaben und Projekte (Service Design und Service Transition). Das Volumen < 50 Millionen Franken wird seit Jahren konstant gehalten.

1.2 Prüfungsziel und -fragen

Die Eidgenössische Finanzkontrolle (EFK) hat überprüft, ob die IT EDA über alle Störungssituationen hinweg sicherstellt, dass sie die Kerngeschäfte gemäss den vertraglichen Vereinbarungen mit ihren Kunden gewährleisten kann. Die grundlegenden Fragen waren:

1. Ist klar definiert, welche Kerngeschäfte gemäss vertraglichen Vereinbarungen mit den Kunden gewährleistet werden müssen?

2a. Besteht eine Auswirkungsanalyse, in welcher die möglichen Störungsszenarien dargelegt und alle benötigten Ressourcen aufgezeigt werden, die zur Sicherstellung der Kerngeschäfte benötigt werden (Büroautomation, Telekommunikation, Netzwerk, Basisanwendungen wie Identity and Access Management, Zutrittssysteme, Infrastruktur, Personal usw.)?

2b. Werden die definierten Störungsszenarien regelmässig geübt?

3a. Steht die für den Betrieb der definierten Kerngeschäfte notwendige IT-Infrastruktur im Störungsfall innert nützlicher Frist wieder zur Verfügung (Server, Netzwerke, u. a.)?

3b. Besteht ein Kontinuitätsplan, der die zeitgerechte Wiederherstellung nach einem Störungsfall aufzeigt?

4. Unterstützt die IT EDA ihre Kunden bei deren Planung und Tests des Business Continuity Managements (BCM)?

5. Sind Vereinfachungen möglich?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Hans Ulrich Wiedmer (Revisionsleitung) und Stefan Wagner vom 17. Februar bis 31. März 2020 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger.

Prüfungsvorgehen, Prüfungshandlungen und die Beurteilung des IT Service Continuity Managements (IT SCM) erfolgt auf Basis der ISO-Standards 22301 «Business Continuity Management», ISO 27031 «Guidelines for information and communication technology readiness for business continuity» sowie ITIL V3. Bei der Beurteilung werden die Maturitätslevel nach COBIT verwendet, welche im Anhang 4 beschrieben sind. Die EFK wendet ein auf diesen Standards basierendes Hilfsmittel sinngemäss für IT SCM an, wie bereits bei anderen IT-Leistungserbringern der Bundesverwaltung.

Die Ergebnisbesprechung hat am 16. April 2020 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK seitens EDA umfassend und zuvorkommend erteilt, obschon die IT EDA aufgrund der Coronakrise mit Homeoffice und Rückholaktionen des EDA unter grossem Druck stand. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 05. Juni 2020 statt. Teilgenommen haben:

Die Chefin des Stabs des Generalsekretariats EDA, seitens Direktion für Ressourcen die Direktorin, die Chefin des Stabs und die Chefin Rechnungswesen, der Chef Informatik EDA, der Chef Engineering und Betrieb und der Chef Beschaffung und Portfoliomanagement.

Von Seiten der Internen Revision EDA hat ein Revisionsexperte teilgenommen.

Von Seiten der EFK haben der Federführende, der Mandatsleiter, der Revisionsleiter und der Revisionsmitarbeiter teilgenommen.

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

EIDGENÖSSISCHE FINANZKONTROLLE

2 Ausrichtung des IT Service Continuity Managements am übergeordneten Business Continuity Management

Um das IT SCM zielgerichtet ausprägen zu können, ist die Berücksichtigung von Vorgaben aus dem übergeordneten BCM und eine Synchronisation mit diesem von grundlegender Bedeutung.

Im Jahr 2017 schuf das EDA, gestützt auf Vorarbeiten der Generalsekretärenkonferenz, mit einer Richtlinie die Grundlage für das BCM im Departement. Die Richtlinie hält fest, dass beim Aufbau des BCM in der Regel in vier Phasen vorgegangen wird:

- Phase 1: Business lmpact Analyse (BIA) erstellen
- Phase 2: BCM-Strategie definieren
- Phase 3: Business Continuity Plan (BCP) erstellen, Massnahmen erarbeiten und umsetzen
- Phase 4: Testen, üben, schulen und periodisch überprüfen.

Diese vier Phasen gemäss der Richtlinie von 2017 wurden bisher im EDA nicht vollständig umgesetzt. Es besteht keine BIA, keine BCM-Strategie und auch kein BCP. Die einzelnen Direktionen haben eine BCM-Dokumentation mit unterschiedlichem Reifegrad erarbeitet. Bei der Identifikation der kritischen Geschäftsprozesse wurde uneinheitlich vorgegangen. Die Direktion für Ressourcen (DR) beispielsweise weist keine kritischen Prozesse aus, identifiziert aber Betriebsunterbrüche als Risiko.

Das Generalsekretariat des EDA (GS-EDA) hat im September 2018 einen eintägigen Kurs zum BCM organisiert. Zudem wurde seitens des Generalsekretärs der Auftrag gemäss Richtlinie aus dem Jahr 2017 nochmals präzisiert, u. a. mit folgendem Hinweis:

«Das BCM wird entsprechend den Bedürfnissen des EDA und in Übereinstimmung mit der BCM-Richtlinie vom 1. Juli 2017 umgesetzt, soweit sie sich als geeignet erweist. Für die Formalisierung des BCM werden keine zusätzlichen Ressourcen bereitgestellt, weshalb es einfach und pragmatisch bleiben muss.»[1]

Die Direktionen verfügen zwar über ein etabliertes Risikomanagement, jedoch noch nicht über ein ausgebautes BCM gemäss der gängigen Methodik.

Beurteilung

Das EDA hat aus Sicht der EFK dem BCM eine eher untergeordnete Beachtung geschenkt. Die Prioritäten wurden im Departement anders gesetzt. Die EFK hat den Eindruck gewonnen, dass Bedeutung, Nutzen und Wirtschaftlichkeit von BCM-Massnahmen umstritten

[1] Freie Übersetzung, Originalzitat: « Le BCM est mis en œuvre en fonction des besoins du DFAE et en respectant la directive sur le BCM du 1er juillet 2017, dans la mesure où elle s'avère pertinente. Aucune ressource supplémentaire n'est allouée à la formalisation du BCM, raison pour laquelle ce dernier doit rester simple et pragmatique. » Quelle: Mandat du secrétaire général aux directions du DFAE concernant le Business Continuity Management (BCM) du 8 octobre 2018, S. 1.

sind, und dass die Wahrnehmung des Auftrags bei den verschiedenen Stellen in den Direktionen und im Generalsekretariat uneinheitlich ist. In der Konsequenz fehlen grundlegende Voraussetzungen, woran sich das IT SCM ausrichten und messen kann.

Da das EDA die Ressourcen zentralisiert hat, wäre der Aufbau von schlanken aber effizienten Grunddokumenten zu einem BCM mit dem gewünschten minimalen Aufwand möglich. Die BIA lässt sich aus dem Risikomanagement ableiten, ergänzt mit den notwendigen Parametern gemäss Standard. Der BCP sollte die Mindestmassnahmen definieren, die für alle Direktionen gelten, um auf aussergewöhnliche Ereignisse vorbereitet zu sein.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem GS-EDA, den Auftrag zum Auf- und Ausbau des Business Continuity Management im EDA zu präzisieren. Insbesondere sollen das GS und die Direktionen zusammen mit der IT EDA ihre Mindestanforderungen (u. a. Business lmpact Analyse) und die Durchführung gemeinsamer Übungen konkretisieren.

Stellungnahme der Direktion für Ressourcen

Le SG accepte cette recommandation et va la mettre en œuvre en collaboration avec les directions du DFAE.

3 Ausgestaltung des IT Service Continuity Managements

Das IT SCM soll sicherstellen, dass ein IT-Service-Provider auch im Falle aussergewöhnlicher Ereignisse die mit den Nutzern vereinbarten Minimalanforderungen bereitstellen kann. Dazu bedarf es risikomindernder Massnahmen und einer gezielten Wiederherstellungsplanung für die relevanten IT-Dienste.

Die wesentlichen Komponenten des IT SCM in Anlehnung an ITIL V3 sind praktisch dieselben wie beim BCM nach ISO 22301:

1. Policy: Grundlagen und wesentliche Vorgaben.
2. Impact Analyse: Kritische Kernprozesse mit den dafür erforderlichen Ressourcen und den Risiken, auf die man sich vorbereiten will. Analyse der Beziehungen untereinander und der Auswirkungen, wenn Elemente wegfallen.
3. Strategie: Grundsätzliche Handlungsanweisungen zur Reaktion auf die erkannten Risiken. Ableitung der Massnahmen zur Minimierung der erkannten Risiken. Vorgaben zum Ablauf der Störungsreaktion und des Wiederanlaufs. Festlegen der notwendigen Ressourcen.
4. Planung: Ausarbeiten der Pläne (Vorgehen und zeitlicher Ablauf) betreffend Wiederanlauf der kritischen Systeme oder Dienste. Festlegen der dazu notwendigen Organisation (Major Incident Management).
5. Tests / Sensibilisierung: Durchführen und Auswerten von Übungen anhand konkreter Szenarien, um eine kontinuierliche Verbesserung zu erreichen. Sensibilisierung und Schulung der Mitarbeitenden auf allen Stufen.

Es ist aus Sicht der EFK nicht erforderlich, dass für jede Komponente ein eigenes Dokument erstellt wird, jedoch sollten alle Aspekte in hinreichender Tiefe adressiert werden.

3.1 Die Leistungen werden von den Kunden gut bewertet…

Die IT EDA versteht sich nicht nur als zentraler Leistungserbringer mit umfassenden Dienstleistungen für ihre Leistungsbezüger. Sie legt auch Wert auf eine enge Zusammenarbeit mit der Geschäftsseite. Diesbezüglich ist sie bereits gut aufgestellt hinsichtlich dieser expliziten Stossrichtung der neuen IKT-Strategie Bund 2020–2023.

Die IT EDA sieht sich umsetzungsorientiert, pragmatisch, bedarfsorientiert, mit einem klaren Fokus auf die Nachfrage und die fristgerechte Erbringung der notwendigen Leistungen. Alle zwei Jahre wird eine Kundenzufriedenheitsumfrage durchgeführt. Generell werden die Leistungen der IT EDA in verschiedenen Dimensionen sehr gut bewertet. 2018 wurde insbesondere die für die vorliegende Prüfung des IT SCM relevante Kenngrösse «Verfügbarkeit» insgesamt mit der Note 5.2 (bei einer Skala von 1 bis 6) bewertet. Auch die System-Antwortzeiten (4.5) und die Supportdienstleistungen bei Störungen (4.8) wurden gut bewertet.

Laut IT EDA gab es in den letzten zwei Jahren bei Fachanwendungen keine Ereignisse, die zu einem Datenverlust führten. Das detaillierte technische Monitoring der verschiedenen Infrastrukturelemente dient zur Früherkennung von Störungen und unterstützt eine hohe Service-Kontinuität. Kritische Massnahmen, wie beispielsweise die redundante Anbindung ans Internet, werden jährlich für alle Länder validiert.

Die vorliegende Prüfung fand gegen deren Ende unter erschwerten Bedingungen aufgrund der Coronakrise statt. Die Mitarbeitenden der IT EDA standen unter ausserordentlichem Druck, einerseits wegen der grossflächigen Umstellung auf Homeoffice, andererseits durch die Unterstützung der Rückholaktion von im Ausland gestrandeten Schweizern.

Die IT EDA setzt für den Fernzugriff auf das Bundesnetz auf Windows Direct Access (WDA). Ende März hatten 1300 Mitarbeitende Remote-Zugriff für Arbeiten aus dem Homeoffice. Nach anfänglichen Performance-Schwierigkeiten, die jedoch sehr gut gemeistert wurden, verlief der Betrieb ab Anfang April stabil.

3.2 … aber es besteht Verbesserungspotenzial

Die von ihren Nutzern als gut beurteilte operative Leistungsfähigkeit der IT EDA steht im Kontrast zu erheblichen Lücken insbesondere bei der Dokumentation des IT SCM. Es gibt auch unterschiedliche, teilweise inkonsistente Sichten bezüglich der Kritikalität von Fachanwendungen (Rangliste, Einschätzung aus dem Betriebsteam, Service-Level gemäss Schutzbedarfsanalyse, Einschätzung Helpdesk). Zudem gibt es eine hohe Abhängigkeit von Schlüsselpersonen. Abläufe und Prozesse sind in den Köpfen von Mitarbeitenden vorhanden. Sie werden auch entsprechend umgesetzt, sind jedoch nicht nachvollziehbar zu Papier gebracht. Daher zeigt die Bewertung anhand der gewählten Standards ein wenig reifes Bild des IT SCM.

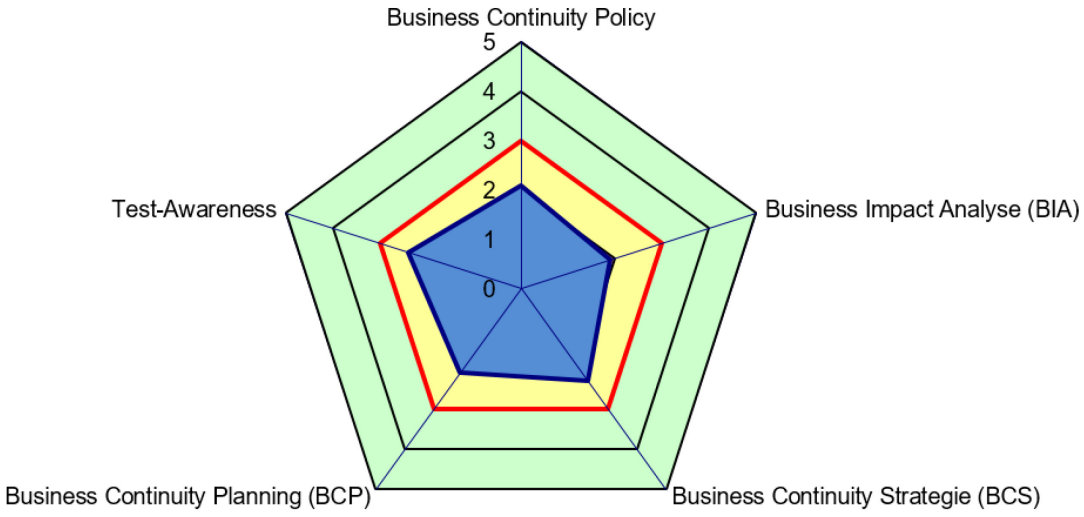

Abb. 1: Feststellung des Reifegrads der wesentlichen Komponenten des IT SCM gemäss ISO 22301 / 27301 / ITIL V3

Beurteilung

Gemessen an den relevanten Standards ist das IT SCM der IT EDA noch zu wenig reif und insbesondere aufgrund des geringen Dokumentationsgrades anfällig bei Personalfluktuationen. Der Reifegrad liegt generell zwischen Maturitätslevel 2 «Wiederholbar» und 3 «Definiert» (vgl. Anhang 4). Im Minimum sollte ein Maturitätswert von 3 angestrebt werden. Es besteht das Risiko, je nach Störungssituation, das bisherige Leistungsniveau nicht halten zu können, mit entsprechenden Konsequenzen für die Geschäftsprozesse. Allerdings kann die IT EDA den Reifegrad nicht ohne Mitwirkung der Geschäftsseite verbessern. Die IT EDA braucht weitergehende Vorgaben, um das IT SCM zu verbessern (vgl. dazu Empfehlung 1).

Wichtige Elemente zur Unterstützung der Service-Kontinuität sind vorhanden. Es fehlen jedoch weitgehend die dazugehörende Dokumentation und dadurch auch die konkreten Massnahmen, welche der IT-Betrieb umsetzen muss. Die EFK sieht hier einfach zu erreichende Verbesserungsmöglichkeiten. Eine effiziente Dokumentation hilft, den Betrieb bei unterschiedlichen Störungssituationen sicherzustellen und vermindert die Abhängigkeit von einzelnen Schlüsselpersonen.

In den folgenden Unterkapiteln werden die wesentlichen Elemente des IT SCM vertieft behandelt.

3.3 Wichtige Anforderungen des Geschäfts an das IT Service Continuity Management sind nicht ausreichend klar definiert

Die bereits in Kapitel 2 thematisierte Richtlinie des EDA zum BCM kann als Business Continuity Policy gemäss Standard verstanden werden. Sie ist implizit auch die Grundlage für das IT SCM. Sie legt fest, wie die entsprechenden Anforderungen der Geschäftsseite an die IT definiert werden sollen.

Als Basis für die Leistungsdefinition der IT EDA dient der Service-Katalog, aus welchem die Kunden Leistungen abrufen können. Die Service-Definition stützt sich auf diejenige des Informatiksteuerungsorgans des Bundes, wurde jedoch noch verfeinert. Anstelle von Service-Level-Agreements sind die Service-Klassen im Service-Katalog mit den entsprechenden Angaben im Anwendungsportfolio massgebend.

Gegenüber den Kunden ist kein systematisches Reporting über die Qualität der Services etabliert, zudem wird die Dauer einer Störung nicht in jedem Fall erhoben.

Zum Zweck einer Priorisierung hat die IT EDA eine Rangliste der wichtigsten Fachanwendungen erstellt, von der Leitung der DR verabschieden lassen und mit dem IT-Verantwortlichen der Konsularischen Direktion validiert. In der Schutzbedarfsdokumentation stehen ebenfalls Angaben zum BCM. Diese und weitere Daten in Portfolios sind nicht systematisiert, harmonisiert und mit allen Direktionen abgestimmt. Beispielsweise fehlt die RPO-Angabe (Recovery Point Objective), welche den Zeitraum des maximalen Datenverlusts angibt resp. definiert, von welchem Zeitpunkt in der Vergangenheit ein aus Sicht der Geschäftsprozesse und aller verbundenen Anwendungen konsistenter Datenbestand wiederhergestellt werden kann. Dort muss die Geschäftsseite Vorkehrungen treffen, um die in dieser Zeit erfassten oder von verbundenen Anwendungen gesendeten Daten wiederherstellen zu können. Die Angaben zur Wiederherstellungszeit RTO (Recovery Time Objective) sind nicht einheitlich. Die Angaben in der Schutzbedarfsdokumentation sind nicht

immer konsistent mit der Kombination aus Service-Klasse gemäss Service-Katalog, Angabe im Portfolio sowie der individuell im Störungsfall vergebenen Priorität, welche zwischen IT und Business festgelegt wird.

Beurteilung

Die BCM-Richtlinie des Departements erfüllt grundsätzlich den Zweck einer Policy. Die Umsetzung eines wirtschaftlichen und effektiven IT SCM erfordert jedoch deren konsequente Umsetzung. Dies bedingt u. a. die Definition kritischer Geschäftsprozesse und Kernparameter der von der IT zu erbringenden Leistungen. Dies bedingt auch eine Abstimmung mit der Kundenseite, die ihrerseits Vorkehrungen treffen muss, beispielsweise für die manuelle Überbrückung ihrer Prozesse während der Störung oder allenfalls auch zwecks Nacherfassung von Daten. Diese Voraussetzungen sind aktuell im EDA noch nicht erfüllt. Die IT EDA muss sich hier künftig klarer positionieren und diese erforderlichen Angaben konsequent einfordern. Wenn auf übergeordneter Stufe keine klaren BCM-Vorgaben vorhanden sind, kann die IT EDA das IT SCM nur intuitiv und aus ihrer Sicht betreiben. Dies kann jedoch bei einem aussergewöhnlichen Ereignis dazu führen, dass falsche Prioritäten gesetzt oder der Betrieb nicht erwartungsgemäss aufrechterhalten werden kann.

3.4 Eine Auswirkungsanalyse und eine Strategie liegen nicht vor

Eine Business Impact Analyse (BIA) ist nicht vorhanden. Nur einzelne Elemente liegen vor, wie z. B. die definierten Geschäftsprozesse des EDA. Einige Direktionen haben ihre kritischen Geschäftsprozesse identifiziert. Aufgrund der Nähe zwischen IT und Geschäftseinheiten wird davon ausgegangen, dass die Prioritäten dank guter direkter Zusammenarbeit und informeller Kommunikation klar sind.

Eine systematische, durchgängige Zuordnung der kritischen Prozesse zu den dafür benötigten IT-Ressourcen fehlt. Auch Störungsszenarien (i. S. «was wäre wenn») sind nicht definiert. Hingegen werden die auftretenden Störungen im Betrieb zum Anlass für die Planung und Umsetzung laufender Verbesserungen genommen.

BCM- oder IT SCM-Strategien liegen nicht vor. Die Richtlinie des EDA zum Business Continuity Management (BCM) vom 28. Juni 2017 definiert die erwarteten Inhalte und hält explizit fest: «Jede Direktion muss über eine BCM-Strategie verfügen. Diese richtet sich nach den konkreten Gegebenheiten. Unter Umständen kann sie in einem sehr kurzen Dokument dargestellt werden.»[2]

Beurteilung

Zwischen der teilweise vorhandenen Dokumentation des Kerngeschäftes mit entsprechenden Prioritäten und den notwendigen IT-Mitteln besteht eine Lücke. Ausserdem existiert keine Analyse möglicher Störungsszenarien sowie eine Strategie mit den Grundsätzen zur Reaktion.

Damit fehlt eine systematische Vorbereitung auf ausserordentliche Ereignisse. Es besteht aus Sicht der EFK ein erhöhtes Risiko, dass bei solchen Ereignissen kritische Prozesse nicht in der erforderlichen Zeit weiter unterstützt werden können.

[2] Quelle: Richtlinie des EDA zum Business Continuity Management (BCM) vom 28. Juni 2017, S. 5.

3.5 Bei der Kontinuitätsplanung bestehen nicht dokumentierte Restrisiken und Lücken bei den Wiederanlaufplänen

Restrisiken sind nicht systematisch dokumentiert und akzeptiert

Seit Jahren ist das Gesamtbudget der IT EDA plafoniert. Daher wird aus wirtschaftlichen Überlegungen u. a. bei der Vorhaltung von Hardware Zurückhaltung geübt. Bei 70 von 170 Vertretungen wird nur mit einem Server gearbeitet. Dies stützt sich auf einen Entscheid durch den Projektausschuss, in welchem die Business-Seite ebenfalls Einsitz hatte. Ein Server-Ersatz kann an einem solchen Standort demzufolge relativ lange dauern. Es ist nicht festgelegt, wie dieses Restrisiko auf Geschäftsseite zu berücksichtigen ist.

Die Durchführung von Wiederherstellungsprozessen ist komplex und hängt sehr stark von erfahrenen Fachleuten ab. Die Abhängigkeit von Schlüsselpersonen wird laut IT EDA regelmässig adressiert, hat aber noch keinen Niederschlag in der Service Continuity Planung gefunden.

Pläne unterschiedlicher Form und Tiefe sind vorhanden, sollen aber aktualisiert werden

Technische Wiederanlaufpläne (engl. Disaster Recovery Plan, DRP) liegen vor. Detaillierungsgrad und Aktualität sind aber stark unterschiedlich. Teilweise sind dies eigenständige Dokumente, teilweise gibt es entsprechende Abschnitte in Betriebshandbüchern. Diese sind jedoch teils unvollständig oder veraltet oder wurden nicht ausreichend erprobt.

Es besteht kein formeller, übergreifender Kontinuitätsplan (Business Continuity Plan, BCP) für generelle Störungen (Ebene Netzwerke / Datenbanken, Stromausfall, Wassereinbruch, Personalausfälle etc.).

Organisation und Kommunikation im «ad-hoc»-Modus

Generell und auch bei Störungssituationen wird auf eine enge Zusammenarbeit zwischen IT und Business und auf eine konsequente Führung über die Linie geachtet. Dies wird seitens IT EDA als wirkungsvoll und zureichend beurteilt und aus ihrer Sicht durch die hohe Kundenzufriedenheit bestätigt.

Die Details der Führung, die Zuständigkeiten und die Übergänge im generellen Ereignisfall erfolgen ad hoc. Für den Pikettdienst besteht eine ausführliche Dokumentation.

Beurteilung

Elemente einer Kontinuitätsplanung sind vorhanden und bewähren sich. Jedoch bestehen Restrisiken, welche nicht dokumentiert und von Verantwortungsträgern auch nicht formell akzeptiert sind.

Ein Auftrag zur Aktualisierung der Wiederanlaufpläne wurde erteilt. Die Wiederanlaufpläne der einzelnen Systeme müssen im Gesamtkontext noch auf Interdependenzen überprüft werden. Die Pläne müssen durch die Kunden validiert werden, insbesondere müssen die Kunden ihre Restrisiken verstehen und akzeptieren können.

Die pragmatische Führung hat sich bisher bewährt. Trotzdem ist es sinnvoll, die wichtigsten Elemente der Notfallorganisation und der zu befolgenden Abläufe in einer auch im Störungsfall verfügbaren Form zu dokumentieren. Die Pikettorganisation ist zweckmässig dokumentiert und bewährt sich im laufenden Betrieb vielfach.

3.6 Technische Tests werden ad hoc geplant und durchgeführt

Für eine systematische Planung und Durchführung von Tests fehlt die Grundlage in Form definierter Störungsszenarien (wie bereits in Kapitel 3.4 erwähnt). Elementare Tests werden dennoch durchgeführt, ausgewertet und entsprechende Massnahmen getroffen. In den vergangenen Jahren umfasste dies folgende Infrastrukturen bzw. Tests:

- Active Directory (AD) Disaster Recovery
- SCCM (System Center Configuration Manager)
- RAPs: Risk Assessment Programs (ein Angebot von Microsoft, genutzt in den Bereichen Client Security, Server Patching, Exchange, Active Directory, Sharepoint und Datenbanken). Zudem werden ähnliche Tests mit anderen Lieferanten (Storage, Backup) durchgeführt.

Verschiedene Aktionen, etwa der Server-Neuaufbau, erfolgen ohnehin regelmässig im regulären Betrieb und müssen nicht separat geübt werden.

Wenn im regulären Betrieb eine Taskforce zum Einsatz kommt, werden anschliessend in einem Debriefing die Lehren gezogen und Massnahmen zur Verbesserung definiert.

Beurteilung

Es liegt keine systematische, risikobasierte Planung und Durchführung von Tests vor. Die Erfahrungen mit auftretenden Störungen im laufenden Betrieb sowie Angebote des Herstellers Microsoft (RAP) werden zwar genutzt, um Tests durchzuführen und Verbesserungen zu erreichen. RAPs könnten nach Umsetzung der Massnahmen für eine erneute Prüfung und mithin Erfolgsmessung verwendet werden. Ohne systematische, dokumentierte Tests besteht das Risiko, dass beim Eintreten eines Problems unter Hochdruck zuerst eine Lösung gefunden werden muss. Tests sollten auch dazu dienen, technische Schnittstellen und die Zusammenarbeit mit Lieferanten und Leistungserbringern zu überprüfen.

Nach Taskforce-Einsätzen werden Debriefings durchgeführt. Dies ist nützlich für die kontinuierliche Verbesserung der Leistungserbringung.

3.7 Tests des Business Continuity Managements mit den Kunden werden weder angeboten noch nachgefragt

Im Rahmen eines Business Continuity Managements sollten die Kunden die Reaktion auf bestimmte Szenarien regelmässig unter Einbezug der IT testen. Es besteht jedoch weder eine Nachfrage von Kundenseite, noch gibt es seitens IT EDA ein entsprechendes Angebot.

Beurteilung

BCM-Tests sind wesentlich, um die definierten Massnahmen zu erproben. Sie orientieren sich an den BCM-Bestrebungen der Kunden. Die IT EDA sollte ihre Bereitschaft zur Mitwirkung bei solchen Tests signalisieren, hingegen muss die Verantwortung auf Kundenseite liegen.

3.8 Regelmässige Massnahmen zur Sensibilisierung sind erforderlich

Die Wichtigkeit einer kontinuierlichen Leistungserbringung und entsprechende Schulungs- und Sensibilisierungsmassnahmen sind laufende Bestandteile in der täglichen Arbeit und auch Teil der Mitarbeiterführung in der IT EDA. Explizites Schulungsmaterial und regelmässige Anlässe spezifisch zu IT SCM hat die EFK kaum vorgefunden. Beim Eintritt neuer Mitarbeitenden werden jedoch laut IT EDA entsprechende Aufgabenbereiche durchlaufen. Die IT EDA legt grossen Wert auf die Aus- und Weiterbildung der Mitarbeitenden. Die Gewährleistung der Service-Kontinuität ist integraler Bestandteil solcher Ausbildungen.

Mit dem BIT besteht ein regelmässiger Austausch zu aktuellen fachlichen Themen.

Beurteilung

Die Investitionen in die Aus- und Weiterbildung von Mitarbeitenden sind sehr begrüssenswert und bilden eine wesentliche Grundlage für eine professionelle Leistungserbringung. Jedoch müssen die Bestrebungen zur Sensibilisierung aller Mitarbeitenden anhand konkreter Szenarien verstärkt werden. Die Förderung des Problem- und Lösungsbewusstseins auch über Teamgrenzen hinweg ist wesentlich und sollte einer systematischen Planung unterliegen. Regelmässige Schulungsanlässe dienen einer allgemeinen Erhöhung der Fähigkeit zur fristgerechten Erkennung und Lösung von Problemen, fördern die Zusammenarbeit über Teamgrenzen hinweg und sorgen für eine «unité de doctrine» beim Vorgehen im Ereignisfall. Zudem sollten Schulungen auch die Resultate von IT-SCM-Tests aufnehmen und zur Verbesserung dienen. Bei Sensibilisierungsmassnahmen sind auch die Leistungsbezüger, andere Leistungserbringer und Lieferanten einzubeziehen.

3.9 Erste Massnahmen wurden eingeleitet, jedoch noch nicht konsequent fortgesetzt

Bereits im Jahr 2018 hatte die IT EDA erste Massnahmen zum systematischen Aufbau eines Kontinuitätsmanagements der IT EDA in die Wege geleitet. Ein Entwurf eines BCM-Konzepts lag Anfang 2018 vor, vermischte aber noch stark die Elemente von BCM und SCM. Diese Arbeiten wurden allerdings nicht weitergeführt. Einerseits wegen der unklaren Erwartungen auf der Departementsebene und der nur ungenügend vorhandenen Voraussetzungen aufseiten der Direktionen des EDA, andererseits aufgrund des Stellenwechsels des Sachbearbeiters. Im Blick auf ein entsprechendes Projekt wurde 2019 eine Studie «IT SCM EDA» verfasst, welche die IST-Situation, Massnahmen, technische Varianten und einen Kostenrahmen definiert, jedoch keinen Zeitplan enthält. In diesem Rahmen sollen die Wiederanlaufpläne aktualisiert und ergänzt werden. Das Projekt wurde jedoch bis zum Prüfungsabschluss noch nicht gestartet.

Beurteilung

Die vorangehenden Kapitel haben Handlungsbedarf für die IT EDA aufgezeigt. Es bestehen bereits Ansätze zur Weiterentwicklung des IT SCM. Eine konsequente Zieldefinition und die konkrete Planung und Umsetzung der erforderlichen Massnahmen stehen noch aus. Diese Verbesserungsmassnahmen sollten im Rahmen eines klaren Auftrags weiterverfolgt werden, in Abstimmung mit der übergeordneten Stelle und den Leistungsbezügern.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt der Direktion für Ressourcen, das IT Service Continuity Management zielgerichtet und pragmatisch anhand des in der EDA-Richtlinie referenzierten Standards BS 25999 bzw. dessen Nachfolger ISO 22301 auszubauen. Grundlegend sind die mit den vorgesetzten Stellen und den Kunden zu vereinbarenden Anforderungen und Parameter (v. a. maximaler Datenverlust / Recovery Point Objective und Wiederherstellungszeit / Recovery Time Objective) für die Sicherstellung der Service-Kontinuität. Insbesondere zu berücksichtigen sind die systematische Abstimmung auf die kritischen Kernprozesse aus einer Business Impact Analyse und die Erstellung bzw. Überarbeitung der Wiederanlaufpläne. Die Planung und Durchführung von Übungen und Tests im Betrieb und zusammen mit den Leistungsbezügern und weiteren Dienstleistern sind ebenfalls wichtig.

Stellungnahme der Direktion für Ressourcen

La DR accepte cette recommandation et va la mettre en oeuvre en collaboration avec les travaux relatifs au BCM.

Anhang 1: Rechtsgrundlagen und andere Dokumente

Rechtstexte
Regierungs- und Verwaltungsorganisationsgesetz (RVOG), SR 172.010
Bundesinformatikverordnung (BinfV), SR 172.010.58
Richtlinie des EDA zum Business Continuity Management (BCM) vom 28. Juni 2017
Mandat du secrétaire général aux directions du DFAE concernant le Business Continuity Management (BCM) du 8 octobre 2018

Anhang 2: Abkürzungen

BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analyse
BIT	Bundesamt für Informatik und Telekommunikation
COBIT	Control Objectives for Information and Related Technology
DRP	Disaster Recovery Plan
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFK	Eidgenössische Finanzkontrolle
IT	Informationstechnologie
ITIL	IT Infrastructure Library
IT EDA	Informatik EDA, zentraler Telematik-Leistungserbringer aller Organisationseinheiten des EDA
SCM	Service Continuity Management
RPO	Recovery Point Objective
RTO	Recovery Time Objective
WDA	Windows Direct Access

Anhang 3: Glossar

BCM	Business Continuity Management[3]: Betriebskontinuitätsmanagement (BKM; englisch business continuity management (BCM)) 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 (etwa Betriebsstörungen) – zu schützen bzw. alternative Abläufe zu ermöglichen.[1] Ziel ist somit die Sicherstellung des Fortbestands des Unternehmens im Sinne ökonomischer Nachhaltigkeit im Angesicht von Risiken mit hohem Schadensausmass.
DRP	Disaster Recovery Plan[4]: Ein Disaster-Recovery-Plan (DRP) – manchmal auch als Business Continuity Plan (BCP) oder Business Process Contingency Plan (BPCP) bezeichnet – beschreibt, wie ein Unternehmen mit einem möglichen Desaster umzugehen hat. Falls ein DRP besteht, kann das Unternehmen die Auswirkungen des Desasters minimieren und ihre geschäftskritischen Prozesse schnell fortführen. Die Disaster-Recovery-Planung beinhaltet in der Regel eine Analyse der Geschäftsprozesse und des Bedarfs. Sie kann auch einen Schwerpunkt zur Prävention beinhalten.
SCM	Service Continuity Management[5]: IT Service Continuity Management (IT SCM) managt Risiken, die gravierende Auswirkungen auf die IT-Services haben können. Dieser ITIL-Prozess stellt sicher, dass der IT-Service-Provider auch im Falle aussergewöhnlicher Ereignisse die in den Service-Levels vereinbarten Minimalanforderungen bereitstellen kann; dies geschieht durch risikomindernde Massnahmen und durch eine gezielte Wiederherstellungsplanung für die IT-Services. IT SCM sollte in einer Weise gestaltet sein, dass es das Business Continuity Management (BCM) unterstützt.

[3] https://de.wikipedia.org/wiki/Betriebliches_Kontinuit%C3%A4tsmanagement; Abfrage vom 13.08.2018
[4] https://www.searchsecurity.de/definition/Disaster-Recovery-Plan-DRP; Abfrage vom 13.08.2018
[5] https://wiki.de.it-processmaps.com/index.php/IT_Service_Continuity_Management; Abfrage vom 11.02.2020

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: Maturitätslevel nach COBIT

Skala

0	Level 0: Nicht existent Es ist kein Prozess erkennbar. Das Unternehmen hat nicht einmal den Bedarf erkannt, dass das Thema in Angriff genommen werden soll.
1	Level 1: Initial Es bestehen Anzeichen, dass das Unternehmen den Bedarf erkannt hat, das Thema zu behandeln. Es existieren jedoch keine standardisierten Prozesse, es ist vielmehr ein ad-hoc-Ansatz in Verwendung, der individuell und situationsbezogen angewandt wird. Der gesamthafte Managementansatz ist nicht organisiert.
2	Level 2: Wiederholbar Prozesse wurden so weit entwickelt, dass gleichartige Verfahren von unterschiedlichen Personen angewandt werden, die dieselbe Aufgabe übernehmen. Es besteht kein formales Training oder eine Kommunikation der Standardverfahren und die Verantwortung ist Einzelpersonen überlassen. Es wird stark auf das Wissen von Einzelpersonen vertraut, demzufolge sind Fehler wahrscheinlich.
3	Level 3: Definiert Verfahren wurden standardisiert und dokumentiert und durch Trainings kommuniziert. Die Einhaltung der Prozesse ist jedoch der Einzelperson überlassen und die Erkennung von Abweichungen ist unwahrscheinlich. Die Verfahren sind nicht ausgereift und sind ein formalisiertes Abbild bestehender Praktiken.
4	Level 4: Managed Es ist möglich, die Einhaltung von Verfahren zu überwachen und zu messen sowie Aktionen dort zu ergreifen, wo Prozesse nicht wirksam funktionieren. Prozesse werden laufend verbessert und folgen «Good Practices». Automatisierung und Werkzeugunterstützung finden eingeschränkt und nicht integriert statt.
5	Level 5: Optimiert Prozesse wurden, basierend auf laufender Verbesserung und Vergleichen mit anderen Unternehmen, auf ein Best-Practice-Niveau verbessert. Die IT wird integriert für die Workflow-Automatisierung verwendet, stellt Werkzeuge für die Verbesserung der Qualität und Wirksamkeit zur Verfügung und macht das Unternehmen flexibel, sich Änderungen anzupassen.